

**Jaarrapportage Functionaris Gegevensbescherming
Passagiersinformatie-eenheid Nederland**

2025

<i>Datum</i>	<i>6 februari 2026</i>
<i>Status</i>	<i>Definitief</i>

Colofon

Afzendgegevens	Minister van Justitie en Veiligheid Turfmarkt 147 2511 DP Den Haag Postbus 20301 2500 EH Den Haag www.rijksoverheid.nl/jenv
Contact	T 070 370 68 89
Bijlage(n)	-
Auteurs	Functionaris voor gegevensbescherming Pi-NL FG-Pi-NL@minjenv.nl

Inhoud

COLOFON	2
1 INLEIDING	4
2 SAMENVATTING.....	5
3 WAARBORGEN EN BEVINDINGEN	6
4 STATISTIEKEN.....	17
5 BIJLAGEN	21
5.1 LIJST VAN PASSAGIERSGEGEVENS.....	21
5.2 LIJST VAN STRAFBARE FEITEN	22
5.3 PASSAGIERSGEGEVENS: API EN PNR	23

Dit is de jaarrapportage over het jaar 2025 van de functionaris voor gegevensbescherming (hierna: FG) van de Passagiersinformatie-eenheid Nederland (hierna: Pi-NL). Deze rapportage vindt zijn grondslag in artikel 18, lid 2 van de Wet gebruik van passagiersgegevens voor de bestrijding van terroristische en ernstige misdrijven (hierna: PNR-wet). Hierin is bepaald dat de FG jaarlijks vóór 1 juli een rapportage zendt aan de minister van Justitie en Veiligheid, de beide Kamers der Staten-Generaal en de Autoriteit Persoonsgegevens (hierna: AP) over het voorgaande kalenderjaar. In deze rapportage gaat de FG in op de wijze waarop controle is uitgeoefend op de verwerking van de persoonsgegevens (de passagiersgegevens) door de Pi-NL en de wijze waarop de waarborgen voor de gegevensbescherming zijn uitgevoerd. De rapportage bevat tevens statistieken over de mate waarin passagiersgegevens op grond van de artikelen 9a tot en met 16 van de PNR-wet zijn verstrekt, doorgegeven of verzocht.

Over de Passagiersinformatie-eenheid Nederland

Op 18 juni 2019 is de PNR-wet in werking getreden. De wet implementeert de Richtlijn 2016/681/EU van het Europees Parlement en de Raad van 27 april 2016 over het gebruik van passagiersgegevens van luchtreizigers voor het voorkomen, opsporen, onderzoeken en vervolgen van terroristische misdrijven en ernstige criminaliteit (hierna: PNR-richtlijn). De PNR-richtlijn voorziet in een verplichting voor de lidstaten om een passagiersinformatie-eenheid in te richten en luchtvaartmaatschappijen voor te schrijven dat zij passagiersgegevens van vluchten waarover zij voor hun normale bedrijfsvoering beschikken, te versturen naar de passagiersinformatie-eenheid van de lidstaat waarvan of waarnaar een vlucht plaatsvindt. Naast de passagiersgegevens van luchtvaartmaatschappijen wordt door de Pi-NL geen passagiersgegevens verzameld van andere vervoersmodaliteiten.

De Pi-NL:

- *Vergelijkt* passagiersgegevens met door de minister van Justitie en Veiligheid aangewezen databanken. De Pi-NL signaleert daarbij zelf geen personen in databanken. Het signaleren van personen wordt gedaan door de instanties die een bevoegdheid hebben om te signaleren. Daarnaast vergelijkt de Pi-NL passagiersgegevens met zorgvuldig getoetste sets van risicocriteria, zoals bepaald reisgedrag en reisroutes. Op deze manier komen mogelijk kwaadwillende personen in beeld bij de opsporingsautoriteiten.
- *Deelt* passagiersgegevens met organisaties die deze gegevens vorderen of verzoeken bij de Pi-NL. De organisaties die deze passagiersgegevens mogen vorderen of verzoeken staan in de PNR-wet beschreven.
- *Analyseert* passagiersgegevens om getoetste sets van risicocriteria bij te stellen en nieuwe risicocriteria op te stellen. Dit doet de Pi-NL in samenwerking met de bevoegde instanties binnen Nederland.¹

Rollen

De minister van Justitie en Veiligheid is de verwerkingsverantwoordelijke voor de verwerking van passagiersgegevens door de Pi-NL. De Nationaal Coördinator Terrorismebestrijding en Veiligheid (hierna: NCTV) is door de minister van Justitie en Veiligheid gemandateerd om taken uit te voeren vanuit zijn rol als verwerkingsverantwoordelijke die voortvloeien uit de PNR-wet. De Commandant van de Koninklijke Marechaussee (hierna: KMar) is beheersmatig verantwoordelijke voor de Pi-NL. De Justitiële Informatiedienst van het ministerie van Justitie en Veiligheid en het Joint IV Commando van het ministerie van Defensie zijn de verwerkers die passagiersgegevens verwerken ten behoeve van de Pi-NL. De FG houdt toezicht op de toepassing en naleving van de privacywetgeving² door de Pi-NL.

¹ Zie voor de bevoegde instanties in Nederland: [https://eur-lex.europa.eu/legal-content/NL/TXT/PDF/?uri=CELEX:52018XC0606\(01\)](https://eur-lex.europa.eu/legal-content/NL/TXT/PDF/?uri=CELEX:52018XC0606(01))

² De PNR-wet en de van toepassing zijnde artikelen onder de Wet politiegegevens.

Samenvatting

Samenvattend kan worden gesteld dat het management en de medewerkers van de Pi-NL zich bewust zijn van het belang van gegevensbescherming. Om het bewustzijn verder te versterken, wordt aanbevolen medewerkers regelmatig te trainen in de interne privacyprocedures en hen bewust te maken van de relevante privacyrisico's in hun dagelijkse werk. De wettelijke waarborgen voor het beschermen van persoonsgegevens, zijn aanwezig, gecontroleerd en functioneren naar behoren.

De FG bevestigt haar eerdere standpunt in de jaarrapportage 2024 dat de algemene bewaartermijn voor de Pi-NL drie jaar passend acht. Zij adviseert deze bewaartermijn voorlopig ongewijzigd aan te houden totdat de evaluatie van de Europese Commissie duidelijkheid geeft over mogelijke aanpassingen aan de richtlijn.

Het implementatietraject op basis van de API-verordening rechtshandhaving is in 2025 aangevangen. In 2025 zijn de Europese Commissie en lidstaten gestart met onderhandelingen over de uitvoeringshandelingen. De NCTV en de Pi-NL zijn betrokken bij het implementatietraject en de uitvoeringshandelingen.

De Statement of Compliance die in 2024 voor de Pi-NL en het Joint IV Commando van het ministerie van Defensie is afgegeven, is verlengd door de Commandant van de KMar in december 2025.

Voor wat betreft de verwerking van passagiersgegevens door de Justitiële Informatiedienst is in 2025 een nieuwe 'in control verklaring' afgegeven.

Door de verhoogde terroristische dreiging in Nederland en de voorstelbare dreiging die gepaard ging met de door Nederland georganiseerd NAVO-top van 24 tot en met 26 juni 2025, is tijdelijk de intra-EU selectie opgeschort. In de zomer van 2025 is opnieuw geëvalueerd of de intra-EU selectie opnieuw tijdelijk opgeschort moest worden. Er bleek onvoldoende aanleiding om opnieuw tot opschorting van de intra-EU selectie over te gaan. In de zomer is een intra-EU selectie ingevoerd conform het selectie-advies. De FG heeft een onafhankelijke controle uitgevoerd en bevestigd dat de ingevoerde selectie correct functioneert.

In 2025 is een hercontrole en interne audit uitgevoerd. Uit deze hercontrole blijkt dat de verbetermaatregelen uit het verbeterplan volledig zijn uitgevoerd. De maatregelen voldoen in opzet en bestaan aan de gestelde normen. Daarnaast zijn bij de overige normen die zijn onderzocht in de interne audit geen relevante afwijkingen geconstateerd.

