A1a

Ministerie van Justitie en Veiligheid

De Minister van Justitie en Veiligheid

Beveiligingsautoriteit
Ministerie van Justitie en Veiligheid

Turfmarkt 147
2511DP Den Haag
Postbus 20301
2500EH Den Haag
www.rijksoverheid.nl/jenv

Datum
17 augustus 2020

Projectnaam
0

Ons kenmerk
3003564

Dossiernummer
0

Bijlagen
4

nota

Nota: Aanbieden rapportage artikel 18 PNR-wet

Algemene leiding
Minister
Datum/eindparaaf

5.1.2
Datum/paraaf

Door tussenkomst van
5.1.2.e
Datum/paraaf

5.1.2.e
Datum/paraaf

5.1.2.e
Datum/paraaf

Van
5.1.2.e
Datum/paraaf

1 Doel nota

De bijgaande aanbiedingsbrief van de functionaris voor de gegevens-bescherming (FG) van de Passagiersinformatie-eenheid Nederland (Pi-NL) aan de Eerste en Tweede Kamer en de Autoriteit Persoonsgegevens aan te bieden.

2 Aanleiding, gevraagde actie(s) en advies

De rapportage vloeit voort uit de verplichting van artikel 18 lid 2 dat de FG jaarlijks een rapportage aan de Minister, de Eerste en Tweede Kamer en de Autoriteit Persoonsgegevens (hierna: AP) zendt over het voorgaande kalenderjaar voor 1 juli. De Kamers en AP waren geïnformeerd over het uitstel via een brief.

Het aanbieden van de bijgaande brieven met als bijlage de jaarrapportage 2019 aan de Eerste en Tweede Kamer via DBO. En het aanbieden van de brief aan de AP via 5.1.2e I&I.
De NCTV verzorgt een beleidsreactie naar aanleiding van de jaarrapportage 2019 en verzoekt of u de rapportage gelijktijdig met hun beleidsreactie wilt aanbieden.

Beveiligingsautoriteit
Ministerie van Justitie en Veiligheid
Ministerie Binnenlandse Zaken en Koninkrijksrelaties

Datum
17 augustus 2020

Ons kenmerk
3003564

3 Toelichting op het advies

In artikel 18.2 van de PNR wet is bepaald dat naast het opstellen van de rapportage wordt ingegaan op de wijze waarop controle is uitgeoefend op de verwerking van de persoonsgegevens door de Pi-NL en de wijze waarop Pi-NL de waarborgen voor de gegevensbescherming heeft uitgevoerd. De rapportage bevat daarnaast statistieken over de mate waarin passagiersgegevens zijn verstrekt, doorgegeven of opgevraagd.

Ik had u geïnformeerd dat de rapportage vertraging had opgelopen.

4 Dilemma's

Een dilemma is dat FG's van het Rijk normaal gesproken geen verantwoording afleggen aan het parlement of de AP, maar aan de verwerkingsverantwoordelijke. De wet schrijft in dit specifieke geval tevens voor wat de FG moet rapporteren. Het bepalen van het juiste abstractieniveau van de rapportage is ingewikkeld. Mede daarom heeft de FG naast deze rapportage een departementaal vertrouwelijk persoonlijk verslag opgesteld. Dit verslag heeft de opdrachtgever van Pi-NL (NCTV) ontvangen. Het is als achtergrondinformatie bij de nota gevoegd.

5 Politieke en bestuurlijke context

Politiek

Het PNR-dossier is een politiek gevoelig dossier. Bij de wetsbehandeling heeft de Minister de nadruk gelegd op de waarborgen ter bescherming van de persoonsgegevens.
Een passage van de Minister uit het nader verslag d.d. 1 februari 2019 over het gebruik van bijzondere gegevens staat in de jaarrapportage. Dit omdat het verwerken van bijzondere gegevens verboden is. Bij controle bleek dat het uitfilteren van bijzondere persoonsgegevens nog niet goed was ingeregeld. Dit is zo snel mogelijk en met terugwerkende kracht hersteld.
Ik schrijf dat het wettelijk verplichte register nog niet aanwezig is. De NCTV gaf in haar reactie op een eerder concept aan dat het er wel is. Ondanks dat ik niet heb kunnen vaststellen dat het register er in 2019 was, heb ik de opmerking van de NCTV overgenomen in de rapportage.

Bij de uitwisseling tussen buitenlandse bevoegde instanties die rechtstreeks Pi-NL bevragen of Nederlandse bevoegde instanties die een EU-Pi bevragen zijn de notificaties over en weer nog niet ingeregeld. Dit is in 2019 geen issue omdat alle verzoeken via het proces van internationale rechtshulpverzoeken verliepen. Pi-NL was daardoor niet betrokken bij de verwerkingen.

De NCTV zal een en ander in zijn beleidsreactie nader toelichten.

Bestuurlijk

Bestuurlijk valt de FG onder 5.1.2e, directie DI&I, BVA.
Het dossier PNR valt onder de verantwoordelijkheid van 5.1.2e, waarbij de NCTV de dossierhouder is.

6 Communicatie

De NCTV is in de lead en stemt de woordvoering af met Defensie en Pi-NL.

5.1.2.i

Beveiligingsautoriteit
Ministerie van Justitie en Veiligheid
Ministerie Binnenlandse Zaken en Koninkrijksrelaties

Datum
17 augustus 2020

Ons kenmerk
3003564

7 Afstemming

De FG heeft de rapportage laten meelezen door 5.1.2e DI&I en de adviseur 5.1.2e 5.1.2e is gevraagd mee te lezen. Door vakanties en tijdgebrek aan hun zijde is dat laatste niet gelukt.

De NCTV heeft een eerder concept op verzoek van de FG afgestemd met Ministerie van Defensie (de eigenaar van Pi-NL) en Pi-NL om feitelijke onjuistheden uit de rapportage te halen en kennis te nemen van de rapportage.

8 Bijlagen

1. Een aanbiedingsbrief aan de Tweede Kamer – verzenden aan de Kamer door DBO
2. Een aanbiedingsbrief aan de Eerste Kamer – verzenden aan de Kamer door DBO
3. Een aanbiedingsbrief aan de AP – 5.1.2e DI&I
4. Jaarrapportage artikel 18 PNR-wet – 2019 – als bijlage bij de brieven
5. Achtergrondinformatie: Persoonlijk intern verslag van de FG aan de verwerkingsverantwoordelijke – DEP-V

A1b

Nationaal Coördinator
Terrorismebestrijding en Veiligheid
Ministerie van Justitie en Veiligheid

5.1.2e

Programma
Luchtvaartbeveiliging en
detectie reisbewegingen

Turfmarkt 147
2511 DP Den Haag
Postbus 16950
2500 BZ Den Haag
www.nctv.nl

Contactpersoon
5.1.2.e
Senior beleidsmedewerker

T 5.1.2.e
E 5.1.2.e @
nctv.minjenv.nl

Datum
27 augustus 2020

Ons kenmerk
3006835

nota

Update jaarrapportage artikel 18 Functionaris Gegevensbescherming Pi-NL

Aanleiding
De Functionaris Gegevensbescherming van de Passagiersinformatie-eenheid Nederland (hierna: FG Pi-NL) heeft haar definitieve jaarrapportage 2019 conform artikel 18 PNR-wet opgeleverd. Deze rapportage zit inmiddels in 5.1.2e richting MinJenV. U wordt hierbij alvast geïnformeerd over de rapportage en vervolgstappen. De rapportage is door de FG Pi-NL ook reeds ter informatie aan de NCTV gestuurd.

Toelichting
De Pi-NL werkt onder de beleids- en verwerkingsverantwoordelijkheid van de Minister JenV. De jaarrapportage van de FG Pi-NL vloeit voort uit de verplichting van artikel 18 van de Wet gebruik van passagiersgegevens voor de bestrijding van terroristische en ernstige misdrijven (hierna: PNR-wet), die stelt dat de FG Pi-NL jaarlijks een rapportage aan MinJenV, de Eerste en Tweede Kamer en de Autoriteit Persoonsgegevens (AP) stuurt. De rapportage ziet op de wijze waarop controle is uitgeoefend op de verwerking van de persoonsgegevens 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 zijn verstrekt, doorgegeven of verzocht. De rapportage beslaat de periode van 18 juni 2019 (startdatum Pi-NL) tot en met 31 december 2019.

De FG Pi-NL concludeert in haar rapportage dat de wettelijke waarborgen voor het beschermen van persoonsgegevens aanwezig zijn en functioneren. Als belangrijkste aandachtspunt wordt het monitoren van geautomatiseerde waarborgen voor gegevensbescherming in de door de Pi-NL gebruikte applicatie Travel information portal (TRIP) genoemd. De FG Pi-NL stelt dat een software-update van TRIP de bestaande functionerende waarborgen ongewild te niet kan laten gaan. Deze conclusie wordt in de rapportage niet nader toegelicht. Navraag bij de FG Pi-NL leert dat dat de directe aanleiding voor deze conclusie ligt in uitgevoerde periodieke updates van de TRIP software. Daarbij is het in een enkel geval voorgekomen dat instellingen van geautomatiseerde waarborgen (zoals een notificatie aan de FG Pi-NL) niet goed zijn meegenomen in de wijziging of onbedoeld waren gewijzigd. Dit punt is bekend (en na constatering ook direct opgelost) bij de Pi-NL, Justid-IBO en PLR/DR. Omdat TRIP een nieuw systeem is, vinden er nog regelmatig updates plaats om aan de wensen van gebruikers te

voldoen. De FG Pi-NL geeft daarom als aandachtspunt mee om bij elk toekomstig verzoek tot wijziging aandacht te hebben voor eventuele veranderingen in de achterliggende dwarsverbanden. PLR/DR zal extra aandacht vragen bij Justid-IBO en Pi-NL voor het zorgvuldig testen van aanpassingen in de software op eventuele wijzigingen in bestaande geautomatiseerde waarborgen.

PLR/DR zal een beleidsreactie opstellen waarin verder wordt ingegaan op de conclusies uit de jaarrapportage. Met de FG Pi-NL is afgesproken dat de Minister JenV de jaarrapportage samen met de beleidsreactie naar de Eerste en Tweede Kamer stuurt.

Naast de jaarrapportage heeft de FG Pi-NL een departementaal vertrouwelijk intern verslag opgesteld. De 5.1.2e heeft aan de FG Pi-NL gevraagd of dit verslag ook naar de Tweede Kamer moet worden meegestuurd. De FG Pi-NL stelt dat het interne verslag is bedoeld als achtergrondinformatie voor minJenv als verwerkingsverantwoordelijke. De verwerkingsverantwoordelijke (minJenV), opdrachtgever (NCTV), eigenaar (5.1.2e Def) en opdrachtnemer (Pi-NL) moeten van sommige uitvoeringszaken in detail op de hoogte zijn om de juiste maatregelen te 5.1.2i

In het interne verslag worden geen zaken genoemd die fundamenteel verschillen van de conclusies uit de jaarrapportage die naar de Kamers en het AP gaat. Op één punt, de documentatieplicht, wordt in het interne verslag geconstateerd dat hieraan onvoldoende is voldaan. Zo wordt gesteld dat a) een verwerkingsregister conform art. 22 PNR-wet ontbreekt; b) een proces om DPIA's op te stellen en/of af te stemmen met de FG ontbreekt; en c) wordt geadviseerd om een specifieke data science DPIA voor de analysetaken van de Pi-NL op te stellen.
Kennelijk heeft de FG Pi-NL hierin echter geen aanleiding gevonden om deze constateringen in de jaarrapportage op te nemen. Ten aanzien van bovengenoemde punten zijn onze overwegingen:

- ad a) Er is een verwerkingsregister, maar deze moet nog worden aangevuld met gegevens van de Passagiersinformatie-eenheden en de bevoegde instanties van andere lidstaten. Hieraan wordt in gezamenlijkheid met de andere lidstaten en de betreffende Passagiersinformatie-eenheden gewerkt. Naar verwachting wordt dit in 2020 gerealiseerd.
- ad b) In 2017 is voor de Pi-NL een DPIA (Data Protection Impact Assessment, in het Nederlands: gegevensbeschermingseffectbeoordeling) uitgevoerd. In 2019 en 2020 is deze DPIA geactualiseerd. Pi-NL hoeft voor verwerkingen die binnen haar wettelijk mandaat vallen en die in deze DPIA staan beschreven geen nieuwe DPIA('s) op te stellen. Wel zal zij gedegen risico-inschattingen van de gegevensverwerking blijven maken, mitigerende maatregelen in kaart blijven brengen en hier uitvoering aan geven.
- ad c) Gestelde onder b) geldt hier ook; er is geen separate 'data science DPIA' nodig, wel zal Pi-NL gedegen risico-inschattingen van de gegevensverwerking (in casu: haar analysetaken) moeten blijven maken, mitigerende maatregelen in kaart brengen en hier uitvoering aan geven.

PLR/DR zal het interne verslag gebruiken om verder met de PI-NL en de FG Pi-NL in gesprek te gaan en zal het tevens agenderen in het bestuurlijk overleg met de eigenaar 5.1.2e Defensie), opdrachtnemer (Pi-NL) en opdrachtgever (NCTV). Ook heeft PLR/DR op alle genoemde punten in het interne verslag een reactie voorbereid.

Planning en vervolgstappen
De komende weken zullen benut worden voor het opstellen van een gezamenlijke beleidsreactie op de jaarrapportage samen met het ministerie van Defensie. Op verzoek van bureau SG Defensie wordt de beleidsreactie mede ondertekend door de minister van Defensie, aangezien deze verantwoordelijk is voor de continuïteit van de dienstverlening en de bedrijfsvoering van de Pi-NL op de lange termijn. Het streven is de beleidsreactie, gezien de gangbare termijn van zes weken, uiterlijk begin oktober naar de Kamers te sturen.

Bijlagen
- Nota FG Pi-NL Aanbieden rapportage artikel 18 PNR-wet d.d. 17 augustus 2020 (aangepast d.d. 21 augustus 2020)
- Jaarrapportage artikel 18 d.d. 17 augustus 2020
- Intern verslag FG Pi-NL d.d. 18 augustus 2020

A1c

Ministerie van Justitie en Veiligheid

MJenV

Beveiligingsautoriteit
Ministerie van Justitie en Veiligheid
Ministerie Binnenlandse Zaken en Koninkrijksrelaties

Turfmarkt 147
2511DP Den Haag
Postbus 20301
2500EH Den Haag
www.rijksoverheid.nl/jenv

Contactpersoon
5.1.2.e

Datum
10 juni 2020

Ons kenmerk
2950276

nota

Uitstel rapportage FG Art. 18 PNR wet

Algemene leiding
Minister
Datum/eindparaaf

5.1.2
Datum/paraaf

Concipiënt
5.1.2.e
Datum/paraaf

1. Doel nota
   Uw akkoord om bijgaande uitstelbrief van de functionaris gegevensbescherming (FG) van de Passagiersinformatie-eenheid Nederland (Pi-NL) naar de Eerste en Tweede Kamer, en naar de Autoriteit Persoonsgegevens te versturen.

2. Aanleiding/gevraagde actie/advies
   De aanleiding voor deze nota is de vertraging die is opgelopen in het opstellen van de rapportage van de FG. De rapportage wordt normaliter voor 1 juli verstuurd; deze termijn is dit jaar niet haalbaar (zie toelichting).

3. Toelichting
   In Artikel 18.2 van de PNR wet is bepaald dat de FG jaarlijks voor 1 juli een rapportage naar de Eerste en Tweede Kamer en naar de Autoriteit Persoonsgegevens zendt over het voorgaande kalenderjaar. In deze rapportage wordt ingegaan op de wijze waarop controle is uitgeoefend op de verwerking van de persoonsgegevens door de Passagiersinformatie-eenheid en de wijze waarop de waarborgen voor de gegevensbescherming zijn uitgevoerd. De rapportage bevat daarnaast statistieken over de mate waarin passagiersgegevens zijn verstrekt, doorgegeven of verzocht.

   Het opstellen van de rapportage heeft vertraging opgelopen in verband met de fysieke en organisatorische beperkingen als gevolg van de huidige

coronacrisis, die met name de benodigde uitwisseling van vertrouwelijke informatie belemmerde. Daarom wordt nu verzocht een uitstelbericht te versturen.
Zodra de rapportage gereed is zal ik deze aan u doen toekomen en zal deze door de NCTV worden voorzien van een beleidsreactie.

4. Afstemming
De brief is afgestemd tussen de FG en NCTV

5. Bijlagen
Uitstelbrief aan Tweede en Eerste Kamer, en Autoriteit Persoonsgegevens

Beveiligingsautoriteit
Ministerie van Justitie en Veiligheid
Ministerie Binnenlandse Zaken en Koninkrijksrelaties

Datum
10 juni 2020

Ons kenmerk
2950276

A2

Ministerie van Justitie en Veiligheid

DEP. VERTROUWELIJK Openbaar na publicatie

Kwartaal rapportage FG PI-NL bestuurlijk overleg oktober 2019

Versie 1.0

Datum	8 oktober 2019
Status	Definitief

Colofon

Afzendgegevens **Functionaris Gegevensbescherming PI-NL**

Turfmarkt 147
2511DP Den Haag
Postbus 20301
2500EH Den Haag

Auteurs FG PI-NL

Inhoud

Inleiding

In het Contourendocument is vastgelegd dat de Functionaris Gegevensbescherming (hierna: FG) PI-NL 4 maal per jaar t.b.v. het bestuurlijk overleg een rapportage opstelt voor de opdrachtnemer, eigenaar en opdrachtgever/verwerkings-verantwoordelijke.

5.1.2e Pi-NL is volgens de verwerkersafspraak de opdrachtnemer en de PI-NL is de verwerker van de PNR-gegevens. Justid en JIVC zijn verwerkers van PNR-gegevens.

De eigenaar (Ministerie van Defensie/KMar) is verantwoordelijk voor de continuïteit van de (dienstverlening en de bedrijfsvoering van de) Pi-NL op de lange termijn en het toezicht op de algemene bedrijfsvoering.

De opdrachtgever (Ministerie van Justitie en Veiligheid/NCTV) is verantwoordelijk voor het beleid inclusief de bijbehorende wet- en regelgeving en de te maken beleidskeuzes. De opdrachtgever is aansluitend ook verantwoordelijk voor een goede opdrachtformulering. De minister van JenV is, conform artikel 17 PNR, de verwerkingsverantwoordelijke.

Vastgestelde onderdelen van de rapportage zijn:

1. Aantal inzage- en correctieverzoeken incl. de afhandeltijd
2. Voortgang op de audits
3. Bemerkingen en eventuele vragen/aanbevelingen van de AP en acties die hierop zijn ondernomen.

In het contourendocument en het monitoringsdocument staan KPI's voor de PI-NL. Enkele van deze KPI's betreffen het beschermen van persoonsgegevens en/of de werkzaamheden van de FG. In het monitoringsdocument is vastgelegd dat de bron de FG is en de PI-NL rapporteert. Aangezien het hier om werkzaamheden van de FG gaat en de toelichting op deze KPI's door de FG gegeven wordt rapporteert de FG over onderstaande KPI's.

KPI 3 Doel beschermen persoonlijke levenssfeer
- KPI 3.1 Aantal datalekken;
- KPI 3.2 Aantal verwijderingen en correcties dat op verzoek van betrokkenen is gedaan;
- KPI 3.3 Aantal functionarissen dat geautoriseerd is om toegang te hebben tot PNR-data;
- KPI 3.4 Aantal verzoeken door burgers tot inzage opgeslagen PNR-gegevens;

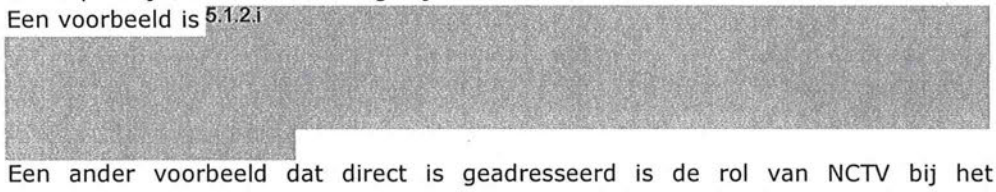
KPI 5.2 Aantal gegrond verklaarde klachten- en bezwaarprocedures tegen de Pi-NL m.b.t. het beschermen van persoonsgegevens.

Naast deze kwartaalrapportages wordt jaarlijks aan de Tweede en Eerste Kamer, de Minister van JenV en de Autoriteit Persoonsgegevens rechtstreeks verslag uitgebracht conform artikel 18 PNR.

Algemeen

De FG PI-NL is in juli 2019 gestart. In het wetgevingstraject en binnen de projectorganisatie is een grote hoeveelheid documentatie opgeleverd.
De documentatie op het gebied van beleid en uitvoering is opgeslagen op schijven bij NCTV en PI-NL waartoe de FG (nog) geen toegang heeft. De FG is daarmee afhankelijk van het delen van relevante informatie door de betreffende medewerkers van de betrokken partijen. Het betrekken bij en informeren van de FG bij zaken, processen en dagelijkse werkzaamheden waarin persoonsgegevens verwerkt worden neemt toe.

De FG constateert op grond van de ontvangen documentatie dat ten aanzien van gegevensbescherming soms keuzen zijn gemaakt die voor verbetering vatbaar zijn. Door voortschrijdend inzicht, het implementeren van beleid en wetgeving, ervaring uit de praktijk en bewustwording blijkt dat.
Een voorbeeld is 5.1.2.i



Een ander voorbeeld dat direct is geadresseerd is de rol van NCTV bij het afhandelen van inzage verzoeken van betrokkenen. In overleg tussen NCTV en FG PI-NL is een andere werkwijze voorgesteld waarbij de NCTV geen rol meer speelt. Dit aangepaste voorstel is vastgelegd in het document procesbeschrijvingen PI-NL en moet nog worden vastgesteld.

Aantal inzage- en correctieverzoeken incl. de afhandeltijd

Zie de toelichting bij KPI 3.4.

Voortgang op de audits

In zowel de Bestuursafspraken als in het Contourendocument is vastgelegd dat tussen opdrachtgever, eigenaar en opdrachtnemer afspraken worden vastgelegd over periodieke onafhankelijke audits en rapportages ten behoeve van privacybescherming van PNR-gegevens door PI-NL, in lijn met de verwerkersovereenkomst.

Er is nog niet in gezamenlijk overleg bepaald welke audits wenselijk zijn. De samenwerkende partijen (o.a. NCTV, PI-NL, FG PI-NL, ADR, I-controllers, CISO) moeten nog een auditplan opstellen.

Bemerkingen en eventuele vragen/aanbevelingen van de AP en acties die hierop zijn ondernomen.

Het eerste contact tussen FG en de Autoriteit Persoonsgegevens (AP) is tot stand gebracht. In Q4 vindt een bestuurlijke en ambtelijke kennismaking plaats tussen AP, PI-NL, NCTV en FG.

KPI 3 Doel beschermen persoonlijke levenssfeer

In het Contourendocument en het Monitoringsdocument staan KPI's voor de PI-NL. Enkele van deze KPI's betreffen het beschermen van persoonsgegevens en daarmee de werkzaamheden van de FG.

KPI 3.1 aantal datalekken PNR
Norm: 0 (nul)
Aan de FG PI-NL zijn geen datalekken o.g.v. PNR of AVG gemeld.
Dit kwartaal is de norm gehaald.

De FG PI-NL wil een onderscheid maken tussen datalekken m.b.t. PNR-gegevens en datalekken o.g.v. de AVG. De FG onderschrijft de norm 0 (nul) voor PNR-datalekken.
Voor AVG-datalekken zal de realiteit waarschijnlijk anders zijn. De laatste kunnen voorkomen in de reguliere bedrijfsvoering waarbij bijvoorbeeld een e-mail met personeelsgegevens aan de verkeerde persoon binnen of buiten PI-NL verzonden wordt. Afspraken over taken en verantwoordelijkheden m.b.t. AVG-datalekken waarbij systemen van Defensie centraal staan en 5.1.2e MinDef een verantwoordelijkheid draagt moeten nog gemaakt worden.

Een belangrijk aandachtspunt is een datalekprocedure. Deze ontbreekt momenteel. Het moet voor alle betrokkenen duidelijk zijn wie welke verantwoordelijkheid, taken en bevoegdheden heeft en hoe eventuele crisiscommunicatie is ingericht en contactgegevens.

KPI 3.2 Aantal verwijderingen en correcties dat op verzoek van betrokkenen is gedaan
Norm: te bepalen door opdrachtgever, eigenaar en opdrachtnemer i.o.m. FG.

Dit kwartaal zijn er geen persoonsgegevens verwijderd noch correcties op verzoek van betrokkene gedaan.

De norm is nog niet vastgesteld.

KPI 3.3 Aantal functionarissen dat geautoriseerd is om toegang te hebben tot PNR-data
Norm: n.a.w.

De autorisatiematrix voor de functionarissen van PI-NL met een autorisatie in TRIP geeft alleen de autorisatie per functionaris aan en niet hoeveel medewerkers per functie.
Wanneer er toegang tot de 5.1.2.i -omgeving is kan uit verschillende systemen de gevraagde informatie gedestilleerd worden.

De autorisatiematrix voor de functionarissen van Justid-IBO met een autorisatie voor TRIP-productie omgeving geeft alleen de autorisatie per functionaris aan en niet hoeveel medewerkers per functie. Deze gegevens zouden via Justid aangeleverd moeten worden.

KPI 3.4 Aantal verzoeken door burgers tot inzage opgeslagen PNR-gegevens
Norm: n.v.t.

Het aantal inzageverzoeken is 4. De afhandeltijd is gemiddeld 18 dagen.
De afhandeltijd van het eerste verzoek was 34 dagen vanwege het ontbreken van templates en onbekendheid en onduidelijkheid over het proces.

Van de 4 verzoeken:
- 5.1.2.e

Er zijn geen correctieverzoeken geweest.

Een aandachtspunt is de wijze van identificatie van betrokkenen. Het proces binnen de overheid is het toezenden van een kopie ID-bewijs. Gezien het soort gegevens dat verstrekt kan worden naar aanleiding van een informatieverzoek is er een risico op identiteitsfraude.
Voor ingezetenen kan op termijn DIGid gebruikt worden. Voor internationale verzoeken is dat niet mogelijk. Een voorstel is de kopieën van ID bewijzen door de KMar te laten controleren op echtheid. De FG kan met de AP overleggen over de wijze van identificatie en de eventuele gevolgen van het niet kunnen vaststellen van de identiteit bij veel voorkomende namen en daarmee het niet kunnen verstrekken van de gevraagde persoonsgegevens.

Zoals bovenstaand beschreven is naar aanleiding van het eerste inzage verzoek het proces, zoals in het document procesbeschrijvingen PI-NL, aangepast. Dit moet nog geformaliseerd worden.

KPI 5.2 Aantal gegrond verklaarde klachten- en bezwaarprocedures tegen de Pi-NL
Norm: in samenspraak tussen besturingsdriehoek en bevoegde instanties te bepalen

De FG PI-NL maakt een onderscheidt tussen klachten- en bezwaarprocedures m.b.t. het beschermen van persoonsgegevens en overige klachten- en bezwaarprocedures.
Voor bezwaren o.g.v. PNR geldt dat er geen beroepsprocedure is omdat de FG PI-NL namens de minister de verzoeken van betrokkenen beantwoordt. De bezwaarprocedure wordt door de AP uitgevoerd. Betrokkenen kunnen een klacht ook rechtstreeks bij de AP indienen.
Een klachtenprocedure voor PI-NL met betrekking tot andere dan privacy klachten valt buiten de werkzaamheden van de FG.

KPI 4 Doel gegevensbescherming

KPI 4.1 Aantal databeveiligingsincidenten (niet zijnde datalek)
"Er is alleen sprake van een datalek als zich daadwerkelijk een beveiligingsincident heeft voorgedaan. Bij een beveiligingsincident moet u bijvoorbeeld denken aan het kwijtraken van een USB -stick, de diefstal van een laptop of aan een inbraak door een hacker. Maar niet ieder beveiligingsincident is ook een datalek. Er is sprake van een datalek als er bij het beveiligingsincident persoonsgegevens verloren zijn gegaan, of als u onrechtmatige verwerking van de persoonsgegevens niet redelijkerwijs kunt uitsluiten. Als alleen sprake is van een zwakke plek in de beveiliging, spreken we van een beveiligingslek en niet van een datalek. U hoeft dan geen melding te doen aan de Autoriteit Persoonsgegevens."
Norm: te bepalen door besturingsdriehoek i.o.m. FG en ADR

De norm is nog niet vastgesteld.

De FG PI-NL adviseert om de CISO van de PI-NL bij het vaststellen van de norm te betrekken.

De aantallen databeveiligingsincidenten worden door PI-NL gerapporteerd en datalekken maken daar onderdeel vanuit.

Op 9 augustus 2019 viel het systeem op de KMK uit. Er is, na telefonisch overleg tussen 5.1.2e 5.1.2e PI-NL en de FG, noodgedwongen uitgeweken naar de 5.1.2.i

Overige constateringen

De FG PI-NL heeft vragen gesteld over 5.1.2.i

Het lijkt dat de passagiersgegevens van intra-EU vluchten van onvoldoende kwaliteit zijn om de bescherming van de persoonsgegevens van alle passagiers voldoende te waarborgen. Door het achterwege blijven van controles door luchtvaartmaatschappijen op namen (bv. roepnaam i.p.v. geboortenamen) of het niet volledig hoeven aan te leveren van datavelden (bv. geboortedatum) worden profielen soms ruimer opgesteld om de gewenste passagiers toch te kunnen vinden.
De vraag is in hoeverre dit gewenst is en/of er een oplossing gevonden kan worden voor het verbeteren van de kwaliteit van de gegevens.

Een belangrijk aandachtspunt is het vervangen van de FG bij onverwachte of langere afwezigheid. Voorwaarden zijn dat iemand de juiste vertrouwensfunctie

bekleed en kennis heeft van WPG en op dat moment direct toegang tot het 5.1.2.i van defensie, de werkplekken van PI-NL en afhankelijk van de duur van de vervanging tot TRIP.

Een ander aandachtspunt is het verwerken van PNR-data binnen de systemen van Defensie. Dit is tweeledig uit te leggen. Ten eerste werkt de FG momenteel binnen de systemen van MinJenV. Het e-mailadres van de 5.1.2i is in het MinJenV-domein. Daarmee komen verzoeken van betrokkenen en antwoorden waarin PNR-gegevens staan onder de verantwoordelijkheid van 5.1.2e MinJenV te vallen. De vraag is of dit wenselijk is. 5.1.2e MinJenV vindt het zelf niet wenselijk. De FG PI-NL is het daarmee eens. Een oplossing daarvoor is gewenst.
Ten tweede is nog onduidelijk in welke systemen medewerkers van PI-NL documentatie kunnen en mogen opslaan. Niet al het werk vindt plaats in TRIP. Bijvoorbeeld de analyse werkzaamheden en presentaties over werkwijzen en successen. Duidelijk is dat het gebruik van namen van verdachten en/of veroordeelden niet dan wel zo beperkt mogelijk buiten TRIP gebruikt kunnen worden. Voor o.a. 5.1.2.i
zijn richtlijnen nodig.

Conclusie

De medewerkers van de PI-NL zijn zich goed bewust van hun werkzaamheden en de rol die het beschermen van de privacy van passagiers daarbij heeft. In deze opstartfase zijn de eerste constateringen gerapporteerd door de FG PI-NL. De basis om verder te werken aan verankering van het beschermen van persoonsgegevens en het kunnen uitoefenen van het interne toezicht lijkt voldoende aanwezig. Bij alle betrokken partijen wordt de noodzaak gevoeld om de uitvoering van de PNR wet tot een succes van te maken.

A3

Ministerie van Justitie en Veiligheid

DEP. VERTROUWELIJK
openbaar bij publicatie

Kwartaal rapportage Q4-2019 FG PI-NL

Versie 1.0

Datum	30 maart 2020
Status	Definitief

Colofon

Afzendgegevens **Functionaris Gegevensbescherming PI-NL**

Turfmarkt 147
2511DP Den Haag
Postbus 20301
2500EH Den Haag
5.1.2i @MinJenV.nl

Auteurs FG PI-NL

Inhoud

Inleiding

Dit is de tweede rapportage van de FG PI-NL en gaat over het vierde kwartaal 2019.

De minister van JenV is, conform artikel 17 PNR, de verwerkingsverantwoordelijke.
In het Contourendocument is vastgelegd dat de Functionaris Gegevensbescherming (hierna: FG) PI-NL 4 maal per jaar t.b.v. het bestuurlijk overleg een rapportage opstelt voor de opdrachtnemer, eigenaar en opdrachtgever/verwerkings-verantwoordelijke. In het bestuurlijke overleg van december 2019 is vastgesteld dat de FG een tertaalcyclus zal gaan aanhouden.
5.1.2e Pi-NL is volgens de verwerkersafspraak de opdrachtnemer en de PI-NL is de verwerker van de PNR-gegevens. Justid en JIVC zijn verwerkers van PNR-gegevens.
De eigenaar (Ministerie van Defensie/KMar) is verantwoordelijk voor de continuïteit van de (dienstverlening en de bedrijfsvoering van de) Pi-NL op de lange termijn en het toezicht op de algemene bedrijfsvoering.
De opdrachtgever (Ministerie van Justitie en Veiligheid/NCTV) is conform het organisatiebesluit van het ministerie van JenV opdrachtgever voor de PI-NL en verantwoordelijk voor het beleid inclusief de bijbehorende wet- en regelgeving en de te maken beleidskeuzes. De opdrachtgever is aansluitend ook verantwoordelijk voor een goede opdrachtformulering.

Vastgestelde onderdelen van de rapportage zijn:

1. Aantal inzage- en correctieverzoeken incl. de afhandeltijd
2. Voortgang op de audits
3. Bemerkingen en eventuele vragen/aanbevelingen van de AP en acties die hierop zijn ondernomen.

In het contourendocument en het monitoringsdocument staan KPI's voor de PI-NL. Enkele van deze KPI's betreffen het beschermen van persoonsgegevens en/of de werkzaamheden van de FG. In het monitoringsdocument is vastgelegd dat de FG de bron van de statistieken is en de PI-NL deze statistieken rapporteert. Aangezien het hier om werkzaamheden van de FG gaat en de toelichting op deze KPI's door de FG gegeven wordt rapporteert de FG over onderstaande KPI's.

KPI 3 Doel beschermen persoonlijke levenssfeer
- KPI 3.1 Aantal datalekken;
- KPI 3.2 Aantal verwijderingen en correcties dat op verzoek van betrokkenen is gedaan;
- KPI 3.3 Aantal functionarissen dat geautoriseerd is om toegang te hebben tot PNR-data;
- KPI 3.4 Aantal verzoeken door burgers tot inzage opgeslagen PNR-gegevens;

KPI 5.2 Aantal gegrond verklaarde klachten- en bezwaarprocedures tegen de Pi-NL m.b.t. het beschermen van persoonsgegevens.

