Ministerie van Justitie en Veiligheid

# Intern Verslag 2019 FG Pi-NL

voor de verwerkingsverantwoordelijke

Versie 1.0

| | |
|---|---|
| Datum | 18 augustus 2020 |
| Status | Definitief |

# Colofon


| | |
|---|---|
| Afzendgegevens | **Ministerie van Justitie en Veiligheid**<br>**Functionaris voor de gegevensbescherming voor de Passaiersinformatie- eenheid Nederland**<br><br>Turfmarkt 147<br>2511DP Den Haag<br>Postbus 20301<br>2500EH Den Haag<br>www.rijksoverheid.nl/jenv |
| Auteur | FG Passagiersinformatie-eenheid Nederland |

# Inhoud

# Inleiding

Apart van de officiële publieke jaarrapportage artikel 18 PNR-wet over 2019 voor het parlement zijn er nog een aantal zaken waarover ik mijn persoonlijke kijk op wil delen. Op een aantal zaken wil ik graag gedetailleerder in gaan zodat u als verwerkingsverantwoordelijke een breder beeld heeft over de implementatie van de waarborgen voor het beschermen van persoonsgegevens.
Over de kwartalen 3 en 4 van 2019 is tevens een rapportage door mij opgesteld ten behoeve van het bestuurlijke driehoeksoverleg, te weten de opdrachtgever Pi-NL (NCTV), de eigenaar (Defensie) en opdrachtnemer (Pi-NL). Dit interne verslag is in concept d.d. 14 juni 2020 aan de NCTV aangeboden.

# Informatieplicht

Toelichting: Zijn een of meerdere processen voor de rechten van de betrokkenen (informatie, inzage, rectificatie, vernietiging) aanwezig. De informatieplicht is geregeld in de overeenkomstig van toepassing zijnde artikelen 24a tot en met 28 uit de Wet op de politiegegevens (hierna: Wpg) en artikel 18 PNR-wet.

De passagiersgegevens ontvangt Pi-NL op grond van artikel 4 PNR-wet van luchtvaartmaatschappijen. Pi-NL kan niet controleren aan de hand van andere databases of de aangeleverde passagiersgegevens juist en of volledig zijn. De juistheid en volledigheid van de passagiersgegevens, zoals geregeld in artikel 4 Wpg, kan verbeterd worden wanneer betrokkenen hun rechten uitoefenen.

De processen waarmee betrokkenen rechten kunnen uitoefenen zijn vastgelegd in procesbeschrijvingen en werkinstructies. De processen zijn nog niet geïmplementeerd, dat staat voor 2020 in de planning. De processen functioneren via een tijdelijke oplossing met de FG als contactpunt. Dit is in lijn met artikel 18 PNR-wet waarin staat dat de FG het contactpunt is voor alle aangelegenheden in verband met de verwerking van persoonsgegevens. De tijdelijke oplossing is niet in werking getreden omdat in 2019 geen van de verzoekers zich heeft geïdentificeerd.

Pi-NL uitte zorgen over de deugdelijke vaststelling van identificatiebewijzen en het misbruik dat derden bij het uitoefenen van de rechten kunnen maken. Bij twijfel zullen aanvullende bewijzen worden gevraagd om de identiteit vast te kunnen stellen of zal geen inzage gegeven kunnen worden.

Betrokkenen kunnen verzoeken om inzage in hun persoonsgegevens en eventuele verstrekkingen daarvan. Bij de logging van verstrekkingen bleek dat bij het verstrekken van persoonsgegevens van een passagier ook de naam van een medepassagier verstrekt wordt conform PNR-wet. Echter in de persoonsgegevens van de medepassagier werd de verstrekking niet geregistreerd. Om te kunnen voldoen aan het recht op inzage is voorgenoemde omissie direct gerepareerd. Hetzelfde gold voor de verstrekking van vluchtlijsten. Deze mogelijkheid was niet goed in TRIP ingeregeld. Ook daar worden nu bij alle betrokkenen vastgelegd dat hun gegevens via een vluchtlijst zijn verstrekt. De FG controleert periodiek de werking van de logging.