Tevens constateert de FG dat de verbeteracties uit eerdere jaarrapportages van de FG zijn opgepakt. De versterking van de privacy capaciteit binnen de Pi-NL in 2025 heeft bijgedragen aan het tijdig uitvoeren en borgen van zowel de verbetermaatregelen uit de audit als de verbeteracties uit eerdere jaarrapportages.

De FG adviseert deze werkwijze – het tijdig uitvoeren en borgen van verbetermaatregelen en verbeteracties – vast te houden.

In 2025 is een Privacy Framework ontwikkeld dat dient ter ondersteuning van structurele monitoring en documentatie van privacyverplichtingen.
selectie

Tenslotte adviseert de FG om de gedocumenteerde aanpak voort te zetten in het kader van de verantwoordingsplicht.

3 Waarborgen en bevindingen

De PNR-wet bevat verschillende waarborgen voor het beschermen van passagiersgegevens van luchtreizigers. In deze wet is tevens een aantal waarborgen uit de Wet politiegegevens (hierna: Wpg) van overeenkomstige toepassing verklaard. Hieronder volgt een beknopte weergave van deze waarborgen (in verband met de leesbaarheid wordt steeds een samenvatting van de wettelijke vereisten gegeven) en de bevindingen van de FG ten aanzien van de aanwezigheid en de werking van deze waarborgen. De wijze waarop de controle is uitgeoefend, bestond uit het inspecteren van beleidsdocumenten, procedures en werkinstructies, het vaststellen of conform deze opzet wordt gewerkt, het inspecteren van 'logbestanden', het inspecteren van diverse registratiesystemen³, het doen van steekproeven⁴, interviews en observaties op de werkvloer.

Functionaris voor gegevensbescherming (art 18 PNR-wet en art 36 Wpg)

De PNR-wet vereist de benoeming van een FG voor de Pi-NL door de verwerkingsverantwoordelijke. De FG ziet toe op de naleving van de relevante bepalingen uit de PNR-wet en de Wpg, op de toewijzing van autorisaties, op de bewustmaking en opleiding van de medewerkers van de Pi-NL die zijn betrokken bij de verwerking van passagiersgegevens en op de audits. De FG informeert en adviseert daarnaast de verwerkingsverantwoordelijke en de medewerkers van de Pi-NL over wettelijke gegevensbeschermingsbepalingen en over de gegevensbeschermingseffectbeoordeling. Ook werkt de FG samen met de AP. Verder is de FG voor een betrokkene⁵ het contactpunt voor alle aangelegenheden in verband met de verwerking van de persoonsgegevens van die betrokkene door de verwerkingsverantwoordelijke. De FG dient voor de uitvoering van diens taken toegang te hebben tot alle gegevens die door de Pi-NL worden verwerkt. De FG kan de AP informeren indien er wordt vastgesteld dat een verwerking van persoonsgegevens door de Pi-NL niet rechtmatig is. De FG wordt door de verwerkingsverantwoordelijke tijdig en naar behoren betrokken bij alle aangelegenheden die verband houden met de bescherming van passagiersgegevens.

Bevindingen 2025: Er is een FG voor de Pi-NL benoemd en ook aangemeld bij de AP. De FG heeft voor betrokkenen als contactpunt gefungeerd en had toegang tot alle noodzakelijke gegevens. De FG is actief betrokken bij wijzigingen in beleid en uitvoering en de effecten daarvan op de bescherming van passagiersgegevens. Er was regelmatig contact tussen de FG, het management en de medewerkers van de Pi-NL en het ministerie van Justitie en Veiligheid.

Contact AP

Artikel 36 Wpg bepaalt dat de FG optreedt als contactpunt voor de AP in zaken en aangelegenheden in verband met de verwerking van persoonsgegevens, en voor zover dienstig het plegen van overleg over enige andere aangelegenheid. In de FG-jaarrapportage over 2023 heeft de FG reeds gewezen op het belang van betrokkenheid van de FG bij communicatie en afstemming met de AP.

In 2025 heeft contact plaatsgevonden tussen de FG en de AP. Dit contact had geen inhoudelijk karakter gericht op afstemming over toezicht of oordeelsvorming. Daarnaast heeft meerdere malen contact plaatsgevonden tussen de NCTV, de minister van Justitie en Veiligheid en de AP.

De FG merkt op dat het toezicht van de AP in deze contacten voornamelijk plaatsvindt op basis van schriftelijke informatie en beoordelingen van de AP op afstand. Vanuit de NCTV is de AP meerdere malen uitgenodigd om de uitvoering van processen en de praktische inrichting daarvan

³ Zoals het register inbreuken in verband met persoonsgegevens, de notificaties van de verstrekkingen en registraties van spoedvorderingen.

⁴ Bijvoorbeeld ten aanzien van afscherming van persoonsgegevens na zes maanden, bijzondere persoonsgegevens, bewaartermijnen, autorisaties.

⁵ De persoon van wie Pi-NL passagiersgegevens verwerkt.

op locatie te bezichtigen, teneinde nadere context te bieden bij gemaakte keuzes. Deze uitnodigingen hebben ook in 2025 niet geleid tot een locatiebezoek of nadere verdieping.

De FG merkt op dat nadere afstemming en verdiepend contact, waaronder het betrekken van de FG bij oordeelsvorming en communicatie richting de minister, van toegevoegde waarde kan zijn. De FG is vanuit haar rol en dagelijkse betrokkenheid bij de organisatie goed gepositioneerd om inzicht te geven in de uitvoeringspraktijk en de gevolgen van beleidskeuzes. Een dergelijke informatiewisseling kan bijdragen aan een zorgvuldige en evenwichtige oordeelsvorming, in het belang van zowel het toezicht als de uitvoering. Dit kan van invloed zijn op de afweging tussen de bescherming van persoonsgegevens van betrokkenen en het belang van de bestrijding van ernstige criminaliteit en terroristische misdrijven.

Privacybewustzijn

In het afgelopen jaar zijn er verschillende activiteiten gedaan om medewerkers bewust te maken van de bescherming van passagiersgegevens:

- Nieuwe medewerkers kregen een presentatie over de bescherming van passagiersgegevens;
- Posters zijn opgehangen en er zijn pop-up meldingen op beeldschermen, bijvoorbeeld over het afsluiten van werkstations;
- Medewerkers kregen waarschuwingen over phishing tijdens overleggen;
- Bij controles werden medewerkers aangesproken op de juiste verwerking van passagiersgegevens.

De FG ziet dat er veel aandacht is voor privacybewustzijn. Om het bewustzijn verder te versterken, wordt aanbevolen medewerkers regelmatig te trainen in de interne privacyprocedures en hen bewust te maken van de relevante privacyrisico's in hun dagelijkse werk.

Verbod op verwerken van bijzondere gegevens (art 19 PNR-wet)

De PNR-wet verbiedt het maken van onderscheid op grond van bijzondere persoonsgegevens, zoals ras, etnische afkomst, religie of gezondheid.

Bevindingen 2025: De Pi-NL verwerkt geen bijzondere persoonsgegevens. Wanneer een luchtvaartmaatschappij bijzondere persoonsgegevens aanlevert, verwijdert het filtersysteem van het Travel Information Portal systeem (hierna: TRIP) geautomatiseerd direct de bijzondere persoonsgegevens.

Een steekproefsgewijze controle door de FG op de verwerking van passagiersgegevens heeft plaatsgevonden. Uit deze steekproef bleek dat geen bijzondere persoonsgegevens zijn aangetroffen. De woorden en kenmerken die op de lijst zijn aangemerkt als bijzondere persoonsgegevens, zijn niet aangetroffen.

De Pi-NL monitort dagelijks of er bijzondere persoonsgegevens in de verwerking voorkomen. Indien dergelijke gegevens toch zouden worden aangeleverd, worden zij onmiddellijk door het geautomatiseerde filtersysteem gefilterd en verwijderd.

De FG adviseert om de uitgevoerde monitoring van bijzondere persoonsgegevens door de Pi-NL centraal te documenteren. Door dit centraal vast te leggen, wordt inzichtelijk welke controles plaatsvinden, door wie en wanneer. Daarnaast kan aantoonbaar worden gemaakt dat monitoring systematisch en volgens de procedures worden uitgevoerd.