Naast deze rapportage wordt jaarlijks verslag uitgebracht aan de Minister, de Tweede en Eerste Kamer en de Autoriteit Persoonsgegevens conform artikel 18 PNR.

In het bestuurlijk overleg wordt deze rapportage mondeling toegelicht door de FG.

Algemeen

Een van de taken van de FG is intern toezicht houden.

Het laatste kwartaal van 2019 heeft dat geresulteerd in een onderzoek 5.1.2.i . De resultaten hiervan zijn aan 5.1.2e PI-NL verstrekt en besproken in een interne evaluatie van PI-NL in bijzijn van de FG.

Sinds 18 december 2019 kunnen gemaskeerde persoonsgegevens ouder dan zes maanden aangevraagd en verstrekt worden. De FG ontvangt van het verstrekken van gemaskeerde persoonsgegevens waarvan de maskering is opgeheven een notificatie ten behoeve van het wettelijke toezicht. Wanneer de maskering niet is opgeheven door de OvJ kan een document verstrekt worden waarin de persoonsgegevens zijn gemaskeerd conform de artikelsgewijze toelichting in de memorie van toelichting op de PNR-wet (artikel 1 jo. 20 lid 4 PNR).

De vordering is een belangrijk instrument in het toezicht om vast te stellen dat een verstrekking rechtmatig heeft plaatsgevonden. De FG heeft verstrekkingen gevonden waarbij geen vordering en/of geen spoedformulier aanwezig was. Na het spoedformulier moet binnen 72 uur de vordering nagezonden zijn. Die termijn was in enkele gevallen overschreden. De bevindingen en het advies om de gebreken te repareren zijn aan 5.1.2e PI-NL gerapporteerd. Dit is gebeurd en er is inmiddels een wijziging in TRIP doorgevoerd waardoor de bevoegde instantie een notificatie ontvangt bij het ontbreken van de vordering.

Een ander taak van de FG is het geven van advies. Hiervoor wordt de FG tijdig en naar behoren betrokken bij alle aangelegenheden die verband houden met de bescherming van persoonsgegevens.

De medewerkers van PI-NL weten de FG goed te vinden voor vragen, discussie en advies. Dit zijn over het algemeen zaken die een privacy adviseur kan uitvoeren. Waar het gaat om beleid(svoorbereiding/-vorming), evaluaties en wetgeving kan het tijdig betrekken van de FG verbeteren. Bij die activiteiten is soms onvoldoende duidelijk dat de activiteit verband kan houden met het beschermen van persoonsgegevens.

Verder bleek bij het vastleggen van de logging van verstrekkingen een omissie. Bij het verstrekken van persoonsgegevens van een passagier waarbij ook de naam van een medepassagier verstrekt, werd de verstrekking niet in het dossier van de medepassagier geregistreerd. Passagiers hebben er in bepaalde gevallen recht op te weten of hun persoonsgegevens verwerkt zijn. Een kloppend dossier is daarbij van belang. Het vastleggen van de logging is ook een wettelijke plicht. De voorgenoemde omissie is gerepareerd.

De constatering uit de vorige kwartaalrapportage was 5.1.2.i Een vijftal oplossingsrichtingen voor korte termijn en/of als permanente oplossing zijn besproken en worden nader uitgewerkt in 2020 met als streven in het eerste kwartaal een tijdelijke oplossing te implementeren.

Een eerste verzoek om te komen tot een risicocriteria set is besproken. De procedure om te komen tot een risicocriteria set is aangescherpt en een gegevensbeschermingseffectrapportage (DPIA) op het profiel zal in 2020 opgesteld worden om inzicht te verkrijgen in de risico's voor de persoonsgegevens en maatregelen te kunnen vaststellen.

5.1.2i [redacted] Naast het AVG, WPG en WIV wordt de PNR als nieuw regime gezien. In het eerste kwartaal van 2020 wordt dit nader besproken om onduidelijkheid en onzekerheid die dat veroorzaakt weg te nemen.

Een FG kan geen werkzaamheden uitvoeren die tot een belangenconflict kunnen leiden. Deze voorwaarde bepaalt de werkzaamheden die de FG voor PINL kan uitvoeren.

Aantal inzage- en correctieverzoeken incl. de afhandeltijd

Zie de toelichting bij KPI 3.4.

Voortgang op de audits

De FG kan in deze rapportage nog geen voortgang, ten opzichte van de vorige rapportage 3-2019, melden.

Bemerkingen en eventuele vragen/aanbevelingen van de AP en acties die hierop zijn ondernomen.

In het vierde kwartaal zou een bestuurlijke en ambtelijke kennismaking tussen AP, PI-NL, NCTV en FG plaatsvinden. Vanwege de feestdagen en agenda technische problemen is dat verschoven naar het eerste tertaal van 2020.

KPI 3 Doel beschermen persoonlijke levenssfeer

In het Contourendocument en het Monitoringsdocument staan KPI's voor de PI-NL. Enkele van deze KPI's betreffen het beschermen van persoonsgegevens en daarmee de werkzaamheden van de FG.

KPI 3.1 aantal datalekken PNR
Norm: 0 (nul)
Aan de FG PI-NL zijn geen datalekken o.g.v. PNR of AVG gemeld.
Dit kwartaal is de norm gehaald.

Er is onderscheid tussen datalekken m.b.t. PNR-gegevens en datalekken o.g.v. de AVG. De FG onderschrijft de norm 0 (nul) voor PNR-datalekken.
Voor AVG-datalekken zal de realiteit waarschijnlijk anders zijn. De laatste kunnen voorkomen in de reguliere bedrijfsvoering waarbij bijvoorbeeld een e-mail met

personeelsgegevens aan de verkeerde persoon binnen of buiten PI-NL verzonden wordt. Afspraken over taken en verantwoordelijkheden m.b.t. AVG-datalekken waarbij systemen van Defensie centraal staan en 5.1.2e MinDef een verantwoordelijkheid draagt moeten nog gemaakt worden.

KPI 3.2 Aantal verwijderingen en correcties dat op verzoek van betrokkenen is gedaan
Norm: te bepalen door opdrachtgever, eigenaar en opdrachtnemer i.o.m. FG.

Dit kwartaal zijn er geen persoonsgegevens verwijderd noch correcties op verzoek van betrokkene gedaan.

KPI 3.3 Aantal functionarissen dat geautoriseerd is om toegang te hebben tot PNR-data
Norm: n.a.w.

De functionarissen die dit kwartaal toegang hebben tot persoonsgegevens in TRIP 5.1.2

KPI 3.4 Aantal verzoeken door burgers tot inzage opgeslagen PNR-gegevens
Norm: n.v.t.

Het aantal inzageverzoeken in dit kwartaal is 1. De afhandeltijd is gemiddeld 4 dagen.

Van de 1 verzoek(en):
- 5.1.2.e

Er zijn geen correctieverzoeken geweest.
Er zijn geen overige verzoeken geweest.

KPI 5.2 Aantal gegrond verklaarde klachten- en bezwaarprocedures tegen de Pi-NL
Norm: in samenspraak tussen besturingsdriehoek en bevoegde instanties te bepalen

Voor bezwaren o.g.v. PNR-wet geldt dat er geen beroepsprocedure is conform art. 31a WPG. De bezwaarprocedure (klachten) wordt door de AP uitgevoerd. Betrokkenen kunnen een klacht ook rechtstreeks bij de AP indienen.

Er zijn de FG geen klachten en/of bezwaren bekend.

KPI 4 Doel gegevensbescherming

KPI 4.1 Aantal databeveiligingsincidenten (niet zijnde datalek)
Norm: te bepalen door besturingsdriehoek i.o.m. FG en ADR (deze is sinds de vorige rapportage nog niet vastgesteld)

De FG PI-NL adviseert om de CISO van de PI-NL bij het vaststellen van de norm te betrekken.

"Er is alleen sprake van een datalek als zich daadwerkelijk een beveiligingsincident heeft voorgedaan. Bij een beveiligingsincident moet u bijvoorbeeld denken aan het kwijtraken van een USB -stick, de diefstal van een laptop of aan een inbraak door een hacker. Echter niet ieder beveiligingsincident is ook een datalek. Er is sprake van een datalek als er bij het beveiligingsincident persoonsgegevens verloren zijn gegaan, of als u onrechtmatige verwerking van de persoonsgegevens niet redelijkerwijs kunt uitsluiten. Als alleen sprake is van een zwakke plek in de beveiliging, spreken we van een beveiligingslek en niet van een datalek. U hoeft dan geen melding te doen aan de Autoriteit Persoonsgegevens."

De aantallen databeveiligingsincidenten worden door PI-NL gerapporteerd en datalekken maken daar onderdeel vanuit.

Overige constateringen

Een verwerkingsverantwoordelijke heeft de plicht zorg te dragen voor de juistheid en volledigheid van de persoonsgegevens (art. 4 WPG). Een zorg blijft de onvoldoende kwaliteit van de passagiersgegevens van intra-EU vluchten zoals aangeleverd door de luchtvaartmaatschappijen. In combinatie met vorderingen om PNR-persoonsgegevens waarin een beperkte hoeveelheid persoonsgegevens (achternaam met soms alleen voornaam of geboortedatum) levert dit risico's op waarbij persoonsgegevens ten onterechte verstrekt worden. 5.1.2.i [redacted] Het aanleggen van een zogenoemde 'white list/false positives´ is nog niet gestart.

De basis ten aanzien van het naleven van de wet en het beschermen van persoonsgegevens is onvoldoende ingericht waardoor de FG PINL bij het uitoefenen van het interne toezicht gehinderd wordt door praktische vraagstukken. Het gaat daarbij met name om de volgende zaken.

- -Een toetsingskader voor het beschermen van persoonsgegevens, informatiebeveiliging en het beperken van risico's. B.v. in de vorm van beleid.
- -Een verwerkingsregister waarin de verwerkingen van persoonsgegevens van zowel passagiers als medewerkers, zakelijke relaties en anderen in zijn opgenomen met de juridische grondslag, bewaartermijnen, aanleverende en ontvangende partijen.
- -Gegevensbeschermingseffectrapportages (DPIA) van de verschillende gegevensverwerkingen binnen PI-NL. Dit betreft zowel persoonsgegevens vallend onder de PNR als de AVG.
- -Processen, systemen en beleid t.a.v. het uitoefenen van rechten door betrokkenen en voor de werkzaamheden van de FG PINL en/of 5.1.2e 5.1.2e PINL. Bijvoorbeeld opslag van ID-bewijzen, vaststellen van identiteit, registratie- en volgsysteem van de verzoeken, bewaartermijn van verzoeken en bijbehorende documentatie, kwaliteit en juistheid van de persoonsgegevens in TRIP.
- -Informeren van de betrokkenen over het verwerken van hun persoonsgegevens en het uitoefenen van hun rechten.

Gezien de achterstand in het opzetten van de privacy organisatie en de afwezigheid van een 5.1.2e kunnen er conflicten ontstaan wanneer er geen duidelijke taakafbakening is tussen de taken van de FG en 5.1.2e . Zo is het

bijvoorbeeld aan de 5.1.2.e om bijvoorbeeld beleid te vormen en aan de FG om daarop toe te zien.

Een aandachtspunt in de vorige rapportage was het vervangen van de FG bij onverwachte of langere afwezigheid. De NCTV heeft met de BVA voor het vervullen van de functie besloten dat alleen bij langdurige afwezigheid een plaatsvervangende FG wordt ingezet. Dit betekent dat gedurende vakanties en kortdurende afwezigheid geen FG beschikbaar is en het interne toezicht niet of later plaatsvindt.

De twee aandachtspuntenpunten uit de vorige rapportage ten aanzien van het verwerken van PNR-data binnen de systemen van Defensie staan nog open. Een architectuurplaat van de diverse systemen waarmee PI-NL werkt en de koppelvlakken tussen de systemen is nog niet ter beschikking gesteld.
5.1.2e Defensie heeft in het bestuurlijk overleg gevraagd of haar ministerie/KMar compliant is ten aanzien van het beschermen van persoonsgegevens. Voor de onderbouwing van het antwoord raadpleegt de FG PINL haar collega's van het ministerie van Defensie.

Conclusie

De medewerkers van de PI-NL zijn zich goed bewust van hun werkzaamheden en de rol die het beschermen van de privacy van passagiers daarbij heeft. Ze zijn zich steeds beter bewust wat dat voor hun rol betekent.

Organisatorisch en bestuurlijk zijn verbeteringen gewenst. De privacy organisatie heeft een achterstand waardoor extra inzet onontbeerlijk is. Dit is tevens nodig om te voorkomen dat de FG PINL in een belangconflict geraakt of compliance uitblijft.

A4

Ministerie van Justitie en Veiligheid

DEP. VERTROUWELIJK
openbaar bij publicatie

Tertaal rapportage FG PI-NL bestuurlijk overleg

Versie 1.0

Datum	Juli 2020
Status	Definitief

Colofon

Afzendgegevens		**Beveiligingsautoriteit Ministerie van Justitie en Veiligheid Ministerie Binnenlandse Zaken en Koninkrijksrelaties** Turfmarkt 147 2511DP Den Haag Postbus 20301 2500EH Den Haag www.rijksoverheid.nl/jenv
Auteurs		FG

Inhoud

Inleiding

Voor u ligt de tertaalrapportage[1] van de Functionaris voor de Gegevensbescherming van de Passagiers-Informatie eenheid Nederland (hierna: FG) en gaat over het eerste tertaal 2020. In het bestuurlijk overleg wordt deze rapportage aan de opdrachtgever, eigenaar en opdrachtnemer[2] mondeling toegelicht door de FG.

Naast de tertaalrapportage brengt de FG jaarlijks verslag uit aan de Minister, de Tweede en Eerste Kamer der Staten-Generaal en de Autoriteit Persoonsgegevens conform artikel 18 PNR. In 2020 is de eerste rapportage over het voorgaande kalenderjaar opgesteld. Bij het finaliseren van deze tertaalrapportage was de gezamenlijke reactie op de jaarrapportage van NCTV en PI-NL nog niet ontvangen.

Algemeen

NCTV en PI-NL hebben de gelegenheid gekregen om op basis van een conceptrapportage te reageren op feitelijke onjuistheden. In een gezamenlijk overleg is de meerwaarde van de bijlage als handig, werkbaar en overzichtelijk benoemd.

Rapporteren

De FG rapporteerde in de laatste 2 rapportages over KPI's. KPI's zijn variabelen om prestaties van een organisatie te analyseren. Een FG houdt intern toezicht en adviseert. Met de commandogroep van PI-NL en de opdrachtgever is besproken om de KPI's alleen door PI-NL in de tertaalrapportage te laten opnemen aangezien zij kunnen sturen op de prestaties van PI-NL. Daarnaast is besproken om de tertaalrapportages te coördineren en vooraf met elkaar af te stemmen.
Ten aanzien van de bestaande KPI's is de FG verzocht een advies te geven. Het advies is opgenomen in de bijlage 1. De huidige KPI's bieden onvoldoende mogelijkheid voor de commandogroep om te sturen. Een KPI is bijvoorbeeld het aantal datalekken of het aantal inzageverzoeken. Echter het aantal datalekken of het aantal inzage verzoeken is moeilijk te sturen.

---

[1] De Minister van JenV is, conform artikel 17 PNR, de verwerkingsverantwoordelijke.
In het Contourendocument is vastgelegd dat de Functionaris Gegevensbescherming (hierna: FG) PI-NL 4 maal per jaar t.b.v. het bestuurlijk overleg een rapportage opstelt voor de opdrachtnemer, eigenaar en opdrachtgever/verwerkings-verantwoordelijke. In het bestuurlijke overleg van december 2019 is vastgesteld dat de FG een tertaalcyclus zal gaan aanhouden.

[2] 5.1.2e Pi-NL is volgens de verwerkersafspraak de opdrachtnemer en de PI-NL is de verwerker van de PNR-gegevens. Justid en JIVC zijn verwerkers van PNR-gegevens.
De eigenaar (Ministerie van Defensie/KMar) is verantwoordelijk voor de continuïteit van de (dienstverlening en de bedrijfsvoering van de) Pi-NL op de lange termijn en het toezicht op de algemene bedrijfsvoering. De opdrachtgever (Ministerie van Justitie en Veiligheid/NCTV) is conform het organisatiebesluit van het ministerie van JenV opdrachtgever voor de PI-NL en verantwoordelijk voor het beleid inclusief de bijbehorende wet- en regelgeving en de te maken beleidskeuzes. De opdrachtgever is aansluitend ook verantwoordelijk voor een goede opdrachtformulering aan de opdrachtnemer.

In de nieuwe opzet van de tertaalrapportage zal de FG ingaan op het wettelijk toezichtskader. Daarbij geeft de FG aan of PI-NL aan de organisatorische en technische waarborgen voor het beschermen van persoonsgegevens alsmede de wettelijke waarborgen voor de gegevensbescherming voldoet. De organisatorische en technische waarborgen worden door de opdrachtnemer, opdrachtgever en eigenaar vastgelegd. Zij zijn verantwoordelijk voor het opstellen van een normenkader aan de hand waarvan zij zelf de voortgang kunnen volgen.
De FG stelt een toetsingskader op en elk tertaal wordt per waarborg de inhoud van de waarborg en de bevindingen beschreven. Aanvullend wordt met een stoplicht de status van de compliance (waarborg aanwezig), implementatie (waarborg uitgevoerd), bevinding (voorwaarde werkend in dit tertaal) aangeduid. De nieuwe opzet (zie bijlage 2) kan bijdragen aan het versterken van de lijnverantwoordelijkheid en de verwerkingsverantwoordelijkheid door per waarborg inzichtelijk te maken welke constateringen het interne toezicht oplevert. Het stoplicht is als volgt opgebouwd:

Op hoofdlijnen voldaan	Groen
Niet geheel voldaan	Oranje
Niet voldaan	Rood
Niet vast te stellen / niet van toepassing	Grijs

De PNR-wet biedt diverse waarborgen voor de gegevensbescherming aan betrokkenen en de FG oefent daar intern toezicht op uit.
- Doelbinding (art. 2)
- Recht op eerbiediging van het privéleven, op bescherming van persoonsgegevens en op non-discriminatie (artt. 6 en 7)
- Toestemming officier van justitie (art. 10)
- Notificeren FG (art. 10 en 13)
- Functionaris voor gegevensbescherming, contactpunt betrokkenen (art. 18)
- Depersonaliseren en verwijderen van persoonsgegevens (art. 20)
- Registreren en of documenteren verwerkingen (artt. 22 en 23)

De waarborgen voor het beschermen van persoonsgegevens uit de Wet politiegegevens (hierna Wpg) zijn van overeenkomstige toepassing verklaard in de PNR-wet artikel 17 op de PNR-gegevens. Het gaat om de volgende onderdelen:
- Juistheid en volledigheid gegevens (art. 4)
- Gegevensbescherming door privacy by design en/of default (artt. 4a en 4b)
- Gegevensbeschermingseffectbeoordeling (GEB/DPIA/PIA) (art. 4c)
- Autorisaties en toegang tot gegevens (artt. 6 en 6a)
- Verstrekken aan derde landen (art. 17a)
- Rechten van betrokkenen (artt. 24a tot en met 31a)
- Audits (art. 33)
- Datalekken (art. 33a)
- Raadplegen Autoriteit Persoonsgegevens (art 33b)
- Functionaris voor de gegevensbescherming (art. 36)

Intern Toezicht

De wet biedt bevoegde instanties de mogelijkheid om rechtstreeks bij een Passenger Information Unit (hierna: PIU) van een andere lidstaat PNR-gegevens op te vragen in geval van een dringende noodzaak (art. 16 PNR). Bij het opstellen van de jaarrapportage voor het parlement (art. 18 PNR) bleek dat meerdere buitenlandse bevoegde instanties (BIU) rechtstreeks bij PINL, met tussenkomst van het LIRC een

internationaal rechtshulpverzoek deden. De FG heeft PINL gevraagd te controleren of in al deze gevallen het inroepen van art. 16 PNR gerechtvaardigd was. Het antwoord is dat deze route gebruikt wordt voor alle verzoeken en niet alleen in het geval van dringende noodzaak.
Tevens waren enkele bevoegde instanties niet juist als derde land geregistreerd. Bij het opstellen van de tertaalrapportage door PI-NL is dit ook gebleken en een correctie van de gegevens wordt in T2 uitgevoerd.

Bij het opstellen van de jaarrapportage bleek tevens dat verscheidene aan PI-NL toebedachte werkzaamheden en bijbehorende vastlegging nog niet in TRIP zijn opgenomen. Dit betreft onder andere de uitwisselingen en notificaties bij rechtstreekse verzoeken van bevoegde instanties aan een PI(U). De FG heeft daardoor nog geen inzicht in de status van het uitrollen van deze wettelijke taken.

Toezicht in TRIP levert inzicht op dat soms kleine onjuistheden voorkomen. Dit zijn slordigheden bij het invoeren of hebben te maken met de werkwijze van het oppakken van zaken. Het is voor PI-NL niet mogelijk om kleine onjuistheden uit de VVA aan te passen.
Mijn advies is om op basis van een autorisatieregeling en vastgelegd proces beleid op te stellen wie, wanneer een kleine onjuistheid uit de VVA mag verbeteren. Denk bijvoorbeeld 5.1.2.i [redacted]. Via de logging en het beleid kan PI-NL zelf controleren wat er wanneer en door wie gewijzigd is en de FG kan intern toezicht houden.

Advies ter bescherming van persoonsgegevens

Het proces voor verzoeken van betrokkenen (hierna: burgerverzoeken) wordt herzien en onderzocht wordt hoe het in TRIP geborgd kan worden. Door het in TRIP te borgen zijn passagiersgegevens daar opgeslagen waar ze verwacht worden. De FG is contactpunt voor betrokkenen en de PI-NL zal de burgerverzoeken (eventueel namens de verwerkingsverantwoordelijke) behandelen. Justid IBO, PI-NL en NCTV werken het verder uit. De verwachting is een oplevering in T2. Naast het inregelen in TRIP moet PI-NL voor het proces voor verzoeken nog werkinstructies en/of beleid opstellen.
Een aandachtpunt in het proces is het vaststellen van de identiteit van de bezoeker en de afstemming over het verzoek met BI's.

Mijn advies is om daarbij waar mogelijk onderscheid te maken tussen inzage in alleen de persoonsgegevens en ten tweede in de verstrekkingen. De verzoeker weet dat de persoonsgegevens bij PI-NL aanwezig moeten zijn. Dus die niet verstrekken kan de idee geven dat er een verstrekking heeft plaatsgevonden. Echter vraagt een verzoeker inzage in de verstrekkingen dan is afstemming met de betreffende bevoegde instantie noodzakelijk (art. 27 Wpg). Alleen in dit laatste geval is overleg met de betreffende bevoegde instantie nodig en daarmee het delen van de persoonsgegevens van de verzoeker. Ik raad af om alle inzage verzoeken met alle bevoegde instanties te delen om ze de mogelijkheid te geven art. 27 Wpg in te roepen. Hiermee wordt het uitoefenen van het recht door de verzoeker ten onrechte beperkt en worden de persoonsgegevens ten onrechte verwerkt door bevoegde instanties.

Nog niet alle verwerkingsmogelijkheden en bijbehorende activiteiten zijn in TRIP ingericht. Onder andere een rechtstreeks verzoek van een bevoegde instantie uit het buitenland, het notificeren daarvan aan de PIU en de spiegelbepaling waarbij een

notificatie van een PIU ontvangen wordt als een Nederlandse bevoegde instantie een verzoek bij een PIU neerlegt en het ontvangen van de passagiersgegevens die die bevoegde instantie van de PIU heeft ontvangen; of het vastleggen van de toestemming van een PIU om hun gegevens die in bezit zijn gekomen van PI-NL te mogen verstrekken aan een derde land.
Vooruitlopend op de verzoeken adviseer ik NCTV en PI-NL om dit in TRIP in te gaan regelen.

Het vastleggen van de logging is een wettelijke plicht. Nog niet alle verwerkingen van passagiersgegevens worden gelogd. Dit wordt gerepareerd in T2.

Een eerste verzoek om te komen tot een risicocriteria set is besproken. De procedure om te komen tot een risicocriteria set is aangescherpt. De FG adviseert om te zorgen dat er voldoende inzicht komt in de risico's voor de verwerking van persoonsgegevens en passende risico beperkende maatregelen vast te stellen.
De uitvoering van de risicocriteria set stelde PI-NL voor de keuze om onderscheid te maken naar 5.1.2.I [redacted] Het doorgeven van alle matches aan de bevoegde instantie zou betekenen dat persoonsgegevens van personen, waarvan bij voorbaat bekend is dat die niet nader onderzocht zullen worden, toch verstrekt zouden worden. 5.1.2.I [redacted]
Voor de toekomst adviseer ik NCTV en PI-NL om beleid vast te stellen hoe met dit soort verzoeken van bevoegde instanties kan worden omgegaan.

Een FG kan geen werkzaamheden uitvoeren die tot een belangenconflict kunnen leiden bij het uitvoeren van het toezicht. Bijvoorbeeld door middel van advies bijdragen aan beleid en daarna toezichthouden op de uitvoering van dat beleid. Ten behoeve van het directeurenoverleg was een advies opgesteld naar aanleiding van vragen over de rol van de FG. De FG en de opdrachtgever van PI-NL zijn op basis van dat document in overleg om de taken af te bakenen.

De FG heeft op verzoek van de NCTV vragen gesteld aan de Autoriteit Persoonsgegevens (AP). Een was voor een enquête van de EU om de implementatie van de PNR-richtlijn. De andere was een verzoek om 5.1.2.I in de Europese Data Protection Board te agenderen zodat het mogelijk een applicatie zou kunnen worden die in de hele EU gebruikt kan worden. De laatste vraag betreft een onderwerp dat feitelijk 5.1.2e MinJenV betreft en waarbij ik voor de PNR-inhoud contactpunt voor de AP ben.

In het Benelux overleg heeft de FG een presentatie geven over het interne toezicht in Nederland.

KPI's

Aantal inzage- en correctieverzoeken incl. de afhandeltijd
Zie de toelichting bij KPI 3.4.

Voortgang op de audits
De FG kan in deze rapportage nog geen voortgang, ten opzichte van de vorige rapportage Q4-2019, melden.

Wel heb ik bij de opdrachtgever van PI-NL de privacy audit uit de Wpg onder de aandacht gebracht, daar die ontbrak in het overzicht van audits en evaluaties.

Bemerkingen en eventuele vragen/aanbevelingen van de AP en acties die hierop zijn ondernomen.
In T1 zou een bestuurlijke en ambtelijke kennismaking tussen AP, PI-NL, NCTV en FG plaatsvinden. Vanwege de verplichting tot het beperken van sociale contacten en de oproep om zo veel mogelijk thuis te werken in verband met de Sars-Covid-19 wordt de kennismaking verschoven naar een nader te bepalen datum.

KPI 3 Doel beschermen persoonlijke levenssfeer
In het Contourendocument en het Monitoringsdocument staan KPI's voor de PI-NL. Enkele van deze KPI's betreffen het beschermen van persoonsgegevens en daarmee de werkzaamheden van de FG.

KPI 3.1 aantal datalekken PNR
Norm: 0 (nul)
Aan de FG PI-NL zijn geen datalekken o.g.v. PNR of AVG gemeld.
Dit kwartaal is de norm gehaald.

Er is onderscheid tussen datalekken m.b.t. PNR-gegevens en datalekken o.g.v. de AVG. De FG onderschrijft de norm 0 (nul) voor PNR-datalekken.
Voor AVG-datalekken zal de realiteit waarschijnlijk anders zijn. De laatste kunnen voorkomen in de reguliere bedrijfsvoering waarbij bijvoorbeeld een e-mail met personeelsgegevens aan de verkeerde persoon binnen of buiten PI-NL verzonden wordt. Afspraken over taken en verantwoordelijkheden m.b.t. AVG-datalekken waarbij systemen van Defensie centraal staan en 5.1.2e MinDef een verantwoordelijkheid draagt moeten nog gemaakt worden.

Er is 1 incident geweest, waarbij het ging om een datalek van een carrier. 5.1.2.i

KPI 3.2 Aantal verwijderingen en correcties dat op verzoek van betrokkenen is gedaan
Norm: te bepalen door opdrachtgever, eigenaar en opdrachtnemer i.o.m. FG.

Dit kwartaal zijn er geen persoonsgegevens verwijderd noch correcties op verzoek van betrokkene gedaan.

KPI 3.4 Aantal verzoeken door burgers tot inzage opgeslagen PNR-gegevens
Norm: n.v.t.

Het aantal inzageverzoeken in dit tertaal is 3. De afhandeltijd is gemiddeld 68 dagen.

Van de 3 verzoek(en):
- 5.1.2.e

Er zijn geen (0) correctieverzoeken geweest.
Er zijn geen (0) overige verzoeken geweest.

KPI 5.2 Aantal gegrond verklaarde klachten- en bezwaarprocedures tegen de Pi-NL
Norm: in samenspraak tussen besturingsdriehoek en bevoegde instanties te bepalen

Voor bezwaren o.g.v. PNR-wet geldt dat er geen beroepsprocedure is conform art. 31a WPG. De bezwaarprocedure (klachten) wordt door de AP uitgevoerd. Betrokkenen kunnen een klacht ook rechtstreeks bij de AP indienen.

Er zijn de FG geen klachten en/of bezwaren bekend die bij de AP zijn ingediend.

Overige constateringen

Opnemen van het strafbare feit in de vordering wordt niet altijd gedaan. Dit bemoeilijkt de controle op doelbinding door PINL en bij het in- en externe toezicht. 5.1.2.i

Door controle en besluitvorming met betrekking tot doorgifte uit de wet bij andere partijen neer te leggen wordt de invloed van PINL beperkt m.b.t. het beschermen van persoonsgegevens op kunnen uitoefenen en het toezicht door de FG verplaatst naar andere organisaties. Persoonsgegevens komen daardoor eerder in het WPG domein waar de uiteindelijke beslissing over doorgifte wordt genomen. Dit geldt ook voor persoonsgegevens die uiteindelijk niet het gezocht subject betreffen.

Uit de vorige rapportage:
Een verwerkingsverantwoordelijke heeft de plicht zorg te dragen voor de juistheid en volledigheid van de persoonsgegevens (art. 4 WPG). Een zorg blijft de onvoldoende kwaliteit van de passagiersgegevens van intra-EU vluchten zoals aangeleverd door de luchtvaartmaatschappijen. In combinatie met vorderingen om PNR-persoonsgegevens waarin een beperkte hoeveelheid persoonsgegevens (achternaam met soms alleen voornaam of geboortedatum) levert dit risico's op waarbij persoonsgegevens ten onterechte verstrekt worden. 5.1.2.i

Over het aanleggen van een zogenoemde 'white list/false positives' wordt inmiddels gesproken.

De basis ten aanzien van het naleven van de wet en het beschermen van persoonsgegevens is onvoldoende ingericht waardoor de FG PINL bij het uitoefenen van het interne toezicht gehinderd wordt door praktische vraagstukken. Het gaat daarbij met name om de volgende zaken.

- Een toetsingskader voor het beschermen van persoonsgegevens, informatiebeveiliging en het beperken van risico's. B.v. in de vorm van beleid.
- Een verwerkingsregister waarin de verwerkingen van persoonsgegevens van zowel passagiers als medewerkers, zakelijke relaties en anderen in zijn opgenomen met de juridische grondslag, bewaartermijnen, aanleverende en ontvangende partijen.
- Gegevensbeschermingseffectrapportages (DPIA) van de verschillende gegevensverwerkingen binnen PI-NL. Dit betreft zowel persoonsgegevens vallend onder de PNR als de AVG.
- Processen, systemen en beleid t.a.v. het uitoefenen van rechten door betrokkenen en voor de werkzaamheden van de FG PINL en/of 5.1.2e 5.1.2e PINL. Bijvoorbeeld opslag van ID-bewijzen, vaststellen van identiteit, registratie- en volgsysteem van de verzoeken, bewaartermijn van verzoeken en bijbehorende documentatie, kwaliteit en juistheid van de persoonsgegevens in TRIP.
- Informeren van de betrokkenen over het verwerken van hun persoonsgegevens en het uitoefenen van hun rechten.

Ten aanzien van het verwerken van PNR-data binnen de systemen van Defensie staan de volgende punten nog open. Een architectuurplaat van de diverse systemen waarmee PI-NL werkt en de koppelvlakken tussen de systemen is nog niet ter beschikking gesteld.
De constatering uit de vorige rapportages was 5.1.2.i ". Een oplossing zou in T1 2020 geïmplementeerd worden. Dit heeft nog niet plaatsgevonden.
5.1.2.i . In T1 zou een nota hierover worden voorgelegd ter bespreking.

5.1.2e Defensie heeft in het bestuurlijk overleg gevraagd of haar ministerie/KMar compliant is ten aanzien van het beschermen van persoonsgegevens. Voor de onderbouwing van het antwoord raadpleegt de FG PINL haar medewerkers van het ministerie van Defensie. Aangezien de informatie departementaal vertrouwelijk is wordt een oplossing gezocht zodat de FG kennis kan nemen van de risico's ten behoeve van het toezicht. Aanvullend daarop schrijven de ADR en ARK in 2019 over 2018 het volgende over de informatiebeveiliging van het Ministerie van Defensie in de openbare rapportages:

a. Rapport Rekenkamer 2018

In 2018 zijn er grote stappen gezet om de informatiebeveiliging te verbeteren; er dient echter nog een stap te worden gezet om de accreditaties van kritieke systemen af te ronden. De aanbeveling over de accreditering (een machtiging en goedkeuring om een systeem te mogen gebruiken) van de kritieke systemen is nog niet afgerond. Het Ministerie van Defensie verwacht dit in 2019 te kunnen afronden. Daarom handhaven wij de onvolkomenheid op informatiebeveiliging.

b. Rapport ADR 2018:

Op basis van rijksbreed onderzoek in 2018 tenslotte naar de informatiebeveiliging en de algemene verordening gegevensbescherming (AVG) komt naar voren dat Defensie goede voortgang maakt met het afhandelen van aanbevelingen (informatie - beveiliging) en met de implementatie AVG. Specifiek voor de AVG is nog aandacht nodig voor het opstellen of actualiseren van data protection impact

assessments en het inventariseren en actualiseren van verwerkersovereenkomsten.