Informatieplicht is ook het verstrekken van informatie over verwerkingsdoelen, identiteit en contactgegevens van de verwerkingsverantwoordelijke, de grondslagen van de verwerkingen, bewaartermijnen en eventuele geautomatiseerde besluitvorming. Op overheid.nl, defensie.nl zijn pagina's aanwezig die informatie geven en de contactgegevens van de FG weergeven. De informatie is beperkt, moeilijk vindbaar en niet duidelijk of in eenvoudige taal opgesteld. Het vinden van informatie en het uitoefenen van de rechten van betrokkenen zijn daarmee wel geïmplementeerd en functioneren, echter naar mijn mening is het een verbeterpunt voor de verwerkingsverantwoordelijke. Voor communicatie vanuit de verwerkingsverantwoordelijkheid is JenV verantwoordelijk.

Er zijn voor zover bij de FG geen klachten bekend die door betrokkenen bij de Autoriteit Persoonsgegevens zijn ingediend.
De informatieplicht is voldoende ondanks de mogelijke verbeterpunten.

## Verantwoordingsplicht

Toelichting: Is er een adequaat proces voor het melden van datalekken en een register voor de registratie van datalekken en zijn er passende beveiligingsmaatregelen voor de beveiliging van persoonsgegevens. De verantwoordingsplicht is geregeld in de van overeenkomstig van toepassing zijnde artikelen 4a, 4b, 6, 6a, 33 en 33a uit de Wpg.

De opdrachtgever registreert en handelt datalekken af. Pi-NL heeft geen eigen register voor het registeren van datalekken en heeft geen eigen datalekprocedure opgesteld die aansluit op die van de opdrachtgever. De interne procedure bij Pi-NL wordt in 2020 opgesteld. Communicatie over datalekken zal via de opdrachtgever en de verwerkingsverantwoordelijke verlopen. De privacyfunctionaris van de opdrachtgever informeert de FG van Pi-NL over datalekken bij Pi-NL.

De opdrachtgever, eigenaar en opdrachtnemer hebben afspraken over het vereiste beveiligingsniveau vastgesteld. Bij Defensie werkt Pi-NL op het extra beveiligde netwerk op daartoe aangewezen locaties. Het beheer en de beveiliging van de lokale infrastructuur en fysieke werkplekken is een verantwoordelijkheid van Defensie. De PNR-gegevens worden alleen op het Nederlandse grondgebied opgeslagen.

Pi-NL heeft met TRIP een systeem met passende beveiligingsmaatregelen voor de beveiliging van persoonsgegevens. Autorisaties voor TRIP om met PNR-gegevens te kunnen werken kent JenV toe aan medewerkers van Pi-NL op verzoek van Pi-NL. De bevoegde instanties vragen zelf voor hun medewerkers autorisaties bij JenV aan. Binnen TRIP wordt voor de diverse functionarissen onderscheid naar autorisaties gemaakt. Een beperkte groep mag met persoonsgegevens werken en binnen die groep is verdere verfijning van de autorisatie geregeld. Medewerkers die met persoonsgegevens werken zijn geauthentiseerd en geautoriseerd voor fysieke en digitale werkomgevingen. De FG houdt intern toezicht op de toegekende autorisaties.
Bij onjuistheden in de autorisatie kunnen die op mijn advies aangepast worden of de functionaliteit in TRIP horende bij een bepaalde autorisatie kan aangepast worden zodat passagiersgegevens niet meer in die functionaliteit voorkomen. Van verwerkingen in TRIP wordt de logging conform de PNR-wet vastgelegd voor de controle van de rechtmatigheid van de gegevensverwerking, de interne controle, het

waarborgen van integriteit, beveiliging van persoonsgegevens en voor strafrechtelijke procedures.

Passagiersinformatie-eenheden van de lidstaten (hierna: PIU's) mogen onderling passagiersgegevens uitwisselen. Voor die uitwisseling is het systeem Secure Information Exchange Network Application (hierna: SIENA) aangewezen in de PNR-richtlijn. SIENA is een applicatie van Europol waarmee informatie wordt uitgewisseld tussen rechtshandhavingsinstanties in Europa. In de PNR-richtlijn staat dat SIENA gebruikt moet worden voor de uitwisseling tussen PIU's en Europol. Informatie uit SIENA kon niet op een veilige manier verwerkt worden door Pi-NL daarom stelde het management vast met internationale rechtshulpverzoeken via Dienst landelijke informatieorganisatie (hierna: DLIO) te werken (zie verder de paragraaf: rechtmatigheid van verwerking). De beste oplossing is een rechtstreekse koppeling tussen de twee systemen en dat vergt aanpassingen in wet- en of regelgeving en inzet van andere organisaties, zoals de Nationale Politie. Een duurzame oplossing die Pi-NL met behulp van Defensie op korte termijn kan implementeren zal in 2020 uitgerold en functioneel zijn.

