Ministerie van Justitie en Veiligheid

Jaarrapportage Functionaris Gegevensbescherming Passagiersinformatie-eenheid Nederland

2024

Datum *3 februari 2025*
Status *Definitief*

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 **7**

4 STATISTIEKEN **18**

5 BIJLAGEN **22**

5.1 LIJST VAN PASSAGIERSGEGEVENS 22
5.2 LIJST VAN STRAFBARE FEITEN 23
5.3 PASSAGIERSGEGEVENS: API EN PNR 24

1 Inleiding

Dit is de jaarrapportage over het jaar 2024 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 voor 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 (hierna: PNR-richtlijn) 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. 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 (NCTV) is door de minister van Justitie en Veiligheid gemandateerd om taken uit te voeren vanuit haar rol als verwerkingsverantwoordelijke die voortvloeien uit de PNR-wet. De Commandant van de Koninklijke Marechaussee 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 privacywetgeving[2] 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)
[2] De PNR-wet en de van toepassing zijnde artikelen onder de Wet politiegegevens.

2 Samenvatting

Samenvattend kan worden gesteld dat het management en de medewerkers van de Pi-NL zich bewust zijn van het belang van gegevensbescherming en zorgvuldig omgaan met de persoonsgegevens die zij verwerken. De wettelijke waarborgen voor het beschermen van persoonsgegevens die zijn gecontroleerd, zijn aanwezig en functioneren voldoende.

Naar aanleiding van het arrest van het Hof van Justitie van de Europese Unie op 21 juni 2022[3] heeft de minister van Justitie en Veiligheid met advies van de FG de algemene bewaartermijn in 2023 aangepast van vijf naar drie jaar. De FG adviseert de algemene bewaartermijn niet te verkorten en derhalve drie jaar aan te houden. Een algemene bewaartermijn van drie jaar is noodzakelijk voor en evenredig aan de doelstellingen van de PNR-wet. Met een bewaartermijn van drie jaar kan er voldaan worden aan de wettelijke verplichting om met de passagiersgegevens een analyse uit te kunnen voeren, te voldoen aan vorderingen en verzoeken van bevoegde instanties en passagiersgegevens te vergelijken met risicocriteria en databanken.

Er is in 2024 door de Pi-NL onderzoek gedaan naar de oorzaken van de niet aangeleverde API-gegevens die wel zouden moeten (kunnen) zijn aangeleverd. Daarnaast zijn oplossingen voor dit probleem in kaart gebracht. Er wordt inmiddels gewerkt aan het doorvoeren van de eerste oplossingen, waardoor verwacht wordt dat er meer API-gegevens geleverd zullen worden aan de Pi-NL. Daarnaast is de API-verordening rechtshandhaving[4] in december 2024 goedgekeurd en vastgesteld door de Europese Raad Justitie en Binnenlandse Zaken. Op 28 januari 2025 treedt de API-verordening in werking. Met de API-verordening rechtshandhaving wordt het aanleveren van API-gegevens door de luchtvaartmaatschappijen aan de PIU's consistent geregeld en wettelijk verplicht, waarmee wordt bijgedragen aan het vereiste van juistheid en volledigheid van gegevens.

De Statement of Compliance is in 2024 voor de Pi-NL en het Joint IV Commando van het ministerie van Defensie opnieuw afgegeven door de Commandant van de Koninklijke Marechaussee.

Voor wat betreft de verwerking van passagiersgegevens door de Justitiële Informatiedienst is in 2024 een nieuwe 'in control verklaring' afgegeven. De Justitiële Informatiedienst verwacht in 2025 volledig 'compliant' te zijn met alle 250 maatregelen die in de Baseline Informatiebeveiliging Overheid staan benoemd.

In het najaar van 2024 heeft de minister van Justitie en Veiligheid besloten om, omwille van de huidige terroristische dreiging in Nederland en de voorstelbare dreiging die gepaard gaat met de door Nederland georganiseerd NAVO-top van 24 tot en met 26 juni 2025, tijdelijk de intra-EU selectie op te schorten. Momenteel worden derhalve de passagiersgegevens van alle intra-EU vluchten verwerkt. In de zomer van 2025 wordt geëvalueerd of er nog steeds sprake is van een terroristische dreiging die reëel en actueel of voorzienbaar is. Indien er géén sprake meer is van een dergelijke dreiging, zal in de zomer van 2025 een selectie gemaakt worden van intra EU-vluchten, waarvan de passagiersgegevens zullen worden verwerkt. Afgelopen jaar is gewerkt aan het ontwikkelen van een nieuw selectiemodel zoals eerder aangekondigd door de minister van Justitie en Veiligheid.

De Auditdienst Rijk (ADR) heeft in 2024 een privacy audit uitgevoerd inzake de passagiersgegevens die de Pi-NL verwerkt. De Pi-NL voldoet niet geheel aan alle normen. Voor een deel van de normen waaraan in de verslagperiode 2020-2023 niet is voldaan zijn in 2024 reeds maatregelen genomen. De Pi-NL heeft een verbeterplan opgesteld waarin de maatregelen worden beschreven die reeds getroffen zijn en nog worden genomen ter verbetering van de

[3] HvJ EU 21 juni 2022, C-817/19, ECLI:EU:C:2022:491.

