Auditdienst Rijk
Ministerie van Financiën

Assurancerapport
Privacy audit Wet politiegegevens Douane 2021

Definitief 1.0

Colofon

Titel	Privacy audit Wet politiegegevens Douane 2021
Uitgebracht aan	Persoonsgegevens
Datum	22 december 2022
Kenmerk	2022-0000310180

Inlichtingen
Auditdienst Rijk
Persoonsgegevens

Inhoud

1 Aanleiding opdracht—5

2 De Douane voldoet in 2021 in belangrijke mate niet aan de Wpg. Het daadwerkelijk bestendigen en borgen van geconstateerde verbeteringen vraagt om structurele aandacht en inzet.—8

2.1 Oordeel met afkeuring—8
2.2 De basis voor ons afkeurend oordeel—8
2.3 Scope onderzoek—9
2.4 Inherente beperkingen onderzoek—9
2.5 Opstellen verbeterrapport en hercontrole—9

3 Implementatie Wpg vraagt om structurele aandacht en inzet—12

3.1 Bevindingen per norm – Wpg beheersingsmaatregelen—12
3.1.1 Doelbinding (in bewerking) vastgelegd in register van verwerkingsactiviteiten, controle op vastlegging doel in DFB nog niet ingericht—12
3.1.2 Noodzakelijkheid & rechtmatigheid verwerking persoonsgegevens niet voor ieder artikel in opzet vastgelegd, controle en toezicht behoeft aandacht—12
3.1.3 Controle op juistheid & volledigheid politiegegevens niet in opzet vastgelegd—12
3.1.4 Instructies verwerking bijzondere categorieën van persoonsgegevens niet in opzet vastgelegd evenals aanvullende beschermingsmaatregelen—12
3.1.5 Geen sprake van geautomatiseerde individuele besluitvorming, wel aandacht noodzakelijk ter preventie van profilering—12
3.1.6 Onderscheid feiten en oordeel in opzet niet beschreven, aangegeven in praktijk enkel feiten worden gehanteerd—13
3.1.7 Bevoegde functionarissen in opzet aangewezen, in 2021 niet actueel—13
3.1.8 Onderscheid verschillende categorieën van persoonsgegevens mogelijk in DFB, in opzet beschreven werkinstructie ontbreekt—13
3.1.9 Reikwijdte: nog niet alle verwerkingen van politiegegevens zijn geïdentificeerd en gedocumenteerd, onderscheid verschillende privacy regimes noodzakelijk—13
3.1.10 Gegevensbescherming door beveiliging en ontwerp: huidig stelsel van technische en organisatorische maatregelen niet toereikend—13
3.1.11 Verwerkersovereenkomsten niet van toepassing, aanvullende afspraken met Belastingdienst over verwerking persoonsgegevens noodzakelijk—14
3.1.12 Geheimhoudingsplicht ingeregeld, aanvullende screening dient verder te worden uitgekristalliseerd—14
3.1.13 Procedure gegevensbeschermings-effectbeoordeling / DPIA beschreven, inzicht privacy risico's ontbreekt—14
3.1.14 Melding datalekken procedureel beschreven, maar geen relatie met de Wpg en in organisatie onbekend—14
3.1.15 Gegevensbescherming door standaardinstellingen uitwerken door een risicoanalyse—15
3.1.16 Autorisaties en toegang tot politiegegevens niet specifiek gericht op de eisen die de Wpg stelt—15
3.1.17 Uitvoering van de dagelijkse politietaak behoeft aandacht in richtlijnen en de gebruikte voorzieningen—16
3.1.18 Geautomatiseerd vergelijken en in combinatie zoeken is niet van toepassing—16
3.1.19 Ondersteunende taken artikel 13—17
3.1.20 Ter Beschikking stellen (voor verdere verwerking) niet van toepassing—17
3.1.21 Bewaartermijnen, verwijderen en vernietigen behoeft aandacht in instructies en gebruikte voorzieningen—17

3.1.22 Verstrekking van politiegegevens aan anderen dan politie en Koninklijke marechaussee hebben wij niet aan de hand van voorbeelden kunnen toetsen—18
3.1.23 Doorgiften aan derde landen behoeft aandacht in register en toezicht—18
3.1.24 Verstrekking aan derden structureel voor samenwerkingsverbanden is inzichtelijk—18
3.1.25 Rechtstreekse verstrekking moet nog op werking getoetst worden—18
3.1.26 Informatie aan de betrokkene, recht op inzage, rectificatie en verwijdering behoeft aandacht in uitwerking volgens de Wpg—18
3.1.27 Vulling register behoeft aandacht en moet vastgesteld worden—18
3.1.28 Documentatie moet op onderdelen verbeterd worden—19
3.1.29 Logging is nog niet conform de daaraan te stellen eisen ingericht. De Wpg geeft formeel nog ruimte tot 2023.—19
3.1.30 Audits hebben nog niet volgens de Regeling periodieke Audit politiegegevens plaatsgevonden—19
3.1.31 Toezichttaken Privacyfunctionaris nog niet formeel belegd en uitgevoerd—19
3.1.32 Toezicht door de Functionaris voor gegevensbescherming heeft nog niet plaatsgevonden—20
3.2 Bevindingen per norm - organisatorische en technische beheersingsmaatregelen—20
3.2.1 Wijzigingenbeheer, Logische toegangsbeveiliging en Beheer van kwetsbaarheden—20
3.2.2 Toepassing van cryptografie voor opslag en transport van gegevens behoeft aantoonbare controle—20
3.2.3 Vulnerability scans en penetratietesten zijn nog niet uitgevoerd op DFB of daarvoor gebruikte platformen—21

4 Aanbevelingen en/of vervolgstappen—22
4.1 Overzicht aanbevelingen en/of vervolgstappen per norm—22

5 Verantwoording onderzoek—25
5.1 Werkzaamheden en afbakening—25
5.2 Gehanteerde Standaard—26
5.3 Verspreiding rapport—26

6 Ondertekening—28

Bijlage 1 Managementreactie Douane—29

1 Aanleiding opdracht

De Wet Politiegegevens (Wpg) is van toepassing verklaard op persoonsgegevens die in het kader van de politietaak worden verwerkt. Door het implementeren van de richtlijn (EU) 2016/680 in de Wpg is deze ook van toepassing geworden op de taken van de Douane, dat sinds 1 januari 2021 een zelfstandig directoraat-generaal is onder het Ministerie van Financiën. De opsporingstaken van buitengewoon opsporingsambtenaren (boa's) van de Douane, waarbij persoonsgegevens in het kader van de politietaak worden verwerkt, vallen zodoende onder de werking van de Wpg.