Bewaartermijn en afscherming (art 20 PNR-wet)

De PNR-wet stelt dat de passagiersgegevens gedurende een termijn van vijf jaar na ontvangst van deze gegevens worden bewaard en dat de passagiersgegevens na deze termijn worden gewist. De ontvangen passagiersgegevens dienen te worden opgeslagen en verwerkt in Nederland of in een andere lidstaat van de Europese Unie. De passagiersgegevens waaruit rechtstreeks de identiteit van een persoon kan worden afgeleid, dienen zes maanden na ontvangst ervan te worden gedepersonaliseerd door afscherming van die gegevens. Daarna kunnen deze gegevens uitsluitend

worden doorgegeven met toestemming van de officier van justitie en na kennisgeving aan de FG, die deze verwerking achteraf controleert.

Bevindingen 2025:

Algemene bewaartermijn

De algemene bewaartermijn voor passagiersgegevens is drie jaar. Een algemene bewaartermijn van drie jaar is noodzakelijk voor en evenredig aan de doelstellingen van de PNR-wet. Met deze termijn kan er voldaan worden aan de wettelijke verplichting om:

- analyse uit te voeren met passagiersgegevens,
- te voldoen aan vorderingen en verzoeken van bevoegde instanties, en
- passagiersgegevens te vergelijken met risicocriteria en databanken.

Onder bepaalde voorwaarden kunnen de passagiersgegevens maximaal vijf jaar worden bewaard. Dit betreft gevallen waarin er een objectieve aanwijzing is dat de passagier een risico kan vormen op het gebied van terrorisme of ernstige criminaliteit.

Europese ontwikkelingen

Op 13 maart 2025 heeft de European Data Protection Board (hierna: EDPB) een statement uitgebracht. Hierin geeft de EDPB aan dat een algemene bewaartermijn van zes maanden de bovengrens zou moeten zijn. Alleen concrete, objectieve risico's kunnen rechtvaardigen dat bepaalde passagiersgegevens langer bewaard blijven. Hoewel het statement van de EDPB geen bindend advies is, heeft het gezag en kan het richtinggevend worden beschouwd bij de interpretatie van bewaartermijnen.

Op dit moment voert de Europese Commissie een evaluatie uit van de PNR-richtlijn, waarbij onder meer de bewaartermijnen worden gezien. In dat kader hebben de NCTV en de FG input geleverd voor deze evaluatie. Op basis van de uitkomsten van de evaluatie kan de Europese Commissie advies uitbrengen aan het Europese Parlement en de Raad. Indien nodig kan de richtlijn worden aangepast.

Advies en controle FG

De FG bevestigt haar eerdere standpunt uit de jaarrapportage 2024 dat de door de Pi-NL gehanteerde algemene bewaartermijn drie jaar is en acht dit passend. Zij adviseert deze bewaartermijn voorlopig ongewijzigd aan te houden totdat de evaluatie van de Europese Commissie duidelijkheid geeft over mogelijke aanpassingen aan de richtlijn.

Indien de richtlijn na afronding van de evaluatie wordt herzien, adviseert de FG de algemene bewaartermijn dienovereenkomstig aan te passen.

Steekproeven bewaartermijnen

De FG heeft aan de hand van een steekproeven gecontroleerd:

1. Passagiersgegevens zonder objectieve aanwijzing:
 - Geen gegevens zijn langer dan drie jaar bewaard.
 - Gegevens zijn geautomatiseerd gewist na drie jaar.
2. Passagiersgegevens met objectieve aanwijzing:
 - Geen gegevens zijn langer dan vijf jaar bewaard.
 - Gegevens zijn geautomatiseerd gewist na vijf jaar.

De Pi-NL monitort periodiek de naleving van de bewaartermijnen. De FG adviseert om deze monitoring centraal te documenteren. Door dit centraal vast te leggen, wordt inzichtelijk welke controles plaatsvinden, door wie en wanneer. Daarnaast kan aantoonbaar worden gemaakt dat monitoring systematisch en volgens de procedures worden uitgevoerd.

Depersonaliseren en monitoring

Het automatisch depersonaliseren van passagiersgegevens in TRIP, het kernsysteem van de Pi-NL, functioneert correct. De FG controleert dit periodiek.

Register (art 22 PNR-wet)

De verwerkingsverantwoordelijke dient een register bij te houden dat contactgegevens bevat van de Pi-NL en andere passagiersinformatie-eenheden in de EU, bevoegde instanties en toegekende autorisaties. Verder draagt de verwerkingsverantwoordelijke zorg voor de vastlegging van verzoeken om passagiersgegevens van bevoegde instanties, Europol en andere passagiersinformatie-eenheden.

Bevindingen 2025: het artikel 22 PNR-wet register is opgesteld door de Pi-NL.

Vastleggen verwerkingen (art 23 PNR-wet)

De verwerkingsverantwoordelijke dient zorg te dragen voor de vastlegging langs elektronische weg van ten minste de volgende verwerkingen: het verzamelen, raadplegen, verstrekken (onder meer in de vorm van doorgiften) en wissen van de passagiersgegevens en de resultaten van de verwerking van die gegevens. Deze 'logbestanden' bevatten in ieder geval informatie over het doel, de datum en het tijdstip van het raadplegen en het verstrekken, de identiteit van de persoon die de passagiersgegevens of een verwerking ervan heeft geraadpleegd of verstrekt en de identiteit van de ontvangers van die gegevens.

Bevindingen 2025: Controle in 2025 wijst uit dat de genoemde verwerkingen zijn gelogd in TRIP en dat deze logbestanden de wettelijk vereiste informatie bevatten.

Menselijke toets (art 8 PNR-wet)

Indien een geautomatiseerde vergelijking van passagiersgegevens met een vordering, databank of risicocriteria een positieve overeenkomst oplevert, moet deze door menselijke tussenkomst worden gecontroleerd. Zo kan worden bepaald of een bevoegde instantie maatregelen moet treffen of nader onderzoek moet doen.

Bevindingen 2025: de menselijke toets na positieve overeenkomst op grond van een geautomatiseerde vergelijking wordt uitgevoerd en door het TRIP-systeem geautomatiseerd afgedwongen.

Juistheid en volledigheid gegevens (art 4 Wpg en 17 PNR-wet)

De verwerkingsverantwoordelijke treft de nodige maatregelen met de bedoeling dat de persoonsgegevens juist en nauwkeurig zijn.

Bevindingen 2025: Naast de Passenger Name Records (hierna: PNR-gegevens) die luchtvaartmaatschappijen verzamelen en aan de Pi-NL doorgeven, kan de Pi-NL in sommige gevallen ook beschikken over Advance Passenger Information (hierna: API-gegevens)⁶. In veel gevallen bevatten deze API-gegevens geautomatiseerd ingelezen gegevens uit het reisdocument. Vergeleken met PNR-gegevens⁷ gaat het vaak om aanvullende en doorgaans geverifieerde informatie. API-gegevens dragen bij aan juistheid en volledigheid van passagiersgegevens, doordat ze een betrouwbare aanvulling vormen op PNR-gegevens. Bij de verwerking van deze gegevens wordt rekening gehouden met het principe van minimale gegevensverwerking en passende beveiligingsmaatregelen.

API-verordening rechtshandhaving

De API-verordening⁸ rechtshandhaving is 19 december 2024 aangenomen door de Europese Raad Justitie en Binnenlandse Zaken en op 28 januari 2025 in werking getreden.

⁶ Zie hoofdstuk 5.3 over het verschil tussen PNR-gegevens en API-gegevens.

⁷ Die deels door de passagier bij de boeking zelf wordt ingevuld.

⁸ Regulation of the European Parliament and of the Council on the collection and transfer of advance passenger information for the prevention, detection, investigation and prosecution of terrorist offences and serious crime, and amending Regulation (EU) 2019/818.