[4] Verordening (EU) 2025/13 van het Europees Parlement en de Raad van 19 december 2024 betreffende de verzameling en de doorgifte van advance passenger information met het oog op het voorkomen, opsporen, onderzoeken en vervolgen van terroristische misdrijven en ernstige criminaliteit, en tot wijziging van Verordening (EU) 2019/818

geconstateerde tekortkomingen. Binnen een jaar - na het definitieve audit rapport – zal een hercontrole worden uitgevoerd op de onderdelen die niet voldeden aan de gestelde normen.

Een belangrijk aandachtspunt is de verbeterpunten in het verbeterplan en de resterende actiepunten op de actielijst te prioriteren, planmatig uit te voeren en te monitoren. Daarnaast adviseert de FG een meer gedocumenteerde aanpak in het belang 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 registratiesystemen[5], het doen van steekproeven[6], 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 betrokkene[7] 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 2024: 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 persoonsgegevens. Er heeft regelmatig contact plaatsgevonden tussen de FG, het management en de medewerkers van de Pi-NL en het ministerie van Justitie en Veiligheid. Er is in 2024 meerdere malen contact geweest tussen de AP en de FG.

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 2024: 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 de als zodanig aangemerkte bijzondere persoonsgegevens. Een steekproefsgewijze controle op de verwerking van passagiersgegevens heeft plaatsgevonden. Uit de steekproef bleek dat geen bijzondere persoonsgegevens zijn aangetroffen. De woorden en kenmerken die op de lijst zijn aangemerkt als bijzondere persoonsgegevens, zijn niet aangetroffen.

In de FG-jaarrapportage 2022 en 2023 is aandacht gevraagd voor het periodiek actualiseren van de lijst met woorden en kenmerken die vallen onder bijzondere persoonsgegevens. Pi-NL heeft in

[5] Zoals het register inbreuken in verband met persoonsgegevens, de notificaties van de verstrekkingen en registraties van spoedvorderingen.
[6] Bijvoorbeeld ten aanzien van afscherming van persoonsgegevens na zes maanden, bijzondere persoonsgegevens, bewaartermijnen, autorisaties.
[7] De persoon van wie Pi-NL passagiersgegevens verwerkt.

2024 nader onderzoek uitgevoerd naar nog niet in kaart gebrachte woorden en kenmerken die vallen onder bijzondere persoonsgegevens. Op basis van dit onderzoek is de lijst met woorden en kenmerken, die vallen onder bijzondere persoonsgegevens, geactualiseerd. Hierdoor worden ook deze bijzondere persoonsgegevens voortaan direct verwijderd door het geautomatiseerde filtersysteem.
Het advies is om periodiek onderzoek te blijven doen naar nog niet in kaart gebrachte bijzondere persoonsgegevens en de lijst met bijzondere persoonsgegevens te actualiseren.

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 2024: Door het Belgische Hof zijn aan het Hof van Justitie van de Europese Unie prejudiciële vragen gesteld over de interpretatie van een aantal onderdelen in de PNR-richtlijn.[8] Een onderdeel betrof de vraag of de PNR-richtlijn zich verzet tegen nationale wetgeving die voor passagiersgegevens een algemene bewaartermijn van vijf jaar voorschrijft, zonder onderscheid naargelang de betrokken passagier wel of geen risico op het gebied van terroristische misdrijven of ernstige criminaliteit vormt.

Uit dit arrest van het Hof van Justitie van de Europese Unie blijkt dat het zich verzet tegen nationale wetgeving die voor passagiersgegevens een algemene bewaartermijn van vijf jaar voorschrijft die zonder onderscheidt geldt voor alle passagiers.

In overweging 25 PNR-Richtlijn staat vermeld: *"De bewaartermijn voor PNR-gegevens dient zo lang te zijn als noodzakelijk is voor en evenredig te zijn aan de doelstellingen, namelijk het voorkomen, opsporen, onderzoeken en vervolgen van terroristische misdrijven en ernstige criminaliteit. Gezien de aard van de gegevens en het gebruik ervan dienen de PNR-gegevens lang genoeg te worden bewaard om er een analyse mee te kunnen uitvoeren en ze bij onderzoek te kunnen gebruiken. Ter voorkoming van onevenredig gebruik dienen de gegevens na de initiële bewaartermijn door afscherming van gegevenselementen te worden gedepersonaliseerd. Om te zorgen voor het hoogste niveau van gegevensbescherming, dient toegang tot de volledige PNR-gegevens, waarmee de betrokkene rechtstreeks kan worden geïdentificeerd, uitsluitend onder zeer strikte en restrictieve voorwaarden te worden toegestaan na die initiële bewaartermijn."*

Algemene bewaartermijn
De algemene bewaartermijn voor passagiersgegevens is, naar aanleiding van het arrest van het Hof, in 2023 met advies van de FG door de minister van Justitie en Veiligheid aangepast van vijf jaar naar drie jaar. Daarmee heeft de minister van Justitie en Veiligheid gevolg gegeven aan het vereiste van het differentiëren van de bewaartermijnen na de initiële bewaartermijn van zes maanden op basis van het arrest van het Hof.