De Wpg schrijft voor dat de verwerkingsverantwoordelijke de naleving van de regels gesteld in de Wpg controleert door middel van een periodieke privacy audit. Volgens artikel 6:5 van het Besluit Politiegegevens dient deze privacy c.q. Wpg audit (hierna Privacy audit) twee jaar na inwerkingtreding van de wet en vervolgens eenmaal in de vier jaar te worden uitgevoerd. De auditverplichting is met ingang van 1 januari 2019 (inwerkingtreding van de nieuwe Wpg) van kracht geworden voor de werkgevers van boa's. Op 19 maart 2019 is het besluit politiegegevens BOA van kracht geworden, waardoor de Douane als werkgever van boa's bij het verwerken van politiegegevens valt onder de Wpg. De Autoriteit Persoonsgegevens (AP) heeft ruimte geboden voor een jaar uitstel op de wettelijke verplichting om binnen twee jaar de resultaten van een externe audit aan haar te bieden. Met de ADR is de audit bij de Douane opgestart in april 2021 om aan deze wettelijke verplichting te voldoen. Door de duur van het onderzoek maakt de Douane gebruik van de mogelijkheid die de AP geeft om het Wpg auditrapport een jaar later bij de AP aan te bieden. Dit betekent concreet dat de Douane tot uiterlijk 31-12-2022 heeft om het rapport van de privacy audit uitgevoerd in 2022, over de controleperiode van 1-1-2020 tot en met 31-12-2021, bij de AP aan te leveren.

Deze assurance-opdracht is door de Auditdienst Rijk (ADR) uitgevoerd in opdracht van de Persoonsgegevens De privacy audit heeft betrekking op de wijze waarop bij de Douane het verwerken van politiegegevens is georganiseerd, de maatregelen en procedures die daarop van toepassing zijn en de werking van deze maatregelen en procedures[1]. Dit vanuit de voor de Douane relevante bepalingen van de Wpg.

Doel onderzoek

Het doel van dit assurance-onderzoek is om met een redelijke mate van zekerheid een oordeel te geven of op adequate wijze uitvoering is gegeven aan de bepalingen van de wet[2] (Wpg specifieke bepalingen). Op basis van dit onderzoek geeft de ADR een oordeel over:

a. de opzet en het bestaan van maatregelen en procedures op 31-12-2021 die in de borging van de wettelijke eisen moeten voorzien;
b. de werking van de getroffen maatregelen en procedures over de periode van 1-1-2020 tot en met 31-12-2021.

Omdat de Douane verplicht is om twee jaar na inwerkingtreding de uitvoering van de gegeven regels middels een privacy audit te laten controleren en de AP een jaar uitstel daarop heeft gegeven, moet het rapport in ieder geval het jaar 2021 volledig omvatten. In afwijking op de controleperiode in de oorspronkelijke opdracht voor het toetsen van de werking, zijn wij in deze audit niet verder teruggegaan in de tijd dan 2021. Redenen hiervoor zijn, de nulmeting over 2020 is als basis genomen voor

[1] Besluit Politiegegevens, artikel 6:5, lid 2.
[2] Regeling periodieke audit politiegegevens

de status van verbetermaatregelen, het ontbreken van toezichtmaatregelen in 2021 en het grotendeels ontbreken van andere maatregelen in bestaan in 2021. Het heeft om deze redenen geen toegevoegde waarde om in de audit voor de werking ook naar 2020 te kijken, voor zover dat überhaupt al mogelijk is.

Concreet betekent dit het beantwoorden van de vraag of in voldoende mate is geborgd dat voldaan wordt aan de wetsartikelen van de Wpg die betrekking hebben op de hoofdgebieden:

- Algemene bepalingen (artikelen 1-7);
- De verwerking van politiegegevens met het oog op de uitvoering van de politietaak (artikelen 8-15);
- De doorgifte of verstrekking van politiegegevens aan anderen dan politie en Koninklijke marechaussee (artikelen 16-24);
- Rechten van de betrokkene (artikelen 24a-31c);
- Controle en toezicht op de gegevensverwerking (artikelen31d-36).

Afbakening

De privacy audit heeft betrekking op de artikelen van de Wpg die van toepassing[3] zijn op de Douane bij de verwerking[4] van politiegegevens[5] in het kader van de opsporingstaken van boa's. Het onderzoek richt zich op de beheersingsmaatregelen in de processen en de systemen die gebruikt worden bij de uitvoering van deze taken en de vastlegging van persoonsgegevens hierbij en alleen op de procedures en maatregelen die de Douane in het kader van de Wpg moet treffen.
De ADR heeft geen onderzoek uitgevoerd naar door derden aan de Douane geleverde faciliteiten, voor zover de verantwoordelijkheid is belegd bij anderen dan de Douane. In dergelijke gevallen en indien van toepassing is wel gekeken naar de gemaakte afspraken met betrekking tot de Wpg tussen de partijen en de regie vanuit de Douane gericht op de realisatie van de afspraken (zie 3.1.11).

Omdat het vanwege de omvang onmogelijk is om bij de Douane alle processen waarin Wpg-verwerkingen plaatsvinden te toetsen aan uitvoering van de Wpg, is na overleg met contactpersonen van de Douane voor de scope van deze audit op basis van risico's, omvang en aard van de werkzaamheden van boa's een selectie gemaakt van te onderzoeken onderdelen en locaties. Zie voor nadere details hoofdstuk 5 - Verantwoording onderzoek.

De beoordeling van de opzet, bestaan en werking omvat de maatregelen en procedures die in de borging van de wettelijke eisen uit hoofde van de Wpg moeten voorzien. Het bestaan is beoordeeld aan de hand van de procedures, werkwijze en vastleggingen (alsook van interviews) met als peildatum 31-12-2021. De werking van procedures en maatregelen is, voor zover mogelijk, beoordeeld over 2021. De werking betreft onder andere het ingerichte systeem voor interne controle en toezicht, waarbij inbegrepen ook de uitvoering van interne audits. De AP heeft aangegeven dat de controleperiode voor het onderzoek en rapport in ieder geval het jaar 2021 volledig moet omvatten, omdat gebruik gemaakt wordt van het jaar uitstel dat de AP heeft gegeven.