De Wpg schrijft periodieke privacy audits voor en dit is nader uitgewerkt in de regeling periodieke audit politiegegevens. De jaarlijkse interne privacy audits heeft de verwerkingsverantwoordelijke nog niet ingepland.

De verantwoordingsplicht is voldoende.

## Privacy by design/default TRIP

Toelichting: Het depersonaliseren van persoonsgegevens na zes maanden als het 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. Privacy by design en of default is geregeld in de overeenkomstig van toepassing zijnde artikelen 4a en 4b Wpg en artikelen 6, 7, 10, 13,18, 19 en 20 PNR-wet.

De rechten op eerbiediging van het privéleven, op bescherming van persoonsgegevens en op non-discriminatie van betrokkenen zijn beschermd door het filteren en geautomatiseerd verwijderen van persoonsgegevens die (in)direct kunnen leiden naar godsdienst of levensovertuiging, ras of etnische afkomst, politieke gezindheid, gezondheid, seksuele leven of geaardheid of lidmaatschap van een vakvereniging. Het is Pi-NL niet toegestaan om bijzondere persoonsgegevens te verwerken wanneer de luchtvaartmaatschappij die aanlevert. Tussen het aanleveren en het opnemen van PNR-gegevens in TRIP worden bijzondere persoonsgegevens gefilterd en verwijderd. Op mijn advies is het filter aangescherpt en worden meer persoonsgegevens verwijderd die indirect naar bijzondere persoonsgegevens konden leiden. Bijvoorbeeld service codes (SSR) die verwijzen naar dieetwensen en medische hulpmiddelen.

Passagiersgegevens ouder dan zes maanden worden sinds 18 december 2019 automatisch gedepersonaliseerd zodat alleen met toestemming de depersonalisering voor een verwerking opgeheven mag worden. De verantwoording hierover wordt vastgelegd. De toestemming van de officier van justitie (hierna: OvJ) is vastgelegd

in de vordering en die wordt vijf jaar bewaard. De toestemming wordt overgenomen in TRIP en de FG controleert de depersonalisering, de aanwezigheid van de toestemming bij controle van de verstrekking van passagiersgegevens die ouder dan zes maanden zijn. De FG ontvangt van deze verstrekkingen een automatische notificatie. Bij de controle wordt vastgelegd dat de notificatie is ontvangen en dat controle plaatsvond. De FG heeft voor de uitvoering van deze taken toegang tot alle PNR-gegevens die door de Pi-NL worden verwerkt.

De bewaartermijn van vijf jaar is in principe ingeregeld. Hoe de waarborg is geïmplementeerd en of die functioneert kan nu nog niet gezegd worden. Op 18 juni 2024 wordt duidelijk of de waarborg functioneert. Andere bewaartermijnen functioneren. De bewaartermijn van 42 dagen voor verstrekkingen is bepaald bij beleid. Deze 42 dagen geeft medewerkers van Pi-NL de gelegenheid om bij vragen die bevoegde instanties achteraf stellen dezelfde verstrekking te gebruiken. Bevoegde instanties hebben 14 dagen gelegenheid om de verstrekking te downloaden. De 42 dagen bewaartermijn functioneert. De 14 dagen bewaartermijn kan de FG niet controleren omdat de verstrekking in het domein van de bevoegde instanties ligt.

De FG ontvangt notificaties wanneer persoonsgegevens aan een derde land zijn verstrekt. Naar aanleiding van de notificatie kan een controle achteraf plaatsvinden. Bij de controle wordt vastgelegd dat de notificatie is ontvangen en dat controle plaatsvond. De FG heeft voor de uitvoering van deze taken toegang tot alle PNR-gegevens die door de Pi-NL worden verwerkt.

Privacy by design en of default is ruim voldoende.

## Documentatieplicht

Toelichting: De aanwezigheid van een gevuld register 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 proces voor de gegevensbeschermingseffectrapportage (hierna: DPIA) waarbij de DPIA's met de FG worden afgestemd. De documentatieplicht is geregeld in de artikelen 22 en 23 PNR-wet en het van overeenkomstige toepassing zijnde artikel 4c en 33b Wpg.