Op grond van deze verordening zijn luchtvaartmaatschappijen verplicht om:

- API-gegevens te verzamelen voor alle vluchten van of naar een land buiten de EU;
- API-gegevens te verzamelen voor alle vluchten binnen de EU⁹ waarna deze aan lidstaten worden verstrekt die deze routes hebben opgenomen in hun nationale selectie;
- deze gegevens te verstrekken aan de Europese Router die wordt beheerd vanuit eu-LISA, waarvandaan de gegevens worden doorgestuurd aan de betreffende Passenger Information Unit (PIU) en grensautoriteiten.

Met deze wettelijke verplichting wordt een consistente aanlevering van API-gegevens gewaarborgd, wat bijdraagt aan de vereiste van juistheid en volledigheid van gegevens.

Implementatietraject

Het implementatietraject op basis van de API-verordening rechtshandhaving is in 2025 gestart. Het traject omvat:

- het opstellen van uitvoeringshandelingen,
- het ontwikkelen van de API/PNR router, en
- de aansluiting van de PIU's en de luchtvaartmaatschappijen op de router.

Uitvoeringshandelingen

Uitvoeringshandelingen zijn aanvullende EU-regels van lagere orde, opgesteld door de Europese Commissie in afstemming met de lidstaten. In 2025 zijn de onderhandelingen over deze uitvoeringshandelingen gestart en naar verwachting duren deze tot de zomer van 2026. De NCTV en de Pi-NL zijn bij deze onderhandelingen betrokken. Ook het Ministerie van Asiel en Migratie en de KMar zijn hierbij betrokken.

API/PNR-router

eu-LISA¹⁰ ontwerpt en ontwikkelt de API/PNR-router in afstemming met de luchtvaartsector en de lidstaten. Voor het ontwerp heeft eu-LISA startbijeenkomsten georganiseerd. De NCTV sluit daarbij aan in afstemming met de Pi-NL en Justid. De verwachte ingebruikname van de API/PNR-router is gepland op 2029. Daarna hebben de PIU's nog twee jaar om aan te sluiten voor het ontvangen van API-gegevens. Voor het ontvangen van PNR-gegevens hebben zij vier jaar. De router zorgt ervoor dat API- en PNR-gegevens veilig en gestructureerd bij de juiste PIU's terechtkomen, waardoor de juistheid en volledigheid van de gegevens wordt ondersteund.

Nationale acties

Tenslotte verkent de NCTV, samen met de KMar, het Ministerie van Asiel en Migratie en de Pi-NL welke aanvullende nationale acties nodig zijn voor de implementatie van de API-verordening rechtshandhaving.

Gegevensbescherming door beveiliging en ontwerp (art 4a Wpg en 17 PNR-wet)

De bescherming van de persoonsgegevens dient door technische en organisatorische maatregelen te zijn gewaarborgd.

Bevindingen 2025: Het kernsysteem van de Pi-NL, TRIP, is volgens de principes van 'gegevensbescherming door beveiliging en ontwerp' gebouwd en ingericht.

Statement of Compliance

De commandant van de KMar is de beheersmatig verantwoordelijke voor de Pi-NL. In 2019 heeft hij een 'Statement of Compliance' afgegeven voor de genomen technische en organisatorische maatregelen voor de Pi-NL en het Joint IV Commando van het ministerie van Defensie. De Statement of Compliance is in 2024 opnieuw afgegeven door de commandant KMar. Voor 2025 is de Statement of Compliance herbevestigd door de commandant KMar, in lijn met afspraken tussen de CISO Defensie en de CISO NCTV, waarmee de geldigheid van de Statement of Compliance is verlengd voor 2025.

⁹ Aankomst en vertrek vinden plaats binnen de EU.

¹⁰ eu-LISA is het Agentschap van de Europese Unie voor het operationeel beheer van grootschalige IT-systemen op het gebied van vrijheid, veiligheid en recht.

Privacy Framework

In 2025 hebben de NCTV en de Pi-NL een Privacy Framework ontwikkeld. Dit framework biedt een gestructureerd overzicht van privacyverplichtingen en bijbehorende beheersmaatregelen. Daarnaast ondersteunt het framework het systematische monitoren, vaststellen en documenteren van de naleving van de privacyverplichtingen. Het framework sluit aan bij het vorige advies van de FG om privacyverplichtingen en bijbehorende monitoring structureel te documenteren en draagt bij aan de verdere invulling van het verantwoordingsbeginsel.

Toestemming van de op afstand van de opsporing geplaatste officier van justitie

Bij de Pi-NL geldt een tweedelige autorisatieprocedure voor het verstrekken van passagiersgegevens:

1. *Toestemming voor alle vorderingen:* Voor alle vorderingen van passagiersgegevens door opsporingsambtenaren wordt toestemming gevraagd van de zaakofficier van justitie. Dit geldt voor zowel recente passagiersgegevens als gegevens ouder dan zes maanden.
2. *Toestemming voor gedepersonaliseerde passagiersgegevens (ouder dan zes maanden):*

Verzoeken van bevoegde autoriteiten om gedepersonaliseerde passagiersgegevens (ouder dan 6 maanden) toegankelijk te maken, vereisen vooraf toestemming. Deze toestemming moet komen van een rechter of onafhankelijke administratieve autoriteit. Dit is voorgeschreven op basis van het arrest van het Hof van Justitie.¹¹

Bij de Pi-NL wordt deze toestemming uitgevoerd door een op afstand van de opsporing geplaatste officier van justitie. Een officier van justitie maakt echter onderdeel uit van de strafketen, waardoor de vraag rijst in hoeverre deze als een dergelijke onafhankelijke autoriteit kan worden beschouwd.

FG-controle en notificatie

De FG ontvangt bij iedere verstrekking van passagiersgegevens ouder dan zes maanden een notificatie. Op basis hiervan controleert de FG of de vereiste toestemming voor het opheffen van depersonalisatie van de passagiersgegevens door de op afstand van de opsporing geplaatste officier van justitie is gegeven. Hiermee is geborgd dat gedepersonaliseerde gegevens alleen worden gepersonaliseerd en vervolgens verstrekt nadat de vereiste toestemming is verleend.

Gegevensbescherming door standaardinstellingen (art 4b Wpg en 17 PNR-wet)

De verwerkingsverantwoordelijke treft passende technische en organisatorische maatregelen om te waarborgen dat standaard alleen die persoonsgegevens worden verwerkt die noodzakelijk zijn voor elk specifiek doel van de verwerking.

De passende technische en organisatorische maatregelen betreffen in ieder geval de hoeveelheid verzamelde persoonsgegevens, de mate waarin zij worden verwerkt, de periode van opslag en de toegankelijkheid van de persoonsgegevens.

Bevindingen 2025:

Selectie intra-EU vluchten

In het voormelde arrest van het Hof van Justitie van de Europese Unie behandelt het Hof de verwerking van passagiersgegevens voor intra-EU vluchten. Het Hof bepaalt dat deze verwerking beperkt moet blijven, tenzij er een terroristische dreiging is die reëel, actueel of voorzienbaar is. Dit betekent dat niet zonder meer alle intra-EU vluchten standaard onderworpen mogen worden aan de gegevensverwerking van de Pi-NL. Er moet een gegronde reden zijn om aan te nemen dat een bepaalde vlucht risico's met zich meebrengt.

Tijdelijke opschorting van intra-EU selectie

In het najaar van 2024 besloot de minister van Justitie en Veiligheid tijdelijk de intra-EU selectie op te schorten. Dit gebeurde vanwege de verhoogde terroristische dreiging in Nederland. Ook speelde de voorstelbare dreiging die gepaard ging met de door Nederland georganiseerd NAVO-top van 24 tot en met 26 juni 2025 een rol.

¹¹ Hof van Justitie EU 21 juni, C-817/19

Evaluatie van dreiging zomer 2025

In de zomer van 2025 is opnieuw geëvalueerd of de intra-EU selectie opnieuw tijdelijk opgeschort moest worden. Er bleek onvoldoende aanleiding om opnieuw tot opschorting van de intra-EU selectie over te gaan.