Verantwoordelijkheden

De Douane is verantwoordelijk voor de opzet, het bestaan en de werking van de relevante beheersingsmaatregelen gedurende de verslagperiode van dit onderzoek. Daarnaast is de Douane verantwoordelijk voor het verstrekken van voldoende en relevante informatie die nodig is voor het toetsen van de beheersingsmaatregelen.

---

[3] Zie Besluit politiegegevens bijzondere opsporingsambtenaren en Besluit politiegegevens.
[4] Elke bewerking of elk geheel van bewerkingen met betrekking tot politiegegevens of een geheel van politiegegevens, al dan niet uitgevoerd op geautomatiseerde wijze, zoals het verzamelen, vastleggen, ordenen, structureren, opslaan, bijwerken of wijzigen, opvragen, raadplegen, gebruiken, verstrekken door middel van doorzending, verspreiden of op andere wijze ter beschikking stellen, samenbrengen, met elkaar in verband brengen, afschermen of vernietigen van politiegegevens.
[5] Elk persoonsgegeven van een geïdentificeerde of identificeerbare natuurlijke persoon dat wordt verwerkt in het kader van de uitvoering van de politietaak.

De verantwoordelijkheid van de ADR is het zodanig plannen en uitvoeren van de assurance-opdracht dat wij daarmee, met een redelijke mate van zekerheid, voldoende en geschikte assurance-informatie verkrijgen voor het door ons af te geven oordeel. Een redelijke mate van zekerheid wil zeggen dat onze assurance-opdracht is uitgevoerd met een hoge mate maar geen absolute mate van zekerheid waardoor het mogelijk is dat wij tijdens onze assurance-opdracht niet alle materiële fouten en fraude ontdekken.

Wij zijn van mening dat de door ons verkregen assurance-informatie voldoende en geschikt is om een onderbouwing voor ons oordeel met een redelijke mate van zekerheid te bieden.

Onafhankelijkheid en kwaliteitsbeheersing

Wij hebben de vereisten van het Reglement Gedragscode ('Code of Ethics') van NOREA nageleefd, welke is gebaseerd op de fundamentele beginselen van integriteit, objectiviteit, vakbekwaamheid en zorgvuldigheid, vertrouwelijkheid en professioneel gedrag. Wij hebben de vereisten uit het Handboek Auditing Rijksoverheid (HARo) nageleefd, inclusief het daarin vastgelegde systeem van Kwaliteitscontrole.

Deze opdracht is uitgevoerd volgens de Richtlijnen voor assurance-opdrachten door IT-auditors (NOREA 3000D). Een assurance-opdracht om te rapporteren over de opzet, het bestaan en de werking van beheersmaatregelen omvat het uitvoeren van werkzaamheden ter verkrijging van assurance informatie met in dit geval een redelijke mate van zekerheid.

Leeswijzer

In het volgende hoofdstuk is de hoofdboodschap (oordeel) van dit onderzoek opgenomen. Dit geeft antwoord op de centrale vraag van het onderzoek. Tevens is een totaaloverzicht opgenomen met de conclusies per norm. In hoofdstuk 3 zijn de bevindingen per norm opgenomen. In hoofdstuk 4 zijn per norm de aanbevelingen ter verbetering van de naleving van de Wpg opgenomen. Hoofdstuk 5 en 6 bevatten de verantwoording van het onderzoek en de ondertekening van het rapport.

2 De Douane voldoet in 2021 in belangrijke mate niet aan de Wpg. Het daadwerkelijk bestendigen en borgen van geconstateerde verbeteringen vraagt om structurele aandacht en inzet.

2.1 Oordeel met afkeuring

Wij hebben bij de Douane onderzocht of aan de bepalingen van de Wet politiegegevens op adequate wijze uitvoering is gegeven. Op grond van onze werkzaamheden en de verkregen informatie concluderen wij met een redelijke mate van zekerheid dat het stelsel van maatregelen en procedures in 2021 in belangrijke mate niet voldoet aan alle van materieel belang zijnde aspecten en daarmee niet effectief is in opzet, bestaan en werking. Op basis hiervan geven wij een afkeurend oordeel.

Ons oordeel is gevormd op basis van de bevindingen die in dit assurancerapport uiteengezet zijn. Het hierbij gehanteerde normenkader, gebaseerd op de artikelen in de wet, omvat de door de Douane te nemen maatregelen. De specifieke, getoetste beheersingsmaatregelen en de resultaten van die toetsingen zijn opgenomen in Tabel 1 en 2 – overzicht conclusie per norm en hoofdstuk 3 waarin een beschrijving van de bevindingen is opgenomen.

2.2 De basis voor ons afkeurend oordeel

Voor 2021 hebben wij vastgesteld dat het merendeel van de maatregelen niet of slechts deels zijn ingericht en geborgd in de organisatie en daarmee niet wordt voldaan aan de daaraan te stellen eisen. In veel gevallen gaat het daarbij ook om de zogenaamde key controls (in Tabel 1 en 2 met 'X' aangegeven). Dit zijn aspecten die een groter risico kunnen vormen voor het beschermen van de privacy van betrokkenen als er niet aan wordt voldaan. Ten opzichte van de nulmeting door de ADR naar de implementatie van de Wpg over 2020 (rapportage mei 2021) zijn er in 2021 nauwelijks vorderingen gemaakt in het daadwerkelijk doorvoeren van destijds geconstateerde verbetermogelijkheden[6]. In de tweede helft, en met name eind 2021 zijn wel verbeteracties opgepakt en in gang gezet, maar dat heeft voor dat jaar nog niet geleid tot concrete en functionerende maatregelen. Voor een aantal maatregelen heeft dat pas in de loop van 2022 (deels) effect gehad en/of moet in veel gevallen het daadwerkelijk bestendigen en borgen in de organisatie op moment van onderzoek nog plaatsvinden. In 2021 heeft er weinig tijd gezeten tussen het opgeleverde rapport van de nulmeting, het oppakken van de verbetermaatregelen en de ruimte die er toen nog was voor het daadwerkelijk effectueren van verbetermaatregelen. Veel van deze maatregelen vragen immers aanzienlijk wat tijd om deze met structurele aandacht en inzet te bestendigen en borgen in de organisatie. Dat neemt echter niet weg dat de Wpg en de BIO, waar het gaat om beveiligingsmaatregelen ook ter bescherming van de privacy, al eerder (begin 2019) van toepassing waren. Voor een overzicht van de afwijkingen van de norm wordt verwezen naar Tabel 1 en 2: Overzicht conclusie per norm.