Een algemene bewaartermijn van drie jaar is noodzakelijk voor en evenredig aan de doelstellingen van de PNR-wet. Met een termijn van drie jaar kan er voldaan worden aan de wettelijke verplichting om met de passagiersgegevens een analyse uit te kunnen voeren, te voldoen aan vorderingen en verzoeken van bevoegde instanties en passagiersgegevens te vergelijken met risicocriteria en databanken.

[8] Prejudiciële beslissing van het Hof in het kader van een geding tussen de Ligue des droits humains en de Ministerraad (België) over de rechtmatigheid van de wet van 25 december 2016 betreffende de verwerking van passagiersgegevens. HvJ EU 21 juni 2022, C-817/19, ECLI:EU:C:2022:491.

Onder bepaalde voorwaarden kan een gedeelte van de passagiersgegevens voor de maximale duur van vijf jaar bewaard blijven. Dit betreft de gevallen waarin er een objectieve aanwijzing is dat de betreffende passagier een risico kan vormen op het gebied van terrorisme of ernstige criminaliteit.

Uit onderlinge communicatie met de AP blijkt dat de AP een andere lezing heeft van het arrest van het Hof van Justitie van de Europese Unie. Zij brengt op basis van het arrest argumenten naar voren dat de algemene bewaartermijn zes maanden zou moeten zijn.

Noodzakelijk en evenredigheid: praktijk

- *Proportionaliteit*

Een algemene bewaartermijn van drie jaar in het belang van de veiligheid van de burgers staat in verhouding tot de inbreuk voor de personen van wie de passagiersgegevens worden verwerkt.

De Pi-NL heeft in samenwerking met de NCTV en de bevoegde instanties per soort passagiersgegeven[9] de relevantie onderzocht na zes maanden. Hieruit kan geconcludeerd worden dat het bewaren van de passagiersgegevens na zes maanden noodzakelijk is voor het voorkomen, opsporen, onderzoeken en vervolgen van terroristische misdrijven en ernstige criminaliteit en dat er niet meer persoonsgegevens worden verwerkt dan strikt noodzakelijk voor het doel van de verwerking.

Ook is gelet op de aard van de persoonsgegevens, een algemene bewaartermijn van drie jaar evenredig. Er worden alleen algemene persoonsgegevens verwerkt. In vergelijking tot bijvoorbeeld banken die op basis van de Wet ter voorkoming van witwassen en financieren van terrorisme wel gevoelige gegevens, zoals financiële gegevens, het Burgerservicenummer, een kopie identiteitsbewijs van al haar klanten minimaal vijf jaar bewaren.

Uit de periodieke besprekingen met de FG's van de Passenger Information Units binnen de lidstaten: (PIU's) blijkt dat de PIU's, met uitzondering van Duitsland, op dit moment nog steeds een algemene bewaartermijn van vijf jaar hanteren. De verwerkingsverantwoordelijken van andere PIU's lijken mede op advies van hun FG's voornemens de algemene bewaartermijn van passagiersgegevens net zoals Nederland aan te passen naar drie jaar. In vergelijking met de bewaartermijnen van passagiersgegevens van veel andere landen buiten de EU is een bewaartermijn van drie jaar beperkt. Zo bewaart de Verenigde Staten alle passagiersgegevens van en naar de Verenigde Staten vijftien jaar. Australië vijf en een half jaar. Canada vijf jaar.

Tenslotte is met het Dreigingsbeeld Terrorisme Nederland (DTN) het dreigingsniveau sinds december 2023 vastgesteld op 4 op een schaal van 1-5. In december 2024 heeft de NCTV een nieuw DTN uitgebracht waarin het dreigingsniveau 4 wordt gehandhaafd. Dat betekent dat er een reële kans is dat een aanslag zal plaatsvinden. Dit hoge dreigingsniveau rechtvaardigt des te meer de noodzakelijkheid en evenredigheid van een algemene bewaartermijn van drie jaar.

- *Subsidiariteit*

Voor dat de PNR-wet in werking trad, werden passagiersgegevens door de bevoegde instanties uitgevraagd bij de verschillende luchtvaartmaatschappijen wereldwijd. De PNR-wet heeft ervoor gezorgd dat het vorderen van passagiersgegevens bij circa 80 luchtvaartmaatschappijen overbodig werd en voortaan werd neergelegd op een centrale locatie, de Pi-NL. De Pi-NL voldoet aan strikte beveiligingsvereisten en wettelijke waarborgen. De AP en de FG houden toezicht op de verwerking van passagiersgegevens door de Pi-NL. Daarnaast zijn de medewerkers van de Pi-NL opgeleid en grondig gescreend. Dit heeft een positief effect op de bescherming van persoonsgegevens van betrokkenen. Door een algemene bewaartermijn te hanteren die korter is dan drie jaar is de kans zeer groot dat de passagiersgegevens door de bevoegde instanties weer worden gevorderd bij de luchtvaarmaatschappijen. Daarbij is het risico op het hanteren van zwarte lijsten opgesteld door luchtvaartmaatschappijen niet uitgesloten. Voorzienbaar is dat het verkorten van de algemene bewaartermijn om die reden de bescherming van persoonsgegevens van betrokkenen in grotere mate zal schaden.