Het registeren en documenteren van de verwerkingen en het bijhouden van een overzicht van functionarissen en (inter)nationale bevoegde instanties is nog niet in een register vastgelegd. De diverse procesbeschrijvingen en werkinstructies zijn een eerste aanzet voor het opstellen van een register. Er is nog geen plan opgesteld. De logging van de verwerkingen van passagiersgegevens wordt in TRIP bijgehouden.

Er zijn afspraken tussen de verwerkingsverantwoordelijke vertegenwoordigd door de opdrachtgever met eigenaar en opdrachtnemer over de rol en taakverdeling onderling. Als mede een afspraak tussen opdrachtgever en opdrachtnemer met onderdeel informatiebeveiliging van Defensie en de leverancier van TRIP over het leveren, onderhouden en regelen van de toegang tot TRIP binnen de Defensie (netwerk)infrastructuur.

Een proces om DPIA's op te stellen en/of af te stemmen met de FG ontbreekt. De DPIA vanuit het wettelijke implementatietraject voor het inrichten van een Pi-NL wordt door de opdrachtgever in 2020 geactualiseerd.
De FG adviseerde eind 2019 om voor analyse taken een zogenoemde data science DPIA op te stellen voor het verwerken van grote hoeveelheden persoonsgegevens die reisgedrag inzichtelijk maken en op grond waarvan passagiers geprofileerd worden.

De verwerkingsverantwoordelijke heeft in 2019 geen gebruik gemaakt van de mogelijkheid om een voorgenomen beslissing aan de Autoriteit Persoonsgegevens voor te leggen.

De documentatieplicht is onvoldoende.

## Rechtmatigheid verwerking

Toelichting: Bij rechtmatigheid van verwerking van alle persoonsgegevens hoort een grondslag aanwezig te zijn voor de rechtmatige verwerking van alle verzamelingen van persoonsgegevens. De rechtmatigheid van de verwerking is geregeld in de artikelen 2 en 5 van de PNR-wet.

Passagiersgegevens mogen volgens de PNR-wet alleen verwerkt worden voor het voorkomen, opsporen, onderzoeken en vervolgen van terroristische misdrijven en ernstige criminaliteit. De strafbare feiten die hieronder vallen zijn opgenomen in bijlage 2 bij de PNR-wet. Daarnaast mogen passagiersgegevens ouder dan zes maanden alleen gepersonaliseerd verstrekt worden wanneer daar een grondslag voor is in de vorm van toestemming van de OvJ en moet de FG genotificeerd worden voor een controle achteraf op de verwerking en toestemming.
De vordering vanuit Nederland of een verzoek van een buitenlandse bevoegde instantie wordt op grond van het nationale recht getoetst aan de doelbinding van de PNR-wet. In Nederland is dat de OvJ. Pi-NL kan de doelbinding en de rechtmatigheid van de verwerking niet in alle gevallen toetsen omdat in de vordering veelal geen strafbaar feit uit bijlage 2 van de PNR-wet is opgenomen. De verantwoordelijkheid ligt daarmee bij het Openbaar Ministerie (hierna: OM) om de doelbinding te toetsen in die gevallen waar de specificatie van het strafbare feit om moverende redenen niet in de vordering staat en alleen verwezen wordt naar een misdrijf waarop naar de wettelijke omschrijving een gevangenisstraf van vier jaren of meer is gesteld conform artikel 67 wetboek van strafvordering.
Pi-NL wijst vorderingen die niet aan de doelbinding voldoen af.

Aangezien de vordering de rechtmatigheid van de verstrekking regelt moet die in TRIP aanwezig zijn bij een verstrekking. Bij een periodieke controle van mij bleek dat bij enkele spoedvorderingen de vordering niet binnen 72 uur schriftelijk was nagezonden. Pi-NL heeft dit gebrek gerepareerd door de bevoegde instanties alsnog om de vordering te verzoeken. Daarnaast is er een aanpassing in TRIP aangebracht waardoor de bevoegde instantie en Pi-NL een herinnering krijgen als de schriftelijke vordering na een mondelinge spoedvordering ontbreekt.