[6] Overigens zijn niet alle Wpg maatregelen in het onderzoek van de ADR over 2020 object van onderzoek geweest. De aard en diepgang van deze audit was ook anders dan nu: het betrof toen geen assurance audit. Met deze assurance audit zijn ook andere en nieuwe verbetermaatregelen geconstateerd.

In hoofdstuk 3 zijn de belangrijkste bevindingen per getoetste maatregel opgenomen. In hoofdstuk 4 zijn de aanbevelingen en/of vervolgstappen naar aanleiding van de geconstateerde bevindingen opgenomen.

2.3 Scope onderzoek

Het onderzoek richt zich alleen op de procedures en maatregelen die de Douane moet treffen voor naleving van de Wpg-eisen. De ADR heeft geen onderzoek verricht naar door derden aan de Douane geleverde faciliteiten, voor zover de verantwoordelijkheid is belegd bij een andere overheidsorganisatie dan de Douane. In dergelijke gevallen is wel gekeken naar de gemaakte afspraken tussen de partijen en de regie vanuit de Douane gericht op de realisatie van de afspraken (zie 3.1.11).

2.4 Inherente beperkingen onderzoek

De conclusie is verder onderworpen aan de inherente beperkingen die in paragraaf 5.1 van dit assurance-rapport zijn genoemd. Ons oordeel is gevormd op basis van bevindingen die in deze rapportage zijn opgenomen. Het hierbij gehanteerde normenkader, gebaseerd op de artikelen in de wet, omvat de door de Douane te nemen maatregelen.

Wij kunnen niet uitsluiten dat, indien wij aanvullende beheersingsmaatregelen zouden hebben onderzocht, wellicht andere onderwerpen zouden zijn geconstateerd die voor rapportering in aanmerking zouden zijn gekomen.

2.5 Opstellen verbeterrapport en hercontrole

De verwerkingsverantwoordelijke is, op grond van artikel 4 lid 1 van de Regeling periodieke audit politiegegevens, verplicht binnen drie maanden een verbeterrapport op te stellen waarin de maatregelen zijn beschreven die getroffen worden ter verbetering van de in de privacy audit geconstateerde tekortkomingen. Op grond van artikel 4 lid 3 kan de hercontrole door de interne auditors worden uitgevoerd. De resultaten van het verbeterrapport en de uitgevoerde hercontrole zullen in de volgende externe privacy audit worden meegenomen.

Tabel 1: Overzicht conclusie per norm – Wpg beheersingsmaatregelen

Nr.	Norm	Key control	Conclusie		
			Opzet	Bestaan	Werking
1.	Doelbinding				
2.	Noodzakelijkheid en rechtmatigheid politiegegevens				
3.	Juistheid en volledigheid politiegegevens				
4.	Bijzondere categorieën van politiegegevens	X			
5.	Geautomatiseerde individuele besluitvorming				
6.	Onderscheid feiten en oordeel				
7.	Autorisaties: aanwijzen functionarissen				
8.	Onderscheid tussen verschillende categorieën van betrokkenen				
9.	Reikwijdte				
10.	Gegevensbescherming door beveiliging en ontwerp	X			
11.	Verwerker en verwerkersovereenkomst	X			

Nr.	Norm	Key control	Conclusie		
			Opzet	Bestaan	Werking
12.	Geheimhoudingsplicht				
13.	Gegevensbeschermingseffectbeoordeling / DPIA	X			
14.	Melding datalekken	X			
15.	Gegevensbescherming door standaardinstellingen				
16.	Autorisaties en toegang tot politiegegevens	X			
17.	Uitvoering van de dagelijkse politietaak				
18.	Geautomatiseerd vergelijken en in combinatie zoeken	X			
19.	Ondersteunende taken				
20.	Ter beschikking stellen (voor verdere verwerking)				
21.	Bewaartermijnen, verwijderen en vernietigen	X			
22.	Verstrekking van politiegegevens aan anderen dan politie en Koninklijke marechaussee	X			
23.	Doorgiften aan derde landen	X			
24.	Verstrekking aan derden structureel voor samenwerkingsverbanden	X			
25.	Rechtstreekse verstrekking				
26.	Informatie aan de betrokkene, recht op inzage, rectificatie en verwijdering	X			
27.	Register	X			
28.	Documentatie	X			
29.	Logging	X			
30.	Audits	X			
31.	Privacyfunctionaris	X			
32.	Functionaris voor gegevensbescherming	X			

Tabel 2: Overzicht conclusie per norm – organisatorische en technische beheersingsmaatregelen

Nr.	Norm	Key control	Conclusie		
			Opzet	Bestaan	Werking
1.	Wijzigingenbeheer	X			
2.	Logische toegangs-beveiliging	X			
3.	Beheer van kwetsbaarheden (patch-management)	X			
4.	Cryptografie	X			
5.	Vulnerability scans en Penetratietesten	X			

Toelichting gebruikte kleuren conclusie per norm:
Groen - Voldoet aan de norm.
Oranje - Voldoet deels aan de norm.
Rood - Voldoet niet aan de norm.
Grijs – Niet onderzocht/nog niet kunnen onderzoeken/niet van toepassing

Criteria met betrekking tot de opzet, het bestaan en de werking:

Opzet	De organisatie heeft de interne beheersingsmaatregen beschreven die, indien deze werken zoals beschreven, een redelijke mate van zekerheid bieden dat voorzien is in de borging van de wettelijke eisen met betrekking tot de verwerking van politiegegevens door boa's.
Bestaan	De organisatie heeft de interne beheersingsmaatregelen overeenkomstig de opzet daadwerkelijk geïmplementeerd en toegepast.
Werking	De organisatie heeft de interne beheersingsmaatregelen gedurende de verslagperiode volgens de opzet toegepast. In het geval van handmatige beheersingsmaatregelen zijn deze toegepast door competente én bevoegde personen.