-Informatiebeveiliging

De afgelopen jaren heeft de ADR rijksbrede onderzoeken uitgevoerd naar de beheersing van informatie - beveiliging. De volwassenheid van het ministerie op het gebied van informatiebeveiliging geeft de volgende bevindingen:
Uit ons vervolgonderzoek in 2018 blijkt dat Defensie vooruitgang heeft geboekt met het afhandelen van de aanbevelingen. 5.1.2e *is gestart met de eerste KPI's die nodig zijn om het IT-kwaliteitssysteem beter te laten functioneren en zij stelt samen met JIVC een verbeterregister op om het IT-landschap, de continuïteit en beveiligingsrisico's beter te kunnen managen.*
Verder is de vernieuwde accreditatieprocedure goedgekeurd. Het risicomanagement voor Informatiebeveiliging steunt sterk op deze procedure.
5.1.2.i [redacted]

- Goede voortgang Algemene verordening gegevensbescherming

Op basis van ons rijksbrede onderzoek geeft dit voor het ministerie van Defensie het beeld dat Defensie in 2018 goede voortgang heeft gerealiseerd bij de implementatie van de AVG. Belangrijke aspecten hierbij zijn de Regeling AVG Defensie met de taken en verantwoordelijkheden van de functionaris voor gegevensbescherming en de decentrale eenheden, een procedure voor het melden van datalekken, het proces voor het indienen voor verzoeken rechten betrokkenen en aandacht voor bewustwordingsacties. Er is een register van verwerkingen aanwezig en de decentrale onder - delen zijn bezig dit te vullen.
Aandachtspunten zijn het, waar nodig, opstellen of actualiseren van Data protection impact assessment (DPIA's) en het inventariseren en actualiseren van verwerkersovereenkomsten. Wij zien wel bij de decentrale uitvoering een verschuiving ten opzichte van de oorspronkelijke planning. De decentrale plannen zijn na vaststelling niet meer aangepast en er is geen gewijzigde planning opgesteld. Defensie verwacht in haar voortgangsrapportage een volledige implementatie van de AVG eind 2019. Om dit te bereiken is naar onze mening een strakkere sturing door 5.1.2e *op de decentrale uitvoering nodig.*

Reactie Ministerie van Defensie:
Algemene verordening gegevensbescherming (AVG)
Aandachtspunten bij de implementatie van de AVG zijn het, waar nodig, opstellen of actualiseren van Data Protection Impact Assessments (DPIA's) en het inventariseren en actualiseren van verwerkersovereenkomsten.
Defensie verwacht in haar voortgangsrapportage een volledige implementatie van de AVG eind 2019. Om dit te bereiken is naar de mening van de ADR een strakkere sturing door 5.1.2e *op de decentrale uitvoering (de defensieonderdelen) nodig. Evenzo is volgens Defensie vanuit de staven van de defensieonderdelen een strakkere sturing nodig op de implementatie. Professionalisering van de AVG-functie bij de decentrale eenheden kan daaraan bijdragen.*

Conclusie

De medewerkers van de PI-NL zijn zich goed bewust van hun werkzaamheden en de rol die het beschermen van de privacy van passagiers daarbij heeft. Ze zijn zich steeds beter bewust wat dat voor hun rol betekent. De start van een juridisch en een informatiebeveiligingsadviseur dragen bij aan het versterken en het verankeren van het beschermen van persoonsgegevens in de organisatie.

Organisatorisch en bestuurlijk blijven verbeteringen gewenst. De privacy organisatie heeft een achterstand waardoor extra inzet onontbeerlijk is om de basis op orde te krijgen en de lijnverantwoordelijkheid in te richten en te verstevigen.

Bijlage 1

Advies voor het instellen van KPI's voor PI-NL ten aanzien van het beschermen van persoonsgegevens.

Het beschermen van persoonsgegevens is een lijnverantwoordelijkheid. De FG houdt toezicht op het naleven van de wet- en regelgeving en het beleid door PI-NL. Daarnaast kan de FG advies geven aan de verwerkingsverantwoordelijke of het lijnmanagement.
De NCTV heeft op 12 maart 2020 advies gevraagd over andere KPI's die beter aansluiten bij het monitoren van het beschermen van persoonsgegevens dan de huidige KPI's. Voor een verwerkingsverantwoordelijke is het sturen op aantallen incidenten, burgerverzoeken m.b.t. inzage, correctie en of verwijderen van gegevens, aantal afgegeven autorisaties en klachten bij de AP lastig tot niet te beïnvloeden. De verwerkingsverantwoordelijke dan wel de verwerker van PNR-gegevens kan meer invloed uitoefenen op het naleven van de verplichtingen uit de wet die de persoonsgegevens beschermen.

De volgende KPI's worden geadviseerd om PI-NL over te laten rapporteren:
- Overall beeld: in-control
- Compliance: voldoet volledig aan de PNR en AVG
- Governance: FG benoemd
- Rechtmatigheid verwerking
- Documentatieplicht
- Verantwoordingsplicht
- Informatieplicht
- Privay by design/default

De FG kan op basis van de rapportage van PI-NL toezicht houden of het geschetste beeld in overeenstemming is met de bevindingen van de FG.

Toelichting op de KPI's
PNR en AVG algemeen beeld: in-control
PI-NL is in-control ten aanzien van de implementatie van de PNR en AVG. PI-NL is in control als het verantwoordelijk management van PI-NL inzicht heeft in de huidige stand van zaken over de implementatie van de PNR en AVG en de risico's met betrekking tot verzamelingen van persoonsgegevens, beschikt over een plan om de PNR en AVG te implementeren, de benodigde resources beschikbaar zijn en dat de voortgang periodiek wordt gemonitord. Tevens moet een FG benoemd zijn. Indien eraan wordt gewerkt om in control te komen, dan scoort PI-NL oranje. Als geen plan voorhanden is en er wordt niet aan gewerkt om op korte termijn alsnog een plan op te leveren, dan scoort PI-NL rood.

PNR en AVG-compliance: voldoet volledig aan de PNR en AVG
PI-NL heeft de PNR en AVG verplichtingen geïmplementeerd in de organisatie. Niet compliant en geen plan leidt tot rood, niet compliant maar wel een plan leidt tot een oranje score.

PNR en AVG-compliance: FG benoemd
De Functionaris Gegevensbescherming is wettelijk verplicht; deze geeft advies binnen de organisatie en moet toezien op de juiste uitvoering van de PNR en AVG binnen PI-NL. De functie en de taken van deze functie zijn specifiek beschreven in de verordening. De KPI ziet toe op het feit of de FG is benoemd dan wel is aangewezen

in een ander organisatieonderdeel om taken uit te voeren. PI-NL scoort groen als een FG benoemd is. PI-NL scoort rood als geen FG is benoemd. De score oranje wordt niet gebruikt bij deze KPI.

Rechtmatigheid verwerking en controle op de doelbinding
Er is sprake van rechtmatigheid van verwerking van alle persoonsgegevens. Hiermee wordt bedoeld dat een grondslag aanwezig is voor de rechtmatige verwerking van alle verzamelingen van persoonsgegevens (PNR en AVG). Indien nog niet duidelijk is of één en ander rechtmatig wordt verwerkt maar wel een plan aanwezig is om dit geregeld te krijgen, wordt oranje gescoord. Geen plan met daarin een duidelijke einddatum leidt tot een rode score.

PNR en AVG-documentatieplicht
Hierbij wordt gekeken naar de volgende punten: De aanwezigheid van een gevuld verwerkingsregister en indien deze er niet is een plan met einddatum; Het actueel zijn van verwerkersafspraken, indien niet actueel wanneer de verwachte einddatum is om deze actueel te hebben; Het hebben van een DPIA proces waarbij de DPIA's met de FG worden afgestemd. Indien één van deze punten niet voorhanden is, maar wel een plan met einddatum wordt de score oranje.

PNR en AVG-verantwoordingsplicht
Hierbij wordt gekeken naar de volgende twee punten: Een adequaat proces voor het melden van datalekken en aanwezig zijn van een register voor de registratie van datalekken; Het hebben van passende beveiligingsmaatregelen voor de beveiliging van persoonsgegevens. Indien één van de punten (register datalekken of passende beveiligingsmaatregelen) niet op orde is maar wel een plan met einddatum wordt oranje gescoord, geen plan met einddatum leidt tot rood. Alleen als beide punten op orde zijn wordt groen toegekend. Ook voor deze KPI geldt dat voor de beoordeling beide punten op orde moeten zijn om groen te scoren.

PNR en AVG-informatieplicht
Hierbij wordt gekeken naar de aanwezigheid een of meerdere processen voor de rechten van de betrokkenen (inzage, rectificatie en bezwaar proces) en de aanwezigheid van duidelijke en transparante informatie hoe betrokkenen hun rechten kunnen uitoefenen. Het ontbreken van één van de processen en geen plan met einddatum leidt tot rood, niet aanwezig wel een plan met einddatum leidt tot oranje.

Privacy by design/default TRIP
Hierbij wordt gekeken naar de volgende punten: het depersonaliseren en verwijderen van zowel bijzondere persoonsgegevens als persoonsgegevens na 5 jaar. De aanwezigheid van de toestemming van de OvJ en de notificatie aan de FG, bij zowel het opheffen van de depersonalisering als het verstrekken aan derde landen, en het depersonaliseren van de verstrekking en de persoonsgegevens in TRIP. Het ontbreken van één van de punten en geen plan met einddatum leidt tot rood, niet aanwezig wel een plan met einddatum leidt tot oranje.

Bijlage 2

Zie PDF bijlage – 2020 T1 Waarborgen voor de gegevensbescherming

A4a

Waarborgen voor het beschermen van persoonsgegevens	Bevindingen functionaris gegevensbescherming	Compliance (voorlopige aanwezig)	Implementatie (voorlopig uitgevoerd)	Bevinding (voorlopig verband in de tekst)	Management reactie verwerkingsverantwoordelijke
Doelbinding (art. 2 PNR)	Doelbinding is niet altijd te controleren omdat het strafbare feit niet altijd gespecificeerd wordt. Controle op de doelbinding is een verantwoordelijkheid van de bij de vordering op te stellen betrokken partijen. In TRIP is het alleen mogelijk voor vooraf bepaalde artikelen uit het wetboek van strafvordering gegevens te vorderen Medewerkers PI-NL en de FG kunnen navraag doen bij de bevoegde instantie naar het strafbare feit bij controle op de doelbinding	✓	!	●	
Recht op eerbiedging van het privéleven, op bescherming van persoonsgegevens en op non-discriminatie (artt. 6 en 7 PNR)	Het verwerken van bijzondere persoonsgegevens is verboden. De meeste gegevens (SSR codes) die naar bijzondere persoonsgegevens kunnen leiden worden geautomatiseerd gefilterd en verwijderd Intern toezicht heroph heeft dit tertaal niet plaatsgevonden	✓	✓	●	
Toestemming officier van justitie (art. 10 PNR)	De toestemming van de OvJ voor het opheffen van de depersonalisering na 6 maanden is door het OM opgenomen in het nieuwe template van de vordering. Nog niet alle teams werken met dit duidelijke template. De zinsnede "betreft ook gegevens ouder dan zes maanden" is geen duidelijke toestemming voor het opheffen van de depersonalisering. Het wordt in de praktijk beschouwd als toestemming	✓	!	!	
Notificeren FG (art. 10 en 13 PNR)	De FG wordt genotificeerd [redacted] wanneer een verstrekking van ongepersonaliseerde gegevens en of aan derde landen wordt gedaan Dit tertaal is de notificateservice [redacted] onderbroken geweest. Dit is hersteld	✓	✓	!	
Functionaris voor gegevensbescherming (art. 18 PNR jo. 36 Wpg) Er is een onafhankelijke interne toezichthoudende FG benoemd	De FG is benoemd Er bjkt onduidelijkheid over de wettelijke taken en positie van de FG. Dit kan leiden tot belangenconflict voor de FG. De FG heeft een overzicht van deze wettelijke taken aan de opdrachtgever van PI-NL gestuurd. Door dit te bespreken kan voorkomen worden dat er een belangenconflict ontstaat als van de FG beleidshandelingen en advies in een prematuur stadium verwacht worden en later toezicht op houdt	✓	✓	✓	
Functionaris voor gegevensbescherming (art. 18 PNR jo. 36 Wpg) De FG is contactpunt voor betrokkenen	Betrokkenen weten de FG te vinden Dit tertaal verliep in 1 casus het eerste contact via dessk van het Ministerie van Defensie. Zij hebben het doorgezet naar de FG PI-NL De FG heeft advies en duidelijker te communiceren over PI-NL en de PNR-wet alsmede betere vindbaarheid van de contactgegevens van de FG	✓	!	!	
Functionaris voor gegevensbescherming (art. 18 PNR jo. 36 Wpg) De FG heeft toegang tot alle gegevens die door de PI-NL worden verwerkt t.b.v. het toezicht	De FG heeft toegang in TRIP tot de persoonsgegevens. Er is geen gebruikershandleiding voor de FG PI-NL geeft aan alleen in TRIP persoonsgegevens op te slaan Dit tertaal heeft er geen intern toezicht plaatsgevonden op andere systemen en of locaties	✓	✓	●	
Functionaris voor gegevensbescherming (art. 18 PNR jo. 36 Wpg) De FG wordt door de verwerkingsverantwoordelijke tijdig en naar behoren betrokken bij alle aangelegenheden die verband houden met de bescherming van persoonsgegevens	Het bjkt nog niet altijd duidelijk wanneer het aangelegenheden betreft die verband houden met de het verwerken van persoonsgegevens en de FG betrokken dient te worden	✓	!	●	
Functionaris voor gegevensbescherming (art. 18 PNR jo. 36 Wpg) De FG ziet toe op het beleid voor het beschermen van persoonsgegevens van de verwerkingsverantwoordelijke	Controle van de aanwezigheid van beleid voor het beschermen van persoonsgegevens Er is geen beleid aanwezig. De FG heeft geen inzage in de werkafspraken naar aanleiding van de bevindingen van de FG zoals eventueel opgenomen in dagjournaals of andere documentatie	✗	✗	✗	
Functionaris voor gegevensbescherming (art. 18 PNR jo. 36 Wpg) De FG ziet toe op de autorisaties en het bijbehorende beleid	De FG heeft toezicht uitgeoefend op de autorisaties en aanpassingen verzocht. De aanpassingen zijn doorgevoerd Het beleid voor het uitgeven van autorisaties is de FG niet bekend	✓	!	!	
Functionaris voor gegevensbescherming (art. 18 PNR jo. 36 Wpg) De FG ziet toe op de bewustmaking en opleiding van medewerkers die betrokken zijn bij de verwerking van persoonsgegevens	De FG ervaart dat door het interne toezicht de bewustwording bij medewerkers van PI-NL toeneemt. De FG had een presentatie voorbereid voor de commandantengroep over het beschermen van persoonsgegevens. Vanwege thuswerken door Sars-covid-19 is deze verschoven. Daarnaast is de FG toegezegd de introductietraining voor nieuwe medewerkers te kunnen beoordelen. Intern topzicht heroph heeft dit tertaal niet plaatsgevonden	●	●	●	
Functionaris voor gegevensbescherming (art. 18 jPNR jo. 36 Wpg) De FG houdt toezicht op de audit (art. 33 Wpg)	De FG heeft de opdrachtgever van PI-NL geinformeerd over het ontbreken van deze audit in de audit planning	●	●	●	
Depersonaliseren en verwijderen van persoonsgegevens (art. 20 PNR) Depersonaliseren van gegevens ouder dan 6 maanden	Na 6 maanden worden persoonsgegevens gedepersonaliseerd in TRIP Persoonsgegevens komen voor in notities. Deze tekstvelden worden nog niet gedepersonaliseerd. Het is bij het aanbieden van deze rapportage nog onbekend of deze persoonsgegevens gedepersonaliseerd (kunnen) worden. Justid IBO en de keyusers PI-NL zoeken uit in hoeverre depersonalisering plaatsvindt en stellen indien noodzakelijk een RfC/VTW op	✓	!	!	
Depersonaliseren en verwijderen van persoonsgegevens (art. 20 PNR) Verwijderen van persoonsgegevens ouder dan 5 jaar	Na 5 jaar worden persoonsgegevens (vorderingen/verzoeken, matches, verstrekkingen, metadata, loggínggegevens, burgerverzoeken) verwijderd De intern toezichthouder heeft vragen gesteld over het beleid ten aanzien van het bewaren van verstrekkingen PIU-PIU, burgerverzoeken en daarmee samenhangende verstrekkingen de tegen het einde van de termijn lopen als ook loggínggegevens van medewerkers waartegen een (mogelijk) strafproces kan gaan lopen/loopt Datamvmalisatie: verwijderen van persoonsgegevens die niet noodzakelijk zijn voor de verwerking Bij ontvangst van de passagiersgegevens worden persoonsgegevens die niet ter zake doen of bijzondere gegevens bevatten verwijderd De verstrekking (het verwerkingsresultaat) wordt in de VVA na 14 dagen verwijderd en in TRIP na 42 dagen. De verstrekking van passagiersgegevens van PI-NL kan gereconstrueerd worden Uit het toezicht blijkt dat de verstrekkingen in TRIP verwijderd zijn. De FG heeft geen toegang tot de VVA die in het WPG domein valt Ontvangen verwerkingsresultaten van PIU's zijn er nog niet. De FG adviseert een bewaartermijn van 4 jaar conform de Wpg omdat een betrokkene recht heeft om te weten of er een verstrekking in de afgelopen 4 jaar heeft plaatsgevonden. PI-NL is verantwoordelijk voor het geven van inzage en kan niet garanderen dat een PIU na 4 jaar hetzelfde verwerkingsresultaat opnieuw aanlevert tenzij daar intra-EU tussen PIU's afspraken over zijn gemaakt	✓	!	!	
Registreren en of documenteren verwerkingen (artt. 22 en 23 PNR) De verwerkingsverantwoordelijke houdt een register bij	Het register bevat de namen en contactgegevens van de verwerkingsverantwoordelijke, de organisatie en de ambtenaren van de Passagiersinformatie-eenheid die belast zijn met de verwerking van passagiersgegevens, en van de functionaris gegevensbescherming, de namen en contactgegevens van de bevoegde instanties, de Passagiersinformatie-eenheden en de bevoegde instanties van andere lidstaten (en derde landen), en de autorisaties die zijn toegekend De FG is niet bekend met het register Intern toezicht heroph heeft dit tertaal niet plaatsgevonden	●	●	●	
Registreren en of documenteren verwerkingen (artt. 22 en 23 PNR) De verwerkingsverantwoordelijke legt de logging van verwerkingen in TRIP vast	Het betreft de verzoeken om passagiersgegevens of de verwerking ervan van bevoegde instanties, de verzoeken om passagiersgegevens van Europol en van PIU's en bevoegde instanties van andere lidstaten, en de verzoeken om passagiersgegevens van derde landen en de doorgiften aan die landen De logging van verwerkingen wordt vastgelegd in TRIP. Er zijn bij het verzamelen van de statistieken onjustheden gevonden waarbij derde landen verkeerd waren geregistreerd. In T2 2020 wordt dit met terugwerkende kracht aangepast	✓	✓	!	
Registreren en of documenteren verwerkingen (artt. 22 en 23 PNR) De verwerkingsverantwoordelijke legt de logging van verwerkingen in TRIP vast	Het betreft vastlegging van ten minste de volgende verwerkingen: het verzamelen, raadplegen verstrekking onder meer in de vorm van doorgiften en wissen van de passagiersgegevens en de resultaten van de verwerking van de gegevens. De vastlegging bevat 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 De logging van verwerkingen wordt op hoofdverwerkingen vastgelegd in TRIP De interne toezichthouder heeft geadviseerd de logging uit te breiden naar alle verwerkingen in TRIP	✓	!	✓	
artikel 17 PNR jo. WPG					
Justheid en volledigheid gegevens (art. 4 Wpg) De verwerkingsverantwoordelijke treft de nodige maatregelen opdat politiegegevens, gelet op de doeleinden waarvoor zij worden verwerkt, juist en nauwkeurig zijn Indien wordt vastgesteld dat onjuiste politiegegevens zijn verstrekt, of dat de politiegegevens op onrechtmatige wijze zijn verstrekt, wordt de ontvanger daarvan onverwijld in kennis gesteld. In dat geval dienen de gegevens te worden gerectificeerd of vernietigd, of wordt de verwerking beperkt	Bekend is dat sommige passagiers verkeerde gegevens verstrekken bij het boeken. Intra Schengen vindt er geen paspoortcontrole plaats. Hierdoor ontbreken deze gegevens. De beschikbare gegevens zijn van een dermate kwaliteit dat de vraag gesteld moet worden of deze wel gebruikt kunnen worden als basis voor een verstrekking. Het sec vergelijken op een voorletter, achternaam en geboortejaar maakt dat van meerdere passagiers persoonsgegevens sneller gedeeld worden dan wenselijk is. De beperkte subject informatie in de vordering draagt daarmee onvoldoende bij aan een voldoende bescherming van passagiers De FG begrijpt dat bij inkomende vluchten de API-data (gegevens uit het reisdocument) wel worden aangeleverd door de luchtvaartmaatschappij maar bij uitgaande vluchten niet. Dit heeft consequenties voor het naleven van dit artikel. En art. 4 PNR dat de luchtvaartmaatschappij verplicht alle voor de bedrijfsvoering beschikbare gegevens aan PI-NL te verstrekken Intern toezicht heroph heeft dit tertaal niet plaatsgevonden	●	●	●	
Gegevensbescherming door privacy by design en/of default (artt. 4a en 4b Wpg) Gegevensbescherming door beveiliging en ontwerp De verwerkingsverantwoordelijke en de verwerker treffen passende technische en organisatorische maatregelen	De technische ontwerp maatregelen zijn op hoofdlijnen ongewijzigd gebleven en via privacy by design worden verwerking en het beschermen van persoonsgegevens conform PNR-wet afgedwongen. Door RfC's zijn wijzigingen in het ontwerp aangebracht. De FG is betrokken bij wijzigingen die de persoonsgegevens raken Bij het gebruik van persoonsgegevens voor analyses zijn eventueel vastgestelde waarborgen de FG onbekend Periodieke evaluatie en eventueel actualiseren van de technische en organisatorische maatregelen heeft de interne toezichthouder nog niet kunnen vaststellen Toezicht op de organisatorische maatregelen heeft in het kader van de beperkingen door sars-covid-19 dit tertaal niet plaatsgevonden	✓	!	●	
Gegevensbescherming door privacy by design en/of default (artt. 4a en 4b Wpg) Gegevensbescherming door standaardinstellingen De verwerkingsverantwoordelijke en de verwerker treffen passende technische en organisatorische maatregelen	De standaardinstellingen in TRIP waarborgen dat alleen de gegevens verwerkt worden die voor het doel van de verwerking noodzakelijk zijn. De persoonsgegevens worden niet zonder tussenkomst van een natuurlijk persoon voor een onbepaalt aantal natuurlijke personen toegankelijk gemaakt. De technische en organisatorische maatregelen betreffen o.a. de periode van opslag, mate van verwerking en de toegankelijkheid van de persoonsgegevens. De bewaartermijn is wettelijk geregeld voor 5 jaar TRIP opent in een aparte werkomgeving die losstaat van de regulere werkomgeving 5.1.2 i [redacted] De FG heeft regelmatig verzocht om een geautomatiseerde oplossing 5.1.2 j [redacted] De documenten die hierop geplaatst worden, worden aan het einde van de dienst automatisch verwijderd Er heeft dit tertaal geen toezicht plaatsgevonden op het legen van de persoonlijke download map	✓	!	●	
Gegevensbeschermingseffectbeoordeling (DPIA) (art 4c Wpg)	De DPIA voor PI-NL ten behoeve van de wetsimplementatie is herzien en nog niet vastgesteld Er is een beperkte DPIA opgesteld voor B&V. De data science DPIA voor de risico criteria set Kmar en de beperkte DPIA voor Analisye zijn opgevraagd door de FG	✓	!	●	
Autorisaties en toegang tot gegevens (artt. 8 en 8a Wpg)	Een systeem van autorisaties wordt bijgehouden door Justid voor toegang tot TRIP PI-NL controleert elk tertaal de autorisaties. Het beleid heromtrent of het toetsingskader van PI-NL is de FG ongebekend De FG controleert de autorisaties en er zijn enkele wijzigingen doorgevoerd dit tertaal	✓	!	!	
Verstrekken aan derde landen (art. 17a Wpg) jo Besluit gebruik van passagiersgegevens voor de bestrijding van terroristische en ernstige misdrijven	Verstrekkingen aan derde landen vinden o.b.v. een AMvB plaats via DLO/LIRC DLIO toetst binnenkomende internationale rechtshulpverzoeken voor ze doorgezet worden naar PI-NL. DLIO toetst de verstrekking (ontvangen van PI-NL) voor ze doorgezet worden naar derde landen PI-NL heeft een eigen verantwoordelijkheid bij het beoordelen van het verzoek. Het is de FG nog niet duidelijk hoe dit is ingeregeld De FG controleert verstrekkingen aan derde landen. Bij een verstrekking aan een derde land ontvangt de FG een automtisch gegenereerde notificatie via 5.1.2 i [redacted] notificatie heeft er tijdelijk uitgelegen dit tertaal. De verstrekkingen in dit tertaal zijn 100% geoontroleerd door de FG	✓	✓	!	

Waarborgen voor het beschermen van persoonsgegevens	Bevindingen functionaris gegevensbescherming	Compliance (voorwaarde aanwezig)	Implementatie (voorwaarde uitgevoerd)	Bevinding (voorwaarde werkend in de tijd)	Management reactie verwerkingsverantwoordelijke
Rechten van betrokkenen (artt. 24a tot en met 31a Wpg) Informatie aan betrokkene De verwerkingsverantwoordelijke verstrekt aan de betrokkene informatie over de verwerking van politiegegevens in een beknopte en toegankelijke vorm en in duidelijke en eenvoudige taal. De informatie wordt met passende middelen, waaronder elektronische, kosteloos verstrekt en in het algemeen in dezelfde vorm als de vorm van het verzoek	Informatie op een toegankelijke, duidelijke en in eenvoudig opgestelde taal ontbreekt. Er is zeer beperkt informatie te vinden op overheidswebsites. De FG adviseert een PINL/PNR website in te richten naar analogie van de FIU	✓	!	✗	
Rechten van betrokkenen (artt. 24a tot en met 31a Wpg) Verstrekking van informatie aan betrokkene	De verstrekking van informatie over verwerkingsdoelen, identiteit en contactgegevens verwerkingsverantwoordelijke, rechten van betrokkene, grondslagen, bewaartermijnen, eventuele geautomatiseede besluitvorming is nog niet ingeregeld. De FG adviseert dit op te nemen op een website en een standaard teksten voor diverse communicatiemiddelen	✓	✗	✗	
Rechten van betrokkenen (artt. 24a tot en met 31a Wpg) Recht op inzage	Het proces voor het uitoefenen van het recht op inzage is in T1 2020 besproken en wordt in T2 via privacy by design ingeregeld in TRIP. PINL krijgt waarschijnlijk het mandaat om namens de verwerkingsverantwoordelijke de verzoeken af te handelen waarbij de FG contactpunt voor de betrokkene blijft. Betrokkenen kunnen altijd inzage in hun persoonsgegevens krijgen. Inzage in de verstrekking van de gegevens moet nadrukkelijk worden aangevraagd en kan o.g.v. art 27 Wpg beperkt of geweigerd worden. Voorlopig is er een work-around via de FG en de verwerkingsverantwoordelijke. Er zijn 2 verzoeken om inzage via de workaround afgehandeld.	✓	!	!	
Rechten van betrokkenen (artt. 24a tot en met 31a Wpg) Formaliteiten	De deugdelijke vaststelling van de identiteit van verzoeker vindt plaats aan de hand van een kopie ID. Het documentnummer wordt vastgelegd en het ID wordt voorlopig bewaard tot het afloöen van de klacht- en beroepstermijn. Het beleid hiervoor ontbreekt nog. Er zijn zorgen bij PINL over mogelijk misbruik van ID-bewijzen. In T2 wordt dat verder uitgewerkt door opdrachtgever en opdrachtnemer i.o.m. bevoegde instanties.	✓	!	!	
Rechten van betrokkenen (artt. 24a tot en met 31a Wpg) Uitzonderingen	Inzage en of correctie/verwijdingsverzoeken worden afgewezen als dat een noodzakelijke en evenredige maatregel is. Er is geen beleid vastgesteld wanneer een afwijzing als noodzakelijke en evenredige maatregel gezien wordt. Het is onduidelijk hoe bij het terugplaatsen van een backup van TRIP deze wijzigingen behouden blijven. Dit tertaal is dit niet voorgekomen.	✗			
Rechten van betrokkenen (artt. 24a tot en met 31a Wpg) Recht op rectificatie en vernietiging	In TRIP is het voor de FG mogelijk een beperkt aantal velden te rectificeren of persoonsgegevens te verwijderen. Als een verwijdering ongewenst is kan ene beperking op de verwerking van bepaalde persoonsgegevens geplaatst worden. Het is mijns inziens onwaarschijnlijk dat op dit moment een beperking van de verwerking in TRIP kan worden gerealiseerd. Er is nog geen beleid vastgesteld wanneer een verzoek ingewilligd wordt en hoe dat vastgelegd wordt in TRIP (ook bij het neerzetten van een backup moeten die gegevens aangepast blijven). Dit tertaal is dat niet voorgekomen.	✓			
Rechten van betrokkenen (artt. 24a tot en met 31a Wpg) Toepasselijkheid Awb	Een beslissing op verzoek van betrokkene geldt als een besluit. Er zijn 2 besluiten op verzoek genomen.	✓	✓	✓	
Rechten van betrokkenen (artt. 24a tot en met 31a Wpg) Klacht bij de AP	Betrokkenen kunnen een klacht tegen de verwerking van hun persoonsgegevens bij de AP indienen. De AP neemt binnen 3 maanden een beslissing (besluit). De AP kan betrokkene bijstand verlenen. Dit tertaal heeft de AP geen contact met de FG opgenomen om navraag te doen over een ontvangen klacht.	✓			
Audits (art. 33 Wpg) Privacy/IT audit elke 4 jaar (art 6.5 lid 1 Bpg) interne audit jaarlijks (art 6.5 lid 5 Bpg) De verwerkingsverantwoordelijke controleert de waarborgen voor de gegevensbescherming uit de toepasselijke wetgeving via een privacy audit. En stuurt een afschrift aan de AP. Binnen een jaar vindt hercontrole plaats op de onderdelen die in de audit onvoldoende waren.	De privacy audit heeft tot doel op systematische wijze te toetsen of aan de bepalingen van de op adequate wijze uitvoering is gegeven. Hiertoe vindt een beoordeling plaats van de volgende aspecten binnen de organisatie van de auditee: de opzet en het bestaan van maatregelen en procedures die in de borging van de wettelijke eisen moeten voorzien: de werking van de getroffen maatregelen en procedures. De audit is niet opgenomen in het audit en evaluatie plan van de opdrachtgever van PI-NL.				
Audits (art. 33 Wpg) Privacy audit elke 4 jaar (art 6.5 lid 1 Bpg) interne audit jaarlijks (art 6.5 lid 5 Bpg) De verwerkingsverantwoordelijke controleert de waarborgen voor de gegevensbescherming uit de toepasselijke wetgeving via een privacy audit. En stuurt een afschrift aan de AP. Binnen een jaar vindt hercontrole plaats op de onderdelen die in de audit onvoldoende waren.	De interne audit heeft betrekking op één dan wel een aantal onderdelen van de wet en heeft tot doel voor het onderdeel of de onderdelen van de wet waar de interne audit zich op richt, op systematische wijze te toetsen of aan de bepalingen van de op adequate wijze uitvoering is gegeven. Hiertoe vindt een beoordeling plaats van de volgende aspecten binnen de organisatie van de auditee: de opzet en het bestaan van maatregelen en procedures die in de borging van de wettelijke eisen moeten voorzien: de werking van de getroffen maatregelen en procedures. De audit is niet opgenomen in het audit en evaluatie plan van de opdrachtgever van PI-NL.				
Datalekken (art. 33a Wpg) De verwerkingsverantwoordelijke meldt een datalek binnen 72 uur na kennisname ervan aan de AP tenzij het niet waarschijnlijk is dat de inbreuk een risico voor de rechten en vrijheden van betrokkenen inhoudt.	De procedure datalek bij de opdrachtgever van PINL is aangepast zodat piket op de hoogte is. Zij beoordelen incidenten en handelen namens de verwerkingsverantwoordelijke datalekken af en informeren de FG. De aansluting met het proces bij PINL en het proces bij PINL is nog niet vastgesteld.	✓	✗	✗	
Raadplegen Autoriteit Persoonsgegevens (art 33b Wpg) Voorafgaande raadpleging voorgenomen verwerking De verwerkingsverantwoordelijke of verwerker raadpleegt de AP over voorgenomen verwerkingen waarbij de aard van de verwerking een hoog risico voor de rechten en vrijheden van betrokkenen met zich mee brengen derik aan gebruik maken van nieuwe technologieën, mechanismes, procedures en of grootschalige verwerking van persoonsgegevens plaatsvindt en of wanneer een DPIA uitwijst dat de risico's onvoldoende of niet beperkt kunnen worden.	Een proces voor de voorgenomen raadpleging ontbreekt. Dit tertaal heeft er voorzover de FG bekend is geen voorgenomen raadpleging van de AP plaatsgevonden.				
AVG volgt in T2					

A5

Ministerie van Justitie en Veiligheid

DEP. VERTROUWELIJK
openbaar na publicatie

Tertaal rapportage FG PI-NL - T2 2020

t.b.v. Bestuurlijk overleg

Versie 1.0

Datum	November 2020
Status	Definitief

Colofon

Afzendgegevens **Functionaris voor de gegevensbescherming voor de Passagiersinformatie-eenheid Nederland**

Turfmarkt 147
2511DP Den Haag
Postbus 20301
2500EH Den Haag
www.rijksoverheid.nl/jenv
5.1.2i @MinJenV.nl

Auteurs FG

Inhoud

1 Inleiding

Voor u ligt de toelichting op de tertaalrapportage[1] van de Functionaris voor de Gegevensbescherming (hierna: FG) van de Passagiers-Informatie eenheid Nederland (hierna: Pi-NL) en gaat over het tweede tertaal 2020. In het bestuurlijk overleg wordt deze rapportage met de opdrachtgever, eigenaar en opdrachtnemer[2] besproken en/of toegelicht door de FG.
De tertaalrapportage geeft de bevindingen van de FG weer die in mei tot en met augustus zijn gedaan.
De verantwoording over de wijze van handelen en/of een planning naar aanleiding van een bevinding ligt in de lijn bij de opdrachtnemer, de eigenaar en de opdrachtgever. De opdrachtgever Pi-NL en opdrachtnemer op basis van een conceptrapportage gereageerd om feitelijke onjuistheden naar voren te brengen en om verduidelijkende vragen te stellen.

Naast de tertaalrapportage brengt de FG jaarlijks verslag uit aan de Minister, de Tweede en Eerste Kamer der Staten-Generaal en de Autoriteit Persoonsgegevens conform artikel 18 PNR. In 2020 is de eerste rapportage over het voorgaande kalenderjaar opgesteld. Bij het finaliseren van deze tertaalrapportage lag de Artikel 18 PNR Jaarrapportage 2019 nog ter goedkeuring bij onze Minister.