Invoering selectiemodel voor intra-EU vluchten

In de zomer is een intra-EU selectie ingevoerd conform het selectie-advies. Dit model is ontwikkeld op basis van uitgebreide risicoanalyse en relevante gegevensonderzoeken. Het maakt het mogelijk intra-EU vluchten systematisch te selecteren op basis van voorspelbare risico's. Alleen intra-EU vluchten van geselecteerde Europese luchthavens worden verwerkt door de Pi-NL. Passagiersgegevens van intra-EU vluchten van niet geselecteerde Europese luchthavens worden automatisch gefilterd en gewist.

Toezicht en toetsing door de FG

De FG heeft een onafhankelijke controle uitgevoerd om te verifiëren dat de ingevoerde selectie correct functioneert. Deze controle bevestigde dat uitsluitend passagiersgegevens van intra-EU vluchten van geselecteerde luchthavens worden verwerkt. Gegevens van intra-EU vluchten van niet geselecteerde luchthavens worden automatisch gefilterd en gewist.

Het advies is om de luchthavenselectie periodiek te herzien. Hiermee kan worden beoordeeld of de risico's op terroristische misdrijven of ernstige criminaliteit nog actueel zijn. Daarnaast kan zo worden vastgesteld of de selectie van luchthavens nog steeds passend is.

Voor de maatregelen die door de Pi-NL zijn genomen met betrekking tot de periode van opslag en de toegankelijkheid van de passagiersgegevens wordt verwezen naar de paragrafen

"Bewaartermijn en afscherming (art 20 PNR-wet)" en "Autorisaties en toegang (art 6 en 6a Wpg en 17 PNR-wet)".

Gegevensbeschermingseffectbeoordeling (art 4c Wpg en 17 PNR-wet)

Wanneer een verwerking, waarschijnlijk een hoog risico voor de rechten en vrijheden van personen oplevert, voert de verwerkingsverantwoordelijke voorafgaande aan de verwerking een beoordeling uit van het effect van de voorgenomen verwerkingsactiviteiten op de bescherming van persoonsgegevens. Indien nodig verricht de verwerkingsverantwoordelijke een toetsing om te beoordelen of de verwerking overeenkomstig de gegevensbeschermingseffectbeoordeling wordt uitgevoerd, zulks ten minste wanneer sprake is van een verandering van het risico dat de verwerkingen inhouden.

Bevindingen 2025: De gegevensbeschermingseffectbeoordeling ziet op de verwerking van passagiersgegevens door de Pi-NL met behulp van TRIP. De initiële gegevensbeschermingseffectbeoordeling is uitgevoerd in 2015/2016. De gegevensbeschermingseffectbeoordeling is opnieuw uitgevoerd in 2020 en 2023/2024. In 2026 zal opnieuw een gegevensbeschermingseffectbeoordeling worden uitgevoerd.

Op basis van de vastgestelde gegevensbeschermingseffectbeoordeling 2024 zijn een aantal mitigerende maatregelen voorgeschreven. Alle voorgestelde mitigerende maatregelen zijn geïmplementeerd.

Addendum gegevensbeschermingseffectbeoordeling 2025

In 2025 is vanwege een wijziging in het verwerkingsproces een addendum bij de bestaande gegevensbeschermingseffectbeoordeling opgesteld. Dit addendum wordt gebruikt voor wijzigingen die geen hoog risico voor betrokkenen oplevert, maar wel moet worden gedocumenteerd. Het addendum beschrijft de wijziging, beoordeelt de eventuele risico's en legt vast of aanvullende maatregelen nodig zijn. Het addendum en de bijbehorende uitkomsten zijn afgestemd met de NCTV en vervolgens vastgesteld door de NCTV.

Borging van risico's

Het addendum borgt een proportionele en zorgvuldige beoordeling van de wijziging, zonder dat een nieuwe gegevensbeschermingseffectbeoordeling nodig is. Hiermee wordt voldaan aan de

verantwoordingsplicht en blijft inzichtelijk dat de verwerking in lijn is met de PNR-wet en PNR-richtlijn.

Het advies is om de huidige werkwijze voort te zetten: wijzigingen zonder hoog risico worden vastgelegd in een addendum. Wanneer zich een wijziging voordoet die wel een hoog risico oplevert, dient een gegevensbeschermingseffectbeoordeling uit te worden gevoerd. Daarnaast is het aan te bevelen om de bestaande praktijk van periodieke toetsing voort te zetten. Bij deze toetsing, die elke drie jaar plaatsvindt, wordt gecontroleerd of de verwerking van passagiersgegevens nog in overeenstemming is met de bestaande gegevensbeschermingseffectbeoordeling, de PNR-wet en de PNR-richtlijn. De gegevensbeschermingseffectbeoordeling wordt waar nodig geactualiseerd.

Autorisaties en toegang (art 6 en 6a Wpg en 17 PNR-wet)

De verwerkingsverantwoordelijke dient een systeem van autorisaties te onderhouden dat voldoet aan de vereisten van zorgvuldigheid en evenredigheid.

Bevindingen 2025: De FG heeft door middel van een steekproef gecontroleerd of de feitelijke bevoegdheden – systeemautorisaties - overeenkwamen met de vastgelegde autorisaties. Dit bleek het geval te zijn.

Iedere drie maanden ontvangt de Pi-NL van de Justitiële Informatiedienst een overzicht van medewerkers die toegang hebben tot TRIP, inclusief hun systeemautorisaties. Hiermee wordt elk kwartaal gecontroleerd of autorisaties passen bij de uitvoering van de functie.

In 2025 is de procesbeschrijving autorisatiebeleid opgesteld en vastgesteld. In de procesbeschrijving autorisatiebeleid is vastgelegd hoe toegang tot passagiersgegevens wordt beheerd.

Geadviseerd wordt om deze controles ook centraal vast te leggen. Door dit centraal vast te leggen, wordt inzichtelijk welke controles plaatsvinden, door wie en wanneer. Daarnaast kan aantoonbaar worden gemaakt dat monitoring systematisch en volgens de procedures worden uitgevoerd.

Verwerkers (art 6c Wpg en 17 PNR-wet)

Ook de partijen die persoonsgegevens verwerken ten behoeve van de verwerkingsverantwoordelijke dienen passende technische en organisatorische maatregelen en procedures te hebben geïmplementeerd zodat bij de verwerking wordt voldaan aan privacyregelgeving. Afspraken over de verwerkingen door een verwerker zijn geregeld in een verwerkersovereenkomst.

Bevindingen 2025: De verwerkingsverantwoordelijke voor de verwerkingen van de Pi-NL maakt gebruik van twee verwerkers: de Justitiële Informatiedienst van het ministerie van Justitie en Veiligheid en het Joint IV Commando van het ministerie van Defensie. Met deze twee verwerkers zijn in 2019 verwerkersovereenkomsten gesloten. In 2025 is begonnen aan de herziening van deze verwerkersafspraken.

In control verklaring en implementatie BIO-maatregelen Justid

Voor wat betreft de verwerking van passagiersgegevens door de Justitiële Informatiedienst is in 2025 een nieuwe 'in control verklaring' afgegeven. Hierbij is tevens bevestigd dat de overeengekomen technische en organisatorische maatregelen in de verwerkersovereenkomst zijn geïmplementeerd en worden nageleefd. Met de in control verklaring wordt bevestigd dat de risico's adequaat worden beheerst en de processen op orde zijn. En de overige afspraken in de verwerkersovereenkomst worden nageleefd.

De Justitiële Informatiedienst heeft bevestigd nog niet volledig 'compliant' te zijn met alle 250 maatregelen die in de Baseline Informatiebeveiliging Overheid (BIO) staan benoemd. De Justitiële Informatiedienst werkt actief aan de uitvoering van deze maatregelen en zet deze inspanningen in 2026 voort en werkt daarbij ook aan de transitie naar BIO 2.0.

Het advies blijft om jaarlijks de in control verklaring bij de Justitiële Informatiedienst op te vragen en te documenteren. Zorg dat de verwerker de BIO-maatregelen blijft implementeren en bewaak de voortgang hiervan.

Statement of Compliance

Voor 2025 is de Statement of Compliance herbevestigd door de commandant van de KMar, waarmee de geldigheid van de Statement of Compliance is verlengd. Met de Statement of Compliance wordt bevestigd dat de technische en organisatorische maatregelen zoals overeengekomen in de verwerkersovereenkomst zijn genomen en worden nageleefd.¹²

Het advies blijft om jaarlijks de Statement of Compliance, danwel de herbevestiging van de commandant van de KMar op te vragen en te documenteren.