3 Implementatie Wpg vraagt om structurele aandacht en inzet

3.1 Bevindingen per norm – Wpg beheersingsmaatregelen

Per onderwerp uit de Wpg is de ADR tot de volgende bevindingen gekomen:

3.1.1 Doelbinding (in bewerking) vastgelegd in register van verwerkingsactiviteiten, controle op vastlegging doel in DFB nog niet ingericht

De Douane verwerkt politiegegevens in het kader van de opsporingstaak en strafrechtelijke afdoening. Hierbij worden persoonsgegevens en de aard van de overtreding verwerkt met name in proces-verbalen en daarna een vastlegging hiervan in Douane Fraude Bestrijding (DFB). Het doel van verwerkingen betreft art. 8, art. 9 en art. 13 is ("in bewerking") is in opzet vastgelegd in het register van verwerkingsactiviteiten. De ADR heeft echter geen proces in opzet en bestaan aangetroffen dat toeziet op (de vastlegging van) doelbinding.

3.1.2 Noodzakelijkheid en rechtmatigheid verwerking persoonsgegevens niet voor ieder artikel in opzet vastgelegd, controle en toezicht behoeft aandacht

Op welke manier de Douane borgt dat er enkel persoonsgegevens worden verwerkt die daartoe toereikend, ter zake dienend en beperkt zijn tot wat noodzakelijk is, komt niet uit de ontvangen documentatie naar voren. Enkel voor art. 8 verwerkingen is er in opzet documentatie aanwezig waaruit op te maken is welke persoonsgegevens vastgelegd moeten worden in een proces-verbaal in het kader van strafrechtelijke en juridische verplichtingen. Uit gesprekken komt echter naar voren dat iedere boa een eigen manier heeft voor het invullen en verwerken van een proces-verbaal. Uit de ontvangen documentatie valt tevens niet op te maken welke organisatorische en technische maatregelen getroffen zijn die borgen dat enkel persoonsgegevens verwerkt worden die noodzakelijk zijn voor de verwerking.

3.1.3 Controle op juistheid & volledigheid politiegegevens niet in opzet vastgelegd

Er zijn niet in opzet beschreven processen en werkinstructies aangeleverd waaruit blijkt dat de Douane controles heeft ingericht op de kwaliteit ten behoeve van de borging van de juistheid en nauwkeurigheid van persoonsgegevens. Aangegeven is dat dit in de praktijk wordt vormgegeven middels een 4 ogen-principe dan wel via de afdeling contentieus of de hulpofficier van justitie.

3.1.4 Instructies verwerking bijzondere categorieën van persoonsgegevens niet in opzet vastgelegd evenals aanvullende beschermingsmaatregelen

Er zijn niet in opzet beschreven processen en werkinstructies aangeleverd ten aanzien van de verwerking van bijzondere persoonsgegevens. Ook al staat in het register van verwerkingsactiviteiten aangegeven dat er in 'principe' geen bijzondere persoonsgegevens verwerkt worden, blijkt echter in de praktijk dat er tamelijk gevoelige c.q. vertrouwelijke persoonsgegevens worden verwerkt zoals het BSN, kopie ID/rijbewijs en een omschrijving van de strafbare feiten. Beschrijf de risico's die hierbij kunnen spelen (misbruik van het gegeven nationaliteit voor discriminerende profilering bijvoorbeeld) en de maatregelen die hiervoor getroffen zijn of moeten worden.

3.1.5 Geen sprake van geautomatiseerde individuele besluitvorming, wel aandacht noodzakelijk ter preventie van profilering

In het register van verwerkingsactiviteiten staat aangegeven dat er geen sprake is van geautomatiseerde individuele besluitvorming. De ADR heeft geen procedures dan wel werkinstructies ontvangen die de omgang met en het verbod op

geautomatiseerde besluitvorming uiteenzetten. Dit geldt tevens voor bewustwordingsactiviteiten ter preventie van profilering.

3.1.6 Onderscheid feiten en oordeel in opzet niet beschreven, aangegeven in praktijk enkel feiten worden gehanteerd

In opzet is er geen proces beschreven dat borgt om politiegegevens die op feiten gebaseerd zijn te onderscheiden van politiegegevens die op persoonlijk oordeel zijn gebaseerd. Aangegeven is dat te allen tijde enkel feiten beschreven mogen worden in een proces-verbaal. Middels het vier-ogen-principe van onder andere een technische coach wordt hier een check op uitgevoerd. Het belang van feitelijke constateringen wordt meegegeven bij de opleiding dan wel opfriscursussen.

3.1.7 Bevoegde functionarissen in opzet aangewezen, in 2021 niet actueel

De Douane beschikt over een in opzet beschreven lijst van, door de verantwoordelijke aangewezen, bevoegde functionarissen voor de Wpg. Deze lijst wordt ondersteund door een mandaat. Uit de praktijk blijkt dat ook accountmanagers toestemming verlenen tot nader onderzoek. Aangegeven is dat deze namen tevens vermeld dienen te worden in de lijst met bevoegde functionarissen. De ADR heeft geconstateerd dat dit voor 2021 niet het geval is. Inmiddels is deze lijst actueel.

3.1.8 Onderscheid verschillende categorieën van persoonsgegevens mogelijk in DFB, in opzet beschreven werkinstructie ontbreekt

De Douane beschikt niet in opzet over een werkinstructie betreffende het vastleggen van een onderscheid tussen verschillende categorieën van betrokkenen. Wel heeft de ADR vastgesteld dat hier binnen DFB de mogelijkheid is ingericht. Daarnaast benoemen de verwerkingen in het register van verwerkingsactiviteiten de verschillende categorieën van betrokkenen. Aangegeven is dat in praktijk vermeld wordt welke betrokkenen er bestaan (verbalisant, verdachte, slachtoffer) bij het opmaken van een proces-verbaal en het opvoeren in DFB. De ADR heeft het bestaan hiervan niet kunnen vaststellen.

3.1.9 Reikwijdte: nog niet alle verwerkingen van politiegegevens zijn geïdentificeerd en gedocumenteerd, onderscheid verschillende privacy regimes noodzakelijk

De Douane heeft nog niet alle verwerkingen van politiegegevens binnen de organisatie geïdentificeerd en gedocumenteerd. Er is een eerste inschatting gemaakt van de verwerkingen en deze zijn opgenomen in het register van verwerkingsactiviteiten. De scheiding tussen AVG en Wpg vloeit voort uit de sfeerovergang van toezicht naar opsporing. De Douane besteedt hier aandacht aan in verschillende handboeken en nieuwsbrieven en informatie naar de regio's. Het ontbreekt echter aan voldoende bewustzijn binnen de regio's.