2 Intern Toezicht

2.1 Kwaliteit

Een wettelijke verplichting is om de juistheid van de gegevens te bewaken. Het punt kwaliteit was opnieuw een aandachtspunt dit tertaal nadat in de T1 2020 rapportage aandacht was gevraagd voor de kwaliteit van de gegevens in TRIP. In de afwijkingen in de ingevoerde datavelden in TRIP constateerde ik onvoldoende verbetering. Mijn ervaring leert dat deze onvolkomenheden ontstaan bij het invoeren van de gegevens uit de vordering door de BI en bij controle voorafgaand aan verdere verwerking onopgemerkt blijven door Pi-NL. Bv. tik- en spelfouten, het verkeerd overnemen van gegevens uit de vordering, verkeerd invoeren van instanties. Daarnaast kan een systeemfout in TRIP de oorzaak zijn. Bv. een tijdsperiode die verkeerd wordt

---

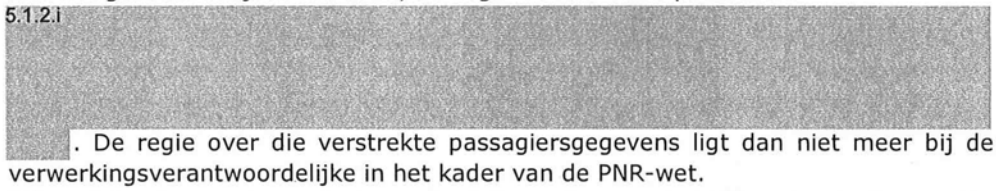
[1] De Minister van JenV is, conform artikel 17 PNR, de verwerkingsverantwoordelijke.
In het Contourendocument is vastgelegd dat de Functionaris Gegevensbescherming (hierna: FG) PI-NL 4 maal per jaar t.b.v. het bestuurlijk overleg een rapportage opstelt voor de opdrachtnemer, eigenaar en opdrachtgever/verwerkings-verantwoordelijke. In het bestuurlijke overleg van december 2019 is vastgesteld dat de FG een tertaalcyclus zal gaan aanhouden.

[2] 5.1.2e Pi-NL is volgens de verwerkersafspraak de opdrachtnemer en de PI-NL is de verwerker van de PNR-gegevens. Justid en JIVC zijn verwerkers van PNR-gegevens.
De eigenaar (Ministerie van Defensie/KMar) is verantwoordelijk voor de continuïteit van de (dienstverlening en de bedrijfsvoering van de) Pi-NL op de lange termijn en het toezicht op de algemene bedrijfsvoering. De opdrachtgever (Ministerie van Justitie en Veiligheid/NCTV) is conform het organisatiebesluit van het ministerie van JenV opdrachtgever voor de PI-NL en verantwoordelijk voor het beleid inclusief de bijbehorende wet- en regelgeving en de te maken beleidskeuzes. De opdrachtgever is aansluitend ook verantwoordelijk voor een goede opdrachtformulering aan de opdrachtnemer.

uitgevoerd. De afwijkingen met de vordering kunnen bijvoorbeeld een onrechtmatige verstrekking en/of onjuiste managementinformatie tot gevolg hebben.
Dit tertaal kwamen een paar onrechtmatige verstrekkingen voor. Deze zijn of als bug afgehandeld en/of Pi-NL heeft melding gedaan bij de 5.1.2e van de opdrachtgever Pi-NL. Pi-NL heeft naar aanleiding van mijn dringend advies dit tertaal extra aandacht gegeven aan het verbeteren en borgen van de kwaliteit van de gegevens in de datavelden.
Mijn advies is om de incidenten die leiden tot onrechtmatige verstrekkingen te registeren, de oorzaak te onderzoeken en vast te leggen met een gemotiveerd besluit voor de gekozen aanpak. Daarnaast adviseer ik om een plan van aanpak vast te leggen eventueel in overleg met Justid-Ibo welke handelingen uitgevoerd mogen en/of moeten worden als een document onrechtmatig verstrekt is.

De API-data lijken niet altijd aangeleverd te worden wanneer een carrier ze bij een uitgaande vlucht aan de autoriteit in het land van aankomst moet verstrekken. Of bij inkomende vluchten. De API-data zijn persoonsgegevens - uit het identiteitsbewijs - die de kwaliteit van de persoonsgegevens in TRIP kan verbeteren en daarmee de kwaliteit van de verstrekking aan de BI's.

2.2 Verstrekking DLIO

De controle en besluitvorming met betrekking tot doorgifte op grond van internationale verzoeken is via lagere regelgeving bij andere partijen belegd. Hierdoor wordt de invloed van PINL beperkt m.b.t. het beschermen van persoonsgegevens en verplaatst het interne toezicht zich naar andere organisaties. De persoonsgegevens komen daardoor eerder in het Wpg-domein omdat daar de uiteindelijke beslissing over doorgifte wordt genomen. Dit geldt ook voor persoonsgegevens die uiteindelijk niet het gezocht subject betreffen, de zogenoemde valse positieven.
5.1.2.i

. De regie over die verstrekte passagiersgegevens ligt dan niet meer bij de verwerkingsverantwoordelijke in het kader van de PNR-wet.
Mijn advies is om de controle en besluitvorming op doorgifte op grond van een internationaal verzoek binnen het nationale domein af te handelen en bij voorkeur in een nationale applicatie zoals TRIP en de VVA.

2.3 Menselijke toets

De objectieve menselijke toets is in de wet en in de procesbeschrijving van beoordelen en verstrekken vastgelegd. In de praktijk verwerkt de behandelende medewerker de match/de vordering/het verzoek. Voor dat een besluit tot het verstrekken van persoonsgegevens genomen wordt, kijkt een tweede medewerker op hetzelfde scherm mee. Dit is een 4-ogen-principe.
Bij mijn controle van de menselijke toets blijkt dat noch het uitvoeren van de menselijke toets noch het 4-ogen-principe in TRIP worden gedocumenteerd[3]. De consequentie is dat de verwerkingen uitgevoerd door deze twee medewerkers noch achteraf te reconstrueren zijn noch is het mogelijk toezicht te houden voor de diverse toezichthouders.
Mijn advies is om, in het kader van de verantwoordingsplicht, de menselijke toets alsmede het 4-ogen-principe dusdanig te documenteren zodat toezicht hierop mogelijk wordt.

---

[3] Documenteren is het vastleggen van de handelingen in TRIP door middel van het loggen van de gegevens van de gebruiker en de handeling.

2.4 Autorisaties

Op basis van de documenten die ik van Pi-NL heb ontvangen, blijkt dat de autorisaties in TRIP niet per rol zijn ingeregeld, noch dat duidelijk is welke medewerker bij welke passagiersgegevens kan. Een voorbeeld is het niet per rol inregelen van de autorisaties zo heeft de FG in TRIP niet alleen leesrechten, maar ook schrijfrechten. De FG zou onder andere vorderingen kunnen afhandelen en verstrekkingen uitvoeren. Of gebruikers die niet met persoonsgegevens werken, kunnen via rapportages wel die gegevens verwerken.
Mijn advies was om een inventarisatie op basis van dataminimalisatie en need-to-know te maken ten behoeve van de herinrichting van de autorisaties. Dit advies is opgepakt.

2.5 Verwerkingen

In de T1 rapportage was gerapporteerd, dat nog niet alle wettelijke verwerkingsmogelijkheden en bijbehorende activiteiten in waren TRIP ingericht. Voor T2 geldt dat nog. Onder andere een rechtstreeks verzoek van een bevoegde instantie uit het buitenland, het notificeren daarvan aan de PIU en de spiegelbepaling waarbij een notificatie van een PIU ontvangen wordt als een Nederlandse bevoegde instantie een verzoek bij een PIU neerlegt en het ontvangen van de passagiersgegevens die die bevoegde instantie van de PIU heeft ontvangen; of het vastleggen van de toestemming van een PIU om hun gegevens die in bezit zijn gekomen van PI-NL al dan niet te mogen verstrekken aan een derde land.
Vooruitlopend op binnenkomende verzoeken adviseer ik een planning op te stellen om de uitwerking ter hand te nemen.

2.6 Risico criteria set

In de T1 rapportage is het eerste verzoek om te komen tot een risicocriteria set (hierna: RCS) besproken. Tevens is geadviseerd om beleid vast te stellen hoe met verzoeken van bevoegde instanties kan worden omgegaan als het bijzondere gegevens kan betreffen door gecombineerde gegevens te combineren.
Naar aanleiding van de evaluatie door Pi-NL heb ik mijn bevindingen over het gebruik van de RCS aan de opdrachtgever en opdrachtnemer aangeboden. De twee belangrijkste conclusies en/of vragen zijn:

- Zijn er Wpg-gegevens uitgewisseld?
- Heeft de commissie voldoende tijd gehad om de evaluatie tot zich te kunnen nemen? Is de samenstelling van de commissie voldoende objectief?

De beantwoording en/of bespreking van alle conclusies en/of vragen heeft nog niet plaats gevonden.

2.7 Bewust zijn

Het afgelopen tertaal heb ik een aantal presentaties gegeven aan het MT+ van Pi-NL om de kaders van het beschermen van persoonsgegevens te verduidelijken. Thema's waren een inleiding, de gegevensbeschermingseffectrapportage/data protection impact assessment en de verantwoordingsplicht.
Het bewustzijn en de kennis over het beschermen van persoonsgegevens neemt toe.

2.8 Basis op orde

In de vorige rapportage is aandacht gevraagd voor het orde brengen van de basis. De basis ten aanzien van het naleven van de wet en het beschermen van persoonsgegevens is nog onvoldoende ingericht. Er is enige voortgang geboekt en het aanstellen van een privacyfunctionaris biedt perspectief. Het gaat in de basis om de volgende zaken:

- Een normenkader voor het beschermen van persoonsgegevens, informatiebeveiliging en het beperken van risico's. B.v. in de vorm van vastgesteld beleid en/of het vastgestelde niveau van de risicobereidheid.

Zodat duidelijk is welk niveau de verwerkingsverantwoordelijke een voldoende mate van het beschermen van de persoonsgegevens vindt.

- Een verwerkingsregister waarin alle verwerkingen van persoonsgegevens van zowel passagiers als medewerkers, zakelijke relaties en anderen in zijn opgenomen met de juridische grondslag, bewaartermijnen, aanleverende en ontvangende partijen. Dit is niet hetzelfde als het register uit art. 22 PNR. Ik adviseer dit omdat het register overzicht geeft over bv. waar welke passagiersgegevens staan en in welke applicatie ze verwerkt worden, wat de bewaartermijn en grondslag voor verwerking is. Bij incidenten, voor DPIA's, bij aanpassingen aan processen en/of systemen is er een overzicht waarop teruggevallen kan worden.
- Gegevensbeschermingseffectrapportages (DPIA) van de verschillende gegevensverwerkingen binnen PI-NL. Een wettelijke DPIA bij het invoeren van de wet geeft op een zeer hoog abstractieniveau weer of betrokkenen risico's lopen ten aanzien van hun rechten en vrijheden. Op uitvoerend niveau kan in een DPIA per proces op details ingegaan worden. KMar, NP en OM geven aan dit ook zo ingericht te hebben. Bijvoorbeeld het vastleggen van besluiten over het uitvoeren van een DPIA bij het aanpassen van processen en/of grote veranderingen in applicaties.
- Processen, systemen en beleid aanvullen en opstellen. Bijvoorbeeld besluiten over de opslaglocaties en bewaartermijnen, overzichten van werkafspraken die de gegevensbescherming raken en opgeslagen zijn in verslagen en journaals.
- Informeren van de betrokkenen over het verwerken van hun persoonsgegevens in begrijpelijke taal en het efficiënt kunnen uitoefenen van hun rechten.

3 Conclusie

De medewerkers van de PI-NL zijn zich goed bewust van hun werkzaamheden en de rol die het beschermen van de privacy van passagiers daarbij heeft. Ze zijn zich steeds beter bewust wat dat voor hun rol en werkzaamheden betekend.
De adviseurs voor juridische zaken, privacy en informatiebeveiliging dragen goed bij aan het versterken en het verankeren van het beschermen van persoonsgegevens in de organisatie alsmede het oppakken van het eerste en tweede lijn advies en het uitvoeren van werkzaamheden met betrekking tot bescherming van persoonsgegevens. De privacy organisatie komt daardoor tot stand en er wordt gewerkt aan het op orde krijgen van basis.

Bijlage 1 2020 T2 Waarborgen voor de gegevensbescherming

Zie voor bijlage 1 bijgevoegde Pdf-bijlage.

Toelichting op bijlage 1

In de tertaalrapportage ga ik in op de wettelijk waarborgen. Daarbij geef ik aan of PI-NL aan de organisatorische en technische waarborgen voor het beschermen van persoonsgegevens alsmede de wettelijke waarborgen voor de gegevensbescherming voldoet. De organisatorische en technische waarborgen worden door de opdrachtnemer, opdrachtgever en eigenaar vastgelegd. Zij zijn verantwoordelijk voor het opstellen van een normenkader aan de hand waarvan zij zelf de voortgang kunnen volgen.

De tertaalrapportage is gebaseerd op het toetsingskader van de FG. Elk tertaal wordt per waarborg de inhoud van de waarborg en de bevindingen beschreven. Aanvullend wordt met een stoplicht de status van de compliance (waarborg aanwezig), implementatie (waarborg uitgevoerd), bevinding (voorwaarde werkend in dit tertaal) aangeduid. De opzet (zie bijlage 1) kan bijdragen aan het versterken van de lijnverantwoordelijkheid en de verwerkingsverantwoordelijkheid door per waarborg inzichtelijk te maken welke constateringen het interne toezicht oplevert. Het stoplicht is als volgt opgebouwd:

Op hoofdlijnen voldaan	Groen
Niet geheel voldaan	Oranje
Niet voldaan	Rood
Niet vast te stellen / niet van toepassing	Grijs

De PNR-wet biedt diverse waarborgen voor de gegevensbescherming aan betrokkenen en de FG oefent daar intern toezicht op uit.

- Doelbinding (art. 2)
- Recht op eerbiediging van het privéleven, op bescherming van persoonsgegevens en op non-discriminatie (artt. 6 en 7)
- Toestemming officier van justitie (art. 10)
- Notificeren FG (art. 10 en 13)
- De waarborgen voor het beschermen van persoonsgegevens uit de Wet politiegegevens (hierna Wpg) zijn van overeenkomstige toepassing verklaard in de PNR-wet artikel 17 op de PNR-gegevens. Het gaat om de volgende onderdelen:
  - Juistheid en volledigheid gegevens (art. 4)
  - Gegevensbescherming door privacy by design en/of default (artt. 4a, 4b)
  - Gegevensbeschermingseffectbeoordeling (GEB/DPIA/PIA) (art. 4c)
  - Autorisaties en toegang tot gegevens (artt. 6 en 6a)
  - Verstrekken aan derde landen (art. 17a)
  - Rechten van betrokkenen (artt. 24a tot en met 31a)
  - Audits (art. 33)
  - Datalekken (art. 33a)
  - Raadplegen Autoriteit Persoonsgegevens (art 33b)
  - Functionaris voor de gegevensbescherming (art. 36)
- Functionaris voor gegevensbescherming, contactpunt betrokkenen (art. 18)
- Depersonaliseren en verwijderen van persoonsgegevens (art. 20)
- Registreren en of documenteren verwerkingen (artt. 22 en 23)

A5a

Titel en verwijzing wetartikel	Nr.	Bevindingen functionaris gegevensbescherming - oordeel = mening geeft ook algemeen advies - niet hoe ze het moeten doen wel evt in gesprek om advies te geven TERTAAL 2 - 2020	Compliance (voorwaarde aanwezig)	Bestaan (voorwaarde uitgevoerd)	Werking (voorwaarde werkend in dit tertaal)	Management reactie verwerkingsverantwoordelijke TERTAAL 2 - 2020
Doelbinding en doorwerking (artt. 2 jo. 9 lid 2 en 12 lid 2 PNR; 4 en 7 WPG) Ernstige misdrijven en terrorisme o.g.v. bijlage 2	1.1	Afwezigheid van een specifiek artikel naar een van de misdrijven uit bijlage 2 bij de wet heeft geleid tot verwarring in de communicatie over de rechtmatigheid van een verstrekking naar het buitenland. Uiteindelijk bleek de verstrekking rechtmatig conform doelbinding. Het opnemen van het artikel had dit kunnen voorkomen. Op een verstrekking staat de doelbinding verwoord, er wordt niet naar het betreffende wetsartikel verwezen. De doorwerking van de doelbinding is niet opgenomen op de verstrekking, noch de noodzaak om toestemming te vragen bij doorverstrekking als het om een verstrekking aan een derde land gaat of een eventuele bewaartermijn die gesteld kan worden. De Engelstalige tekst lijkt van de richtlijn afwijkende juridische bewoording te hebben: *"The qualified instances are only allowed to process the received data - as long as this is part of their priviliges and competences - for the benefit of prevention, tracking doxin, investigation or prosecution of terronst acts or serious criminal acts"*. Heeft PINL geen rol in het beoordelen van de proportionaliteit en/of subsidiariteit bij tussenkomst van DLIO zoals n.a.v. de T1 rapportage wordt gesteld?	✓	✓	✓	
Doorgifte passagiersgegevens (art. 5 PNR)	2.1	Doorgifte aan de bevoegde instanties is geborgd. Er is niet geconstateerd dat via TRIP aan onbevoegden is verstrekt. Er is een aantal keer onrechtmatig verstrekt aan een bevoegde instantie. Dit heeft PINL gemeld aan de [redacted] NCTV. Deze constateerde dat het geen datalekken waren.	✓	✓	✓	
Verwerking passagiersgegevens (art. 6 PNR) jo. AMVB Besluit gebruik PNR-gegevens voor de bestrijding van terroristische en ernstige misdrijven jo. artt. 4.3 en 4.6 Bpg	3.1	Verwerkingen van B&V zijn conform de wet, daarbij is nog geen spontane verstrekking geconstateerd. Een aandachtspunt dat ik ter tafel van de opdrachtgever en -nemer heb gebracht is de kwaliteit van de invoer (het overnemen) van de vordering in TRIP door de BI en de controle daarop door PI-NL.	✓	✓	✓	
Beoordelingscriteria (artt. 6 jo. 7, 8 en 20 PNR)	4.1	Een eerste RCS heeft in T1-2020 gelopen. De bevindingen daarvan zijn begin augustus aan de opdrachtgever- en opdrachtnemer van PI-NL toegezonden. Enkele vragen zijn: * zijn er WPG gegevens uitgewisseld? Er wordt verwezen naar informatie die uit verklaringen aan de grens lijken te komen. * Is de juiste taakverdeling bij het analyseren van de resulaten tussen de PI en PI-NL gevolgd? * het ontbreken van een rechtvaardiging bij het gebruik van een filter in het daarvoor bestemde tekstveld. * Is de samenstelling van de commissie onafhankelijk genoeg om de objectiviteit van de RCS mede te laten bepalen. Verstrekkingen aan de BI zijn o.g.v. de RCS rechtmatig gedaan. Misschien zou de documentatie rondom de vaststelling en evaluatie van de RCS in TRIP vastgelegd kunnen worden, zodat het op 1 plaats terug te vinden is.	!	!	!	
Beoordelingscriteria (artt. 6 jo. 7 en 19 PNR)	4.2	De RCS is uitgevoerd [redacted] 5.1.2 j Bijzondere gegevens mogen niet verwerkt worden ook niet als via gecombineerde en/of indirecte passagiersgegevens bijzondere persoonsgegevens kunnen worden afgeleid. Mijn advies is om voor de toekomst een besluit te nemen hoe omgegaan wordt met verzoeken waarbij het verbod op het verwerken van bijzondere gegevens, al dan niet door combinatie van gegevens, in het gedrang kan komen, dan wel bias kan ontstaan in de resultaten door profilering.	✓	✓	!	
Menselijke toets bij geautomatiseerd vergelijken (artt. 6 jo. 8 PNR en 4a en 4b WPg; 4.3 en 4.6 Bpg jo 13 lid 1 subs a en d en 18 Wpg)	5.1	Het is niet mogelijk om na te gaan of de menselijke toets heeft plaatsgevonden. Mijn advies is om de menselijke toets vast te leggen (loggen) en daarbij rekening te houden met controle door PI-NL zelf en de diverse toezichthouders?	✓	!	!	
Menselijke toets bij geautomatiseerd vergelijken (artt. 6 jo. 8 PNR en 4.3 en 4.6 Bpg jo 13 lid 1 subs a en d en 18 Wpg)	5.2	Mijn advies is om een overzicht van de kennis en vaardigheden die - de voor TRIP geautoriseerde - medewerkers moeten hebben om hun werk naar behoren uit te kunnen voeren op te stellen en te monitoren of die kennis en vaardigheden aanwezig zijn.	✓	!		
Menselijke toets bij geautomatiseerd vergelijken (art. 6 jo. 1 PNR en Besluit aanwijzing van de SIS II-databank)	5.3	De doelbinding wordt via [redacted] 5.1.2 j gecontroleerd. Hierbij worden naar verluid geen persoonsgegevens verstrekt. Het is mij nog onduidelijk waar de [redacted] 5.1.2 j worden opgeslagen, want het bewijsmateriaal wordt niet in TRIP opgenomen. Intern toezicht heeft hierop dit tertaal niet plaatsgevonden.				
Verstrekking resultaat PIU aan BI (artt. 9a jo 8 PNR)	6.1	Rechtstreeks opvragen passagiersgegevens bij een PIU ihkv een onmiddellijke dreiging door een BI is wettelijk geregeld. Mijn advies is om dit in TRIP in te regelen zodat: - de notificatie van de PIU ontvangen en bewaard kan worden alsmede - de door de BI ontvangen verstrekking van de PIU in TRIP bewaard kan worden en - als het een niet via NL reizende passagier betreft ook t.b.v. burgerverzoeken teruggevonden kan worden.				
Verstrekking passagiersgegevens aan PIU (artt. 10 PNR jo. AMvB)	7.1	Mijn advies is om in TRIP in te regelen dat een spontane verstrekking in TRIP verwerkt en gelogd kan worden.				
Verstrekking passagiersgegevens aan PIU (artt. 10 lid 1, 2 en 4 en art. 8 lid 2 PNR jo. AMVB Besluit gebruik PNR-gegevens voor de bestrijding van terroristische en ernstige misdrijven)	7.2	PIU-PIU uitwisseling is sinds het in gebruik nemen [redacted] 5.1.2 j mogelijk. Verzoek en verstrekking worden door DLIO van een advies voorzien of tot verstrekking aan de PIU overgegaan kan worden. De communicatie hierover vindt plaats in [redacted] 5.1.2 j ook alle toebehoren zijn geplaatst. De verstrekking wordt in TRIP geteld als het in [redacted] 5.1.2 j geplaatst t.b.v. DLIO. Als tot verstrekking aan PIU besloten is dan wordt die verstrekking niet meer in TRIP geteld noch vastgelegd t.b.v. het passagiersdossier. Het advies van DLIO in [redacted] 5.1.2 j is niet toegankelijk voor de toezichthouders. Als besloten wordt om niet te verstrekken staan de passagiersgegevens in [redacted] 5.1.2 j in het WPG-domein. Welke afspraken zijn er met Europol t.a.v. het wissen van deze documenten? Mijn advies is om **alle** afhandelingen met DLIO via TRIP/VVA te laten verlopen zodat de passagiersgegevens pas in [redacted] 5.1.2 j komen als ze daadwerkelijk versterkt worden aan de PIU. Deze voorgestelde werkwijze zorgt ook voor het vastleggen van de dubbele verstrekking in TRIP en hopelijk in het passagiersdossier. Het wordt voor de toezichtshouders daarmee ook mogelijk om toezicht te houden op de verstrekkingen n.a.v. het advies van DLIO. Hoe wordt de zinsnede, dat PI-NL passagiersgegevens alleen per geval door geeft aan een bevoegde instantie, geïnterpreteerd? Dit om het toezicht daarop af te stemmen.	✓	!	✗	

Verstrekking passagiersgegevens aan PIU (artt. 10 PNR jo. AMvB)	7.3	Alle verstrekkingen van passagiersgegevens >6mnd worden gedaan met toestemming van de nationale OvJ van de PIU LS. Mijn advies is om vast te leggen wat het beleid is wanneer DLIO op zich laat wachten en de verstrekking die PI-NL heeft klaargezet ogv <6maanden daardoor over de 6 maanden grens heen gaat, terwijl er geen toestemming is voor het opheffen van de maskering? De notificaties t.b.v. controle achteraf worden vanuit TRIP verzonden op het moment dat de verstrekking in **5.1.2.i** is geplaatst en wacht op advies van DLIO. Is dit het moment waarop de FG de controle zou moeten uitoefenen of pas als besloten is daadwerkelijk aan de PIU te verstrekken? Of in beide gevallen? Na de eerste week PIU-PIU uitwisseling heb ik mijn bevindingen aan de opdrachtgever en opdrachtnemer gestuurd. Bij het uitwisselen van passagiersgegevens tussen PIU's heeft de passagier heeft er recht op te weten aan wie PI'NL zijn gegevens de afgelopen 4 jaar heeft verstrekt. De passagier wiens gegevens door Pi-NL uit een LS zijn ontvangen staat zelf niet in TRIP. De resultaten van de LS staan onder verstrekkingen opgeslagen en dat betekent dat dat document na 42 dagen voor PINL niet meer terug te vinden is. Op dit moment is deze passagier ook in het burgerloket niet te vinden t.b.v. burgerverzoeken. Noch lijkt het er op dat een geüploade verstrekking momenteel aan een passagiersdossier kan worden toegevoegd indien de passagier wel bij PINL bekend is	✓	!	✗	
Verstrekking passagiersgegevens aan PIU (artt. 10 PNR jo. AMvB) Noodzakelijk rechtstreeks verzoek van BIU	7.4	Ik heb vernomen dat dit onderdeel niet wordt geïmplementeerd in TRIP en bij PI-NL en door alle PIU's de BIU's worden verwezen naar hun eigen PIU. Klopt dat? Rechtstreeks opvragen passagiersgegevens bij PINL ihkv een onmiddellijke dreiging door een BIU is wettelijk geregeld. Mijn advies is om dit in TRIP in te regelen zodat: - de notificatie van de PIU ontvangen en bewaard kan worden alsmede - de door de BI ontvangen verstrekking van de PIU in TRIP bewaard kan worden en - als het een niet via NL reizende passagier betreft ook t.b.v. burgerverzoeken teruggevonden kan worden				
Toestemming officier van justitie (art. 10 PNR)	8.1	Is tijdens de controles in T2 aanwezig. Een aandachtspunt is het secuur overnemen van de toestemming op de vordering in TRIP. I.t.t. hetgeen de opdrachtnemer aangeeft wordt de vastgestelde clausule niet in elke vordering gebruikt. *"Bepaalt dat deze vordering betrekking heeft op reeds gedepersonaliseerde gegevens ouder dan zes maanden"*	✓	✓	✓	
Notificeren FG (art. 10 en 13 PNR)	4.1	**5.1.2.i** notificaties hebben er opnieuw uit gelegen in dit tertaal, gedurende 1 maand. Gelukkig is er een back-up notificatie in de vorm van **5.1.2.i**. De notificaties voor vluchtlijsten >6 maanden werken inmiddels. Er werden geen notificaties van vluchtlijsten >6mnd verzonden. Dit was bij het implementeren van de functie in TRIP niet meegenomen. Per toeval stuitte ik er op. Alle vluchtlijsten zijn door de FG handmatig opgezocht en gecontroleerd. De controle kan efficient vastgelegd worden zolang het niet om bulk verstrekkingen gaat >25 verstrekkingen. Voor bulk verstrekkingen is de werkwijze niet efficient. Noch is er een norm voor steekproeven bij controles. Het vastleggen van de communicatie tussen FG en PI-NL over de bevindingen in TRIP is nog niet mogelijk. De communicatie via e-mail is inefficient en achteraf moeilijk te reconstrueren voor toezichthouders.	✓	✓	!	
Extra Push luchtvaartmaatschappij (art. 11 PNR)	5.1	Voor zover mij bekend zijn er geen extra pushes bij PI-NL opgevraagd door PIU's. Mijn advies is om in te regelen dat dit verzoek en deze verwerking in TRIP vastgelegd kunnen worden. Dit geldt ook voor de spiegelbepaling waarbij PINL extra pushes kan opvragen bij PIU's.	✓	!		
Verstrekken aan Europol (art. 12 PNR jo. 5:7 Bpg jo. AMvB)	8.1	Verzoeken van Europol zijn gedocumenteerd. Hier geldt dezelfde t.a.v. met het verstrekken aan DLIO t.b.v. hun advies als bij de PIU-PIU verstrekking. Mijn advies is daarom ook hier om de afstemming met DLIO t.b.v. Europol via TRIP/VVA te laten verlopen en pas na een besluit tot verstrekken aan Europol de te verstrekken passagiersgegevens in **5.1.2.i** te plaatsen.	✓	!	✗	
Doorgifte aan derde landen (art. 13 PNR jo. 17a Wpg)	7.1	In TRIP **5.1.2.a** EU-LS opgenomen. Dit is gewijzigd in derde land. De wijziging was in eerste instantie niet overal doorgevoerd. De vraag of **5.1.2.a** als derde land beschouwd moeten worden is beantwoord door de opdrachtgever van PINL. Allen worden ze t.h.k.v. PNR-wet als derde land beschouwd. De notificatie functioneert voor derde landen. Daar waar de status van landen is gewijzigd naar die van derde land is een handmatige controle uitgevoerd op reeds gedane verstrekkingen.	✓	✓	!	
Doorgifte aan derde landen (art. 13 PNR jo. 17a Wpg en 5:1 lid 3 Bpg)	7.2	Voor zover bekend heeft doorgifte van passagiersgegevens van een andere PIUzonder hun toestemming aan een derde land dit tertaal niet plaatsgevonden. Mijn advies is om in TRIP de vastlegging van de de documentatie en logging van al dan niet verkregen toestemming van een andere PIU in te regelen.				
Verzoek PI-NL aan PIU (artt. 14, 15 en 16 PNR jo 4a, 4b, 25 en 28 Wpg)	8.1	PI-NL kan via **5.1.2.i** verzoeken aan PIU doen en resultaten aan de BI verstrekken. De eerste bevindingen heeft de FG begin augustus doorgegeven aan de opdrachtgever en -nemer van PI-NL. Het belangrijkste is: * De passagier heeft er recht op te weten aan wie PINL zijn gegevens de afgelopen 4 jaar heeft verstrekt. De passagier wiens gegevens zijn ontvangen staat zelf niet in TRIP. De resultaten staan onder verstrekkingen opgeslagen en dat betekent dat dat document na 42 dagen voor PINL niet meer terug te vinden is. Op dit moment is deze passagier ook in het burgerloket voor de FG ook niet te vinden, dus kan er een evt inzageverzoek niet voldaan worden. Noch lijkt het er op dat een geuploade verstrekking momenteel aan een passagiersdossier kan worden gekoppeld indien de passagier wel bij PI'NL bekend is. Mijn advies is om de bewaartermijnen, documentatie en registratie in TRIP in te regelen.	✓	!	!	
Verzoek PI-NL aan PIU (artt. 14, 15 en 16 PNR)	9.1	Voor zover mij bekend zijn er door PINL geen extra pushes opgevraagd bij PIU's. Zie ook art. 11 PNR.				
Verzoek BI aan PIU (artt. 14, 15 en 16 PNR jo. 4a, 4b, 25 en 28 Wpg)	10.1	Rechtstreeks opvragen van passagiersgegevens bij een PIU door een BI ihkv een onmiddellijke dreiging. Klopt het dat deze verwerking niet wordt geïmplementeerd in TRIP en bij PI-NL en BIU's worden verwezen naar hun eigen PIU? Rechtstreeks opvragen passagiersgegevens bij PINL ihkv een onmiddellijke dreiging door een BIU is wettelijk geregeld. Mijn advies is om in TRIP in te regelen dat de notificatie van de PIU ontvangen en bewaard kan worden. de ontvangen passagiersgegevens opgeslagen, bewaard en doorzocht kunnen worden en aan het passagiersdossier gekoppeld zijn t.b.v. burgerverzoeken.				
Juistheid en volledigheid passagiersgegevens (artt. 17 PNR jo. 4 Wpg en 1, 5, 6, 20 PNR) De verwerkingsverantwoordelijke treft de nodige maatregelen opdat politiegegevens, gelet op de doeleinden waarvoor zij worden verwerkt, juist en nauwkeurig zijn.	11.1	Voor verwerking conform doelbinding zie art. 1 PNR. Voor verwerking o.g.v. rechtmatigheid en wetmatigheid zie artt. 5 en 6 PNR. Voor bewaartermijn zie art. 20 PNR.				