Rechten van betrokkene (art 24a t/m 31c Wpg en 17 PNR-wet)

Een betrokkene ontvangt duidelijke informatie over de verwerking van zijn/haar persoonsgegevens. Op zijn/haar schriftelijke verzoek, ontvangt de betrokkene binnen zes weken inzage in de verwerking van zijn/haar persoonsgegevens. Betrokkene kan deze gegevens laten rectificeren of vernietigen indien deze niet juist zijn, respectievelijk in strijd met een wettelijk voorschrift zijn verwerkt.

Bevindingen 2025: De informatie over de verwerking van passagiersgegevens is beschikbaar op de website rijksoverheid.nl/onderwerpen/luchtvaart/reisgegevens-luchtvaart.

In 2025 zijn 35 inzageverzoeken van betrokkenen binnengekomen, waarvan er twee tevens een verzoek tot verwijdering behelsde. De Pi-NL heeft viermaal het behandelingsproces van 6 weken verdaagd met de wettelijk toegestane termijn van vier weken. Alle inzageverzoeken waarvan de wettelijke termijn afliep in 2025 zijn binnen de wettelijke termijn afgehandeld. De FG heeft opgetreden als contactpunt voor alle betrokkenen.

Bij de afhandeling van verzoeken van betrokkenen is vastgesteld dat de huidige identificatieprocedure mogelijk onvoldoende zekerheid biedt over de identiteit van verzoeker. Dit kan leiden tot het risico van ongeautoriseerde kennisneming van persoonsgegevens.

De FG adviseert om te onderzoeken of de identificatieprocedure kan worden versterkt. Hierbij moet rekening worden gehouden met praktische uitvoerbaarheid en de benodigde middelen voor implementatie.

Audits (art 33 Wpg en 17 PNR-wet)

Vierjaarlijks dient een *privacy audit* plaats te vinden bij de Pi-NL en jaarlijks een *interne audit* ter voorbereiding op de privacy audit. De privacy audit heeft betrekking op de wijze waarop het verwerken van persoonsgegevens is georganiseerd, de maatregelen en procedures die daarop van toepassing zijn en de werking van deze maatregelen en procedures.

Bevindingen 2025:

Context en eerdere audit

In 2024 heeft de Auditdienst Rijk (ADR) een privacy-audit uitgevoerd naar de verwerking van passagiersgegevens door de Pi-NL. Uit het rapport over 2020–2023 bleek dat enkele normen nog niet volledig werden gehaald. In reactie hierop heeft de Pi-NL in afstemming met de NCTV een verbeterplan opgesteld met bijbehorende verbetermaatregelen.

Hercontrole en interne audit 2025

In 2025 is een hercontrole en interne audit uitgevoerd. Uit deze hercontrole blijkt dat de verbetermaatregelen uit het verbeterplan volledig zijn uitgevoerd en nu in opzet en bestaan voldoen aan de gestelde normen. Daarnaast zijn bij de overige normen welke zijn onderzocht in de interne audit geen relevante afwijkingen geconstateerd.

¹² Zie ook onder het kopje Gegevensbescherming door beveiliging en ontwerp in deze rapportage.

Het advies richt zich op het systematisch monitoren en het centraal documenteren van de verbetermaatregelen uit de audit waarvoor blijvende monitoring nodig is. Door dit centraal vast te leggen, wordt inzichtelijk welke controles plaatsvinden, door wie en wanneer. Daarnaast kan aantoonbaar worden gemaakt dat monitoring systematisch en volgens de procedures worden uitgevoerd.

Melding inbreuk in verband met persoonsgegevens (art 33a Wpg en 17 PNR-wet)

De verwerkingsverantwoordelijke meldt een inbreuk in verband met persoonsgegevens direct en uiterlijk binnen 72 uur aan de AP, nadat hij ervan heeft kennisgenomen. Een melding blijft achterwege als het niet waarschijnlijk is dat de inbreuk een risico voor de rechten en vrijheden van personen met zich meebrengt.

Bevindingen 2025: Taken omtrent het beoordelen en melden van inbreuken in verband met persoonsgegevens is door de minister van Justitie & Veiligheid gemandateerd aan de NCTV. Mogelijke inbreuken in verband met persoonsgegevens door de Pi-NL geconstateerd dienen binnen 24 uur gemeld te worden bij de privacy coördinator van de NCTV. Door de Pi-NL zijn binnen 24 uur in 2025 zeven mogelijke inbreuken in verband met persoonsgegevens gemeld aan de privacy coördinator van de NCTV. De privacy coördinator heeft vijf meldingen beoordeeld als inbreuken in verband met persoonsgegevens. Naar het oordeel van de privacy coördinator was het niet waarschijnlijk dat de inbreuken in verband met persoonsgegevens een risico opleverde voor de rechten en vrijheden van betrokkene. Melding bij de AP en het informeren van betrokkenen was om die reden niet nodig. Door de Pi-NL zijn maatregelen genomen om herhaling van dergelijke inbreuken te voorkomen.

De Pi-NL ontvangt en documenteert de terugkoppeling van de privacy coördinator van de NCTV op de meldingen van mogelijke inbreuken in verband met persoonsgegevens die door de Pi-NL zijn gedaan.

De FG constateert dat datalekken zijn opgevolgd en dat procedures zoals het vier-ogen-principe bestaan. Tegelijkertijd blijft het belangrijk om medewerkers alert te houden en processen te blijven toetsen om fouten of onzorgvuldig handelen te voorkomen.

Advies blijft om de FG na constatering van een mogelijke inbreuk in verband met persoonsgegevens binnen 24 uur te betrekken. Daarnaast adviseert de FG scherp te behouden bij het verstrekken van passagiersgegevens op verzoek van een bevoegde instanties. Er blijft aandacht nodig voor correcte uitvoering.

Spoedprocedure (H2.5 Aanwijzing opsporingsbevoegdheden)

In geval van dringende noodzaak behoort bij het indienen van een vordering door een bevoegde instantie een *spoedprocedure*¹³ tot de mogelijkheden. Een dergelijke spoedvordering dient vervolgens binnen 72 uur te worden geformaliseerd.

Bevindingen 2025: Van de 244 spoedvorderingen zijn er 30 niet geformaliseerd, een hoger percentage dan in 2024. Een deel van de formalisatie van de spoedvorderingen vindt buiten de termijn van 72 uur plaats. Dit heeft geleid tot een verdere afname van het percentage dat tijdig wordt geformaliseerd.

Tijdige formalisatie blijft een aandachtspunt voor de opsporingsdiensten en het Openbaar Ministerie, zoals onderstaande cijfers laten zien. De FG adviseert dat de kwestie wordt opgepakt in overleg tussen het Openbaar Ministerie en de NCTV.

¹³ Bij een spoedvordering verleent het Openbaar Ministerie mondelinge toestemming. De mondelinge toestemming dient binnen 72 uur te worden geformaliseerd. Dit betekent dat schriftelijke toestemming door het Openbaar Ministerie na een mondelinge toestemming vereist is voor de rechtmatigheid van de vordering en derhalve de verstrekking.

	2022		2023		2024		2025	
	#	%	#	%	#	%	#	%
Totaal aantal spoedvorderingen	327	100%	273	100%	246	100%	244	100%
Waarvan binnen termijn geformaliseerd	105	32%	126	46%	44	18%	37	15%
Waarvan buiten termijn geformaliseerd	197	60%	135	50%	193	78%	177	73%
Waarvan niet geformaliseerd	25	8%	12	4%	9	4%	30	12%

Tabel 1: formalisatie van spoedvorderingen door het Openbaar Ministerie. De gegevens in dit tabel dateren van 12 januari 2026.

CONCLUSIE

De wettelijke waarborgen voor het beschermen van persoonsgegevens zijn aanwezig in het primaire proces van de Pi-NL. Ook de interne cultuur en actiebereidheid om passagiersgegevens te beschermen zijn goed verankerd bij de Pi-NL.