Er is geen overzicht van alle systemen en processen waar Wpg-gegevens in staan. De Douane is voornemens om eind 2022 alle AVG-verwerkingen in beeld te hebben. Wpg-verwerkingen zullen daarna moeten volgen. DFB is gebouwd voor de intreding van de Wpg voor boa's. Een onderscheid tussen de verschillende privacy regimes is hierin niet aanwezig. Aangegeven is dat in het nieuwe systeem Douane Onregelmatigheden (DON), naar verwachting operationeel in mei 2023, deze scheiding wel wordt aangebracht.

3.1.10 Gegevensbescherming door beveiliging en ontwerp: huidig stelsel van technische en organisatorische maatregelen niet toereikend

Bij de Douane is risicomanagement onderdeel van het Integraal informatiebeveiligingsbeleid (IIB) vastgesteld door de Belastingdienst. De Douane beschikt aanvullend over een procedure DPIA en heeft een risicoregister opgesteld waarin gesignaleerde risico's met betrekking tot applicatiebouw en ingekochte applicaties zijn opgenomen. Echter is aangegeven dat er nog geen risicoanalyse uitgevoerd is waarmee inzicht is verkregen in de gesignaleerde risico's voor de bescherming van persoonsgegevens in relatie tot de gewijzigde Wpg.

Aangegeven door de Douane is dat zij heeft geconstateerd dat het huidige stelsel van technische en organisatorische maatregelen niet toereikend is om de persoonsgegevens die verwerkt worden in het kader van de politietaak te beschermen. Dit komt mede omdat de Douane nog geen volledig beeld heeft van het toepassingsgebied van de Wpg en doordat de bestaande beveiligingsmaatregelen uit de periode voor de nieuwe Wpg dateren. De Douane is voornemens een risicoanalyse uit te voeren naar verwerkingen in het nieuwe systeem DON. Daarnaast is er voor de Wpg een epic (architectuur product) opgesteld waarin specifiek aandacht is voor beveiligingsmaatregelen.

3.1.11 Verwerkersovereenkomsten niet van toepassing, aanvullende afspraken met Belastingdienst over verwerking persoonsgegevens noodzakelijk

In het register van verwerkingsactiviteiten wordt door de Douane aangegeven dat bij de vermelde verwerkingen geen sprake is van verwerkers. Hierdoor zijn er geen formele verwerkersovereenkomsten beschikbaar. Wel heeft de Douane op hoofdlijnen samenwerkingsafspraken met de Belastingdienst vastgelegd gezien systemen zoals DFB (nog) worden beheerd door de Belastingdienst. Deze afspraken betreffen echter geen afspraken over het verwerken van persoonsgegevens in het kader van de politietaak (Wpg).

3.1.12 Geheimhoudingsplicht ingeregeld, aanvullende screening dient verder te worden uitgekristalliseerd

In het IIB staat aangegeven dat de medewerkers een geheimhoudingsplicht hebben. Vanuit de geheimhoudingsplicht is het beleid dat aan elke nieuwe medewerker en uitzendkracht een VOG wordt gevraagd. Aangegeven is dat er momenteel een discussie loopt over aanvullende screening van boa's. Vraag is namelijk of enkel een VOG voor boa's, die vallen onder de benoemde categorie van artikel 3 Bpg BOA, afdoende waarborgen biedt en of een strengere screening/controle gewenst is. Hier spelen, naast de regels rond geheimhouding, ook de beheersmaatregelen rond integriteitsaspecten.

3.1.13 Procedure gegevensbeschermings-effectbeoordeling / DPIA beschreven, inzicht privacy risico's ontbreekt

De Douane beschikt in opzet over een procedure voor het opstellen van een Data protection impact assessment (DPIA). Deze procedure is echter geënt op de AVG en dient nog uitgebreid te worden met aanvullende eisen vanuit de Wpg. Aangegeven is dat de Douane voornemens is om een DPIA uit te voeren op de verwerkingen in het nieuwe systeem DON. Momenteel is die DPIA nog niet uitgevoerd waardoor er nog geen inzicht is in de privacyrisico's voor de betrokkenen. Door het ontbreken van inzicht in deze risico's kan er geen passend stelsel van maatregelen worden ingericht.

3.1.14 Melding datalekken procedureel beschreven, maar geen relatie met de Wpg en in organisatie onbekend

De Douane kent de Procedure meldplicht datalekken, Ministerie van Financiën, Versie 1.0, Datum 19 september 2019, Status Definitief. In deze procedure zijn de verantwoordelijkheden omschreven en belegd bij: Meldpunt Datalekken, CIO, Privacy Officer, FG en CISO. Uit de interviews komt naar voren dat de Procedure meldplicht datalekken vaak onbekend is. Daarnaast wordt er bij datalekken alleen gedacht aan gegevens en niet aan de devices: porto's, telefoons en laptops die zoekraken/vermist worden. Hierdoor wordt er risico gelopen dat niet alle datalekken worden gemeld.
Verder hebben we geen informatie aangetroffen waaruit blijkt dat de Douane de risico's classificeert in hoog/middel/laag van inbreuken op de beveiliging van persoonsgegevens. Daardoor zou bij een voorval met een hoog risico kunnen dat betrokkenen voor hun rechten en vrijheden niet in kennis worden gesteld van een inbreuk op de beveiliging.

Daarnaast is er nog een uitdaging, de volledigheid van de proces-verbalen in de registratie. Vanuit het perspectief van interne beheersing is het een uitdaging om te checken of alle aangevraagde DFB-nummers ook daadwerkelijk resulteren in een binnengekomen proces-verbaal. Het missen van een proces-verbaal kan namelijk duiden op een mogelijk datalek. De Douane is zich hiervan bewust dat er geen beheersingsmaatregelen voor getroffen zijn.