[9] Zie bijlage 5.1 Lijst passagiersgegevens, voor de verschillende soorten passagiersgegevens.

Advies en controle FG
De FG adviseert een algemene bewaartermijn van drie jaar aan te houden.

De FG heeft aan de hand van een steekproef gecontroleerd of passagiersgegevens in 2024, waarvoor geen objectieve aanwijzing was voor langer bewaren, langer zijn bewaard dan drie jaar. Dit was niet het geval. Deze passagiersgegevens zijn geautomatiseerd gewist na drie jaar.

Pi-NL bestaat in juni 2024 vijf jaar. De FG heeft aan de hand van een steekproef gecontroleerd of passagiersgegevens, waarvoor een objectieve aanwijzing was voor langer bewaren, langer zijn bewaard dan 5 jaar. Dit was niet het geval. De passagiersgegevens zijn geautomatiseerd gewist na vijf jaar.

Het automatisch depersonaliseren van passagiersgegevens in TRIP, het kernsysteem van de Pi-NL, functioneert en de FG controleert dit periodiek. De FG ontvangt een notificatie bij verstrekking van passagiersgegevens ouder dan zes maanden. De FG heeft de verstrekkingen op basis van de notificaties gecontroleerd en geconstateerd dat in alle gevallen specifieke toestemming van de officier van justitie aanwezig was voor deze doorgifte.

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 2024: het artikel 22 PNR-wet register is in 2024 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 2024: Controle in 2024 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 om te bepalen of een bevoegde instantie maatregelen moet treffen of nader onderzoek moet doen.

Bevindingen 2024: 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 2024: Naast de Passenger Name Records (PNR-gegevens) die luchtvaartmaatschappijen verzamelen en aan de Pi-NL doorgeven, kan de Pi-NL in een aantal gevallen ook beschikken over Advance Passenger Information (API-gegevens)[10]. In bijna alle

[10] Zie hoofdstuk 5.3 over het verschil tussen PNR-gegevens en API-gegevens.

gevallen bevatten deze API-gegevens geautomatiseerd ingelezen gegevens uit het reisdocument. In vergelijking met PNR-gegevens (die deels door de passagier bij de boeking zelf wordt ingevuld) betreft het dan extra en in de meeste gevallen geverifieerde informatie. De API-gegevens dragen daarmee positief bij aan de verwerking van juiste en volledige passagiersgegevens.

Uit de jaarrapportage van de FG 2023 blijkt dat in 2023 ongeveer de helft van de luchtvaartmaatschappijen die API-gegevens zouden moeten (kunnen) aanleveren dit ook daadwerkelijk aan de Pi-NL hebben aangeleverd. Het advies was om dit uit te breiden en er zorg voor te dragen dat alle luchtvaartmaatschappijen die beschikken over API-gegevens deze gegevens aanleveren aan de Pi-NL.

Er is in 2024 door de Pi-NL onderzoek gedaan naar de oorzaken van de niet aangeleverde API-gegevens die wel zouden moeten (kunnen) zijn aangeleverd. Daarnaast zijn oplossingen in kaart gebracht. Er wordt inmiddels gewerkt aan het doorvoeren van de eerste oplossingen, waardoor verwacht wordt dat er meer API-gegevens geleverd zullen worden aan de Pi-NL. Dit zal doorgaan in 2025.

Daarnaast is de API-verordening[11] rechtshandhaving 12 december 2024 aangenomen door de Europese Raad Justitie en Binnenlandse Zaken. De API-verordening treedt op 28 januari 2025 in werking. De implementatie is voorzien in de periode 2028-2030. Deze API-verordening, tezamen met de API-verordening grensbewaking[12], vervangen de API-Richtlijn die gericht is op het gebruik van API-gegevens voor grenscontroles. De API Richtlijn laat wel toe dat API gegevens door luchtvaartmaatschappijen worden verzameld en aangeleverd aan de PIU's, maar dit is niet verplicht voor vluchten die vertrekken vanuit de EU en alleen van toepassing op vluchten afkomstig uit derde landen naar de EU. Dit verklaart grotendeels waarom een groot deel van de API-gegevens niet worden verstrekt door de luchtvaartmaatschappijen aan de Pi-NL.
Luchtvaartmaatschappijen zijn op grond van de API-verordening rechtshandhaving verplicht om voor alle vluchten die vertrekken van of aankomen in een land buiten de EU en voor (door de betreffende lidstaat geselecteerde) vluchten die plaatsvinden binnen de EU[13], API-gegevens te verzamelen en te verstrekken aan de PIU's.
Met de API-verordening rechtshandhaving wordt het aanleveren van API-gegevens door de luchtvaartmaatschappijen aan de PIU's consistent geregeld en wettelijk verplicht, waarmee wordt bijgedragen aan het vereiste van juistheid en volledigheid van gegevens.