In het 'Besluit gebruik van passagiersgegevens voor de bestrijding van terroristische en ernstige misdrijven' regelt dat taken uit de PNR-wet zijn belegd bij DLIO uit het Besluit beheer politie. Bijvoorbeeld verzoeken van en verstrekkingen aan bevoegde instanties uit lidstaten, derde landen, Europol en spontane verstrekkingen van Pi-NL

aan een PIU (PIU is een passagiersinformatie-eenheid in een lidstaat) worden via internationale rechtshulpverzoeken afgehandeld door DLIO. Dit houdt in dat verzoeken om en verstrekkingen van persoonsgegevens tevens daar inhoudelijk beoordeeld worden (artikel 17a Wpg).

De minister heeft per 'Besluit van de Minister van Justitie en Veiligheid van 18 juni 2019, nr. 2624966' het Schengeninformatiesysteem van de tweede generatie (hierna: SISII) aangewezen als database waaraan getoetst kan worden of gesignaleerde personen van, naar of via Nederland vliegen. De vergelijking is daarmee rechtmatig. Wanneer bij de vergelijking van de passagiers met de gesignaleerde personen een 'hit' gevonden wordt controleert Pi-NL door middel van menselijke tussenkomst het resultaat. Als de medewerker de hit bevestigd dan wordt Bureau Sirene gevraagd om de doelbinding van de signalering aan de PNR-wet te controleren. Als de gesignaleerde persoon verdacht wordt van een strafbaar feit conform de PNR-wet kunnen de passagiersgegevens verstrekt worden aan de bevoegde instantie die de signalering heeft opgegeven. De rechtmatigheid van de verstrekking is geborgd. Ik ben nog niet toegekomen aan het toezicht op de verplichte menselijke toets. Dit staat voor 2020 op mijn planning.

Het verrijken en controleren van de passagiersgegevens aan de hand van politiesystemen en politiegegevens vindt plaats via een work around. Pi-NL mag deze werkzaamheden niet uitvoeren omdat ze niet met politiegegevens mag werken. De work around is een samenwerkingsverband van bevoegde instanties ondergebracht bij het Ministerie van Defensie. Na het controleren en verrijken gaat een alert naar de bevoegde instantie(s).

Pi-NL heeft nog geen feedbackloop tot stand gebracht waarmee een zogenoemde 'white list' of valse positieven lijst opgesteld kan worden. Dit is nodig voor passagiers die bijvoorbeeld met iemand anders die wel gesignaleerd is verward worden of slachtoffer zijn geweest van identiteitsfraude. Aan de hand van een 'white list' kan Pi-NL besluiten de gegevens van de passagier niet te verstrekken aan de bevoegde instantie. De 'white list' wordt naar verwachting in 2020 geïmplementeerd.

De gronden voor rechtmatigheid zijn vastgelegd in de wet en geïmplementeerd in de uitvoering. De doelbinding is niet in alle gevallen vast te stellen door Pi-NL zelf. Pi-NL kan te allen tijde navraag doen naar de doelbinding en wordt daarvan op de hoogte gesteld.
De FG kan een onrechtmatige verwerking van passagiersgegevens melden aan de Autoriteit Persoonsgegevens. Van deze mogelijkheid is geen gebruik gemaakt.

De rechtmatigheid van de verwerking is voldoende.

## Compliance: FG benoemd

Toelichting: Heeft de verwerkingsverantwoordelijke een Functionaris Gegevensbescherming (FG) benoemd? De FG is verplicht volgens de PNR-wet. De FG geeft advies en moet toezien op de juiste uitvoering door Pi-NL van de waarborgen voor het beschermen van persoonsgegevens uit de PNR-wet. De functie en de taken van deze functie zijn specifiek beschreven in de AVG (artikelen 37 tot en met 39) en nader gespecificeerd in de artikelen 18 PNR-wet en 36 Wpg.

Eind juni 2019 ben ik gestart en in september door de opdrachtgever aangemeld bij de Autoriteit Persoonsgegevens.
De FG adviseert over en ziet toe op de naleving van de wet- en regelgeving en het beleid ten aanzien van het beschermen van persoonsgegevens door Pi-NL. Mijn bevindingen uit periodieke controles op alle vorderingen en of verstrekkingen deel ik met Pi-NL en waar nodig de opdrachtgever van Pi-NL. De bevindingen worden nagelopen en in sommige gevallen leidt het tot aanpassingen in TRIP en of wijzigingen in werkinstructies.
De FG rapporteert elk tertaal aan het bestuurlijk driehoeksoverleg, te weten de opdrachtgever Pi-NL (NCTV), de eigenaar (Defensie) en opdrachtnemer (Pi-NL) in hetgeen niet in de weg staat aan rechtstreekse rapportage aan de verwerkingsverantwoordelijke.