De privacy audit uit 2024 liet verbeterpunten zien, die door de Pi-NL zijn opgepakt in een verbeterplan. Uit de hercontrole blijkt dat de verbetermaatregelen volledig zijn uitgevoerd en voldoen aan de gestelde normen.

Voor enkele maatregelen geldt dat deze jaarlijks gemonitord moeten worden. De FG adviseert om de monitoring structureel centraal te documenteren, om consistentie en verantwoording te waarborgen.

De FG constateert dat de verbeteracties uit eerdere jaarrapportages van de FG zijn opgepakt en uitgevoerd. De FG adviseert deze lijn vast te houden.

Tenslotte blijft de FG toezien op de brede naleving van privacy principes en beveiliging van passagiersgegevens.

Hieronder volgen de statistieken over de mate waarin passagiersgegevens op grond van de artikelen 9a tot en met 16 van de PNR-wet zijn verstrekt, doorgegeven of verzocht in 2025.

Toelichting:

In onderstaande tabel worden de volgende afkortingen gebruikt:

- BINL: Nederlandse bevoegde instantie, zoals vermeld in de PNR-wet (het Openbaar Ministerie, de politie, de bijzondere opsporingsdiensten, de Koninklijke Marechaussee en de Rijksrecherche).
- OvJ: officier van justitie
- PIU: Passenger Information Unit, te weten een passagiersinformatie-eenheid uit een andere lidstaat
- BIEU: Bevoegde instantie uit een Europese lidstaat.

Nota bene 1: Op dit moment verstrekt de Pi-NL niet rechtstreeks aan derde landen. Indien een derde land om passagiersgegevens verzoekt, verloopt dit via een internationaal rechtshulpverzoek aan het (Landelijk) Internationaal Rechtshulp Centrum.

Nota bene 2: één vordering kan in de praktijk tot nul, een of meerdere verstrekkingen leiden (bijvoorbeeld omdat een passagier meerdere vluchten heeft gemaakt).

1	Vorderingen	
1.1	Totalen algemeen	
1.1.1	Aantal aangemaakte vorderingen	3.792
1.1.2	Aantal aangemaakte vorderingen met toestemming OvJ demaskeren	699
	BINL - PINL	
1.2	Aantal vorderingen van BINL aan PINL TRIP (9 PNR)	
1.2.1	Aantal ontvangen vorderingen van BI NL	2.481
1.2.2	Aantal verzoeken met toestemming OvJ demaskeren	426
	BINL - PINL - PIU - PINL - BINL	
1.3	Aantal verzoeken door PINL bij PIU t.b.v. BINL (14 PNR lid 2 en 3)	
1.3.1	Aantal ontvangen vorderingen van BI NL met toestemming vorderen bij PIU	392
1.3.2	Aantal verzoeken met toestemming OvJ demaskeren	92
1.3.3	Aantal door Pi-NL verstuurde verzoeken aan PIU tv BINL	365
	BINL - PIU - BINL	
1.4	Aantal door BI NL rechtstreeks verstuurde verzoeken aan PIU (16 PNR lid 1 en 2) i.h.k.v. dringende noodzaak	
1.4.1	Aantal ontvangen afschriften van verzoek BINL verzonden door PIU	-
	PIU- PIU	
1.5	PIU - PIU (10 PNR lid 2)	
1.5.1	Ontvangen verzoeken van PIU	894

1.5.2	Aantal verzoeken PIU met toestemming OvJ-EU demaskeren	197
	PIU- PIU Spontaan	
1.6	Ontvangen verzoeken van PIU (10 PNR lid 2)	
1.6.1	Aantal spontane verstrekkingen aan PIU (10 PNR lid 1 jo. 6 lid 1 en 2) o.g.v. vergelijking databank of RCS	-
	PINL - PIU	
1.8	Aantal spontane verzoeken van PINL aan PIU (14 PNR lid 1)	
1.8.1	Aantal spontane verzoeken	-
	PIU - PINL Extra pushes	
1.9	Aantal ontvangen PIU verzoeken om extra push van luchtvaartmaatschappijen aan PINL (11 PNR)	
1.9.1	Aantal ontvangen verzoeken van PIU om extra NL push	-
1.10	PINL - PIU Extra pushes	
1.10.1	Aantal naar PIU verstuurde Pi-NL-verzoeken extra push van luchtvaartmaatschappij (15 PNR lid 1)	-
	BIEU - PINL - BIEU	
1.11	BIEU-verzoeken met dringende noodzaak rechtstreeks aan PINL (10 PNR lid 4 jo 13 PNR)	
1.11.1	Aantal BIEU-verzoeken aan Pi-NL	-
1.11.2	Aantal BIEU-verzoeken met toestemming OvJ demaskeren	-
1.11.3	Aantal door PINL verzonden afschriften van verzoek BI EU aan PIU	-
	Europol - PI-NL - Europol	
1.12	Aantal verzoeken van Europol (via DLIO/Siena) aan Pi-NL (12 PNR lid 1)	
1.12.1	Aantal ontvangen verzoeken van Europol	363
1.12.2	Aantal verzoeken met toestemming OvJ demaskeren	49
	3e land - PI-NL - 3e Land	
1.13	Aantal verstrekkingen door PINL aan 3e land van PNR-data (13 PNR lid 1)	
1.13.1	Aantal ontvangen verzoeken van 3e land	54
1.13.2	Aantal verzoeken met toestemming OvJ demaskeren	27
1.13.3	Verzoek om toestemming PIU verzonden door PINL aan PIU	-
	PIU - PINL - 3e Land	
1.14	Aantal verstrekkingen door PINL aan 3e land van data van andere PIU zonder voorafgaande toestemming PIU (13 PNR lid 2)	
1.14.1	Notificatie verzonden door PINL aan PIU	-

2	Verstrekingen	
2.1	Totalen algemeen	
2.1.1	Aantal verstrekkingen o.g.v. vordering/verzoek subject	11.228
2.1.2	Aantal verstrekte vluchlijsten	67
2.1.3	Aantal verstrekkingen o.g.v. SIS2 matches	8.114
2.1.4	Aantal verstrekkingen o.g.v. risico criteria set	2.282
2.1.5	Aantal verstrekkingen van persoonsgegevens waarvan de depersonalisatie is opgeheven	2.701
	BINL - PINL (9 PNR)	
2.2	Aantal verstrekkingen van PINL aan BINL	
2.2.1	Aantal verstrekkingen van PINL aan BINL	10.313
2.2.2	Aantal verstrekkingen van persoonsgegevens waarvan de depersonalisatie is opgeheven aan BINL	2.288
	BINL - PINL - PIU - PINL - BINL	
2.3	Aantal verzoeken door PINL bij PIU t.b.v. BINL (14 PNR lid 2 en 3)	
2.3.1	Aantal verstrekkingen van PIU via PINL aan BI NL	526
2.3.2	Aantal verstrekkingen van PIU in Siena (NB. 100% overnemen)	-
2.3.3	Aantal verstrekkingen PIU van persoonsgegevens waarvan de depersonalisatie is opgeheven tbv BINL	-
	BINL-PIU - BINL	
2.4	Aantal door BI NL rechtstreeks verstuurd verzoeken aan PIU (16 PNR lid 1 en 2) i.h.k.v. dringende noodzaak	
2.4.1	Van BINL ontvangen kopie van PIU-verstrekkingen	-
	PIU - PIU (10 PNR lid 2)	
2.5	Aantal verstrekkingen (via DLIO/Siena) aan PIU	
2.5.1	Aantal verstrekkingen (via DLIO/Siena) aan PIU	1.704
2.5.2	Aantal verstrekkingen van persoonsgegevens waarvan de depersonalisatie is opgeheven aan PIU	268
	PIU- PIU Spontaan	
2.6	Aantal spontane verstrekkingen aan PIU (10 PNR lid 1 jo. 6 lid 1 en 2) o.g.v. vergelijking databank of RCS	
2.6.1	Spontane verstrekking van PINL aan PIU	1
2.7	Aantal door PINL ontvangen spontane verstrekkingen van PIU t.b.v. BINL doorgegeven aan BINL (09a PNR jo. 8 PNR)	
2.7.1	Aantal ontvangen spontane verstrekking van PIU	-
2.7.2	Aantal door Pi-NL aan BINL doorgegeven spontane verstrekkingen van PIU	-
2.8	Aantal spontane verzoeken van PINL aan PIU (14 PNR lid 1)	
2.8.1	Aantal ontvangen spontane verstrekkingen van PIU	-