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 2024: 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 Koninklijke Marechaussee (KMar), de beheersmatig verantwoordelijke voor de Pi-NL, heeft in 2019 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 zoals overeengekomen in de Verwerkersafspraak PNR gegevens (verwerkersovereenkomst). Door de FG is in de jaarrapportage 2023 geadviseerd de in 2019 door de Commandant KMar afgegeven 'Statement of Compliance' opnieuw te bezien en af te geven. De Statement of Compliance is in 2024 opnieuw afgegeven door de Commandant KMar.

[11] 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.
[12] Beide API verordeningen hebben een verschillend doel en een verschillende reikwijdte. Voor rechtshandhaving bestaat bijvoorbeeld de mogelijkheid om luchtvaartmaatschappijen te verplichten om API-gegevens voor intra-EU vluchten aan te leveren, dat is bij grensbewaking niet het geval.
[13] Aankomst en vertrek vinden plaats binnen de EU.

Dataminimalisatie en in control verklaringen verwerkers
De aandachtspunten in de FG jaarrapportage 2023 met betrekking tot:

- het verwerken van passagiersgegevens buiten het TRIP-systeem om; en
- de noodzaak om van de verwerkers[14] de bevestiging te ontvangen dat de risico's adequaat worden beheerst en de processen op orde zijn,

zijn opgepakt.

De bestandenpostbus waarin de communicatie tussen de betrokkene en de FG in het kader van een inzageverzoek werd opgeslagen wordt niet meer gebruikt. Alle passagiersgegevens worden verwerkt binnen TRIP. Communicatie met betrokkenen via de mail worden nadat de mails zijn geplaatst in TRIP direct verwijderd.

Toestemming van de op afstand van de opsporing geplaatste OvJ in TRIP
Het Openbaar Ministerie heeft naar aanleiding van het voormelde arrest van het Hof van Justitie van de Europese Unie in 2023 besloten dat naast de toestemming van de zaaksofficier van justitie voor alle vorderingen van passagiersgegevens van opsporingsambtenaren, hierop ook toestemming is vereist van een onafhankelijke op afstand van de opsporing geplaatste officier van justitie. De gegeven toestemming door de op afstand van de opsporing geplaatste officier van justitie is vanaf 2024 door de FG te controleren en wordt geregistreerd in TRIP.

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 2024: In het voormelde arrest van het Hof van Justitie van de Europese Unie oordeelt het Hof dat de verwerking van passagiersgegevens voor intra-EU vluchten beperkt moet blijven tot vluchten waarbij een reëel en actueel of voorspelbaar risico op terroristische misdrijven of ernstige criminaliteit bestaat. Dit betekent dat niet 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.

Op basis van dit arrest had de Pi-NL conform het besluit van de minister van Justitie en Veiligheid haar proces in 2023 aangepast en een selectie gemaakt van intra-EU vluchten, waarvan zij de passagiersgegevens verwerkte.

In het najaar van 2024 heeft de minister van Justitie en Veiligheid besloten om, omwille van de huidige terroristische dreiging in Nederland en de voorstelbare dreiging die gepaard gaat met de door Nederland georganiseerd NAVO-top van 24 tot en met 26 juni 2025, tijdelijk de intra-EU selectie op te schorten. Momenteel worden derhalve de passagiersgegevens van alle intra-EU vluchten verwerkt.

In de zomer van 2025 wordt geëvalueerd of er nog steeds sprake is van een terroristische dreiging die reëel en actueel of voorzienbaar is. Indien er géén sprake meer is van een dergelijke dreiging, zal in de zomer van 2025 een selectie gemaakt worden van intra EU-vluchten, waarvan de passagiersgegevens zullen worden verwerkt.

Afgelopen jaar is gewerkt aan het ontwikkelen van een nieuw selectiemodel zoals eerder aangekondigd door de minister van Justitie en Veiligheid. Met het nieuwe selectiemodel wordt niet meer op nationaal luchthavenniveau vluchten geselecteerd, maar op het niveau van Europese luchthavens. Dit betekent concreet dat uitsluitend intra-EU vluchten van geselecteerde Europese luchthavens worden verwerkt door de Pi-NL. De passagiersgegevens van intra-EU vluchten van

[14] Zie hierover meer in de paragraaf Verwerkers van deze jaarrapportage.

niet geselecteerde Europese luchthavens worden automatisch gefilterd en gewist. Dit model wordt echter, omwille van het besluit om tijdelijk passagiersgegevens van alle intra-EU vluchten te verzamelen, nog niet ingezet.

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 2024: De gegevensbeschermingseffectbeoordeling is uitgevoerd. De gegevensbeschermingseffectbeoordeling ziet op de verwerking van passagiersgegevens door de Pi-NL met behulp van TRIP. De initiële gegevensbeschermingseffectbeoordeling is uitgevoerd in 2015/2016. Het uitvoeren van een gegevensbeschermingseffectbeoordeling is geen eenmalige opdracht, maar een continu proces vanwege veranderingen van de gegevensverwerkingen, risico's en context.