Juistheid en volledigheid passagiersgegevens (artt. 17 PNR jo. 4 Wpg) Juistheid en nauwkeurigheid; kwaliteit	11.2	De passagiersgegevens zijn niet gevalideerd. De juistheid en volledigheid van de gegevens voldoet daardoor niet. Er wordt geen waarschuwing meegegeven bij verstrekkingen dat het ongevalideerde gegevens betreft. Er is geen geautomatiseerde optie in TRIP waarbij unieke passagiers herkend en gekoppeld kunnen worden b.v. o.b.v. meerdere vluchten waarbij overlap in een bepaald persoonsgegevens is. Mijn advies is om passagiersgegevens van 1 passagier van meerdere vluchten in TRIP aan elkaar te verbinden. Een dergelijke koppeling kan de verschillende PNR dosssiers van 1 unieke passagier verrijken. Door een menselijke toets er aan te koppelen waarmee bepaald kan worden dat de dossiers bij elkaar horen en dat op te slaan voor toekomstig gebruik kan het de efficientie van het werk van PINL vergroten, het kan voorkomen dat elke medewerker bij elk nieuw verzoek opnieuw dezelfde dossiers handmatig moet opzoeken en vergelijken, het kan de waarde voor de ontvanger vergroten als de gegevens van 1 unieke persoon in 1 document op vlucht naast elkaar staan i.t.t. het ontvangen van 25 losse pdf's. Creditcardgegevens worden niet compleet of deels gehast doorgegeven terwijl de carrier ze wel heeft. Voor het vaststellen van het juiste subject wordt in de vordering het creditcardnummer regelmatig gebruikt	!	!	!	
Juistheid en volledigheid passagiersgegevens (artt. 17 PNR jo. 4 Wpg) Informeren ontvanger	11.3	Er zijn een aantal keren verstrekkingen gedaan die onjuist dan wel onrechtmatig waren. Een vastgestelde procedure om ontvangers van verstrekkingen onverwijld in kennis te stellen van onjuiste passagiersgegevens dan wel onrechtmatige verstrekkingen ontbrak. Met betrekking tot de onrechtmatige verstrekking wordt een proces n.a.v. een datalek opgesteld. En een incidentenregister wordt n.a.v. de praktijk ingericht.	✓	!	✗	
Juistheid en volledigheid passagiersgegevens (artt. 17 PNR jo. 4 Wpg en 20 PNR) Documentatie en registratie	11.4	Voor documentatie en registratie zie artt. 22 en 23 PNR.				
Gegevensbescherming door privacy by design en/of default (artt. 17 PNR jo. 4a en 4b Wpg) Gegevensbescherming door beveiliging en ontwerp - noodzakelijkheid en rechtmatigheid De verwerkingsverantwoordelijke en de verwerker treffen passende technische en organisatorische maatregelen	12.1	Bij het doorontwikkelen van TRIP is privacy by design of default een vast onderdeel. Enkele punten t.a.v. de naleving zijn opgenomen bij de menselijke toets, PIU-PIU uitwisseling. Opdrachtgever PINL heeft eigenaar en opdrachtnemer PINL een mitigerende maatregel gevraagd in juli 2020 en om periodiek controles te laten uitvoeren op de mappen die gebruikt zijn voor downloads en de mate waarin de Pi-NL medewerkers handmatig bestanden met downloads uit de betreffende mappen verwijderen. De FG zou hierover door PINL periodiek gerapporteerd worden door PINL. Er zijn in T2 geen rapportages ontvangen over de periodieke controles van PINL. Overige passende technische en organisatorische maatregelen zijn dit tertaal niet in het interne toezicht meegenomen omdat beleid m.b.t. het beschermen van persoonsgegevens (een organisatorische maatregel) nog ontbreekt en eventuele organisatorische maatregelen die in de dagjournaals zijn opgenomen, zijn voor mij niet toegankelijk.	✓	✓	!	
Gegevensbescherming door privacy by design en/of default (artt. 17 PNR jo. 4a, 4b, 24 Wpg en 10 en 18 PNR en 6 samenwerkingsafspraken TRIP 2019) Gegevensbescherming door beveiliging en ontwerp - noodzakelijkheid en rechtmatigheid De verwerkingsverantwoordelijke en de verwerker treffen passende technische en organisatorische maatregelen	12.2	In T2 is een technische voorziening voor het vastleggen en verwerken van burgerverzoeken geimplementeerd. De verzoeken van de afgelopen 12 maanden zijn ingevoerd. Een bijpassende rapportagetool is niet gerealiseerd. Ten aanzien van de burgerverzoeken kan de efficientie vergroot worden door betrokkenen naast het emailadres ook er op te wijzen dat identificatie verplicht is als mede de andere andere voorwaarden die met een verzoek gepaard gaan. Een slim webformulier kan hierbij behulpzaam zijn waarbij veilig een kopie ID geupload kan worden alsmede aanvullende informatie op de website.	✓	✓	!	
Gegevensbescherming door privacy by design en/of default (artt. 17 PNR jo. 4a en 4b Wpg en 20 PNR) Gegevensbescherming door beveiliging en ontwerp - noodzakelijkheid en rechtmatigheid Verwerking o.g.v. need-to-know/have	12.3	Zie voor doelbinding en rechtmatigheid artt. 5 en 6 PNR. Zie voor notificeren art. 10 PNR. Voor need-to-know passagiersgegevens per verwerking zie art. 20 PNR.				
Gegevensbescherming door privacy by design en/of default (artt. 17 PNR jo. 4a en 4b Wpg) Gegevensbescherming door beveiliging en ontwerp - noodzakelijkheid en rechtmatigheid Controle op de kwaliteit door verwerker en/of verwerkingsverantwoordelijke	12.4	Mijn bevindingingen ten aanzien van verwerkingen in TRIP geef ik periodiek door aan Pi-NL. Ik constateerde dit tertaal geen verbetering want dezelfde bevindingen herhalen zich keer op keer. Het gaat om een accurate invoer van de vordering in TRIP en de verwerking en verstrekking. Bijvoorbeeld vluchtlijsten niet op de juiste wijze verstrekken betekent dat de verstrekking niet in het dossier van de passagier komt, namen van de OvJ opnemen bij de autoriteit, naam van het onderzoek opnemen bij het parketnummer, een ruimere zoekperiode dan in de vordering is opgenomen, de toestemming om depersonaliseren op te heffen niet overgenomen. De foutief verstrekte vluchtlijsten zijn niet gerepareerd waardoor de documentatieplicht in het passagiersdossier niet voldoet. Een kwaliteitscontrole of vier-ogenprincipe blijkt niet ingericht, noch gedocumenteerd te worden. Er zijn onrechtmatige en onjuiste verstrekkingen verricht. De consequenties waren volgens de **5.1.2e** NCTV minimaal.	!	!	✗	
Gegevensbescherming door privacy by design en/of default (artt. 17 PNR jo. 4a en 4b Wpg) Gegevensbescherming door beveiliging en ontwerp - noodzakelijkheid en rechtmatigheid Risico analyse	12.5	Dit tertaal is de PIU-PIU verstrekking via **5.1.2.f** Het is mij nog niet duidelijk of er afspraken zijn (met Europol - de **5.1.2.f** -) over het wissen van geuploade verstrekkingen die bij een negatief advies van DLIO/ENU toch niet verstrekt worden. Dan wel of er een risicio-analyse is uitgevoerd ten behoeve van de risico's die deze verwerking heeft op de rechten en vrijheden van betrokkenen waarbij onder andere bovenstaande is afgewogen. Mij is niet bekend dat een risicoanalyse aanwezig is die het risiconiveau aantoont en identificeert, evalueert en mitigeert alsmede systematisch en periodiek maatregelen worden aanpast om factoren die het beschermen van passagiersgegevens tegen ongeoorloofde of onrechtmatige verwerking en tegen opzettelijk verlies, vernietiging of beschadiging in gevaar brengen.	✗	✗	✗	
Gegevensbescherming door privacy by design en/of default (artt. 17 PNR jo. 4a en 4b Wpg) Gegevensbescherming door beveiliging en ontwerp - noodzakelijkheid en rechtmatigheid Gegevensbeschermingsbeleid	12.6	Er is nog geen gegevensbeschermingsbeleid ontwikkeld en vastgesteld.	✗	✗	✗	
Gegevensbescherming door privacy by design en/of default (artt. 17 PNR jo. 4a en 4b Wpg) Gegevensbescherming door beveiliging en ontwerp - noodzakelijkheid en rechtmatigheid Privacy by design / default	12.7	Bij ontwikkelingen en wijzigingen in TRIP wordt privacy by design/default in acht genomen.	✓	✓	✓	
Gegevensbescherming door privacy by design en/of default (artt. 17 PNR jo. 4a en 4b Wpg) Gegevensbescherming door beveiliging en ontwerp - noodzakelijkheid en rechtmatigheid Compliance	12.8	Bij verwerkingen binnen TRIP kan de verwerkingsverantwoordelijke aantonen dat de verwerking wordt verricht in overeenstemming met de wet.	✓	✓	✓	
Gegevensbescherming door privacy by design en/of default (artt. 17 PNR jo. 4a en 4b Wpg) Gegevensbescherming door beveiliging en ontwerp - noodzakelijkheid en rechtmatigheid Tussenkomst natuurlijke persoon voor toegankelijk maken	12.9	Zie art. 8 PNR voor de menselijke toets. De in de wet benoemde menselijke toets wordt bij SISII verstrekkingen uitgevoerd en bij het verwerken van vorderingen en verzoeken. De menselijke toets wordt niet gedocumenteerd en is daardoor voor toezichthouders of in het geval van een strarechtelijk onderzoek niet te controleren.	✓	✓	!	

Gegevensbeschermingseffectbeoordeling / Data proces impact assessment / privacy impact assessment (DPIA) (artt. 17 PNR jo. 4c Wpg) Beoordelen risico's voor vrijheden	13.1	Er is mij geen overzicht bekend waarin is opgenomen of verwerkingen worden gezien als een hoog risico voor de rechten en vrijheden van personen. Noch is mij bekend of die beoordeling is vastgelegd in bijvoorbeeld een verwerkingsregister.	✓	!	!	
Gegevensbeschermingseffectbeoordeling / Data proces impact assessment / privacy impact assessment (DPIA) (artt. 17 PNR jo. 4c Wpg) Opstellen DPIA	13.2	Bij het opstellen van de wet ten behoeve van het inrichten van PI-NL is een strategische DPIA uitgevoerd. Deze is herzien en vastgesteld. N.a.v. de presentaties van de FG in het MT+ heeft LSO een aanzet tot een DPIA opgesteld. B&V had daarvoor een concept opgesteld.	✓	!	!	
Gegevensbeschermingseffectbeoordeling / Data proces impact assessment / privacy impact assessment (DPIA) (artt. 17 PNR jo. 4c Wpg) Vaststellen uitvoeren, evalueren en herzien DPIA	13.3	Mijn advies is om de DPIA in een PDCA cyclus danwel bij P&C op te nemen.	✓	!	!	
Autorisaties en toegang tot passagiersgegevens (artt. 17 PNR jo. 6 en 6a Wpg jo Samenwerkingsafspraken)	14.1	De FG heeft toegang tot de loggingsresultaten. Het toekennen en intrekken van autorisaties is door de verwerkingsverantwoordelijke geregeld. De voorwaarden waaraan een gebruiker van TRIP moet voldoen staan op het startscherm van TRIP. Zijn deze voorwaarden vastgesteld, worden ze gemonitord en zijn ze nog actueel?	✓	✓	✓	
Autorisaties en toegang tot passagiersgegevens (artt. 17 PNR jo. 6 en 6a Wpg jo Samenwerkingsafspraken)	14.2	Per scherm is niet vastgelegd welke persoonsgegevens daar getoond worden aan welke gebruiker. Schermen worden door meerdere gebruikers gedeeld. Hierdoor is het onduidelijk wie welke informatie in TRIP kan zien en of dat op basis van need to know is. Het hebben van toegang betekent niet dat je gebruik van de toegang mag maken als het niet nodig is. Er is geen onderscheid tussen verschillende functies per autorisatie voor een scherm of m.b.t. lezen en/of bewerken. Bijvoorbeeld: de FG kan naast het inzien van verstrekkingen deze ook uitvoeren of de teamleiders hebben niet de juiste autorisaties voor rapportages om het team aan- en/of bij te sturen. Er wordt onderzocht per functie/rol wie welke informatie nodig heeft en en voorstel voor het inrichten van de autorisaties gedaan.	✓	!	!	
Autorisaties en toegang tot passagiersgegevens (artt. 17 PNR jo. 6 en 6a Wpg jo Samenwerkingsafspraken)	14.3	In de reactie op de T1-2020 geeft PINL aan dat er een proces is voor het toewijzen, wijzigen en intrekken van autorisaties t.b.v. de toegang tot passagiersgegevens.	✓	✓		
Autorisaties en toegang tot passagiersgegevens (artt. 17 PNR jo. 6 en 6a Wpg jo Samenwerkingsafspraken)	14.4	Een periodieke controle op de uitgegeven autorisaties wordt uitgevoerd door [redacted]. Deze heeft zelf geen toegang tot TRIP. Vindt er eveneens een controle in TRIP plaats op het integer gebruik van de autorisatie?	✓	✓		
Verwerker (artt. 17 PNR jo. 6c Wpg) Verwerking wordt geregeld in een schriftelijke overeenkomst. Verwerker heeft passende technische en organisatorische maatregelen en informeert verwerkingsverantwoordelijke - vooraf schriftelijk bij het in dienst nemen van een ander verwerker incl. mogelijkheid tot bezwaar - zonder vertraging bij inbreuk op de beveiliging	15.1	Er is een verwerkersafspraak vastgesteld tussen opdrachtgever en -opdrachtnemer van PI-NL.	✓	✓	✓	
Verwerker (artt. 17 PNR jo. 6c Wpg) Verwerking in gesloten systeem	15.2	Het is niet mogelijk om na te gaan in hoeverre verwerkingen in een gesloten systeem plaatsvinden. Het interne toezicht heeft in T2 niet plaatsgevonden.				
Geheimhoudingsplicht (artt. 17 PNR jo. 7 Wpg)	16.1	In de verstrekking is niet opgenomen dat de ontvanger van de passagiersgegevens een geheimhoudingsplicht heeft. Hoe worden de gebruiker en ontvanger van de PNR-gegevens gewezen op de geheimhoudingsplicht en de consequenties van schending van de plicht?	!	!	!	
Geheimhoudingsplicht (artt. 17 PNR jo. 7 Wpg en 1 PNR)	16.2	Zie voor doelbinding en rechtmatigheid artt. 5 en 6 PNR. Voor need-to-know passagiersgegevens per verwerking zie art. 20 PNR.				
Geheimhoudingsplicht (artt. 17 PNR jo. 7 Wpg jo. 6.4 Bpg en 20 PNR)	16.3	De verstrekkingen van nationale passagiersgegevens voldoen aan de documentatieplicht. De verstrekkingen aan PIU's voldoen sinds de [redacted] niet meer volledig aan de documentatieplicht. De vastlegging in het dossier van de passagier bij ontvangst van gegevens van een andere PIU komen niet in het dossier terecht.	✓	!	✗	
Verstrekken aan derde landen (artt. 17 PNR jo. 17a Wpg en Besluit gebruik van passagiersgegevens voor de bestrijding van terroristische en ernstige misdrijven)	17.1	Voor [redacted] geldt dat ze als derde land worden beschouwd sinds het einde van dit tertaal. [redacted] waren niet juist ingevoerd in TRIP en werden t.b.v. PNR-wet als EU beschouwd. Vanaf 01.01.2021 00:00 uur zal de Brexit naar alle waarschijnlijkheid een feit zijn. Hoe wordt geborgd dat verzoeken om passagiersgegevens dan op de juiste wijze verwerkt worden?	✓	✓	!	
Verstrekken aan derde landen (artt. 17 PNR jo. 17a Wpg en Besluit gebruik van passagiersgegevens voor de bestrijding van terroristische en ernstige misdrijven)	17.2	De verstrekkingen aan derde landen voldoen weer aan de documentatie en notificatie plicht. De verstrekkingen die gedaan zijn aan deze derde landen als zijnde BIU-EU heeft de FG handmatig opgezocht en gecontroleerd aangezien verstrekkingen van gegevens <6 mnd aan een BIU-EU geen notificatieplicht kennen. De registratie in TRIP is aangepast zodat voor rapportages de juiste gegevens gegenereerd kunnen worden.	✓	✓	!	
Verstrekken aan derde landen (artt. 17 PNR jo. 17a Wpg en Besluit gebruik van passagiersgegevens voor de bestrijding van terroristische en ernstige misdrijven)	17.3	Doorgifte van passagiersgegevens aan derde landen vindt plaats via DLIO. Worden de gegevens verstrekt onder de voorwaarde dat deze door de ontvangende autoriteit worden vernietigd zodra de doeleinden zijn verwezenlijkt? Worden aan de verstrekking de wettelijke bewaartermijnen gesteld?	✓	✓	✓	
Verstrekken aan derde landen (artt. 17 PNR jo. 17a Wpg en Besluit gebruik van passagiersgegevens voor de bestrijding van terroristische en ernstige misdrijven)	17.4	Er zijn voorzover bekend geen gegevens van andere lidstaten aan derde landen verstrekt. Is er een proces om toestemming van de andere PIU te verkrijgen en de uitkomst te documenteren? Is er een proces om een notificatie te sturen aan de andere PIU wanneer het onmogelijk was om toestemming voor verstrekking te verkrijgen?	✓	✓	✓	
Rechten van betrokkenen (artt. 17 PNR jo. 24b Wpg jo. 25 en 28 Wpg en Samenwerkingsafspraken TRIP 2019) Informatie aan betrokkene De verwerkingsverantwoordelijke verstrekt aan de betrokkene informatie over de verwerking van politiegegevens in een beknopte en toegankelijke vorm en in duidelijke en eenvoudige taal. De informatie wordt met passende middelen, waaronder elektronische, kosteloos verstrekt en in het algemeen in dezelfde vorm als de vorm van het verzoek.	18.1	De informatie uit de wet is aanwezig. Mijns inziens is dat niet de gewenste begrijpelijke informatie t.b.v. de betrokkene m.b.t. * de verwerkingsdoelen van de passagiersgegevens; * de rechten van de betrokkene op inzage, rectificatie en vernietiging; * het recht een klacht in te dienen bij de Autoriteit persoonsgegevens; * de contactgegevens van die autoriteit; en in specifieke gevallen: - de rechtsgrondslag van de verwerking; - de bewaartermijn van de politiegegevens; - in voorkomend geval, de categorieën van de ontvangers van de politiegegevens; en indien noodzakelijk, extra informatie, in het bijzonder wanneer de politiegegevens zonder medeweten van de betrokkene worden verzameld. - het bestaan van geautomatiseerde besluitvorming, met inbegrip van profilering, en nuttige informatie over de onderliggende logica, alsmede het belang en de verwachte gevolgen van die verwerking voor de betrokkene.	✓	!	!	
Rechten van betrokkenen (artt. 17 PNR jo. 24b Wpg) Verstrekking van informatie aan betrokkene	18.2	Er is geen verzoek om informatie ontvangen waarbij het uitstel, de beperking of het achterwege laten van de informatieverstrekking alsmede de duur van deze maatregel onderbouwd diende te worden.	✓	✓	✓	

Rechten van betrokkenen (artt. 17 PNR jo. 25 en 27 Wpg) Recht op inzage	18.3	Het proces voor het uitoefenen van inzage is door de opdrachtgever overgedragen aan de opdrachtnemer. Het mandaat om de verzoeken af te handelen is gepubliceerd waardoor het [redacted] PI-NL namens de verwerkingsverantwoordelijke kan acteren. De workaround via de FG is daarmee vervallen vanaf T3-2020. Het proces is in TRIP via privacy by design ingeregeld. Het verkijgen van de managementinformatie lijkt nog niet te zijn ingeregeld. In T2-2020 zijn 3 burgerverzoeken tot inzage ingediend. [redacted]	✓	✓	✓	
Rechten van betrokkenen (artt. 17 PNR jo. 26 Wpg) Formaliteiten	18.4	De identiteit van betrokkenen wordt deugdelijk vastgesteld via een kleurenkopie van het paspoort. Aanvullende vragen kunnen gesteld worden als het ID de identiteit onvoldoende uitsluitsel geeft. In het nieuwe proces waar PINL de verzoeken afhandelt wordt het kopie ID gecontroleerd door medewerkers met ervaring en hun kennis wordt opgefrist. Verzoeken van minderjarigen en onder curatele gestelden kunnen alleen door de wettelijke vertegenwoordigers gedaan worden. Hoe wordt dit bij meerderjarige onder curatele gestelden uitgevoerd?	✓	✓	!	
Rechten van betrokkenen (artt. 17 PNR jo. 27, 25 en 28 Wpg) Uitzonderingen	18.5	Er is geen kennelijk ongegrond of buitensporig verzoek ontvangen waarbij de weigering onderbouwd en toegelicht dienda te worden.	✓	✓		
Rechten van betrokkenen (artt. 17 PNR jo. 28 Wpg) Recht op rectificatie en vernietiging	18.6	Er is geen verzoek tot rectificatie en/of vernietiging van de PNR-gegevens ontvangen waarbij de ontvanger van de gegevens en de leverancier van de gegevens geinformeerd moeten worden over de rectificatie en/of vernietiging.	✓	!		
Rechten van betrokkenen (artt. 17 PNR jo. 29 en 31a Wpg) Toepassselijkheid Awb	18.7	De betrokkene wordt bij de ontvangstbevestiging en het besluit over het burgerverzoek geinformeerd over de toepasselijkheid van de Awb en het indienen van een beroep of bemiddeling door de AP.	✓	✓	✓	
Rechten van betrokkenen (artt. 17 PNR jo. 29 Wpg) Toepassselijkheid Awb	18.8	Er is geen verzoek van de Nationale Ombudsman ontvangen.				
Rechten van betrokkenen (artt. 17 PNR jo. 31a, 24a en 29 Wpg) Klacht bij de AP	18.9	De betrokkene wordt bij de ontvangstbevestiging en het besluit over het burgerverzoek geinformeerd over het kunnen indienen van een klacht bij de AP.	✓	✓	✓	
Audits (artt. 17 PNR jo. 33 Wpg en art 6.5 leden 1 en 5 Bpg en de Regeling Periodieke Audit passagiersgegevens en art. 9 Samenwerkingsafspraken TRIP 2019) De verwerkingsverantwoordelijke controleert de waarborgen voor de gegevensbescherming uit de toepasselijke wetgeving via een privacy audit. En stuurt een afschrift aan de AP. Binnen een jaar vindt hercontrole plaats op de onderdelen die in de audit onvoldoende waren	19.1	De privacy audit en de interne audits waren nog niet ingepland, zo is in T1 gemeld. In T2 is er nog geen planning of plan van aanpak met de FG gedeeld. Van de resultaten van de audit uit T1 t.a.v. het functioneren de technische voorzieninng TRIP t.a.v. (informatie)beveiliging heeft de FG nog geen kennis kunnen nemen.	✓	!	✗	
Datalekken (artt. 17 PNR jo. 33a Wpg) De verwerkingsverantwoordelijke meldt een datalek binnen 72 uur na kennisname ervan aan de AP tenzij het niet waarschijnlijk is dat de inbreuk een risico voor de rechten en vrijheden van betrokkenen inhoudt	20.1	PINL heeft in T2 nog onvoldoende geborgd dat incidenten met passagiersgegevens gedetecteerd worden. Dit hangt samen met het onderwerp kwaliteit en interne controle (bv. 4-ogen-principe). De opdrachtgever van PINL heeft een intern proces datalekken vastgesteld. PINL heeft nog geen proces vastgesteld en aan de medewerkers gecommuniceerd. De taken, verantwoordelijkheden en bevoegdheden t.a.v. dit punt zijn nog niet duidelijk.	✓	!	✗	
Raadplegen Autoritet passagiersgegevens (artt. 17 PNR jo. 33b en 4c Wpg) Voorafgaande raadpleging voorgenomen verwerking met hoog risico voor betrokkene	21.1	Er is geen DPIA geweest noch een vraag die aan de AP is voorgelegd. Er is geen document waaruit blijkt wanneer een voorgenomen verwerking aan de AP voorgelegd kan of moet worden.	✓	!		
Functionaris voor gegevensbescherming (art. 18 PNR jo. 36 Wpg)	22.1	De FG is benoemd. De FG kan toezicht houden op de uitvoering van de waarborgen door PINL voor het beschermen van passagiersgegevens - het naleven van PNR en van overeenkomstige toepassing zijnde artikelen Wpg - het toewijzen van autorisaties - de verwerking van passagiersgegevens door PI-NL. De FG kan nog geen toezicht houden op de uitvoering van de waarborgen door PINL voor het beschermen van passagiersgegevens - het beleid van de verwerkingsverantwoordelijke m.b.t. het beschermen van persoonsgegevens - de audits - de uitvoering van de DPIA - de bewustmaking en opleiding van de medewerkers van PINL die betrokken zijn bij de verwerking van passagiersgegevens. De FG heeft op verzoek twee adviezen aangeboden t.b.v. het BO over - het scheiden van de taken van de FG en een privacy adviseur - de KPI's m.b.t. het beschermen van persoonsgegevens	✓	!	!	
Functionaris voor gegevensbescherming (art. 18 PNR jo. 36 Wpg) Rapportage art. 18	22.2	Het tijdig aanbieden van de artikel 18 rapportage over 2019 is nog niet geborgd. Het proces is nog niet vastgesteld. De statistieken voor de rapportage kunnen inmiddels geautomatiseerd uit TRIp gehaald worden.	✓	✓	!	
Functionaris voor gegevensbescherming (art. 18 PNR jo. 36 Wpg) Contactpunt	22.3	Betrokkenen kunnen contact opnemen met de FG. Het emailadres is gepubliceerd. Voor de afhandeling is in TRIP een module ingericht. Efficientie kan verbeteren door betrokkenen naast het emailadres te informeren over de (on)mogelijkheden en vereisten t.a.v. verzoeken. Bijvoorbeeld door een slim webformulier op te nemen dat alleen verzonden kan worden als de verplichte velden zijn ingevuld en een kopie ID bewijs is toegevoegd.	✓	✓	!	
Functionaris voor gegevensbescherming (art. 18 PNR jo. 36 Wpg) Autorisatie en documentatie	22.4	De FG heeft toegang tot de passagiersgegevens in TRIP en loggingresultaten van verwerkingen in TRIP. Passagiersgegevens die op andere plaatsen zijn opgeslagen zijn voor de FG niet toegankelijk. Denk b.v. aan postvakken in outlook waar verderingen en verstrekkingen zijn opgeslagen of de map downloads op de persoonlijke(?) schijf.	✓	✓	!	
Functionaris voor gegevensbescherming (art. 18 PNR jo. 36 Wpg) Tijdig betrekken van FG	22.5					
Functionaris voor gegevensbescherming (art. 18 PNR jo. 36 Wpg) Toezicht op compliance	22.6	De FG kan toezicht houden op wetgeving en vastgestelde interne processen. Het toezicht op intern beleid is niet mogelijk omdat gegevensbeschermingsbeleid nog ontbreekt en sommige (werk)afspraken die de gegevensbescherming raken in documenten (bv. dagjournaal) zijn opgenomen die voor de FG niet toegankelijk zijn.	✓	!	!	

Functionaris voor gegevensbescherming (art. 18 PNR jo. 36 en 6 Wpg) Autorisaties en beleid	22.7	Zie voor het toezicht op autorisaties ook art. ?? In T2 is het beleid van de autorisaties ontvangen en is geconstateerd dat theorie en praktijk niet met elkaar overeenstemmen. Het advies aan PINL was: - Inventariseren per tabblad of/en zo ja, welke persoonsgegevens daar verwerkt worden - Inventariseren welke persoonsgegevens elke rol/functie nodig heeft op basis van need to know - De inventarisaties naast elkaar leggen en afwijkingen/aanpassingen vastleggen - Aanpassingen bespreken en via VTW implementeren - Autorisaties opnieuw vaststellen en uitvoeren - Protocol/proces inrichten voor o tijdig intrekken autorisaties o.a. bij vertrekkende medewerkers en/of medewerkers die van functie/rol veranderen o wijzigingen in tabbladen a.g.v. VTW die autorisatie per rol/functie kunnen beïnvloeden o periodieke evaluatie en monitoring van de autorisaties en rol/functie	✓	✓	!	
Functionaris voor gegevensbescherming (art. 18 PNR jo. 36 Wpg) Bewust zijn en opleiden	22.8	Aan het MT+ zijn in T2 3 presentaties gegeven door de FG om de algemene kaders van gegevensbescherming toe te lichten. De introductiecursus voor nieuwe medewerkers van PINL is bekeken en een reactie aan het **5.1.2.e** PINL gestuurd. Er wordt door PINL aan een nieuwe introductiecursus gewerkt. T.b.v. opnemen van het beschermen van persoonsgegevens leveren de jurist en privacy medewerker van PINL input. N.a.v. mijn vragen over kwaliteit en juistheid van de ingevoerde gegevens in de VVA zijn teamsessies gehouden voor alle medewerkers van B&V. In T3 staan nog een aantal teamsessies gepland. Mijn advies is dat PINL zelf intern medewerkers opleidt en met bewustmakingsacties de discussie stimuleert. Als de basis op orde is kan dat gefocust zijn op de eigen interne risico's en risico beperkende maatregelen. Tot die tijd kan het algemene vormgegeven worden.	✓	✓	✓	
Functionaris voor gegevensbescherming (art. 18 jo. PNR o. 36 en 33 Wpg) Audits	22.9	Zie voor het toezicht op audits art. 17 PNR jo. 33 Wpg				
Verwerkingsverbod op bijzondere passagiersgegevens (art. 19 PNR)	23.1	In T2 is tijdens het reguliere toezicht niet geconstateerd dat bijzondere gegevens verwerkt zijn.	✓	✓	✓	
Depersonaliseren en verwijderen van passagiersgegevens (art. 20 PNR jo. 17 PNR en Wpg) Wissen verwerkingsresultaten en witte lijst	24.1	Verwerkingsresultaten worden langer bewaard dan noodzakelijk is voor de doorgifte aan een BI. In december 2019 heeft de **5.1.2e** NCTV aangegeven dat 42 dagen voldoende is om de werkzaamheden van TRIPgebruikers efficient te kunnen laten verlopen. Dit in overleg met de keyuser PINL, toenmalige productowner en FG. In TRIP kan het verwerkingsresultaat altijd gereconstrueerd worden en is het bewaren van het resultaat in bv. pdf-vorm niet noodzakelijk en voornamelijk nice-to-have. Daarbij worden pdf's niet gemaskeerd na zes maanden of gemaskeerd als de gegevens al ouder dan 6 maanden waren. Naar aanleiding van een verzoek van de FO *(WPG regime heeft andere bewaartermijnen)* om de termijn in de VVA op te rekken van 14 dagen naar 6 maanden heeft PINL de opvraagbaarheid *(het loskoppelen van de link naar het document op de server)* na 42 dagen on hold gezet. Alle verwerkingsresultaten in TRIP worden nu zonder bewaartermijn bewaard zolang er geen besluit is genomen (sinds ongeveer 3 maanden). In hoeverre moeten verwerkingsresultaten in de VVA 6 maanden bewaard worden als de BI alle verstrekkingen zelf in hun eigen systeem opslaan om te verwerken? Mijn advies is om de termijn van 42 dagen te hanteren voor TRIP en een besluit te nemen hoever de dienstverlening naar VVA gebruikers gaat. Als besloten wordt tot het afwijken van de 42 dagen termijn en die op te rekken naar 6 maanden dan moet voor elke opvraging van het verwerkingsresultaat dat bij verstrekken al ouder was dan 6 maanden een verantwoording worden gegeven. Dit zou ook geregeld moeten wordn voor gegeven die gedurende de 6 maanden termijn na verstrekking ouder dan 6 maanden worden. Gegevens ouder dan zes maanden moeten gedepersonaliseerd worden. In bepaalde gevallen worden passagiersgegevens via **5.1.2.i** verstrekt en in alle gevallen komen spoed/mondelinge vorderingen binnen via **5.1.2.i** Het is onduidelijk hoelang deze berichten bewaard blijven in	✓	!	✗	
Depersonaliseren en verwijderen van passagiersgegevens (art. 20 PNR) Depersonaliseren van passagiersgegevens ouder dan 6 maanden	24.2	Zie hierboven bij wissen verwerkingsresultaat. In TRIP worden passagiersgegevens ouder dan 6 maanden geautomatiseerd gedepersonaliseerd. Een punt van zorg is het niet onderbouwen van het raadplegen van gegevens ouder dan 6 maanden of jonger in de daarvoor bedoelde verantwoordingsvelden in TRIP. Standaard staat het TRIP ID in dat veld en enkele gebruikers vullen daar niets in. De persoonsgegevens van gebruikers (medewerkers BI, OM, PINL, FG) worden niet gedepersonaliseerd na 6 maanden. Mijn advies is om hier een besluit over te nemen en dat in TRIP/VVA door te voeren. Iedereen heeft recht op het beschermen van persoonsgegevens.	✓	✓	!	
Depersonaliseren en verwijderen van passagiersgegevens (art. 20 PNR jo. 4 Wpg) Verwijderen van passagiersgegevens	24.3	Het controleren of het verwijderen van passagiersgegevens ouder dan 5 jaar functioneert is pas mogelijk vanaf 19.06.2024. Volgens een test van de leverancier werkt het verwijderen. De test is risicovol omdat de datum handmatig naar een datum in toekomst wordt gezet. Het verwijderen van passagiersgegevens op verzoek van betrokkene om vernietiging is nog niet voorgekomen. De werking hiervan is dus nog niet gecontroleert. Het verwijderen van de verwerkingsresultaten is besproken bij het wissen van verwerkingsresultaten.	✓			
Registreren en of documenteren verwerkingen (artt. 22 en 23 PNR) Register en documentatie	25.1	De opdrachtgever van PINL heeft aangegeven dat het register bestaat. De FG heeft nog geen kennis kunnen nemen van het register. De documentatie is vastgelegd in TRIP.	✓	!	!	
Registreren en of documenteren verwerkingen (artt. 22 en 23 PNR jo. 6 Wpg) Loggegevens van verwerkingen	25.2	De loggegevens worden na een wijziging in TRIP sinds T2 vastgelegd. Een aandachtspunt is het veiligstellen van loggegevens die de bewaartermijn dreigen te naderen en als bewijsmateriaal (kunnen) dienen.	✓	✓	✓	
Registreren en of documenteren verwerkingen (artt. 22 en 23 PNR) Loggegevens	25.3	Zie ook art. 8 PNR, de menselijke tussenkomst wordt niet gelogd waardoor controle hierop niet mogelijk is.	✓	!	✗	

A6

Ministerie van Justitie en Veiligheid

DEP. VERTROUWELIJK
Openbaar na publicatie

Tertaal rapportage FG PI-NL - T3 2020

t.b.v. Bestuurlijk overleg Pi-NL

Versie 1.0

Datum	maart 2021
Status	Definitief

Colofon

Afzendgegevens	**Functionaris voor de gegevensbescherming voor de Passagiersinformatie-eenheid Nederland** Turfmarkt 147 2511DP Den Haag Postbus 20301 2500EH Den Haag www.rijksoverheid.nl/jenv
Bijlage(n)	T3 2020 Rapportage Waarborgen
Auteurs	Functionaris voor de gegevensbescherming voor de Passagiersinformatie-eenheid Nederland

Inhoud

1 Inleiding

Voor u ligt de toelichting op de tertaalrapportage[1] van de Functionaris voor de Gegevensbescherming (hierna: FG) van de Passagiers-Informatie eenheid Nederland (hierna: Pi-NL) en gaat over het derde tertaal 2020. In het bestuurlijk overleg hebben de opdrachtgever, eigenaar en opdrachtnemer[2] gelegenheid vragen te stellen aan de FG. De tertaalrapportage geeft een samenvatting van de belangrijkste bevindingen weer die van september tot en met december zijn gedaan.

De verantwoording over de wijze van handelen en/of een planning naar aanleiding van een bevinding ligt in de lijn bij de opdrachtnemer, de eigenaar en de opdrachtgever. De opdrachtgever en opdrachtnemer hebben op basis van een conceptrapportage een reactie gegeven om mogelijke feitelijke onjuistheden naar voren te brengen en om verduidelijkende vragen te stellen.

Naast de tertaalrapportage brengt de FG jaarlijks verslag uit aan de Minister, de Tweede en Eerste Kamer der Staten-Generaal en de Autoriteit Persoonsgegevens conform artikel 18 PNR. In december 2020 is de eerste rapportage over het voorgaande kalenderjaar 2019 door de minister aan het parlement aangeboden.