2.9	Aantal PINL-verstrekkingsen om extra push van luchtvaartmaatschappijen aan PIU (11 PNR)	
2.9.1	Aantal PI-NL-verstrekkingsen aan PIU van extra NL push	-
2.10	Aantal van PIU ontvangen PIU-verstrekkingsen extra push van luchtvaartmaatschappij (15 PNR lid 1)	
2.10.1	Aantal verstrekkingsen van PIU van extra PIU push aan PINL	-
	BIEU - PINL - BIEU	
2.11	PINL rechtstreekse verstrekkingsen aan BIEU met dringende noodzaak (10 PNR lid 4 jo 13 PNR)	
2.11.1	Aantal verstrekkingsen door Pi-NL aan BI EU	-
2.11.2	Aantal verstrekkingsen van persoonsgegevens waarvan de depersonalisatie is opgeheven aan BI EU	-
	Europol - PI-NL- Europol	
2.12	Aantal verstrekkingsen PINL (via DLIO/Siena) t.b.v. Europol (12 PNR lid 1)	
2.12.1	Aantal PI-NL-verstrekkingsen aan Europol	1.426
2.12.2	Aantal PI-NL-verstrekkingsen van persoonsgegevens waarvan de depersonalisatie is opgeheven aan Europol	60
	3e land - PI-NL - 3e Land	
2.13	Aantal verstrekkingsen door PINL aan 3e land van PNR-data (13 PNR lid 1)	
2.13.1	Aantal verstrekkingsen door PINL aan 3e land	134
2.13.2	Aantal verstrekkingsen van persoonsgegevens waarvan de depersonalisatie is opgeheven aan 3e landen	85
2.13.3	Aantal vooraf gegeven toestemmingen van PIU	-
2.13.4	Aantal akkoord verwerkingsverantwoordelijk	-
	PINL - 3e Land zonder voorafgaande toestemming PIU	
2.14	Aantal verstrekkingsen door PINL aan 3e land van data van andere PIU zonder voorafgaande toestemming PIU (13 PNR lid 2)	
2.14.1	Aantal verstrekkingsen PIU-verstrekkingsen door PINL aan 3e land	-
2.14.2	Aantal verstrekkingsen van persoonsgegevens waarvan de depersonalisatie is opgeheven aan 3e landen	-

5.1 Lijst van passagiersgegevens¹⁴

1. PNR-bestandslocatie.
2. Datum van reservering en afgifte van het biljet.
3. Geplande reisdatum of -data.
4. Naam of namen.
5. Adres en contactgegevens, waaronder telefoonnummer en e-mailadres.
6. Alle betalingsinformatie, met inbegrip van het factuuradres.
7. Volledige reisroute voor dit specifieke PNR.
8. Informatie betreffende reizigers die gebruik maken van een loyaliteitsprogramma voor frequent reizen.
9. Reisbureau of reisagent.
10. Reisstatus van de passagier, met inbegrip van bevestigingen, check-in-status en «no-show» of «go-show»-informatie.
11. Opgesplitste of opgedeelde PNR-informatie.
12. Algemene opmerkingen, waar onder wordt begrepen alle beschikbare informatie over niet-begeleide minderjarigen jonger dan 18 jaar, zoals naam en geslacht van de minderjarige, leeftijd, talen die de minderjarige spreekt, naam en contactgegevens van de persoon die de minderjarige begeleidt naar het vertrek en de aard van de relatie van deze persoon met de minderjarige, naam en contactgegevens van de persoon die de minderjarige afhaalt bij aankomst en de aard van de relatie van deze persoon met de minderjarige, functionaris voor vertrek en aankomst.
13. Informatie uit de biljetuitgifte («ticketing field»-informatie), waaronder wordt begrepen het biljetnummer, de uitgiftedatum van het reisbiljet, biljettentickets voor enkele reizen en geautomatiseerde prijsnotering van reisbiljetten.
14. Zitplaatsinformatie, waaronder het zitplaatsnummer.
15. Informatie over gemeenschappelijke vluchtnummers.
16. Alle bagage-informatie.
17. Aantal en namen van de andere reizigers in het PNR.
18. Alle verzamelde API-gegevens (Advance Passenger Information), waaronder wordt begrepen soort, nummer, land van afgifte en geldigheidsdatum van een identiteitsdocument, nationaliteit, familienaam, voornaam, geslacht, geboortedatum, luchtvaartmaatschappij, vluchtnummer, datum van vertrek, datum van aankomst, luchthaven van vertrek, luchthaven van aankomst, tijdstip van vertrek, tijdstip van aankomst.
19. Alle vroegere wijzigingen in de onder de punten 1 tot en met 18 genoemde passagiersgegevens.

¹⁴ Bijlage 1 bij de PNR-wet.

5.2

Lijst van strafbare feiten¹⁵

1. Deelneming aan een criminele organisatie.
2. Mensenhandel.
3. Seksuele uitbuiting van kinderen en kinderpornografie.
4. Illegale handel in verdovende middelen en psychotrope stoffen.
5. Illegale handel in wapens, munitie en explosieven.
6. Corruptie.
7. Fraude, met inbegrip van fraude ten nadele van de financiële belangen van de Unie.
8. Witwassen van opbrengsten van criminaliteit en valsemunterij, met inbegrip van namaak van de euro.
9. Computercriminaliteit/cybercriminaliteit.
10. Milieumisdrijven, met inbegrip van de illegale handel in bedreigde diersoorten en de illegale handel in bedreigde planten- en boomsoorten.
11. Hulp bij illegale binnenkomst en illegaal verblijf.
12. Moord, doodslag en zware mishandeling.
13. Illegale handel in menselijke organen en weefsels.
14. Ontvoering, wederrechtelijke vrijheidsberoving en gijzeling.
15. Georganiseerde en gewapende diefstal.
16. Illegale handel in cultuurgooederen, waaronder antiquiteiten en kunstvoorwerpen.
17. Namaak van producten en productpiraterij.
18. Vervalsing van administratieve documenten en handel in valse documenten.
19. Illegale handel in hormonale stoffen en andere groeibevorderaars.
20. Illegale handel in nucleaire of radioactieve stoffen.
21. Verkrachting.
22. Misdrijven die onder de rechtsmacht van het Internationaal Strafhof vallen.
23. Kaping van vliegtuigen/schepen.
24. Sabotage.
25. Handel in gestolen voertuigen.
26. Industriële spionage.

NB: naast bovenstaande ernstige misdrijven vallen ook de in artikel 83 en 83b van het Wetboek van Strafrecht benoemde terroristische misdrijven onder de doelbinding van de Pi-NL.

¹⁵ Bijlage 2 bij de PNR-wet.

5.3

Passagiersgegevens: API en PNR

Artikel 4 van de PNR-wet stelt dat een luchtvaartmaatschappij van elke vlucht aan de passagiersinformatie-eenheid de passagiersgegevens verstrekt waarover zij ten behoeve van haar bedrijfsvoering beschikt. Conform de bijlage bij de wet betreft dit de Passenger Name Records (PNR) en de Advance Passenger Information (API) - voor zover de luchtvaartmaatschappij hier dus over beschikt.

PNR is de informatie die een luchtvaartmaatschappij nodig heeft om haar eigen bedrijfsproces goed te kunnen uitvoeren. Bijvoorbeeld de datum van reservering, contactgegevens, bagage-informatie en eventuele beschikbare check-in en boardinggegevens.

API is informatie die door overheidsinstanties wordt gebruikt voor hun (grens)toezichttaken; deze wordt dus specifiek door luchtvaartmaatschappijen met dit doel verzameld. API betreft de gegevens uit het reisdocument (zoals naam en nationaliteit), over de vlucht (zoals het vluchtnummer en tijdstip van vertrek) en over de reisroute.