In de gegevensbeschermingseffectbeoordeling Pi-NL 2020 zijn de wijzigingen in de processen, systemen en procedures van de Pi-NL beschreven. De gegevensbeschermingseffectbeoordeling Pi-NL 2023 beschrijft de verdere optimalisatie van al deze processen, systemen en procedures, alsmede alle gewijzigde gegevensverwerkingen als gevolg van het voormelde arrest van het Hof van Justitie van de Europese Unie.

In 2024 is de gegevensbeschermingseffectbeoordeling van advies van de FG voorzien en vastgesteld door de NCTV. Op basis van de gegevensbeschermingseffectbeoordeling zijn een aantal mitigerende maatregelen voorgeschreven. De meeste maatregelen zijn genomen. Aan de overige maatregelen wordt gewerkt om deze te implementeren.

Het advies aan de verwerkingsverantwoordelijke is om de voortgang van de implementatie van de maatregelen in de gegevensbeschermingseffectbeoordeling te monitoren en om iedere drie jaar - of eerder in het geval van wijziging van het risico van de verwerking - te toetsen of de verwerkingen nog plaats vinden overeenkomstig de gegevensbeschermingseffectbeoordeling en waar nodig de gegevensbeschermingseffectbeoordeling aan te passen.

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 2024: 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 van het ministerie van Justitie en Veiligheid een overzicht van de medewerkers van Pi-NL, die toegang hebben tot TRIP, met de daar bijhorende systeemautorisaties. Op die wijze wordt eens per drie maanden gecontroleerd of de autorisaties overeenkomen met de autorisaties die noodzakelijk zijn voor het uitvoeren van de betreffende functie.

Uit een controle door de FG bleek dat een vanuit een ministerie gedetacheerde medewerker die een maand daarvoor was gestopt met zijn werkzaamheden voor de Pi-NL nog steeds de

autorisaties had binnen TRIP. Uit de logbestanden bleek dat er vanaf de datum dat de medewerker niet meer werkzaam was voor de Pi-NL, niet meer is ingelogd door de betreffende medewerker. De autorisaties van de betreffende medewerker zijn direct beëindigd.

Geadviseerd wordt een procesbeschrijving vast te stellen met de maatregelen op welke wijze tijdige de-autorisatie plaatsvindt. Implementeer de maatregelen binnen de Pi-NL. De periodieke controles op de autorisaties dienen te worden vastgelegd en bewaard.

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 2024: 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 de FG-jaarrapportage 2022 en 2023 is hierbij als aandachtspunt aangegeven dat de verwerkers moeten aantonen dat de overeengekomen technische en organisatorische maatregelen in de verwerkersovereenkomst zijn geïmplementeerd en worden nageleefd.

Voor wat betreft de verwerking van passagiersgegevens door de Justitiële Informatiedienst is in 2024 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. De overeengekomen maatregelen - die in de Baseline Informatiebeveiliging Overheid staan benoemd – zijn grotendeels geïmplementeerd. En de overige afspraken in de verwerkersovereenkomst worden nageleefd.
De verwerkingsverantwoordelijke is in 2024 in gesprek gegaan met de Justitiële Informatiedienst over de voortgang op de maatregelen. De Justitiële Informatiedienst verwacht in 2025 volledig 'compliant' te zijn met alle 250 maatregelen die in de Baseline Informatiebeveiliging Overheid staan benoemd. Uit de TRIP Voortgangsrapportage 2024 blijkt dat de Justitiële Informatiedienst vordering maakt en dat de planning is dat alle BIO maatregelen eind 2025 zijn geïmplementeerd. De Justitiële Informatiedienst heeft extra capaciteit beschikbaar gesteld voor het implementeren van de maatregelen.
Het advies aan de verwerkingsverantwoordelijke is nog steeds om met de Justitiële Informatiedienst in gesprek te blijven over de voortgang op de maatregelen. Daarnaast is het advies om jaarlijks de in control verklaring bij de Justitiële Informatiedienst op te vragen en te documenteren.

Voor wat betreft de verwerking van passagiersgegevens door het Joint IV Commando van het ministerie van Defensie is in 2024 een nieuwe 'Statement of Compliance' afgegeven. Met de Statement of Compliance wordt bevestigd dat de technische en organisatorische maatregelen zoals overeengekomen in de verwerkersovereenkomst zijn genomen en worden nageleefd.

Het advies is om jaarlijks de Statement of Compliance bij het Joint IV Commando van het ministerie van Defensie 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 en 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 2024: De informatie over de verwerking van passagiersgegevens is beschikbaar op de website rijksoverheid.nl/onderwerpen/luchtvaart/reisgegevens-luchtvaart.

In de FG-jaarrapportage 2022 en 2023 was het advies opgenomen om op de website duidelijker te maken wat de rol is van de Pi-NL en dat de Pi-NL een *vergelijkende* functie[15] heeft en niet zelf *signaleert.* Dit heeft in 2024 plaatsgevonden.

In 2024 zijn 31 inzageverzoeken van betrokkenen binnengekomen, waarvan er één 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 2024 zijn binnen de wettelijke termijn afgehandeld. De FG heeft opgetreden als contactpunt voor alle betrokkenen.