De registratie van datalekken vindt bij de Douane plaats in een Excel bestand. In dit bestand is niet specifiek aangegeven of het datalek een relatie heeft met Wpg gegevens. In 2021 zijn 28 datalekken geweest en hoe deze zijn afgehandeld. Uit navraag blijkt dat In 2021 er 1 incident is waarbij MOGELIJK Wpg gegevens zijn gelekt. Maatregelen per datalek om soortgelijke toekomstige inbreuken te voorkomen, worden niet vermeld.
Alle geregistreerde 28 datalekken zijn gemeld aan de AP. Tevens dienen datalekken tijdig aan de AP te worden gemeld. Daartoe is het nodig dat de tijdstippen van datalek en melding aan de AP worden vastgelegd. Het tijdstip van melding aan de AP wordt niet bijgehouden in dit Excel-bestand.

3.1.15 *Gegevensbescherming door standaardinstellingen uitwerken door een risicoanalyse*

De Douane dient binnen de organisatie de gegevensbescherming te waarborgen, door onder meer het opzetten van risicoanalyses voor haar systemen, waaronder die waarin Wpg-gegevens worden vastgelegd. Momenteel is er een deels afgeronde risicoanalyse opgesteld voor de applicatie DFB. Hierdoor is het toezicht op het naleven van beveiligingsmaatregelen specifiek voor de Wpg nog niet voldoende uitgewerkt en ingericht. Voor de applicatie DON, de opvolger van DFB, zal een risicoanalyse worden opgesteld. Zie voor de risicoanalyses tevens "Gegevensbeschermings-effectbeoordeling".

3.1.16 *Autorisaties en toegang tot politiegegevens niet specifiek gericht op de eisen die de Wpg stelt*

De Douane gaat uit van een systeem van autorisaties dat personen alleen toegang krijgen tot die gegevens die vanuit hun functie nodig zijn en vanuit de wet mogen, het need-to-know principe.

De interne beheersing van de autorisaties van de Douane focust zich in algemene zin op de logische toegangsbeveiliging waarvoor een proces is ingericht dat ook jaarlijks wordt getoetst. Het gaat daarbij om het beheersen van het proces van instromen, doorstromen en uitstromen van medewerkers en het tijdig intrekken en aanpassen van toegangsrechten voor systemen en niet specifiek voor de Wpg. Toegang tot systemen en functiescheiding is op basis van een rollenmodel en SOD-regels (segregation of duties) ingericht. Daarvoor gebruikt men een IMS-systeem. Indien een medewerker vertrekt c.q. uit dienst gaat dan betreft dit een automatisch proces waarbij een signaal wordt afgegeven op basis van de datum uit dienst in het SAP-systeem aan IMS. Dit proces wordt door HRM beheerd.

Voor het autoriseren van personen tot de Wpg-gegevens in het systeem DFB is er een autorisatiematrix / functiescheidingsmatrix die de soll-positie weergeeft. Deze autorisatiematrix / functiescheidingsmatrix is niet specifiek ingericht voor Wpg. De Douane legt de gegevens uit de proces-verbalen in DFB vast als artikel 8 registratie. Zodra de Officier van Justitie besluit dat er juridisch sprake is van een zaak, dan dienen de betrokken gegevens conform de Wpg vanuit een artikel 8-omgeving te worden overgebracht naar een artikel 9-omgeving. Deze artikel 9-omgeving mag alleen benaderbaar zijn door personen die belast zijn met opsporing. Deze informatie wordt dan vastgelegd in ATD dan wel SUMMIT (systeem van de politie). Daarnaast kan in DFB geen onderscheid worden gemaakt naar ouderdom van gegevens die op grond van de Wpg dient te worden gemaakt. De gegevens uit de Procesverbalen worden vastgelegd in een artikel 8-omgeving. De datum van vastlegging bepaalt de bewaartermijn in een artikel 8-omgeving. Volgens de Wpg dienen deze gegevens na een jaar in een artikel 8-omgeving via het hit-no hit principe beschikbaar te blijven. Deze gegevens mogen volgens de Wpg alleen na

verkregen toestemming benaderbaar zijn. Zie ook onder "Uitvoering van de dagelijkse politietaak".

De autorisatie van personen tot DFB gebeurt, na het besluit van de teamleider om de autorisatie toe te kennen, via de goedkeuringslokketten met gemandateerde medewerkers die in IMS roltoekeningen toetsen aan de gestelde criteria.

In het dossiersysteem ATD/Caseware worden de documenten van de proces-verbalen als scans (de scans zijn niet doorzoekbaar) vastgelegd. De toegang tot ATD/Caseware wordt apart geregeld. Een administratief medewerker kent een gebruiker vervolgens mutatie- of raadpleegrechten toe tot een specifiek dossier in ATD/Caseware. Aangegeven is dat binnen ATD/Caseware enkel de toegewezen medewerker en accountmanager toegang hebben tot het dossier. Er worden tussentijds geen autorisaties ingetrokken. Wanneer iemand uit dienst gaat wordt de hoofdautorisatie ingetrokken waardoor je in de onderliggende systemen waaronder ATD/Caseware niet meer kan.

Jaarlijks wordt een controleprogramma Beveiliging opgesteld en uitgevoerd. De hierin vastgelegde controles worden uitgevoerd op de autorisaties door medewerkers van team 3 en 10 van de DLSO. Deze controles zijn gericht op de logische toegangsbeveiliging van de systemen van de Douane en niet specifiek gericht op de eisen die de Wpg stelt zoals voor het kunnen vaststellen dat alleen functionarissen van opsporing toegang hebben tot de artikel 9 gegevens en dat artikel 8 gegevens na een jaar na registratie achter een schot worden geplaatst en daarna alleen toegang kan worden verkregen op basis van een goedgekeurd verzoek voor specifiek aangegeven gegevens van de achter het schot geplaatste gegevens.

3.1.17 *Uitvoering van de dagelijkse politietaak behoeft aandacht in richtlijnen en de gebruikte voorzieningen*

Er zijn geen richtlijnen voor het verwerken van politiegegevens volgens de Wpg. Niet is altijd even duidelijk wanneer in het verwerken van gegevens de Wpg van toepassing is. In het Proces Aanhouden verdachte "Van de aanhouding wordt een proces-verbaal opgemaakt in het DFB-bestand van de Douane". Dit kan worden beschouwd als de eerste verwerking.
De overgang van controle en opsporingsactiviteiten is in praktijk soms lastig te duiden. Het raadplegen van bepaalde politiegegevens gebeurt ook in de controlesfeer, opsporingsinformatie is dan weer input voor risicovinding in het toezichtsproces.