Het bestuurlijk overleg stemde in met het beëindigen van deze tertaalrapportages om te voorkomen dat er gerapporteerd wordt om het rapporteren. De bevindingen die de FG de afgelopen 18 maanden heeft gedeeld en voor zover die nog niet zijn opgepakt of ingepland door opdrachtgever en opdrachtnemer blijven mijns inziens relevant en vragen om een besluit. Het nemen van een besluit, het prioriteren en of uitvoeren van risico beperkende maatregelen naar aanleiding van de bevindingen ligt bij de opdrachtgever, opdrachtnemer en of eigenaar. Wanneer besluiten zijn of worden genomen die de passagiersgegevens kunnen raken zal de FG daarbij betrokken moeten worden.
Het eindigen van de tertaalrapportage wordt vervangen door een jaarplan intern toezicht. De bevindingen naar aanleiding van de jaarplanning en ad hoc toezichtsactiviteiten deel ik met het bestuurlijk overleg. Samen – binnen onze verantwoordelijkheden - beschermen we de passagiersgegevens optimaal.

---

[1] De Minister van JenV is, conform artikel 17 PNR, de verwerkingsverantwoordelijke.
In het Contourendocument is vastgelegd dat de Functionaris Gegevensbescherming (hierna: FG) PI-NL 4 maal per jaar t.b.v. het bestuurlijk overleg een rapportage opstelt voor de opdrachtnemer, eigenaar en opdrachtgever/verwerkings-verantwoordelijke. In het bestuurlijke overleg van december 2019 is vastgesteld dat de FG een tertaalcyclus zal gaan aanhouden.

[2] 5.1.2e Pi-NL is volgens de verwerkersafspraak de opdrachtnemer en de PI-NL is de verwerker van de PNR-gegevens. Justid en JIVC zijn verwerkers van PNR-gegevens.
De eigenaar (Ministerie van Defensie/KMar) is verantwoordelijk voor de continuïteit van de (dienstverlening en de bedrijfsvoering van de) Pi-NL op de lange termijn en het toezicht op de algemene bedrijfsvoering. De opdrachtgever (Ministerie van Justitie en Veiligheid/NCTV) is conform het organisatiebesluit van het ministerie van JenV opdrachtgever voor de PI-NL en verantwoordelijk voor het beleid inclusief de bijbehorende wet- en regelgeving en de te maken beleidskeuzes. De opdrachtgever is aansluitend ook verantwoordelijk voor een goede opdrachtformulering aan de opdrachtnemer.

2 Intern Toezicht

2.1 Autorisaties

De autorisaties zijn nog niet op basis van need-to-know of need-to-do ingericht voor alle gebruikers van TRIP. Bijvoorbeeld accountmanagement blijkt bij passagiersgegevens te kunnen en ikzelf kan altijd nog vorderingen afhandelen.
Met een paar quick wins zijn enkele aanpassingen gedaan om toegang voor onbevoegden tot passagiersgegevens dicht te zetten en exports van de passagiersgegevens verder te beperken.
Met het oog op de actualiteit en de politieke gevoeligheid van dit dossier zal ik niet hoeven te benadrukken dat dit onderwerp mijn aandacht behoudt en snelle besluitvorming gewenst is.

2.2 Bewaartermijnen en depersonaliseren na 6 maanden

De bewaartermijnen voor verstrekkingsdocumenten zoals in beleid vastgesteld zijn begin 2020 opgeschort. Hierdoor konden gebruikers van TRIP de passagiersgegevens inzien die ouder dan 6 maanden waren zonder de depersonalisering op te heffen.
In december heeft de opdrachtgever de opdrachtgeven de bewaartermijn te herstellen en alle documenten te verwijderen.
N.B. het verwijderen van de verstrekkingsdocumenten is in 2021 verkeerd uitgevoerd. Het gevolg is dat alle gelogde informatie over de verstrekking en daarmee het verwerken van de persoonsgegevens is verwijderd door Justid-IBO. Aan het herstel van de loggegevens wordt gewerkt.

2.3 Bijzondere gegevens

De PNR-wet verbiedt het maken van onderscheid op grond van bijzondere persoonsgegevens, zoals ras, etnische afkomst, godsdienst of gezondheid.
Wanneer een luchtvaartmaatschappij deze gegevens toch aanlevert, filtert TRIP geautomatiseerde deze gegevens uit en ze worden daarmee niet verwerkt door Pi-NL. Deze werkwijze betreft alle velden waarvan bekend is dat ze bijzondere persoonsgegevens (kunnen) bevatten.

Er zijn velden waarin wel bijzondere gegevens te vinden zijn. Passagiers gebruiken bijvoorbeeld gegevens die door de werkgever ter beschikking zijn gesteld om een vlucht te boeken. Hierdoor verwerkt Pi-NL toch bijzondere gegevens. Het betreft officiële e-mailadressen @vakbond, @politiekepartij, @geloof of informele e-mailadressen achternaam_politiekepartij@provider. Pi-NL heeft de aanwezigheid van deze bijzondere gegevens erkend.
Ik adviseer om op korte termijn een besluit te nemen ten aanzien van deze onrechtmatige verwerking van bijzondere persoonsgegevens.

2.4 Kwaliteit

Een wettelijke verplichting is om de juistheid van de gegevens te bewaken. Het punt kwaliteit was de afgelopen twee kwartalen een aandachtspunt. Pi-NL heeft naar aanleiding van mijn dringend advies extra aandacht gegeven aan het verbeteren en borgen van de kwaliteit van de vorderingsgegevens in TRIP. In december stelde ik vast dat de kwaliteit sterk verbeterd is. Nu is het belangrijk om dit succes te verankeren.

In dit tertaal kwamen ook een paar onrechtmatige verstrekkingen voor. Pi-NL heeft melding gedaan bij 5.1.2e van de opdrachtgever.

2.5 Wpg-domein

Bij de behandeling van de PNR-wet heeft het parlement zorgen uitgesproken over het "vakantieregister" dat (persoons)gegevens van onschuldige passagiers in het Wpg-domein zouden komen. Pi-NL is daarom niet in het Wpg-domein actief. Wel mogen ze Wpg-gegevens gebruiken bij de uitvoering van de werkzaamheden.
Door de uitwerking in lagere regelgeving en door de beperkte informatieverstrekking in vorderingen is de praktijk, dat de passagiersgegevens snel het Wpg-domein instromen. Bij het lezen van de wet en behandeling in het parlement zou je anders verwachten.
De gekozen uitwerking in de lagere regelgeving geeft bestaande bevoegde instanties een rol in het proces van Pi-NL. Hetzij door advies uit te brengen over internationale verstrekkingen (bv. DLIO) hetzij door verplicht applicaties (5.1.2.i) van deze organisaties te gebruiken voor het verzenden van passagiersgegevens.
Het is mij nog niet gelukt om (verwerkings)afspraken tussen de betreffende organisaties en opdrachtgever en of opdrachtnemer te achterhalen. Deze afspraken moeten o.a. het beschermen van passagiersgegevens regelen en de doorwerking van de doelbinding.

Daarnaast draagt het feit dat TRIP met ongevalideerde gegevens werkt ook niet bij aan het beschermen van de passagiersgegevens van de niet-gezochte passagier. Als 5.1.2e op een intra-EU-vlucht vliegt terwijl zijn doopnaam 5.1.2e is zal hij niet gevonden worden. Terwijl een andere 5.1.2e met toevallig dezelfde achternaam waarbij geen geboortedatum bekend is wel gevonden wordt.

De beperkte informatieverstrekking in vorderingen is een ander aandachtspunt waardoor passagiersgegevens eerder in het Wpg-Domein kunnen komen.
Wanneer een bevoegde instantie een vordering indient, geven ze in de meeste gevallen slechts een voornaam, achternaam en geboortedatum van het subject op. Mochten meer gegevens van het subject bekend zijn, en als die ook in de vordering staan, kan het mogelijk zijn dat er een beter resultaat uit TRIP komt. In TRIP is op tientallen karakteristieken te zoeken. De huidige werkwijze om beperkte gegevens van het subject in de vordering te gebruiken voor het vinden van een match met ongevalideerde passagiersgegevens vergroot de kans op het verstrekken van passagiersgegevens die een ander individu dan het subject betreffen. Deze passagiersgegevens komen daarmee eerder in het Wpg-domein.
Hoe vaak passagiersgegevens van een ander dan het gezochte subject in het Wpg-domein is mij niet bekend. Er is geen duidelijkheid over de kwaliteit van de verstrekte vermeende matches. Met andere woorden, hoeveel matches worden uiteindelijk een hit en alert.

3 Conclusie

Er zijn enkele aandachtspunten en het beschermen van persoonsgegevens kent altijd ruimte voor verbetering van de organisatorische en technische maatregelen. Ondanks het ontbreken van een basis op het gebied van het beschermen van persoonsgegevens, wordt er zo compliant mogelijk gewerkt. Het op orde brengen van de basis draagt bij aan een gestructureerde aanpak en planning in de lijn, zodat het management overzicht heeft in de risico's en de toe te passen maatregelen om te sturen.

4 Bijlage

4.1 2020 T3 Waarborgen voor de gegevensbescherming

Zie voor bijlage 1 bijgevoegde Pdf-bijlage. De nummering is niet opeenvolgend omdat alleen die waarborgen met een bevinding zijn opgenomen.

Toelichting op bijlage 1

In de waarborgen voor de gegevensbescherming bij de tertaalrapportage ga ik gedetailleerder in op de wettelijk waarborgen. Daarbij geef ik aan of PI-NL aan de organisatorische en technische waarborgen voor het beschermen van persoonsgegevens alsmede de wettelijke waarborgen voor de gegevensbescherming voldoet. De organisatorische en technische waarborgen worden door de opdrachtnemer, opdrachtgever en eigenaar vastgelegd. Zij zijn verantwoordelijk voor het opstellen van een normenkader aan de hand waarvan zij zelf de voortgang kunnen volgen.

De tertaalrapportage is gebaseerd op het toetsingskader van de FG. Elk tertaal wordt per waarborg de inhoud van de waarborg en de bevindingen beschreven. Aanvullend wordt met een stoplicht de status van de compliance (waarborg aanwezig), implementatie (waarborg uitgevoerd), bevinding (voorwaarde werkend in dit tertaal) aangeduid. Het stoplicht is als volgt opgebouwd:

Op hoofdlijnen voldaan	Groen
Niet geheel voldaan	Oranje
Niet voldaan	Rood
Niet vast te stellen / niet van toepassing	Grijs

De PNR-wet biedt diverse waarborgen voor de gegevensbescherming aan betrokkenen en de FG oefent daar intern toezicht op uit.

- Doelbinding (art. 2)
- Recht op eerbiediging van het privéleven, op bescherming van persoonsgegevens en op non-discriminatie (artt. 6 en 7)
- Toestemming officier van justitie (art. 10)
- Notificeren FG (art. 10 en 13)
- De waarborgen voor het beschermen van persoonsgegevens uit de Wet politiegegevens (hierna Wpg) zijn van overeenkomstige toepassing verklaard in de PNR-wet artikel 17 op de PNR-gegevens. Het gaat om de volgende onderdelen:
  - Juistheid en volledigheid gegevens (art. 4)
  - Gegevensbescherming door privacy by design en/of default (artt. 4a, 4b)
  - Gegevensbeschermingseffectbeoordeling (ook wel: GEB/DPIA/PIA) (art. 4c)
  - Autorisaties en toegang tot gegevens (artt. 6 en 6a)
  - Verstrekken aan derde landen (art. 17a)
  - Rechten van betrokkenen (artt. 24a tot en met 31a)
  - Audits (art. 33)
  - Datalekken (art. 33a)
  - Raadplegen Autoriteit Persoonsgegevens (art 33b)
  - Functionaris voor de gegevensbescherming (art. 36)
- Functionaris voor gegevensbescherming, contactpunt betrokkenen (art. 18)
- Depersonaliseren en verwijderen van persoonsgegevens (art. 20)
- Registreren en of documenteren verwerkingen (artt. 22 en 23)

A6a

Titel en verwijzing wetartikel	Nr.	Bevindingen functionaris gegevensbescherming TERTAAL 3 - 2020	Compliance (voorwaarde aanwezig)	Bestaan (voorwaarde uitgevoerd)	Werking (voorwaarde werkend in dit tertaal)	Management reactie verwerkingsverantwoordelijke TERTAAL 3 - 2020
Verwerking passagiersgegevens (art. 6 PNR) jo. AMVB Besluit gebruik PNR-gegevens voor de bestrijding van terroristische en ernstige misdrijven jo. artt. 4:3 en 4:6 Bpg	03.1	5.1.2.i [redacted]	✓	✓	!	
Verstrekking passagiersgegevens aan PIU (artt. 10 PNR jo. AMvB)	07.1	Aangegeven was dat er geen gebruik van de wettelijke mogelijkheid tot spontane verstrekkingen gemaakt zou worden. Dit tertaal zijn passagiersgegevens spontaan verstrekt aan een PIU. Deze verstrekking is niet in TRIP vastgelegd, noch is het proces in TRIP ingeregeld. Toezicht op de verstrekking heeft niet plaatsgevonden.	!	✗	✗	
Verstrekking passagiersgegevens aan PIU (artt. 10 PNR jo. AMvB) Noodzakelijk rechtstreeks verzoek van BIU (art.10 lid 4 PNR)	07.4	Aangegeven was dat er geen gebruik van de wettelijke mogelijkheid gemaakt zou worden waarbij een BI rechtstreeks een verzoek bij een PIU kan indienen. De BI zouden bij de eigen PIU verzoeken moeten indienen. Dit tertaal zijn passagiersgegevens verstrekt aan BIU's via BI's uit NL. Op basis van de beschikbare gegevens in TRIP is niet vast te stellen of dit bevoegde instanties conform de PNR-richtlijn zijn. Bij "Autoriteit" is de "landnaam" opgenomen en de vordering is naar een Nederlands template omgezet i.h.k.v. een internationaal rechtshulpverzoek. De EU heeft een lijst vastgesteld met aangewezen bevoegde instanties. Het is niet met zekerheid te zeggen dat er sinds 18.6.2019 alleen verstrekt is aan instanties die op deze lijst staan.	!	!	!	
Toestemming officier van justitie (art. 10 PNR)	08.1	Een aandachtspunt is toestemming in de mondelinge vordering bij dingende noodzaak. Dit gaat meestal goed, in een enkel geval geeft de OvJ achteraf aan geen toestemming te hebben gegeven en wordt achteraf geen schriftelijke vordering toegevoegd. Het proces is duidelijk en vastgesteld. Voor mondelinge vorderingen is een proces afgesproken waarbij binnen 72 uur een schriftelijke bevestiging moet zijn toegevoegd. De controle op het toevoegen van de bevestiging wordt in TRIP niet consistent in het overzicht weergegeven. Het overzicht is daarmee onbetrouwbaar en controle in de lijn en toezicht is inefficiënt. Bij 73 vordering uit 2020 (tot en met november) is de weergave niet goed vastgelegd. Voor de controle op de rechtmatigheid van deze vorderingen is het noodzakelijk dat de registratie juist is doorgevoerd in alle betreffende datavelden/pagina's.	✓	✓	!	
Notificeren FG (art. 10 en 13 PNR)	09.1	Dit tertaal waren er opnieuw problemen met de notificatie door fouten in de software en administratie. - De notificaties aan de FG bij een verstrekking aan 3e landen functioneerden niet als de gegevens <6mnd waren. - Daarnaast waren sommige 3e landen verkeerd geadministreerd. Aandachtspunt blijft dat bij het uitwerken van oplossing, door middel van een RfC/VTW, een integrale benadering wordt toegepast zodat de software op elk raakvlak juist is geprogrammeerd.	✓	!	!	
Doorgifte aan derde landen (art. 13 PNR jo. 17a Wpg)	12.1	In TRIP wordt op 2 plaatsen aangegeven dat een verzoek het een 3e land betreft. Deze 2 velden zijn niet altijd in lijn met elkaar. Mijn advies is om de software by default deze velden te koppelen.	✓	✓	!	

Titel en verwijzing wetartikel	Nr.	Bevindingen functionaris gegevensbescherming TERTAAL 3 - 2020	Compliance (voorwaarde aanwezig)	Bestaan (voorwaarde uitgevoerd)	Werking (voorwaarde werkend in dit tertaal)	Management reactie verwerkingsverantwoordelijke TERTAAL 3 - 2020
Verzoek PI-NL aan PIU (artt. 14, 15 en 16 PNR jo. 4a, 4b, 25 en 28 Wpg)	13.1	Het is voor een betrokkene niet te achterhalen of een PIU gegevens heeft verstrekt. Zo ja, of en welke gegevens PINL heeft doorgezet naar een BINL. Het vastleggen van de PIU-verstrekking in het passagiersdossier vindt niet plaatst. Daarmee is er ook geen logging van de verwerking vastgelegd, dit betreft ook het exporteren en downloaden van de gegevens.	✓	!	!	
Gegevensbescherming door privacy by design en/of default (artt. 17 PNR jo. 4a en 4b Wpg) Gegevensbescherming door beveiliging en ontwerp - noodzakelijkheid en rechtmatigheid Controle op de kwaliteit door verwerker en/of verwerkingsverantwoordelijke	16.4	Het uitvoeren van controle op de kwaliteit van de invoer van vorderingen bleef achter. Sinds T2 heeft extra aandacht voor de kwaliteitscontrole op het niveau van individuele vorderingen en verstrekkingen geleid tot minder fouten in de administratie in TRIP. De kans op het onjuist administreren van verstrekkingen en het onrechtmatig verstrekken is daardoor verminderd. De kwaliteit van de data, matches en verstrekkingen is verbonden met de ongevalideerde passagiersdata in TRIP. Dit kan onrechtmatige of overvloedige verstrekkingen (bv. een onjuiste Wei Zhang) in de hand werken omdat een zeer beperkt aantal gegevens gematcht kunnen worden.	✓	✓	!	
Gegevensbescherming door privacy by design en/of default (artt. 17 PNR jo. 4a en 4b Wpg) Gegevensbescherming door beveiliging en ontwerp - noodzakelijkheid en rechtmatigheid Privacy by design / default	16.7	Een VTW was niet goed uitgevoerd of een daaropvolgende bug niet goed gerepareerd. De zoekperiode was daarom te ruim. Mijn advies is om de pushdatum opnieuw te programmeren.	✓	✓	!	
Autorisaties en toegang tot passagiersgegevens (artt. 17 PNR jo. 6 en 6a Wpg jo. Samenwerkingsafspraken)	18.1	De autorisaties zijn nog niet aangepast en daarmee te ruim en niet o.b.v. need2know of need2do. Voorstel tot uitwisseling personeel PI-NL/FO geadviseerd als ze dit inrichten dat er aparte accounts worden gemaakt om vanuit te werken in VVA/TRIP zodat het onderscheid duidelijk zichtbaar is en blijft in de logging.	!	✗	✗	
Geheimhoudingsplicht (artt. 17 PNR jo. 7 Wpg)	20.1	5.1.2.i [redacted]	●	●	●	
Verstrekken aan derde landen (artt. 17 PNR jo. 17a Wpg en Besluit gebruik van passagiersgegevens voor de bestrijding van terroristische en ernstige misdrijven)	21.1	Internationale rechtshulpverzoeken werden geregistreerd als zijnde afkomstig van NL-BI, te weten de BI die het verzoek invoerde. Waar het verzoeken van 3e landen betrof zijn geen notificaties aan de FG verzonden waar het gegevens <6 maanden betrof. Matches n.a.v. geautomatiseerde vergelijking met de SIS2 database die door de FO aan een derde land worden doorgegeven, genereren momenteel geen notificatie aan de FG. Dit is feitelijk eenzelfde proces als bij het internationale rechtshulpverzoek.	✓	!	✗	
Verstrekken aan derde landen (artt. 17 PNR jo. 17a Wpg en Besluit gebruik van passagiersgegevens voor de bestrijding van terroristische en ernstige misdrijven)	21.2	In TRIP waren 3e landen foutief geadministreerd. Dit zou in T2 gerepareerd worden. De reparatie is niet goed uitgevoerd waardoor de documentatieplicht niet voldeed. De reparatie is in T3 niet of niet correct uitgevoerd.	✓	✓	!	

Titel en verwijzing wetartikel	Nr.	Bevindingen functionaris gegevensbescherming TERTAAL 3 - 2020	Compliance (voorwaarde aanwezig)	Bestaan (voorwaarde uitgevoerd)	Werking (voorwaarde werkend in dit tertaal)	Management reactie verwerkingsverantwoordelijke TERTAAL 3 - 2020
Datalekken (art. 17 PNR jo. 33a Wpg) De verwerkingsverantwoordelijke meldt een datalek binnen 72 uur na kennisname ervan aan de AP tenzij het niet waarschijnlijk is dat de inbreuk een risico voor de rechten en vrijheden van betrokkenen inhoudt.	24.1	Er zijn diverse incidenten voorgevallen. Uit de werkwijze rondom deze incidenten lijken taken, verantwoordelijkheden en bevoegdheden t.a.v. dit punt zijn nog niet uitgekristaliseerd.				
Functionaris voor gegevensbescherming (art. 18 PNR jo. 36 Wpg) Rapportage art. 18	26.2	In T3 is de art. 18 rapportage aangeboden aan de Minister, staten-generaal en AP.				
Functionaris voor gegevensbescherming (art. 18 PNR jo. 36 Wpg) Tijdig betrekken van FG	26.5	De FG lijkt onvoldoende betrokken te worden bij aangelegenheden die verband kunnen houden met het beschermen van persoonsgegevens. Daarnaast is er geen (governance) structuur ingericht waarbij de FG op bestuurlijk niveau contact heeft.				
Functionaris voor gegevensbescherming (art. 18 PNR jo. 36 en 6 Wpg) Autorisaties en beleid	26.7	Over het 4e kwartaal heb ik geen overzicht van de uitgegeven autorisaties ontvangen.				
Functionaris voor gegevensbescherming (art. 18 PNR jo. 36 Wpg) Bewust zijn en opleiden	26.8	PI-NL heeft i.h.k.v. kwaliteitsverbetering gewerkt aan opleidingen voor TRIp gebruikers van B&V.				
Functionaris voor gegevensbescherming (art. 18 jo. PNR o. 36 en 33 Wpg) Audits	26.9	De FG heeft nog geen resultaten van interne en/of privacy audits ontvangen en dus geen toezicht kunnen uitoefenen op de audits en of de aanbevelingen uit de audits worden uitgevoerd.				
Verwerkingsverbod op bijzondere passagiersgegevens (art. 19 PNR)	27.1	Onderzoek leert dat er nog bijzondere gegevens verwerkt worden en in TRIP staan o.a. het emailadres. Te denken valt aan @cnv.nl, @pvda.nl of 5.1.2e_VVD@hotmail De opdrachtnemer is hiervan op de hoogte gebracht en heeft hetzelfde in eigen onderzoek geconstateerd. Er is nog geen plan van aanpak teruggekoppeld om deze bijzondere persoonsgegevens te verwijderen en het verwerken ervan te staken.				
Depersonaliseren en verwijderen van passagiersgegevens (art. 20 PNR jo. 17 PNR en Wpg) Wissen verwerkingsresultaten en witte lijst	28.1	De verstrekkingsdocumenten worden niet na de beleidstermijn van 14/42 dagen verwijderd en blijven opvraagbaar en worden ook niet gedepersonaliseerd na 6 maanden. Opdrachtgever en Jurist PI-NL stelden vast dat verwijdering na 14/42 dagen zou moeten. In T1 2021 wordt naar dit verwachting met terugwerkende kracht hersteld In TRIP ontbreekt een overzicht van de diverse bewaartermijnen. Dit gebruikt de Douane wel en is nog niet aangepast voor PI-NL. Mijn advies is om dit onder anonimiseringsinformatie op te nemen net zoals voor de Douane.				
Depersonaliseren en verwijderen van passagiersgegevens (art. 20 PNR) Depersonaliseren van passagiersgegevens ouder dan 6 maanden	28.2	Bij de FG is onder de aandacht gebracht dat nog niet alle velden met passagiersgegevens >6mnd in TRIP worden gedepersonaliseerd. Bv bij reishistorie, notities, of PIU-verzoek de onderbouwing. Controle van de tekstvelden bij SSR codes liet zien dat deze gedepersonaliseerd zijn.				

Titel en verwijzing wetartikel	Nr.	Bevindingen functionaris gegevensbescherming TERTAAL 3 - 2020	Compliance (voorwaarde aanwezig)	Bestaan (voorwaarde uitgevoerd)	Werking (voorwaarde werkend in dit tertaal)	Management reactie verwerkingsverantwoordelijke TERTAAL 3 - 2020
Depersonaliseren en verwijderen van passagiersgegevens (art. 20 PNR jo. 4 Wpg) Verwijderen van (bijzondere) passagiersgegevens	28.3	Onderzoek leert dat er bijzondere gegevens verwerkt worden en in TRIP staan in o.a. het emailadres. Te denken valt aan @cnv.nl, @pvda.nl of 5.1.2e VVD@hotmail De opdrachtnemer is hiervan op de hoogte gebracht en heeft hetzelfde in eigen onderzoek geconstateerd. Er is nog geen plan van aanpak teruggekoppeld om deze bijzondere persoonsgegevens te verwijderen en het verwerken ervan te staken.	✓	!	✗	
Registreren en of documenteren verwerkingen (artt. 22 en 23 PNR) Register en documentatie	29.1	De FG heeft nog geen kennis kunnen nemen van het register.				
Registreren en of documenteren verwerkingen (artt. 22 en 23 PNR jo. 6 Wpg) Loggegevens van verwerkingen	29.2	Door het op een verkeerde wijze verstrekken van vluchtlijsten waren deze niet in de passagiersdossier gelogd.	✓	✓	!	
Registreren en of documenteren verwerkingen (artt. 22 en 23 PNR jo. 6 Wpg) Loggegevens van verwerkingen	29.3	Door het verstrekken van resultaten d.m.v. tussenkomst van DLIO wordt de verstrekking slechts 1 maal gelogd in het passagiersdossier, terwijl in de meeste gevallen zowel aan DLIO als aan de PIU wordt verstrekt. De inkomende verstrekkingen van een PIU wordt in zijn geheel niet gelogd in het passagiersdossier als deze aan de BI wordt verstrekt via TRIP.	✓	✓	!	
Registreren en of documenteren verwerkingen (artt. 22 en 23 PNR) Loggegevens	29.4	De logging van downloaden van documenten uit TRIP door gebruikers van PI-NL en de FG werd - na uitvoering van een andere VTW - niet meer vastgelegd. Hierdoor werd dit ook niet in het passagiersdossier geregistreerd. Dit heeft enkele maanden geduurd. Het vastleggen van de logging is uiteindelijk gerepareerd	✓	!	!	

A7

Ministerie van Justitie en Veiligheid

Dep. VERTROUWELIJK openbaar na publicatie
NCTV

Minister van Justitie en Veiligheid
Hoofddirectie Bedrijfsvoering

Turfmarkt 147
2511 DP Den Haag
Postbus 20301
2500 EH Den Haag
www.rijksoverheid.nl/jenv

Contactpersoon
5.1.2.e
Functionaris voor de gegevensbescherming voor de Passagiersinformatie-eenheid Nederland

M 5.1.2.e
5.1.2.e @minjenv.nl

Datum
18 augustus 2021

Bijlagen
2

memo

Toezicht op compliance

Beste 5.1.2.e,

In het kader van het toezicht op het naleven van de PNR-wet verzoek ik om bewijsmiddelen waaruit de compliance, op de waarborgen voor de gegevensbescherming, blijkt.

De vragen waarop voor het houden van toezicht antwoord gezocht staan in de bijlage. Voor het beantwoorden kan het bijgevoegde bestand ingevuld worden. Tevens verzoek ik om documenten waaruit compliance blijkt mee te zenden. Indien compliance alleen ter plaatse gecontroleerd kan worden, bv. in een applicatie, dan verzoek ik om een afspraak voor oktober in mijn agenda in te plannen.

De reactie zie ik graag uiterlijk 27 september aanstaande tegemoet.

Met vriendelijke groet,

5.1.2.e
Functionaris voor de gegevensbescherming
voor de Passagiersinformatie-eenheid Nederland

A7a

nr.	Titel en verwijzing wetartikel	Vragen m.b.t. accountability 2021 - augustus	Antwoord (Procesantwoord, inhoudelijk antwoord of verwijzing naar een document dat als bijlage wordt meegestuurd om compliance aan te kunnen tonen)
1	Doelbinding en doorwerking (artt. 2 jo. 9 lid 2 en 12 lid 2 PNR, 4 en 7 WPG, 1 PNR-richtlijn) Ernstige misdrijven en terrorisme o.g.v. bijlage 2	Hoe wordt de doelbinding gecontroleerd en gedocumenteerd? Bv. bij spoed-vorderingen Hoe kan een toezichthouder dat controleren? Hoe wordt de doorwerking van de doelbinding gecommuniceerd aan ontvangers? Waar is vastgelegd dat dit gecommuniceerd is? Wie controleert de doorwerking van de doelbinding?	
2	Push luchtvaartmaatschappij (art. 4 jo. 11 en bijlage 1 PNR en besluit pushtijden en besluit sancties, 4 WPG, art.8 lid 2 en OW 9 en 10 EU PNR-Richtlijn)	Hoe wordt de aanlevering van alle beschikbare passagiersgegevens (PNR&API) gecontroleerd op juistheid en volledigheid? Wie is verantwoordelijk voor het melden van gebreken/onjuistheden? Via welke methode kunnen beschikbare API-gegevens aangeleverd worden als dat niet via het single window TRIP kan?	
3	Doorgifte passagiersgegevens (art. 5 en bijlage 1 PNR)	Passagiersgegevens zijn samengesteld uit de PNR- en API-gegevens zoals is toegelicht in de memorie van toelichting. Hoe kan een toezichthouder controleren dat een verstrekking via DLIO tevens is verstrekt aan een PIU/Europol/BIU? Hoe worden de twee verstrekkingen aan DLIO en de PIU/Europol/BIU gelogd in het passagiersdossier? Wordt een negatief oordeel van DLIO gedocumenteerd? Zo ja, waar? Welke afspraken zijn er met DLIO gemaakt m.b.t. doelbinding, verwerken, wissen? Kan DLIO eerder ontvangen passagiersgegevens zelfstandig opnieuw verstrekken aan andere verzoekers? Hoe wordt geborgd dat CREW is uitgezonderd van verwerkingen?	
4	Verwerking passagiersgegevens (art. 6 PNR) jo. AMVB Besluit gebruik PNR-gegevens voor de bestrijding van terroristische en ernstige misdrijven jo. artt. 4.3 en 4.6 Bpg en 4 lid 2 PNR-Richtlijn)	Hoe is in de lijn geborgd dat de passagiersgegevens alleen conform wet worden verwerkt? Hoe is de controle in de 1e en 2e lijn geborgd? Op welke plaatsen/ in welke systemen worden passagiersgegevens bij een spontane verstrekking of ontvangt van een spontane verstrekking opgeslagen/verwerkt? Waar kan de FG dit controleren? Waar is dit proces vastgesteld en vastgelegd?	
5	Beoordelingscriteria (artt. 6 jo. 7, 19 en 20 PNR en OW 7 richtlijn) Objectieve criteria en menselijke toets	Hoe kan een toezichthouder controleren of een objectieve toets heeft plaatsgevonden? Is de toets herhaalbaar met gelijke uitkomst? Zo ja, waar wordt dat gedocumenteerd? Hoe kan een toezichthouder controleren welke matches er waren en welke verstrekt zijn? Wat zijn de foutmarges? Wie stelt die vast en met welke methode? Wie houdt tijdens de operatie controle op de foutmarges? Hoe wordt de objectiviteit gewaarborgd? Waar is dat geborgd? Wordt rekening gehouden dat transparantie over de criteria incl. foutmarge aan betrokkene gegeven zou moeten worden?	
6	Beoordelingscriteria (artt. 6 jo. 7, 19 en 20 PNR) Beperkt verwerken persoonsgegevens	Hoe wordt geborgd en gecontroleerd dat er geen bijzondere persoonsgegevens worden verwerkt in criteria? Hoe wordt geborgd en gecontroleerd uit welke periode passagiersgegevens gebruikt worden voor testen bv. de grenspassagedatum? Waar is dat geborgd en gedocumenteerd?	
7	Menselijke toets bij geautomatiseerd vergelijken (artt. 6 jo. 8 PNR en 4a en 4b Wpg, 4.3 en 4.6 Bpg jo 13 lid 1 subs a en d en 18 Wpg)	Hoe is het uitvoeren van de menselijke toets geborgd in de lijn en gedocumenteerd/gelogd? Hoe kan een toezichthouder controleren of de menselijke toets is uitgevoerd? (zie ook bovenstaande vragen)	
8	Menselijke toets bij geautomatiseerd vergelijken (artt. 6 jo. 8 PNR en 4a en 4b Wpg, 4.3 en 4.6 Bpg jo.13 lid 1 subs a en d en 18 Wpg)	Voor autorisaties zie daar. Voor kennis en vaardigheden zie daar	
9	Menselijke toets bij geautomatiseerd vergelijken (art. 6 jo. 1 PNR en Besluit aanwijzing van de SIS II-databank)	Vanaf wanneer zijn de SIS-verstrekkingen gedaan? Wat heeft bureau sirene met de sis-verstrekkingen gedaan omdat ze in eerste instantie niet wilde doorgeven? Hoeveel sis-verstrekkingen zijn gedaan aan bureau sirene en hoeveel zijn door bureau sirene doorgegeven? Hoe kan een toezichthouder controleren of een match op doelbinding bij bureau sirene is gecontroleerd? Waar wordt die doelbindingscheck gedocumenteerd?	
10	Verstrekking resultaat PIU rechtstreeks aan BI (artt. 9a jo 9 PNR)	Hoe en waar wordt gedocumenteerd dat er een PIU-notificatie met het verzoek van de BI is ontvangen? Waar worden de via de BI ontvangen PIU-passagiersgegevens vastgelegd? Hoe wordt dit in het passagiersdossier gelogd? Welke afspraken zijn er met de BI'en / PIU's gemaakt?	