Verder werd in 2023 door de FG geadviseerd om ná het eerste contact dat de betrokkene met de FG legt in het kader van verzoeken rechten van betrokkene, in de vervolgcommunicatie het contact direct tussen de Pi-NL en de betrokkene te laten plaatsvinden. Dit voorkomt de suggestie dat de FG onderdeel is van het genomen besluit op een verzoek rechten van betrokkene, draagt bij aan dataminimalisatie, versnelt en verduidelijkt het proces voor betrokkenen. Dit advies is in 2024 opgevolgd.

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 2024: De Auditdienst Rijk (ADR) heeft in 2024 een privacy audit uitgevoerd inzake de passagiersgegevens die de Pi-NL verwerkt. De privacy audit is uitgevoerd in het kader van de PNR-wet en de artikelen uit de Wpg die van overeenkomstige toepassing zijn verklaard. De ADR onderzocht de procedures en maatregelen van de Pi-NL om te beoordelen of de Pi-NL voldoet aan de normen die zijn opgenomen in deze wetten. De ADR heeft voor de privacy audit gekeken naar de periode tussen 1 januari 2020 tot en met 31 december 2023.

De auditor heeft aan de hand van opzet, bestaan en werking getoetst. Uit de Assurancerapport Privacy Pi-NL 2020-2023[16] blijkt dat de Pi-NL niet geheel voldoet aan de normen. Voor een deel van de normen waaraan in de verslagperiode 2020-2023 niet is voldaan zijn in 2024 reeds maatregelen genomen. De Pi-NL heeft in afstemming met de NCTV een verbeterplan opgesteld waarin de maatregelen worden beschreven die reeds getroffen zijn en nog worden genomen ter verbetering van de geconstateerde tekortkomingen. Conform Wpg art. 33, lid 3 dient de verwerkersverantwoordelijke binnen een jaar - na het definitieve audit rapport - een hercontrole te laten uitvoeren op de onderdelen die niet voldeden aan de gestelde normen. De hercontrole richt zich op de opzet en het bestaan van de maatregelen. De verwerkingsverantwoordelijke heeft de opdracht voor het uitvoeren van de hercontrole en de uitvoering van de interne audit over 2024 aanbesteed.

Acties plannen, uitvoeren en monitoren en documenteren
In de FG-jaarrapportage 2023 is geadviseerd dat de Pi-NL toewerkt naar een meer gedocumenteerd en planmatig invulling van de bescherming van passagiersgegevens. De Pi-NL heeft een actielijst opgesteld met actiepunten die o.a. volgen uit de jaarrapportages van de FG en de interne auditrapportages. In 2024 is door de Pi-NL naar aanleiding van de privacy audit een verbeterplan opgesteld met bijbehorende verbetermaatregelen.
Het advies voor 2024 is om de verbetermaatregelen/acties uit het verbeterplan en de actielijst te prioriteren, te plannen, uit te voeren en te monitoren.

[15] vergelijken van passagiersgegevens met databanken, vorderingen etc.
[16] Zie het Assurancerapport Privacy Pi-NL 2020-2023: https://open.overheid.nl/documenten/6d77bd49-2830-4d4c-80e8-b0ee57fe8b4e/file

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 nadat hij ervan heeft kennisgenomen aan de AP, tenzij het niet waarschijnlijk is dat de inbreuk een risico voor de rechten en vrijheden van personen met zich meebrengt.

Bevindingen 2024: 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 2024 twee mogelijke inbreuken in verband met persoonsgegevens gemeld aan de privacy coördinator van de NCTV. De privacy coördinator heeft de 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.

Advies aan de Pi-NL blijft om alle (mogelijke) inbreuken in verband met persoonsgegevens binnen 24 uur na constatering te melden bij de privacy coördinator van de NCTV. Geadviseerd wordt dat de Pi-NL de terugkoppeling van de privacy coördinator van de NCTV - op de meldingen van mogelijke inbreuken in verband met persoonsgegevens door de Pi-NL - ontvangt en documenteert. Geadviseerd wordt de FG binnen 24 uur te betrekken na constatering van een mogelijke inbreuk in verband met persoonsgegevens.

Spoedprocedure (H2.5 Aanwijzing opsporingsbevoegdheden)

In geval van dringende noodzaak behoort bij het indienen van een vordering door een bevoegde instantie een *spoedprocedure*[17] tot de mogelijkheden. Een dergelijke spoedvordering dient vervolgens binnen 72 uur te worden geformaliseerd.

Bevindingen 2024: De ingediende spoedvorderingen van 1 januari 2024 t/m 25 november 2024 zijn allen geformaliseerd al dan niet binnen de termijn. De openstaande spoedvorderingen die nog niet zijn geformaliseerd dateren van na 25 november 2024. Formalisatie van de spoedvorderingen vindt voor een deel plaats buiten de termijn van 72 uur. Het percentage spoedvorderingen in 2024 dat binnen de termijn is geformaliseerd is afgenomen ten opzichte van 2022 en 2023.
Tijdige formalisatie blijft een aandachtspunt voor het Openbaar Ministerie, zoals onderstaande cijfers laten zien.