De compliance FG benoemd is goed.

## Compliance: om persoonsgegevens te beschermen

Toelichting: Pi-NL heeft de verplichtingen om persoonsgegevens te beschermen uit de PNR-wet geïmplementeerd.

De kaders voor het beschermen van persoonsgegevens zijn aanwezig in wet- en regelgeving en beleid. De implementatie en of het functioneren kunnen verbeterd. Er is geen plan voor het monitoren en actualiseren van de implementatie, een risicoanalyse en de privacy audit. De white list en een DPIA proces ontbreken.

Waarborgen die zijn geïmplementeerd zijn functioneren, namelijk:
- het depersonaliseren van gegevens ouder dan 6 maanden
- het filteren en verwijderen van bijzondere persoonsgegevens of gegevens die daar indirect naar verwijzen
- de toestemming van de OvJ voor het opheffen van de depersonalisering
- het notificeren van de FG bij het verstrekken van passagiersgegevens ouder dan zes maanden en of aan derde landen
- technische maatregelen in TRIP, FG als contactpunt voor betrokkenen

Waarborgen die zijn geïmplementeerd en continue monitoring nodig hebben zijn:
-- het notificeren van de FG
- het depersonaliseren van de gegevens na zes maanden
- de instellingen in de software TRIP of het beveiligingsnetwerk van Defensie kan dor een update onbedoeld wijzigen.

De compliance: om persoonsgegevens te beschermen is voldoende.

## Algemeen beeld: in-control

Toelichting: Pi-NL is in-control als de waarborgen voor het beschermen van persoonsgegevens uit PNR-wet zijn geïmplementeerd. Als het verantwoordelijk management inzicht heeft in de huidige stand van zaken over de implementatie van de waarborgen en de risico's met betrekking tot verzamelingen van persoonsgegevens, beschikt over een plan om de waarborgen te implementeren, de

benodigde resources beschikbaar zijn en de voortgang periodiek wordt gemonitord. Tevens moet een FG benoemd zijn door de verwerkingsverantwoordelijke.

De waarborgen voor het beschermen van persoonsgegevens uit de PNR-wet zijn in voldoende mate aanwezig. Het management van Pi-NL en de verwerkingsverantwoordelijke kunnen de control verbeteren als het de organisatorische maatregelen betreft. Een overzicht van de implementatie van de waarborgen en de risico's van gegevensverwerking die buiten TRIP plaatsvinden en een implementatieplan ontbreken. Het management en de opdrachtgever zijn zich bewust van deze omissies. De staf van Pi-NL is in 2019 niet uitgerust om deze taken op te pakken. In 2020 starten een medewerker voor informatiebeveiliging en een voor juridische zaken hun werkzaamheden ten behoeve van het management. Ik heb een eigen risico-inschatting opgesteld en overgedragen aan het management.

Het onvoldoende in control zijn heeft er niet toe geleid dat de passagiersgegevens onvoldoende beschermd zijn. Iedereen is terdege doordrongen van de gevoeligheid van de verzameling aan persoonsgegevens die Pi-NL beheerd en het belang om de persoonsgegevens te beschermen. De risico's die herkend worden, erkent het management en neemt daarop zijn verantwoordelijkheid door beschermende maatregelen vast te stellen.

Een duidelijker intern normenkader waaraan de in- en externe toezichthouders bij het beschermen van persoonsgegevens kunnen toetsen, inzicht in de operationele risico's bij het werken met persoonsgegevens bijvoorbeeld vastgelegd in een DPIA en prioritering voor een verbeterprogramma zijn instrumenten om in control te komen. Mochten deze instrumenten aanwezig zijn dan heeft de FG daar geen toegang toe noch zijn ze actief ter beschikking gesteld aan de FG.

De samenwerking met Pi-NL is goed. In 2020 blijf ik het management adviseren zodat ze beter in control komen en het beschermen van persoonsgegevens als lijnverantwoordelijkheid ingericht is.