nr.	Titel en verwijzing wetartikel	Vragen m.b.t. accountability 2021 - augustus	Antwoord : (Procesantwoord, inhoudelijk antwoord of verwijzing naar een document dat als bijlage wordt meegestuurd om compliance aan te kunnen tonen)
11	Verstrekking passagiersgegevens aan PIU (artt. 10 PNR jo. AMvB DLIO en art. 31 EU-Europol verordening) Spontaan	Hoe wordt een spontane verstrekking / spontaan ontvangen passagiersgegeven gedocumenteerd? Hoe wordt dit in het passagiersdossier vastgelegd? Welke afspraken zijn er met DLIO gemaakt m.b.t. doelbinding, verwerken, wissen?	
12	Verstrekking passagiersgegevens aan PIU (artt. 10 lid 1, 2 en 4 en art. 8 lid 2 PNR jo. AMvB Besluit gebruik PNR-gegevens voor de bestrijding van terroristische en ernstige misdrijven)	Welke afspraken zijn er met DLIO gemaakt m.b.t. doelbinding, verwerken, wissen? Hoe en waar wordt het advies van DLIO gedocumenteerd? Hoe is DLIO geïnformeerd over de doorwerking van de doelbinding? Hoe is de lijn controle op de doorwerking van de doelbinding geregeld?	
13	Verstrekking passagiersgegevens aan PIU (artt. 10 PNR jo. AMvB DLIO) opheffen depersonaliseren	Welke afspraken zijn er met PIU's gemaakt m.b.t. verstrekken gegevens gepersonaliseerd >6 mnd? Wat als een PIU standaard geen gegevens gepersonaliseerd >6 mnd verstrekt?	
14	Verstrekking passagiersgegevens aan BIU (artt. 10 lid 4 PNR jo. AMvB DLIO) Rechtstreeks verzoek	Zie art. 9a (spiegelbepaling). Waar wordt vastgelegd dat er een notificatie met het verzoek van de BIU verzonden is aan de PIU? Welke afspraken zijn er met de BI'en / PIU's gemaakt?	
15	Toestemming officier van justitie (art. 10 PNR)	Hoe wordt de toestemming van de OvJ bij spoedvorderingen gecontroleerd en tijdig toegevoegd? Hoe is de lijncontrole hierop ingericht? Hoe kan een toezichthouder efficient controleren of de toestemming van de OvJ geformaliseerd is? Welke afspraken zijn er met DLIO en of het OM gemaakt t.a.v. Europol?	
16	Notificeren FG (art. 10 en 13 jo. 18 PNR)	Hoe kan de FG toezicht houden en vastleggen m.b.t. filters, sis-verstrekkingen en watchlisten?	
17	Extra Push luchtvaartmaatschappij (art. 11 PNR en OW 9 en 10 PNR richtlijn)	Hoe wordt de extra push gelogd? Hoe kan een toezichthouder de extra push controleren?	
18	Verstrekken aan Europol (art. 12 PNR jo. 5:7 Bpg jo AMvB DLIO)	Welke afspraken zijn er met DLIO gemaakt bv. doelbinding, verwerken, wissen?	
19	Doorgifte aan derde landen (artt. 13 lid 1 sub a PNR jo 17a Wpg en OW 31, 39, 40 PNR richtlijn en art 542 lid 1 en 4 EU-HSO algemeen	Welke afspraken zijn er met DLIO gemaakt bv. doorzetten verzoek, doelbinding instemmen 3e land op de voorwaarden? Welke afspraken zijn er met ENU gemaakt over het gebruik van 5.1.2 i	
20	Doorgifte aan derde landen (artt. 13 jo. 17 PNR en 17a Wpg en Besluit gebruik van passagiersgegevens voor de bestrijding van terroristische en ernstige misdrijven jo. HSO) Voorwaarden	Welke afspraken zijn gemaakt met DLIO?	
21	Doorgifte aan derde landen (artt. 13 jo. 17 PNR en 17a Wpg en Besluit gebruik van passagiersgegevens voor de bestrijding van terroristische en ernstige misdrijven jo. HSO) Documentatieplicht	Hoe wordt de documentatieplicht vastgesteld en gecontroleerd?	
22	Doorgifte aan derde landen (artt. 13 PNR jo. 17a Wpg en 5:1 lid 3 Bpg) ontbreken voorafgaande toestemming PIU	Hoe wordt de toestemming van de PIU gelogd? Welke afspraken zijn hierover met DLIO gemaakt?	
23	Doorgifte aan derde landen (artt. 13 jo. 17 PNR en 17a Wpg en Besluit gebruik van passagiersgegevens voor de bestrijding van terroristische en ernstige misdrijven) Doorverstrekken	Hoe en waar wordt de toestemming van de ontvanger t.a.v. de voorwaarden van ontvangst vastgelegd? Hoe en waar wordt de notificatie aan de PIU vastgelegd?	
24	Doorgifte aan derde landen - UK (artt 13 PNR jo 542 lid 1 en 4 HSO met de UK Deel 3 Titel 3 n.a.v. Brexit)	Welke afspraken zijn er met DLIO gemaakt?	

nr.	Titel en verwijzing wetartikel	Vragen m.b.t. accountability 2021 - augustus	Antwoord (Procesantwoord, inhoudelijk antwoord of verwijzing naar een document dat als bijlage wordt meegestuurd om compliance aan te kunnen tonen)
25	Verzoek PI-NL aan PIU (artt. 14, 15 en 16 PNR jo. 4a, 4b, 25 en 28 Wpg)	Hoe en op welke wijze worden verstrekking vastgelegd t.b.v. art. 25 lid 1 sub c Wpg?	
26	Doorgifte aan derde landen - UK (artt. 13 PNR jo. 543 sub c jo. 546 HSO met de UK n.a.v. Brexit)	zie art 9a. PIU	
27	Verzoek PI-NL aan PIU (artt. 14, 15 en 16 jo. 4 PNR)	Hoe wordt de extra push gelogd? Hoe kan een toezichthouder de extra push controleren? Hoe wordt dit in het passagiersdossier gedocumenteerd?	
28	Doorgifte aan derde landen - UK (art 13 PNR jo. 546 lid 6 HSO met de UK n.a.v. Brexit) noodzakelijke minimum	Hoe is dit in de praktijk geborgd? Wat wordt verstaan onder het noodzakelijke minimum? Waar is dat vastgelegd?	
29	Verzoek BI aan PIU (artt. 14, 15 en 16 PNR jo. 4a, 4b, 25 en 28 Wpg)	Hoe worden de verzoeken en het antwoord van de PIU gelogd in het passagiersdossier?	
30	Juistheid en volledigheid passagiersgegevens (artt. 17 PNR jo. 4 Wpg en 1, 5, 6, 20 PNR) Doelbinding, bewaartermijn, waarborgen, kennisgeving onjuiste verstrekking	Wie voert de interne kwaliteitscontrole in de 1e en 2e lijn uit bij IBO en PINL op Doelbinding, rechtmatigheid, bewaartermijnen, organisatorische en technische waarborgen? Hoe is het proces om de ontvanger te informeren over onjuist verstrekte of op onrechtmatige wijze verstrekte passagiersgegevens?	
31	Juistheid en volledigheid passagiersgegevens (artt. 17 PNR jo. 4 Wpg) Juistheid, classificatie gegevens	Hoe zijn de passagiersgegevens geclassificeerd? Hoe wordt dat in [redacted] vastgelegd? Zijn er passagiersgegevens gebaseerd op een persoonlijk oordeel? Hoe worden API-data aangeleverd? Hoe wordt de juistheid gecontroleerd? Hoe worden de passagiersgegevens, vorderingsgegevens en of gebruikersgegevens geclassificeerd?	
32	Juistheid en volledigheid passagiersgegevens (artt. 17 PNR jo. 4 Wpg en 20 PNR) Loggegevens, register	Wie hebben toegang tot de logging van verwerkingen? Waar is dat vastgelegd? Hoe is dat geborgd?	
33	Gegevensbescherming door privacy by design en/of default (artt. 17 PNR jo. 4.d en 4b Wpg) Gegevensbescherming door beveiliging en ontwerp - noodzakelijkheid en rechtmatigheid Technische en organisatorische maatregelen	Welke technische en of organisatorische maatregelen zijn er?	
34	Gegevensbescherming door privacy by design en/of default (artt. 17 PNR jo. 4a, 4b, 24 Wpg en 10 en 18 PNR en 6 samenwerkingsafspraken TRIP 2019) Rechten betrokkenen, intern toezicht, DPIA	Welke informatie kan betrokkene over verwerkingen van de eigen passagiersgegevens ontvangen? Hoe worden verwerkingen van passagiersgegevens bij de FG aangemeld? Hoe is het toezicht op verwerkingen van passagiersgegevens binnen de technische voorziening geregeld? Wanneer wordt een DPIA uitgevoerd?	
35	Gegevensbescherming door privacy by design en/of default (artt. 17 PNR jo. 4a en 4b Wpg en 20 PNR) Need-to-know/have/do	Hoe is de autorisatie geregeld zodat alleen die passagiersgegevens verwerkt worden die voor dat doel noodzakelijk zijn? Wie houdt daar in de lijn controle op? Hoe is dit in de autorisatie ingeregeld? Welke technische en organisatorische maatregelen zijn gedefinieerd en of geïmplementeerd?	
36	Gegevensbescherming door privacy by design en/of default (artt. 17 PNR jo. 4a en 4b Wpg) Kwaliteitscontrole	Wie controleert de kwaliteit van de passagiersgegevens? Waar is dat vastgelegd? Wat is de procedure als de kwaliteit niet voldoet?	
37	Gegevensbescherming door privacy by design en/of default (artt. 17 PNR jo. 4a en 4b Wpg) Risico analyse	Wie voert de risico analyse uit? Is er een systeem om risico mitigerende maatregelen systematisch en periodiek te evalueren, risico's te identificeren en adresseren tegen ongeoorloofde en of onrechtmatige toegang en of verwerking? Wie stelt de risico analyse en mitigerende maatregelen vast?	
38	Gegevensbescherming door privacy by design en/of default (artt. 17 PNR jo. 4a en 4b Wpg) Gegevensbeschermingsbeleid-	Wie stelt het gegevensbeschermingsbeleid vast? Indien aanwezig ontvang ik graag een kopie van het vastgestelde beleid en een overzicht waar en hoe de technische en of organisatorische maatregelen zijn geïmplementeerd	

nr.	Titel en verwijzing wetartikel	Vragen m.b.t. accountability 2021 - augustus	Antwoord (Procesantwoord, inhoudelijk antwoord of verwijzing naar een document dat als bijlage wordt meegestuurd om compliance aan te kunnen tonen)
39	Gegevensbescherming door privacy by design en/of default (artt. 17 PNR jo. 4a en 4b Wpg) Privacy by design / default	Hoe en waar wordt privacy by default/design geborgd?	
40	Gegevensbescherming door privacy by design en/of default (artt. 17 PNR jo. 4a en 4b Wpg) Verantwoordingsplicht	Hoe wordt voldaan aan de verantwoordingsplicht m.b.t. privacy by design/default?	
41	Gegevensbescherming door privacy by design en/of default (artt. 17 PNR jo. 4a en 4b Wpg) Tussenkomst natuurlijke persoon	Hoe is de bescherming bij alle geautomatiseerde verwerkingen geregeld dat passagiersgegevens alleen via tussenkomst van een natuurlijke persoon toegankelijk zijn?	
42	Gegevensbeschermingseffectbeoordeling (DPIA/GEB) (art. 17 PNR jo. 4c Wpg) DPIA	Wie controleert of passagiersgegevens volgens de DPIA verwerkt worden? Is er een DPIA voor het aansluiten van de [redacted] databank?	
43	Autorisaties en toegang tot passagiersgegevens (artt. 17 PNR jo. 6 en 6a Wpg jo. Samenwerkingsafspraken) Randvoorwaarden	Waar zijn de voorwaarden voor een autorisatie voor TRIP vastgelegd? Wat zijn die voorwaarden? Zijn de autorisaties gebaseerd op basis van need-to-know/do? Hoe verloopt het proces voor het toewijzen, wijzigen of intrekken van de autorisaties?	
44	Autorisaties en toegang tot passagiersgegevens (artt. 17 PNR jo. 6 en 6a Wpg jo. Samenwerkingsafspraken) 1e en 2e lijns controle	Wie houden eerste en of tweede lijns controle op de autorisaties?	
45	Verwerker (artt. 17 PNR jo. 6c Wpg) Voorwaarden	Zijn de voorwaarden opgenomen in de afspraken?	
46	Verwerker (artt. 17 PNR jo. 6c Wpg) Subverwerker	Zijn er subverwerkers ingeschakeld? Zo ja, welke?	
47	Verwerker (artt. 17 PNR jo. 6c Wpg) Verantwoordingsplicht	Hoe voldoet de (sub)verwerker aan de verantwoordingsplicht?	
48	Geheimhoudingsplicht (artt. 17 PNR jo. 7 Wpg) Doelgroep	Hoe worden gebruikers en ontvangers van passagiersgegevens gehouden aan en of gewezen op hun geheimhoudingsplicht? Is daarvan een voorbeeld beschikbaar? Zijn gebruikers van passagiersgegevens bekend met de consequenties als ze de plicht schenden? Zo ja, hoe is dat vastgelegd?	
49	Geheimhoudingsplicht (artt. 17 PNR jo. 7 Wpg en 1 PNR) Doelbinding	Zie bovenstaand	
50	Geheimhoudingsplicht (artt. 17 PNR jo. 7 Wpg jo. 6.4 Bpg en 20 PNR) Loggegevens	Is voldaan aan de documentatieplicht? Zo ja, kan de documentatie effectief gebruikt worden voor controle in 1e, 2e en 3e lijn en toezicht?	
51	Rechten van betrokkenen (artt. 17 PNR jo. 24b Wpg jo. 25 en 28 Wpg en Samenwerkingsafspraken TRIP 2019) Informatie aan betrokkene	Hoe worden betrokkenen wiens passagiersgegevens zonder hun medeweten worden verzameld geïnformeerd over het bestaan van geautomatiseerde besluitvorming?	
52	Rechten van betrokkenen (artt. 17 PNR jo. 24b Wpg en OW 29 PNR richtlijn) Motiveren informatie aan betrokkene	zie bovenstaand	

nr.	Titel en verwijzing wetartikel	Vragen m.b.t. accountability 2021 - augustus	Antwoord (Procesantwoord, inhoudelijk antwoord of verwijzing naar een document dat als bijlage wordt meegestuurd om compliance aan te kunnen tonen)
53	Rechten van betrokkenen (artt. 17 PNR jo. 25 en 27 Wpg en OW 28 PNR richtlijn) Rechten betrokkene	Hoe kan de FG verzoeken snel doorgeven aan PI-NL? Hoe kan de FG het besluit op verzoek incl. passagiersgegevens tijdig doorgeven aan de verzoeker? Rekening houdend met de termijnen en zonder dat de FG dagelijks of wekelijks op een beveiligde locatie werkt. De FG werkt parttime.	
54	Rechten van betrokkenen (artt. 17 PNR jo. 26 Wpg) Vaststellen identiteit, machtiging	Hoe en waar worden betrokkenen geïnformeerd over deze voorwaarde? Hoe kan een betrokkene veilig voldoen aan deze voorwaarde?	
55	Rechten van betrokkenen (artt. 17 PNR jo. 27, 25 en 28 Wpg) Afwijzen rechten betrokkenen	Wie beslaat of een verzoek wordt afgewezen?	
56	Rechten van betrokkenen (artt. 17 PNR jo. 28 Wpg en OW 28 PNR richtlijn) Recht op rectificatie en vernietiging	Hoe wordt rectificatie, beperken van verwerkingen of wissen van passagiersgegevens gedocumenteerd? Hoe wordt de wijziging bij het terugplaatsen van een back-up behouden?	
57	Rechten van betrokkenen (artt. 17 PNR jo. 29, 24a en 31a Wpg) Beroep AP en Awb	Hoe wordt de betrokkene over het beroep en klachtrecht geïnformeerd? Hoe en waar is die gegeven informatie terug te vinden?	
58	Rechten van betrokkenen (artt. 17 PNR jo. 29 Wpg) Ombudsman	Hoe en waar wordt een eventuele verstrekking van passagiersgegevens aan de Ombudsman en haar eventuele medewerkers vastgelegd? Hoe wordt dat in het passagiersdossier gedocumenteerd?	
59	Audits (art. 17 PNR jo. 33 Wpg en art 6.5 leden 1 en 5 Bpg en de Regeling Periodieke Audit passagiersgegevens en art. 9 Samenwerkingsafspraken TRIP 2019) Privacy audit	Hoe is de uitvoering van privacy audits geborgd? Wat is het auditplan? Hoe is geborgd dat de FG toezicht kan houden op de uitvoering van privacy audits en eventuele hercontroles? Waar worden auditdocumenten gedocumenteerd?	
60	Audits (art. 17 PNR jo. 33 Wpg en art 6.5 leden 1 en 5 Bpg en de Regeling Periodieke Audit passagiersgegevens en art. 9 Samenwerkingsafspraken TRIP 2019) Interne audit	Hoe is de uitvoering van interne audits geborgd? Wat is het auditplan? Hoe is geborgd dat de FG toezicht kan houden op de uitvoering van interne audits en eventuele hercontroles?	
61	Datalekken (art. 17 PNR jo. 33a Wpg) Cyclus	Wie is verantwoordelijk voor het detecteren van incidenten? Hoe wordt gemonitord of er potentiele incidenten zijn? Zijn alle betrokkenen in dit proces op de hoogte van hun taken, verantwoordelijkheden en bevoegdheden? Waar worden incidenten gedocumenteerd? Hoe en waar is geborgd dat de FG toezicht kan houden en de status van incidenten kan volgen?	
62	Datalekken (art. 17 PNR jo. 33a Wpg) Informatieplicht	Hoe is de communicatie aan betrokkenen en of data-eigenaar geregeld? Hoe is geborgd dat de FG tijdig geïnformeerd is?	
63	Raadplegen Autoriteit passagiersgegevens (art. 17 PNR jo. 33b en 4c Wpg) Voorafgaande raadpleging voorgenomen risicovolle verwerking	Wat is het afwegingskader om tot een voorafgaande raadpleging tot een voorgenomen risicovolle verwerking over te gaan? Wie neemt die beslissing?	
64	Functionaris voor gegevensbescherming (art. 18 PNR jo. 36 Wpg)	Hoe is het benoemingsproces geborgd? Hoe en door wie wordt de FG aangemeld bij de AP?	

nr.	Titel en verwijzing wetartikel	Vragen m.b.t. accountability 2021 - augustus	Antwoord (Procesantwoord, inhoudelijk antwoord of verwijzing naar een document dat als bijlage wordt meegestuurd om compliance aan te kunnen tonen)
65	Functionaris voor gegevensbescherming (art. 18 PNR jo. 36 Wpg) Intern toezicht	Hoe is geborgd dat de FG tijdig geïnformeerd wordt over alle zaken die de verwerking van persoonsgegevens kunnen raken? Wat is het taakgebied van de FG? Welke voorwaarden zijn gesteld aan de deskundigheid van de FG? Hoe is geborgd dat de FG toegang heeft tot documentatie met betrekking tot de gegevensbescherming van passagiersgegevens, het toewijzen van autorisaties, registers, registraties, technische en organisatorische waarborgen voor het beschermen van passagiersgegevens? Hoe is geborgd dat de FG de benodigde middelen (financiën en systemen) ter beschikking heeft?	
66	Functionaris voor gegevensbescherming (art. 18 PNR jo. 36 Wpg) Rapportage art. 18	Hoe is geborgd dat de FG de rapportage tijdig aan ontvangers kan aanbieden?	
67	Functionaris voor gegevensbescherming (art. 18 PNR jo. 36 Wpg) Contactpunt	Hoe kan de FG contacten met betrokkenen efficiënt afhandelen en vastleggen? Hoe kan de FG voldoen aan verzoeken van betrokkenen om via een beveiligde omgeving ID-bewijs en of passagiersgegvens uit te wisselen?	
68	Functionaris voor gegevensbescherming (art. 18 PNR jo. 36 Wpg) Toegang gegevens	Hoe is de toegang van de FG tot alle passagiersgegevens - van ontvangst tot wissen/verwijderen - geborgd? Hoe en waar is het toezicht op het verwerken van passagiersgegevens door IBO geborgd?	
69	Functionaris voor gegevensbescherming (art. 18 PNR jo. 36 Wpg) Tijdig betrekken van FG	Hoe is geborgd dat de FG gefaciliteerd is om adviezen voor te kunnen bereiden en daarvoor tijdig en naar behoren betrokken is bij alle aangelegenheden die verband houden met het beschermen van persoonsgegevens?	
70	Functionaris voor gegevensbescherming (art. 18 PNR jo. 36 Wpg) Toezicht op compliance	Hoe wordt de FG gefaciliteerd in het uitoefenen van het toezicht?	
71	Functionaris voor gegevensbescherming (art. 18 PNR jo. 35 en 6 Wpg) Autorisaties en beleid	Hoe wordt de FG gefaciliteerd in het uitoefenen van toezicht op uitgegeven autorisaties en het beleid?	
72	Functionaris voor gegevensbescherming (art. 18 PNR jo. 36 Wpg) Bewust zijn en opleiden	Hoe wordt de FG gefaciliteerd in het toezicht op opleiden en bewust maken van medewerkers	
73	Functionaris voor gegevensbescherming (art. 18 jo. PNR o. 35 en 33 Wpg. 6 5 Bpg en Regeling periodieke audits) Audits	Zie bovenstaand	
74	Verwerkingsverbod op bijzondere passagiersgegevens (art. 19 PNR en OW 15 en 20 PNR richtlijn)	Hoe is geborgd bijzondere passagiersgegevens niet verwerkt worden? Hoe worden deze passagiersgegevens gewist en wie houdt daar in de lijn controle op? Wie controleert of er geen bijzondere persoonsgegevens aanwezig zijn of verwerkt worden? Wie is verantwoordelijk wanneer er bijzondere persoonsgegevens verwerkt worden of aanwezig zijn?	
75	Depersonaliseren en verwijderen van passagiersgegevens (art. 20 PNR) Depersonaliseren van passagiersgegevens	Hoe en waar wordt bij een verzoek van Europol de toestemming van de OvJ vastgelegd? Hoe en waar is vastgelegd of en zo ja in welk geval voor een risicocriteria set gegevens ouder dan 6 maanden gedepersonaliseerd en of gepersonaliseerd mogen worden gebruikt?	
76	Depersonaliseren en verwijderen van passagiersgegevens (art. 20 PNR jo. 4 Wpg en art. 31 EU Europol verordening) Wissen	Welke bewaartermijnen zijn vastgesteld? Wie controleert het naleven van de bewaartermijnen? Welke organisatorische en technische waarborgen zijn er?	

nr.	Titel en verwijzing wetartikel	Vragen m.b.t. accountability 2021 - augustus	Antwoord (Procesantwoord, inhoudelijk antwoord of verwijzing naar een document dat als bijlage wordt meegestuurd om compliance aan te kunnen tonen)
77	Registreren en of documenteren verwerkingen (artt. 22 en 23 PNR) Register en documentatie	Is er een register? Zo ja, waar bevindt het register zich? Hoe kan een toezichthouder dat register inzien en controleren?	
78	Registreren en of documenteren verwerkingen (artt. 22 en 23 PNR jo. 6 Wpg en OW 37 PNR richtlijn) Loggegevens van verwerkingen	Wie controleert of de documentatie de juiste gegevens bevat en functioneert? Wie stelt de autorisatie tot de loggegevens van verwerkingen vast?	
79	Registreren en of documenteren verwerkingen (artt. 22 en 23 PNR) Documentatieplicht	Wie controleert het functioneren van de logging? Waar is dat vastgelegd? Wie controleert de integriteit, beveiliging en vertrouwelijkheid van de passagiersgegevens? Hoe wordt die controle vastgelegd?	

A8

Ministerie van Justitie en Veiligheid

Dep. VERTROUWELIJK openbaar na publicatie
5.1.2e PI-NL
5.1.2e PI-NL

Beveiligingsautoriteit
Ministerie van Justitie en Veiligheid

Turfmarkt 147
2511DP Den Haag
Postbus 20301
2500EH Den Haag
www.rijksoverheid.nl/jenv

Datum
4 augustus 2020

Projectnaam
RCS

Ons kenmerk
0

nota

Bevindingen FG PINL n.a.v. Evaluatie inzet risico criteria
Refnr.: 5.1.2.i

Bevindingen

De documenten met betrekking tot de evaluatie gelezen hebbende kom ik tot de volgende hoofd bevindingen en/of vragen:

- Heeft de commissie voldoende tijd gehad om de evaluatie tot zich te kunnen nemen?
- Wat heeft het analyse team van de BI bijgedragen aan de evaluatie?
- Is bij het uitvoeren de juiste de grondslag voor handelingen vastgesteld en/of besproken en zo wat is de grondslag?
- Zijn er WPG gegevens uitgewisseld?

A. Naar aanleiding van de evaluatie d.d. 12.03.2020

1. Bij het geautomatiseerde vergelijken is de tussenkomst door middel van een menselijke toets verplicht. In de documenten is de menselijke toets niet beschreven. Heeft deze toets plaatsgevonden? Zo ja, hoe is die geborgd?
2. RCS moeten objectief zijn en op wetenschappelijke methoden gestoeld. Hoe is dat geborgd bij het analyseren van een 5.1.2.i en gebruikmakend van de karakteristieken die de BI aandraagt?
   De aanwezigheid van de database TRIP biedt de mogelijkheid om passagiersgegevens te analyseren en op die wijze eventueel karakteristieken te 'vinden' die de BI nog niet heeft ontdekt.
3. De looptijd van de RCS levert het vraagstuk op dat een 1e push gefilterd wordt van een vlucht die na de looptijd van het filter landt. Wat wordt de definitie van de looptijd van een filter?
4. 5.1.2.i

Beveiligingsautoriteit
Ministerie van Justitie en Veiligheid
Ministerie Binnenlandse Zaken en Koninkrijksrelaties

Datum
4 augustus 2020

Ons kenmerk
0

5. 5.1.2.i B&V kan als zij een menselijke toets uitvoeren bepalen dat het een match is en de PNR-gegevens verstrekken. Waarom is dat in dit geval niet gebeurd?
6. De meeste matches vonden in de eerste week van de looptijd plaats. Is hier een verklaring voor?
7. 5.1.2.i wat is dan de toegevoegde waarde van deze RCS? Is dat een voldoende rechtvaardiging voor het doorgeven van persoonsgegevens?
8. 5.1.2.i
9. Bevat de uitgewisselde informatie Wpg-gegevens en/of tot de persoon herleidbare gegevens? Wat is de grondslag voor de uitwisseling van WPG-gegevens en/of informatie uit verklaringen? Is de uitwisseling geautoriseerd en zo ja door wie?
10. Zijn de bevindingen per vlucht gebaseerd op WPG-gegevens en/of gegevens uit verklaringen van reizigers?
11. 5.1.2.i Wat was hier de grondslag voor? Is dit onderdeel van het RCS, het RCS-proces of de afspraken? Zo ja hoe en waar is dat besluit geborgd?
12. 5.1.2.i . Wat was hier de grondslag voor? Is dit onderdeel van het RCS, het RCS-proces of de afspraken? Zo ja hoe en waar is dat besluit geborgd? Is die uitkomst met de BI gedeeld en op welke grondslag?
13. Tabel 3 mocht die opgenomen worden? Zijn dit echte gegevens?
14. Er staat dat "meer informatie uit de praktijk ....meer inzicht zou kunnen geven", bv. na daadwerkelijke controle van de passagier. Wat zou de grondslag zijn voor de BI om deze gegevens met PINL te delen?
15. Is de BI de verplichting nagekomen om alle verstrekkingen aan nader onderzoek te onderwerpen?
16. In hoeverre zijn de karakteristieken die voor de BI leiden tot "geen indicatie" mogelijke uitsluitingsgronden om in het filter op te nemen?
17. Er wordt geschreven over een "mogelijkheid in TRIP" maar dat die niet voldoet en de karakteristiek zou moeten worden bezien. Over welke mogelijkheid gaat het? Wat zou die optie betekenen voor het beschermen van persoonsgegevens?
18. Met betrekking tot het delen van de reishistorie door PINL met de BI opnieuw de vragen t.a.v. de grondslag. Maakt de reishistorie deel uit van de te verstrekken PNR-gegevens? Is dit onderdeel van het RCS, het RCS-proces of de afspraken? Zo ja hoe en waar is dat besluit geborgd?
19. 5.1.2.i

Beveiligingsautoriteit
Ministerie van Justitie en Veiligheid
Ministerie Binnenlandse Zaken en Koninkrijksrelaties

Datum
4 augustus 2020

Ons kenmerk
0

5.1.2.i

20. 5.1.2.i

5.1.2.i

21. Terugkoppeling door BI aan PINL is niet opgenomen in de rapportage inzet risico criteria dd. 06.01.2020. Wat zijn de afspraken en wie heeft die geautoriseerd? Wat is de grondslag? Wat voor gegevens worden uitgewisseld? In hoeverre is het aan PINL om dat uit te zoeken? Wat is de taak van het team Analyse van de BI ten behoeve van de evaluatie van de RCS? 5.1.2.i

22. Wat houdt het in dat er nauwkeuriger moet worden teruggekoppeld? Kan ik een kopie van het template voor de terugkoppeling ontvangen? Dit zat niet als bijlage bij de evaluatie.
23. De kwaliteit van de passagiersgegevens wordt terecht ter discussie gesteld. Het is een gegeven dat bekend was bij het opstellen van de richtlijn. Hoe gaat PINL hier mee om?
24. 5.1.2.i

Wat is het effect op het aantal verstrekkingen?

25. 5.1.2.i

5.2.1

26. Tekstueel: passagiers worden m.i. niet geclassificeerd maar de passagiersgegevens wel.
27. Inhoudelijk: 5.1.2.i
28. Wat is de classificatie van de evaluatie?

B. Naar aanleiding van het verslag van de commissie d.d. 16.03.2020

1. In hoeverre is de samenstelling juist? 5.2.1

Beveiligingsautoriteit
Ministerie van Justitie en Veiligheid
Ministerie Binnenlandse Zaken en Koninkrijksrelaties

Datum
4 augustus 2020

Ons kenmerk
0

2. Wie checkt de juridische en gegevensbeschermingsaspecten aan de kant van de KMAr/PINL bij het opstellen van nieuwe RCS en/of het bijstellen van deze? Wat is het advies van de jurist van PI-NL ten aanzien van het stellen van vragen van de BI aan PI-NL? Wat wordt verstaan onder gerichte vragen in het kader van risico criteria sets?
3. Welke bevindingen heeft de evaluatie van het proces opgeleverd?
4. Welke PNR-gegevens worden doorgegeven op grond van een RCS? Is dit de volledige set of alleen identificerende gegevens? Waar is dat vastgelegd en/of besloten?
5. 5.1.2.i [redacted] Dit levert een betere onderbouwing van de RCS en kan bias voorkomen en/of opsporen.
   5.1.2.i [redacted]. Daarover zijn nu prejudiciële vragen gesteld aan het EUHvJ.
6. Zijn er tussentijdse updates aan de commissie gestuurd?
7. Wat waren de bevindingen van de aanvullende testen?

C. Naar aanleiding van intern toezicht van de filter-verstrekkingen in TRIP

1. Het filter 5.1.2.i [redacted] in TRIP komt overeen met de afspraak.
2. Van de 173 verstrekkingen zijn er 8 gecontroleerd. (5.1.2.i [redacted]
   a. De naam van het PDF is onjuist. Dit is geen verstrekking o.g.v. een vordering maar o.g.v. een filter. Verder staat in het systeem wel over dat het een filter-verstrekking is.
   b. De controle door de FG kan niet efficiënt worden uitgevoerd. Een knop om alle verstrekkingen te openen / downloaden ontbreekt. Of een overzicht waarin de FG in 1 oogopslag kan zien op grond van welke match de verstrekking is gedaan.
   c. Is de wijze van filter verstrekking toekomstbestendig? Is het voor filter verstrekkingen zoals hier waar het om groepen reizigers gaat een oplossing om een groepstemplate te maken?
3. De rechtvaardiging voor het gebruiken van filters wordt niet gemotiveerd in het daarvoor betreffende tekstveld.

Het aanvullen van het filter met de karakteristieken 5.1.2.i [redacted] draagt bij aan het beschermen van persoonsgegevens en het verbeteren van de resultaten uit het filter.

A9

Ministerie van Justitie en Veiligheid

DEP. VERTROUWELIJK
openbaar na publicatie

Bevindingen TRIP

07.06.2021

Datum	11 juni 2021
Status	Definitief

Afzendgegevens **Beveiligingsautoriteit Ministerie van Justitie en Veiligheid Ministerie Binnenlandse Zaken en Koninkrijksrelaties**

Turfmarkt 147
2511DP Den Haag
Postbus 20301
2500EH Den Haag
www.rijksoverheid.nl/jenv

Auteurs 5.1.2.e

Colofon

Inhoud

Inleiding

Op 7 juni 2021 heb ik een aantal zaken in TRIP (opnieuw) bekeken. Hierbij zijn mij de volgende zaken opgevallen.

NB disclaimer: alle schermafbeeldingen komen uit de ACCEPTATIE omgeving. Enige echte data kunnen alleen afkomstig zijn van een carrier die de aanleveringsvoorschriften niet heeft nageleefd.

1 Bevindingen

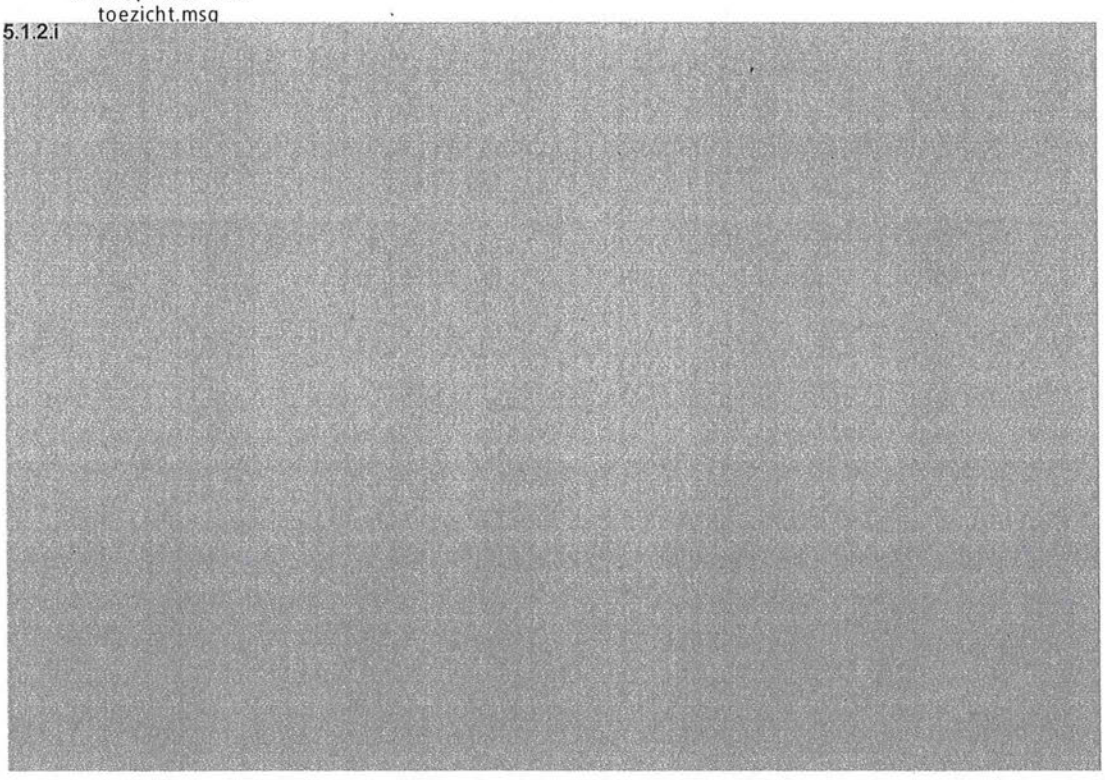
1.1 Exporteren uit TRIP

1 De exportknop (zie email aanpassen trip toezicht) zou m.i. verwijderd worden om verwerkingen die niet gelogd worden in het passagiersdossier tegen te gaan. En daarmee het risico op een incident zoals bij de GGD te beperken. Deze export knop is momenteel nog aanwezig in TRIP. Zowel het verstrekkingsdocument als een uitgebreid excel document kunnen nog geëxporteerd worden (zie beeldmateriaal).