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

Tabel 1: formalisatie van spoedvorderingen door het Openbaar Ministerie. De gegevens in dit tabel dateren van 6 januari 2025.

[17] Bij een spoedvordering verleend het Openbaar Ministerie mondeling 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.

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 aanwezig bij de Pi-NL. De privacy audit die in 2024 heeft plaatsgevonden liet verschillende verbeterpunten zien, die door de Pi-NL in een verbeterplan zijn uitgewerkt. Een belangrijk aandachtspunt is de verbeterpunten in het verbeterplan en de resterende actiepunten op de actielijst te prioriteren, planmatig uit te voeren en te monitoren. Daarnaast adviseert de FG een meer gedocumenteerde aanpak in het belang van de verantwoordingsplicht.

4 Statistieken

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 2024.

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	3.623
1.1.2	Aantal aangemaakte vorderingen met toestemming OvJ demaskeren	638
	BINL - PINL	
1.2	Aantal vorderingen van BINL aan PINL TRIP (9 PNR)	
1.2.1	Aantal ontvangen vorderingen van BI NL	2.614
1.2.2	Aantal verzoeken met toestemming OvJ demaskeren	398
	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	369
1.3.2	Aantal verzoeken met toestemming OvJ demaskeren	89
1.3.3	Aantal door Pi-NL verstuurde verzoeken aan PIU tv BINL	351
	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	830

1.5.2	Aantal verzoeken PIU met toestemming OvJ-EU demaskeren	172
	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
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	127
1.12.2	Aantal verzoeken met toestemming OvJ demaskeren	40
	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	51
1.13.2	Aantal verzoeken met toestemming OvJ demaskeren	28
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	**Verstrekkingen**	
2.1	Totalen algemeen	
2.1.1	Aantal verstrekkingen o.g.v. vordering/verzoek subject	10.307
2.1.2	Aantal verstrekte vluchtlijsten	1.230
2.1.3	Aantal verstrekkingen o.g.v. SIS2 matches	5.452
2.1.4	Aantal verstrekkingen o.g.v. risico criteria set	1.683
2.1.5	Aantal verstrekkingen van gedemaskeerde persoonsgegevens	3.392
	BINL - PINL (9 PNR)	
2.2	Aantal verstrekkingen van PINL aan BINL	
2.2.1	Aantal verstrekkingen van PINL aan BINL	10.412
2.2.2	Aantal verstrekkingen van gedemaskeerde persoonsgegevens aan BINL	2.738
	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	525
2.3.2	Aantal verstrekkingen van PIU in Siena (NB. 100% overnemen)	-
2.3.3	Aantal verstrekkingen PIU van gedemaskeerde persoonsgegevens tv BINL	-
	BINL-PIU - BINL	
2.4	Aantal door BI NL rechtstreeks verstuurde 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	2.160
2.5.2	Aantal verstrekkingen van gedemaskeerde persoonsgegevens aan PIU	493
	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-verstrekkingen om extra push van luchtvaartmaatschappijen aan PIU (11 PNR)	
2.9.1	Aantal PI-NL-verstrekkingen aan PIU van extra NL push	-
2.10	Aantal van PIU ontvangen PIU-verstrekkingen extra push van luchtvaartmaatschappij (15 PNR lid 1)	
2.10.1	Aantal verstrekkingen van PIU van extra PIU push aan PINL	-
	BIEU - PINL - BIEU	
2.11	PINL rechtstreekse verstrekkingen aan BIEU met dringende noodzaak (10 PNR lid 4 jo 13 PNR)	
2.11.1	Aantal verstrekkingen door Pi-NL aan BI EU	1
2.11.2	Aantal verstrekkingen van gedemaskeerde persoonsgegevens aan BI EU	-
	Europol - PI-NL- Europol	
2.12	Aantal verstrekkingen PINL (via DLIO/Siena) t.b.v. Europol (12 PNR lid 1)	
2.12.1	Aantal PI-NL-verstrekkingen aan Europol	563
2.12.2	Aantal PI-NL-verstrekkingen van gedemaskeerde persoonsgegevens aan Europol	123
	3e land - PI-NL - 3e Land	
2.13	Aantal verstrekkingen door PINL aan 3e land van PNR-data (13 PNR lid 1)	
2.13.1	Aantal verstrekkingen door PINL aan 3e land	84
2.13.2	Aantal verstrekkingen van gedemaskeerde persoonsgegevens aan 3e landen	38
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 verstrekkingen door PINL aan 3e land van data van andere PIU zonder voorafgaande toestemming PIU (13 PNR lid 2)	
2.14.1	Aantal verstrekkingen PIU-verstrekkingen door PINL aan 3e land	-
2.14.2	Aantal verstrekkingen van gedemaskeerde persoonsgegevens aan 3e landen	-

5 Bijlagen

5.1 Lijst van passagiersgegevens[18]

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.

[18] Bijlage 1 bij de PNR-wet.

5.2 Lijst van strafbare feiten[19]

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 cultuurgoederen, 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.

[19] 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.