2 Bij het exporteren van bestanden wordt volgens mij geen rechtvaardiging gevraagd door TRIP. Mijn advies zou zijn dit wel op te nemen. Dit kan in een enkel geval geautomatiseerd.

RE Aanpassen TRIP toezicht.msg

5.1.2.i



Chapo.Alfonso.QS0785

TRIP PASSAGIERSDETAILS

Persoonsgegevens	
Voornaam	5.1.2.e
Achternaam	
Volledige naam	
Geboortedatum	
Bron geboortedatum	
Leeftijd	
Geslacht	
Type passagier	
Bron type passagier	
Referentienummer	
Nationaliteit	
Reisstatus	
Geannuleerd obv push	
Frequent Flyer Informatie	
Uitgever	QS

1.2 Rechtvaardigingsgrond voor zoeken in TRIP

1 Analyse zou deze gebruiken om aan te geven waarom gezocht wordt in TRIP. De rechtvaardigingsgrond wordt ingevuld. De vraag is of de wijze waarop het gebeurd voldoende is. De naam van het filter wordt ingevoerd als rechtvaardiging. Het waarom van het draaien van het filter wordt niet aangegeven.

Naam	Versie	Aangemaakt op	Ingangs
Fieldlab test versie 1	1	08-03-2021 10:52	08-03-2
Filtereigenschappen:			
Handhavingsgebied		Meerdere handhav.geb.	
Rechtvaardiging		[redacted]@TRIP.local testen fieldlab	

2 Idem voor B&V wanneer handmatige bevraging met een analysetaak wordt uitgevoerd. Zo ontbreekt ook voor systeembeheer (IBO) de rechtvaardiging bij de bevraging.

3 Idem voor B&V bij de bevraging van Burgerloket. Soms staat er slechts een parketnummer.

1.3 Depersonaliseren persoonsgegevens rapportages

1 Bij diverse rapportages zijn de persoonsgegevens die gebruikt zijn om bij het bevragen van TRIP zichtbaar. Deze persoonsgegevens worden niet gedepersonaliseerd na 6 maanden.
Een functie om te depersonaliseren en een om de depersonalisering op te heffen zorgen ervoor dat aan de wet voldaan kan worden zonder de functionaliteit van de rapportage aan te tasten.
Hebben jullie onderzocht of na 6 maanden alles wordt gedepersonaliseerd dat gedepersonaliseerd hoort te worden? Zo ja, hebben jullie de uitkomsten voor mij?

2 Wanneer bijvoorbeeld P&C en of LSO geautoriseerd zijn voor deze rapportages kunnen zij toegang hebben tot persoonsgegevens.
Hoe ver staat het met de inventarisatie van de (persoons)gegevens die per functie/rol noodzakelijk zijn en het inrichten van de bijbehorende autorisaties? Vorig jaar is daar een opdracht voor gegeven door de COPG/HOT.

FW
Accountcontrole TR

1.4 Acceptatie omgeving TRIP bevat echte PNR-data

Klopt het dat meerdere carriers echte PNR-gegevens in de acceptatie omgeving hebben aangeleverd?

- Wanneer speelde dit?
- Hoeveel carriers en welke zijn betrokken?
- Is de carriers gevraagd om een melding bij de eigen FG en eventueel de AP te overwegen?
- In hoeverre zijn deze data ook verwerkt door gebruikers van de acceptatie omgeving?
- Waarom of hoe heeft dit opnieuw kunnen plaatsvinden als de obfuscate functie n.a.v. het incident vorig jaar was geïmplementeerd?

Terugkoppeling
datalek bij United A

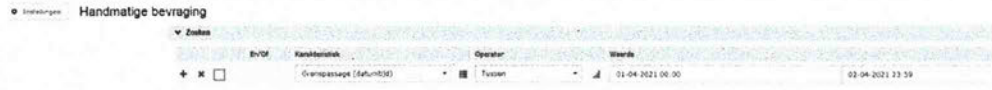
- Wat wordt gedaan om dit in de toekomst te voorkomen?

1.5 Oude bug TRIP

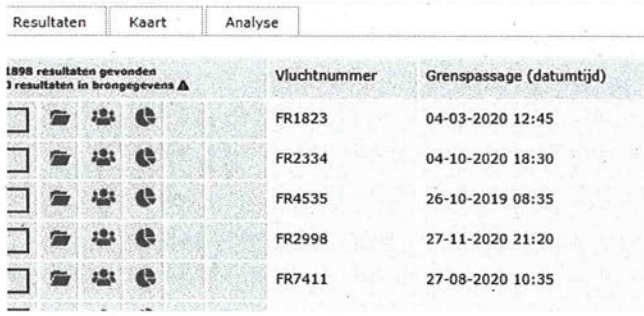
Bij de keyuser heb ik een melding gedaan over een bug(?) waarvan ik dacht dat die eerder dit jaar al was opgelost. De collega's van B&V sprekend, blijkt dat het niet het geval is geweest.
Risico m.b.t. bescherming gegevensbescherming is dat:

- er meer passagiersgegevens op het scherm getoond worden (verwerkt) dan noodzakelijk.
- de verkeerde passagiersgegevens verstrekt kunnen worden (incident) als de medewerker onoplettend is.

Ik zoek op



En krijg de volgende grenspassage data als resultaat



Resultaten | Kaart | Analyse

1898 resultaten gevonden
3 resultaten in brongegevens ▲

Vluchtnummer	Grenspassage (datumtijd)
FR1823	04-03-2020 12:45
FR2334	04-10-2020 18:30
FR4535	26-10-2019 08:35
FR2998	27-11-2020 21:20
FR7411	27-08-2020 10:35

2 Hoor en wederhoor

Graag verneem ik een reactie op bovenstaande.

Nr.	Betrokkene	Hst/Par.	Verzoek te corrigeren tekst	Reactie betrokkene	Reactie FG
1					
2					
3					
4					
5					

A10

Werkafspraken verwerkingsverantwoordelijke, opdrachtgever PI-NL, PI-NL, FG

In aanvulling op het eerdere advies d.d. 5 mei 2020 aan het bestuurlijk overleg 'Functiescheiding Functionaris voor gegevensbescherming en privacy adviseur' waarop geen reactie is ontvangen, hierbij een voorstel voor de werkafspraken tussen de verwerkingsverantwoordelijke, opdrachtgever PI-NL, PI-NL en FG PI-NL gebaseerd op wet- en regelgeving t.b.v. PNR, WPG en AVG alsmede de richtlijnen van de WP29. Afsluitend is een overzicht van taken voor een privacy adviseur opgenomen. Aanvullend kan een regeling zoals de 'Regeling toezichtsbevoegdheden functionarissen voor gegevensbescherming OCW' opgesteld worden om de bevoegdheden van de FG vast te leggen.

Een onduidelijkheid in de toezichtsbevoegdheden van de FG PI-NL t.a.v. het beschermen van persoonsgegevens is de bedrijfsvoering van PI-NL, m.a.w. de gegevensbescherming van medewerkers, relaties e.a. onder de AVG. Is de FG daar ook de interne toezichthouder voor?

Artikel 18 PNR jo. 36 WPG

- FG benoemd door de verwerkingsverantwoordelijke

Verwerkingsverantwoordelijke: - stelt de FG formeel aan - meldt de FG aan bij de AP - informeert de medewerkers over de FG en de bijbehorende taken en bevoegdheden

- FG wordt tijdig en naar behoren betrokken bij alle aangelegenheden die verband houden met de bescherming van persoonsgegevens.

Verwerkingsverantwoordelijke, opdrachtgever PI-NL, PI-NL: - informeren de FG over te nemen besluiten en de genomen besluiten - betrekken de FG proactief tijdig voorafgaand aan (voorgenomen) besluitvorming - verstrekken de FG alle benodigde informatie t.b.v. advies, toezicht, overleg - stelt kaders voor het gegevensbeschermingsniveau en vormt beleid - besluit over en voert risico beperkende maatregelen in FG: - informeert, adviseert en doet aanbevelingen t.b.v. wetgeving, evaluaties, beleid, innovaties, organisatorische, technische, bestuurlijke thema's die betrekking kunnen hebben op persoonsgegevens - houdt toezicht op uitvoering van genomen besluiten en maatregelen

- FG is belast met de controle op de verwerking van de persoonsgegevens door PINL
    - Rechtmatigheid
    - Doelbinding
    - Non-discriminatie

- Bescherming persoonsgegevens

Verwerkingsverantwoordelijke, opdrachtgever PI-NL, PI-NL: - verlenen de FG toegang en hulpmiddelen die nodig zijn t.b.v. een efficiënte controle FG houdt toezicht op: - systemen, processen t.b.v. verwerkingen van persoonsgegevens - doelbinding van de verwerkingen - afwezigheid van bijzondere persoonsgegevens

- FG is belast met de controle op de uitvoering van de desbetreffende waarborgen voor de gegevensbescherming
  - FG controleert achteraf de verstrekking van:
    - gedepersonaliseerde persoonsgegevens/verwerkingsresultaat aan een andere lidstaat (art. 10 lid 3 jo. art. 20 lid 1d)
    - gedepersonaliseerde persoonsgegevens/verwerkingsresultaat aan een 3e land (art. 13 lid 4)
  - FG controleert of naar de betrokkene te herleiden persoonsgegevens gedepersonaliseerd zijn na 6 maanden dan wel verwijderd na 5 jaar (art. 20 lid 1)
  - FG controleert dat er geen bijzondere gegevens of andere gegevens dan vermeld in bijlage 1 PNR-wet worden vastgelegd

Verwerkingsverantwoordelijke, opdrachtgever PI-NL, PI-NL: - verlenen de FG toegang en hulpmiddelen die nodig zijn t.b.v. een efficiënte controle FG controleert: - steeksproefsgewijs verwerkingen door PINL conform wettelijke waarborgen - werking van het systeem

- FG stuurt jaarlijks voor 1 juli een rapportage aan Onze Minister van JenV, de beide Kamers der Staten-Generaal en de AP over het voorgaande kalenderjaar
  - de wijze waarop controle is uitgeoefend op de verwerking van de persoonsgegevens door

Verwerkingsverantwoordelijke, opdrachtgever PI-NL, PI-NL: - geven de FG binnen de gestelde termijn een gezamenlijke reactie op eventuele feitelijke onjuistheden, en evt. tik-/taalfouten van een conceptversie - stellen een beleidsreactie op ogv de conceptversie FG: - stelt planning op in overleg met Verwerkingsverantwoordelijke, opdrachtgever PI-NL, PI-NL - stelt de jaarrapportage op - telt verwerkingsverantwoordelijke, opdrachtgever PI-NL, PI-NL in staat te reageren op feitelijke onjuistheden - biedt de jaarrapportage aan verwerkingsverantwoordelijke Minister JenV aan incl. brieven t.b.v. Staten Generaal via 5.1.2e -lijn (5.1.2e -DBO en FYI: 5.1.2e BVA, 5.1.2e DI&I, 5.1.2e , 5.1.2e) in Digijust. Brief aan AP wordt door 5.1.2e DI&I verzonden met FYI aan bewindspersoon met AP in portefeuille - stelt eventueel een persoonlijk intern nader verslag op - stelt tertaalrapportage op t.b.v. bestuurlijk overleg van de driehoek (opdrachtgever, eigenaar, PINL) i.s.m. tertaalrapportage PI-NL

de PINL

- verantwoording van de FG over eigen handelen

- de wijze waarop de waarborgen voor de gegevensbescherming zijn uitgevoerd
  - technische en organisatorische beveiligingsmaatregelen
  - gegevensbeschermingsbeleid
  - autorisaties
    - *logging van ten minste: het verzamelen, wijzigen, raadplegen, verstrekken onder meer in de vorm van doorgiften, combineren of vernietigen van politiegegevens.*
    - *logging gegevens, worden uitsluitend gebruikt voor de controle van de rechtmatigheid van de gegevensverwerking, voor interne controles, ter waarborging van de integriteit, de beveiliging van de PNR-gegevens en voor strafrechtelijke procedures.*
  - opleiding en bewust handelen van medewerkers
  - verwerkingsregister
- statistieken over de mate waarin passagiersgegevens op grond van de zijn verstrekt, doorgegeven of verzocht

- FG is voor betrokkene het contactpunt voor alle aangelegenheden in verband met de verwerking van de persoonsgegevens van die betrokkene door de verwerkingsverantwoordelijke

Verwerkingsverantwoordelijke, opdrachtgever PI-NL, PI-NL:
- nemen de verwerking van persoonsgegevens door de FG op in verwerkingsregister
- stellen een risico-analyse op
- verlenen de FG toegang en hulpmiddelen die nodig zijn t.b.v. een efficiënte controle
- verzorgen dat verzoeken tijdig conform Awb jo. Wpg afgehandeld kunnen worden bij afwezigheid van de FG
- informeren FG als betrokkenen hun benaderd t.a.v. gegevensbescherming
- regelen dat 5.1.2e MinJenV /MinDef verzoeken t.b.v. PI-NL doorzetten naar FG PI-NL

FG:
- voert verzoeken van betrokkenen in het systeem in
- verzoekt betrokkenen om hun verzoek evt. te repareren
- verzendt besluiten genomen namens de verwerkingsverantwoordelijke door aan de betrokkene

- FG heeft voor de uitvoering van de taken toegang tot alle persoonsgegevens die de PINL verwerkt
- FG kan de AP informeren wanneer zij vaststelt dat een verwerking van persoonsgegevens door de

Verwerkingsverantwoordelijke, opdrachtgever PI-NL, PI-NL:
- zorgen dat de FG toegang heeft tot alle locaties (digitaal en/of fysiek) waar persoonsgegevens i.h.k.v. verwerkt worden

Passagiersinformatie-eenheid niet rechtmatig is

- FG ziet toe op
    - de naleving van de wet
    - het gegevensbeschermingsbeleid van de verwerkingsverantwoordelijke
    - de beleid en toewijzing van de autorisaties
    - de bewustmaking en opleiding van de ambtenaren die zijn betrokken bij de verwerking van persoonsgegevens
    - de (privacy)audits (art. 33 WPG)

Verwerkingsverantwoordelijke, opdrachtgever PI-NL, PI-NL:
- informeren de FG over (wijzigingen in) wet- en regelgeving
- verstrekken het vastgestelde beleid t.a.v. het beschermen van persoonsgegevens, toewijzen van autorisatie, opleiding en audits
- stellen een register op en houden dit bij
- stellen een normenkader op
- richten de privacy governance in incl. een PDCA-cyclus
- voeren jaarlijks vanaf 2020 een interne privacy audit uit
- hebben inzicht in risico's, prioritering en een plan van aanpak om risico's te beperken
- zorgen dat de FG de benodigde informatie en/of hulpmiddelen heeft om het toezicht uit te kunnen oefenen

FG:
- houdt toezicht op
    - systemen, processen t.b.v. verwerkingen van persoonsgegevens
    - aanwezigheid van gegevensbeschermingsbeleid, (verwerkingen)register
    - autorisaties
    - privacy audits, te treffen en/of getroffen maatregelen en de evt. hercontrole

- FG informeert en adviseert de verwerkingsverantwoordelijke en de ambtenaren die persoonsgegevens verwerken over hun verplichtingen ten aanzien van het beschermen van persoonsgegevens

Verwerkingsverantwoordelijke, opdrachtgever PI-NL, PI-NL:
- zorgen dat de FG gelegenheid heeft te informeren en adviseren
- leggen informatie en advies van de FG vast
- informeren de FG gemotiveerd over eventuele opvolging van adviezen o.g.v. risico's, de aard, de omvang, de context en de verwerkingsdoeleinden

FG:
- houdt rekening met:
    - normenkader
    - gegevensbeschermingsbeleid
    - het aan verwerkingen verbonden risico en met de aard, de omvang, de context en de verwerkingsdoeleinden

- FG verstrekt desgevraagd advies over de DPIA (gegevensbeschermingseffectbeoordeling) en ziet toe op de uitvoering en aanwezigheid ervan

Verwerkingsverantwoordelijke, opdrachtgever PI-NL, PI-NL:
- betrekken de FG tijdig bij voorgenomen veranderingen van verwerkingen en/of aanpassingen van systemen

FG:
- kan adviseren of, en over de wijze waarop een risicoanalyse uitgevoerd moet worden

- FG werkt samen met de AP

- FG treedt op als contactpunt voor de AP inzake
    - aangelegenheden in verband met de verwerking van persoonsgegevens
    - voorafgaande raadpleging
    - overleg over enige andere aangelegenheid

AVG

- Contactpersoon voor de AP bij datalekken, verplichte voorafgaande raadplegingen, verstekken van bedrijfsinformatie en andere gelegenheden.

Verwerkingsverantwoordelijke, opdrachtgever PI-NL, PI-NL: - melden informatiebeveiligingsincidenten aan 5.1.2e NCTV conform procesafspraak - informeren de FG tijdig - informeren de medewerkers over het proces - borgen het proces FG: - ziet toe op afhandeling datalek en genomen maatregelen

- De verwerkingsverantwoordelijke bijstaan bij het toezicht op de interne naleving van de AVG. Als onderdeel van deze verplichting erop toe te zien dat de AVG nageleefd wordt, kunnen FG's met name:
    - o informatie verzamelen om verwerkingswerkzaamheden te identificeren;
    - o analyseren en controleren in hoeverre verwerkingswerkzaamheden aan de AVG voldoen; en
    - o de verantwoordelijke informeren, adviseren of aanbevelingen geven.

Verwerkingsverantwoordelijke, opdrachtgever PI-NL, PI-NL: - verstrekken de FG gevraagd en ongevraagd informatie om verwerkingswerkzaamheden te kunnen identificeren - zorgen dat de FG gelegenheid heeft te informeren en adviseren FG: - stelt toezichtskader op - stelt een toezichtsjaarplan op - informeert, adviseert of geeft aanbevelingen aan verwerkingsverantwoordelijke, opdrachtgever PI-NL, PI-NL

- Desgevraagd advies over het data privacy impact assessment te verstrekken en toe te zien op de uitvoering daarvan.
- Bij de uitvoering van taken naar behoren rekening houdt met het aan verwerkingen verbonden risico en met de aard, de omvang, de context en de verwerkingsdoeleinden
- Belangrijke rol in het creëren van een gegevensbeschermingscultuur binnen de organisatie.

Verwerkingsverantwoordelijke, opdrachtgever PI-NL, PI-NL: - richten privacy governance in - zorgen dat de FG de gelegenheid en de middelen heeft - nodigen de FG uit als toehoorder bij interne overleggen en/of i.h.k.v. een vraagstuk FG: - is zichtbaar op locatie bij verwerkingsverantwoordelijke, opdrachtgever PI-NL, PI-NL en schuift periodiek aan bij interne overleggen als toehoorder

- Adviseren bij de implementatie van essentiële elementen van de AVG, zoals:
    - o de beginselen van gegevensverwerking,
    - o de rechten van de betrokkenen
    - o privacy by design en privacy by default
    - o de administratie van gegevensverwerkingen

- beveiliging van het verwerkingsproces
- melding van en communicatie over datalekken

Positie van FG (art.38 AVG):

- Onafhankelijk taken en verplichten te vervullen, geen instructies ontvangen en belangenconflict met andere taken of plichten vermijden (bij externe dus geen verwerkers vertegenwoordigen.)

Verwerkingsverantwoordelijke, opdrachtgever PI-NL, PI-NL: - zorgen voor privacy governance - zorgen voor een privacy functionaris om bovenstaand belangenconflict te vermijden FG: - informeert, adviseert en doet aanbeveling aan verwerkingsverantwoordelijke, opdrachtgever PI-NL, PI-NL

- Naar behoren en tijdig wordt betrokken bij alle aangelegenheden die verband houden met de bescherming van persoonsgegevens.
    - de FG of diens team zo vroeg mogelijk betrekken bij alle aangelegenheden die de bescherming van persoonsgegevens betreffen.

Verwerkingsverantwoordelijke, opdrachtgever PI-NL, PI-NL: - zorgen voor privacy governance - informeren medewerkers over het proces om de FG te betrekken - betrekken de FG bij alle aangelegenheden zoals: aanpassen van bestaande of inrichten van nieuwe verwerkingen, risicoanalyse, evaluatie's van beleid en/of wetgeving, aanpassingen van systemen FG: - informeert, adviseert en doet aanbeveling aan verwerkingsverantwoordelijke, opdrachtgever PI-NL, PI-NL

    - data proces impact assessments, stelt de AVG expliciet dat de FG daar in een vroeg stadium bij betrokken dient te worden en het advies van de FG inwint.
    - Wanneer de FG direct geïnformeerd en geraadpleegd wordt, is het makkelijker de AVG na te leven en wordt privacy by design geboden. Daarom dient dit een standaardprocedure binnen de organisatie te zijn.

Verwerkingsverantwoordelijke, opdrachtgever PI-NL, PI-NL: - zorgen voor privacy governance - stellen een standaardprocedure vast - informeren medewerkers over het proces om de FG te betrekken FG: - informeert, adviseert en doet aanbeveling aan verwerkingsverantwoordelijke, opdrachtgever PI-NL, PI-NL

    - FG als een gesprekspartner binnen de organisatie wordt en dat hij of zij deel uitmaakt van de relevante werkgroepen die binnen de organisatie gegevens verwerken.
        - regelmatig wordt uitgenodigd om aan vergaderingen van het hoger management en het middenmanagement deel te nemen.
        - uit te nodigen wanneer beslissingen met gevolgen voor gegevensbescherming worden genomen.
        - Alle relevante informatie dient tijdig aan de FG doorgegeven te worden om hem in staat te stellen passend advies te geven.

- Aan de mening van de FG dient altijd passende waarde gehecht te worden. Bij geschillen vastleggen waarom het advies van de FG niet gevolgd is.
- FG dient onmiddellijk geraadpleegd te worden indien zich een datalek of ander incident heeft voorgedaan.
- Waar nodig kan de verantwoordelijke of verwerker gegevensbeschermings-richtlijnen of -programma's opstellen waarin aangegeven staat wanneer de FG geraadpleegd dient te worden.

Verwerkingsverantwoordelijke, opdrachtgever PINL en/of PINL:
- betrekken de FG tijdig als gesprekspartner en bij overleggen evt. als agendalid en/of toehoorder
- informeren de FG gemotiveerd over vervolgstappen n.a.v. advies van de FG
- informeren de FG over de aanwezigheid en inhoud van interne (werk)afspraken t.a.v. het tijdig raadplegen van de FG

FG:
- informeert, adviseert en doet aanbeveling aan verwerkingsverantwoordelijke, opdrachtgever PI-NL, PI-NL

- Toegang tot persoonsgegevens en verwerkingen en locaties (fysiek en/of digitaal) waar verwerking plaatsvindt.

Verwerkingsverantwoordelijke, opdrachtgever PI-NL, PI-NL:
- zorgen voor de autorisaties van de FG en eventuele tijdig verlenging
- zorgen voor een plek waar de FG zich toegang kan verschaffen tot digitale persoonsgegevens

- De benodigde middelen ter beschikking te stellen voor het vervullen van deze taken en het in stand houden van zijn deskundigheid. Over het algemeen geldt dat hoe complexer en/of gevoeliger de verwerkingen zijn, hoe meer middelen de FG geboden dienen te worden. De gegevensbeschermingsfunctie dient met het oog op de gegevensverwerking voldoende effectief te zijn en voldoende middelen te hebben.
  - Actieve ondersteuning van de functie van de FG door het hogere management (bijv. op het niveau van het bestuur).
  - Voldoende tijd voor de FG om zijn taken te vervullen. Het is van essentieel belang dat er voldoende tijd is om aan de taken van de FG te besteden. Het is good practice de tijd die nodig is om de functie te vervullen en de prioriteit van de FG-taken te bepalen en tot slot dat de FG (of de organisatie) een werkplan opstelt.

Verwerkingsverantwoordelijke, opdrachtgever PI-NL, PI-NL:
- stellen de benodigde middelen ter beschikking
- stellen normenkader op
- stellen een prioriteitenlijst op

FG:
- stelt toetsingskader op m.b.v. ADR
- stelt jaarplan op o.g.v. AP toezichtskader
- plant toezichtsbezoeken in evt. externe bezoeken i.o.m. 5.1.2e POL / 5.1.2e WPG MinDef

  - Voldoende steun qua financiële middelen, infrastructuur (terrein, faciliteiten, apparatuur) en, waar nodig, personeel.

- Officiële communicatie over de aanwijzing van de FG naar alle medewerkers, zodat zijn bestaan en functie binnen de organisatie bekend is.
- De vereiste toegang tot andere diensten, zoals personeelszaken, de juridische afdeling, de ICT-afdeling, de beveiliging enz., zodat de FG van die andere afdelingen de essentiële steun, input en informatie ontvangt.

Verwerkingsverantwoordelijke, opdrachtgever PI-NL, PI-NL: - communiceren over de o aanwezigheid van de FG o taken van de FG o bevoegdheden van de FG

- Doorlopende training. FG's dienen de kans te krijgen bij te blijven op het gebied van gegevensbescherming. Het streven moet zijn het kennisniveau van de FG doorlopend te verhogen en hij moet aangemoedigd worden om aan trainingen over gegevensbescherming en andere vormen van professionele ontwikkeling deel te nemen, zoals deelname aan privacy-fora, workshops enz.
- Op basis van de grootte en structuur van de organisatie, kan het nodig zijn een FG-team aan te stellen (een FG en zijn personeel). In dergelijke gevallen dienen de interne structuur van het team en de taken en verantwoordelijkheden van elk lid duidelijk aangegeven te worden. Wanneer de taken van de FG door een externe dienstverlener vervuld worden, mag een team van werknemers van dat bedrijf de taken van een FG ook als team uitvoeren, onder leiding van een aangewezen hoofdcontactpersoon voor de klant.

Verwerkingsverantwoordelijke:

- Faciliteert de FG bij de taken met o.a. financiën, middelen en mensen

Verwerkingsverantwoordelijke, opdrachtgever PI-NL, PI-NL: - stellen de benodigde middelen ter beschikking aan de FG

- Is verantwoordelijk voor de naleving van de wetten en moet die naleving kunnen aantonen

Verwerkingsverantwoordelijke, opdrachtgever PI-NL, PI-NL: - Richten privacy governance in - Houden bij hoe de naleving van de wet is en geven de FG toegang FG: - controleert naleving van de wet - adviseert en doet aanbevelingen

- Contactgegevens FG zowel intern als extern (algemeen email, postadres of telefoonnummer) beschikbaar maken, publiceren en aan de AP melden voor het FG register.
- Is verantwoordelijk voor het uitvoeren van de gegevensbeschermingseffectrapportage (DPIA) en vraagt advies aan de FG over de DPIA:
    - of er al of niet een DPIA uitgevoerd moet worden;
    - welke methodiek voor de DPIA gebruikt moet worden;
    - of de DPIA intern uitgevoerd of uitbesteed moet worden;
    - welke waarborgen (zoals technische en organisatorische maatregelen) ingebouwd moeten worden om eventuele risico's voor de rechten en belangen van de betrokkenen te beperken;
    - of de DPIA correct uitgevoerd is en de conclusies daaruit (de vraag of de verwerking door moet gaan en welke waarborgen er ingebouwd moeten worden) aan de AVG voldoen.
    - indien de verantwoordelijke het niet met het advies van de FG eens is, dient in de documentatie van de DPIA specifiek schriftelijk aangegeven te worden waarom het advies niet overgenomen is.

Verwerkingsverantwoordelijke, opdrachtgever PI-NL, PI-NL: - betrekt de FG bij het te nemen besluit over en uitvoeren van een DPIA - legt een DPIA voor aan de AP als blijkt dat risico beperkende maatregelen niet afdoende zijn om persoonsgegevens te beschermen FG: - informeert, adviseert en doet aanbevelingen - legt contact met de AP t.b.v. de voorgenomen raadpleging

- De verwerkingsverantwoordelijke wordt aangeraden om de specifieke taken van de FG en de reikwijdte daarvan duidelijk aan te geven, bijvoorbeeld in het contract van de FG maar ook in aan medewerkers, het bestuur (en, waar nodig, andere belanghebbenden) verstrekte informatie, met name waar het gaat om het uitvoeren van een DPIA.

Verwerkingsverantwoordelijke: - legt de specifieke taken en reikwijdte vast en communiceert die intern

- Is verplicht een register van de verwerkingsactiviteiten die onder hun verantwoordelijkheid plaatsvinden bij te houden. Een dergelijk register is een van de middelen die de FG in staat stelt zijn taak te vervullen om op naleving toe te zien en de verantwoordelijke of de verwerker te informeren en adviseren.

Verwerkingsverantwoordelijke, opdrachtgever PI-NL, PI-NL: - geeft de FG toegang tot het register - legt verwerkingen van de FG vast in het register FG: - informeert, adviseert en doet aanbevelingen

Voor uitgebreidere informatie over de taken van de FG en de verantwoordelijkheden voor de verwerkingsverantwoordelijke zie het document profiel FG WP29 (31 pagina's).

Taken Privacy adviseur

WPG art. 34

De verwerkingsverantwoordelijke benoemt een of meer privacyfunctionarissen. De privacyfunctionaris dient de verwerkingsverantwoordelijke en de personen die voor de verwerkingsverantwoordelijke werkzaam zijn van advies en ziet namens de verwerkingsverantwoordelijke toe op de verwerking van politiegegevens overeenkomstig het bij of krachtens de wet bepaalde. De privacyfunctionaris houdt t.b.v. de verwerkingsverantwoordelijke een overzicht bij van de schriftelijke vastlegging van de gegevens in een register (art. 22 PNR) van:

1. de namen en contactgegevens van
   1.1. de verwerkingsverantwoordelijke,
   1.2. de organisatie en
   1.3. de ambtenaren van de Passagiersinformatie-eenheid die belast zijn met de verwerking van passagiersgegevens, en van de functionaris gegevensbescherming;
2. de namen en contactgegevens van
   2.1. de bevoegde instanties,
   2.2. de Passagiersinformatie-eenheden en
   2.3. de bevoegde instanties van andere lidstaten (en
   2.4. derde landen); en
3. de autorisaties die zijn toegekend.

i.h.k.v. de Wpg artt. 31 lid 2 en 32 kan gedacht worden aan:

- de naam en de contactgegevens van de verwerker of verwerkers en van iedere verwerkingsverantwoordelijke ten behoeve van wie de verwerker handelt en, in voorkomend geval, van de functionaris voor gegevensbescherming
- de categorieën van verwerkingen die namens iedere verwerkingsverantwoordelijke zijn uitgevoerd indien van toepassing, doorgiften van politiegegevens aan een derde land of een internationale organisatie, onder vermelding van dat derde land of die internationale organisatie, indien door de verwerkingsverantwoordelijke uitdrukkelijk daartoe geïnstrueerd
- indien mogelijk, een algemene beschrijving van de technische en organisatorische maatregelen, conform artikel 4a Wpg
  - te waarborgen en te kunnen aantonen dat de verwerking van PNR-gegevens wordt verricht in overeenstemming met hetgeen bij of krachtens wet is bepaald
  - het gegevensbeschermingsbeleid en de gegevensbeschermingsbeginselen op een doeltreffende manier uit te voeren respectievelijk toe te passen
  - bij de bepaling van de verwerkingsmiddelen en de verwerking zelf de nodige waarborgen, zoals pseudonimisering, in de verwerking in te bouwen ter naleving van hetgeen bij of krachtens de wet is bepaald en ter bescherming van de rechten van de betrokkenen
  - Het treffen van passende technische en organisatorische maatregelen om een beveiligingsniveau te waarborgen dat op het risico is afgestemd, met name met betrekking tot de verwerking van de bijzondere categorieën van politiegegevens, bedoeld in , en op een zodanige manier dat de politiegegevens beschermd zijn tegen ongeoorloofde of onrechtmatige verwerking en tegen opzettelijk verlies, vernietiging of beschadiging.
  - Bij het treffen van de maatregelen rekening houden met

..1. de aard, de reikwijdte, de context en de doeleinden van de verwerking, alsmede met de qua waarschijnlijkheid en ernst uiteenlopende risico's voor de rechten en vrijheden van natuurlijke personen
..2. rekening met de stand van de techniek en de uitvoeringskosten.

- De maatregelen worden periodiek geëvalueerd en zo nodig geactualiseerd.

- de doelen van de onderzoeken
- de verstrekking of doorgifte van PNR-gegevens
- de feitelijke of juridische redenen die ten grondslag liggen aan een afwijzing
- een inbreuk op de beveiliging van persoonsgegevens, inclusief de feiten omtrent de inbreuk, de gevolgen ervan en de maatregelen die zijn getroffen ter correctie.

Verder:

- het ondersteunen en monitoren van de privacy governance
- eerste lijns advies aan medewerkers, waaronder advies over en afhandelen VTW's en afstemmen met JZ voor 2e lijns advies
- opstellen gegevensbeschermingsbeleid incl. een bewustwordingsprogramma
- opstellen en monitoren verwerkingsregister voor de verwerkingen waar het afdelingsmanagement voor verantwoordelijk is
- afhandelen inzage verzoeken in Burgerloket i.s.m. B&V
- ondersteunen bij risico analyses en DPIA en monitoren voor de verwerkingen waar het afdelingsmanagement voor verantwoordelijk is
- ondersteunen van lijnmanagement bij de naleving van de privacywetgeving
- uitvoeren of coördineren van de privacywerkzaamheden
- aanspreekpunt zijn voor het netwerk privacy, zowel in- als extern
- gevraagd en ongevraagd adviseren over privacygerelateerde onderwerpen.
- inventariseren, beoordelen, bijhouden en melden van afdelinggerelateerde verwerkingen
- behandelen van privacygerelateerde vraagstukken
- uitvoeren van PIA's/privacy risicoanalyses
- rapporteren over de status van privacy aan het lijnmanagement
- contact onderhouden en samenwerken met Juridische zaken, Beleid, Informatiebeveiliging, Inkoop en FG