Daarnaast kan in DFB geen onderscheid worden gemaakt naar ouderdom van gegevens die op grond van de Wpg dient te worden gemaakt. Zie ook onder "Autorisaties en Toegang tot politiegegevens".
De gegevens uit de proces-verbalen worden vastgelegd in een artikel 8-omgeving. Volgens de Wpg dienen deze gegevens na een jaar in een artikel 8-omgeving te worden gearchiveerd. Deze gearchiveerde gegevens mogen volgens de Wpg alleen na verkregen toestemming benaderbaar zijn.

3.1.18 *Geautomatiseerd vergelijken en in combinatie zoeken is niet van toepassing*

Er wordt gesproken over toepassing van de artikelen 8 t/m 13 van de Wpg. Artikelen 10, 11 en 12 zijn niet van toepassing voor de Douane. Artikel 8 en 9 verschillen er voornamelijk in dat bij art. 9 verwerking (door POSS) daadwerkelijke tussenkomst/bemoeienis (aansturing van de opsporing) is van een officier van justitie voor verdere verwerking van politiegegevens. Daarnaast is geautomatiseerd vergelijken in ATD/Caseware technisch niet mogelijk omdat de documenten van het proces-verbaal als scan zijn opgeslagen. Verder heeft een persoon op basis van autorisaties alleen toegang tot specifieke dossiers.

3.1.19 *Ondersteunende taken artikel 13*

De Douane verwerkt, door eigen interne afdelingen, zelf de gegevens van proces-verbalen van de BOA's in DFB en de Wpg-waarnemingen van de BOA's in het Douane Toezicht Journaal (DTJ), thans het Douane Toezicht Register (DTR)

De Wpg is bij de Douane van toepassing op de verwerking van politiegegevens door BOA's van de Douane, maar alleen voor zover die verwerking plaatsvindt in het kader van hun opsporingstaak (van strafbare feiten) en niet in het kader van de toezichttaak. Wanneer een strafbaar feit ter plaatse wordt geconstateerd worden o.a. de volgende gegevens vastgelegd: tijdstip en plaats van de vondst en de vermoedelijke overtreding van bijvoorbeeld de Opiumwet. Dit wordt opgeslagen in een proces-verbaal (PV). Deze worden in een sjabloon vastgelegd. Het PV wordt geprint en ondertekend. Als de PV's nodig zijn voor de werkzaamheden binnen het HARC-team worden deze via het DIC gedeeld met het Harc-team.

Naast DFB speelt het register van verwerkingen het Douane Toezicht Journaal (DTJ) een belangrijke rol bij het verwerken van politiegegevens in het Douanetoezicht. DTJ is een systeem waarin de BOA's onregelmatigheden kunnen melden, wanneer zij een strafbaar feit ontdekken. Een feitenrelaas van de werkzaamheden wordt opgenomen in het DTR. Het HARC-team is geautoriseerd voor de registratie en bepaalt of er nader onderzoek zal plaatsvinden. Het moment dat een strafbaar feit wordt geconstateerd gaat het onderzoek over op opsporing.
Vanuit het DTJ wordt een extract gemaakt met de gebeurtenissen van de afgelopen 3 maanden ter inzicht voor de verbalisanten. Er staan ook gegevens van verdachten in DTJ, alleen in geval van onregelmatigheden.

In mei 2022 is het DTJ vervangen door het Douane Toezicht Register (DTR). Uit DTR hebben wij een drietal voorbeelden gezien hoe een onregelmatigheid heeft geleid tot een strafbaar feit. Omdat DTJ inmiddels is vervangen door DTR en het hier om toezicht gaat, hebben wij een onderzoek naar de werking van DTJ in 2021 niet zinvol geacht.

3.1.20 *Ter Beschikking stellen (voor verdere verwerking) niet van toepassing*

Er wordt gesproken over toepassing van de artikelen 9 en 10 van de Wpg. Artikel 10 is niet van toepassing voor de Douane. Daarnaast is er geen sprake van externe verwerking. De Douane verwerkt haar eigen gegevens door haar eigen interne afdelingen.

3.1.21 *Bewaartermijnen, verwijderen en vernietigen behoeft aandacht in instructies en gebruikte voorzieningen*

Door de Douane is een lijst van bewaartermijnen met grondslagen opgesteld. Hierop zijn vermeld de bewaartermijnen van gegevens inzake WPG-artikel 8 en 9 en de voorwaarden van bewaring.

Opslag van WPG-gegevens vindt plaats:

- Op de gemeenschappelijke Q-schijf worden digitale pv's inclusief bewijsmateriaal bewaard als een volledig digitaal archief vanaf 2008 tot heden naast DFB. Op basis hiervan valt op te maken dat er hier geen schoning plaatsvindt volgens bepaalde Wpg bewaar-/vernietigingstermijnen. Onbekend in de organisatie is wat hiervoor de instructies zijn en wie bij deze gegevens kunnen.
- DFB en ATD/Caseware, het dossiersysteem van POSS, bevatten geen bewaartermijnen conform Wpg. Ook is er aangegeven dat er geen proces is ingericht dat de bewaartermijnen binnen ATD/Caseware monitort. Dit is volgens POSS een centrale Douane verantwoordelijkheid die bij IM ligt. De bewaartermijn van een dossier gaat lopen als een zaak onherroepelijk is geworden. Dat kan soms wel enige tijd duren voordat het zover is.
- Verder worden ook (beveiligde) netwerkschijven (C:, N: en Q:) en e-mail gebruikt voor tussentijds opslaan van gegevens. Interne afspraak vanuit leidinggevende is om deze gegevens te verwijderen zodra deze zijn

opgenomen in KRM (Klant Register Management) en ATD/Caseware. Het schonen betreft uiteindelijk een eigen verantwoordelijkheid van de medewerkers. Het is de geïnterviewden niet bekend of hier intern toezicht of controles op wordt gehouden.

3.1.22 *Verstrekking van politiegegevens aan anderen dan politie en Koninklijke marechaussee hebben wij niet aan de hand van voorbeelden kunnen toetsen*

Er zijn geen voorbeelden van verstrekkingen buiten het Wpg domein.

3.1.23 *Doorgiften aan derde landen behoeft aandacht in register en toezicht*

Anders dan het doorgeven van politiegegevens aan Europese Lidstaten via Napels II, worden er niet aan derde landen politiegegevens doorgegeven volgens art. 17a. Het register van gegevensverwerkingen is op dit punt niet helemaal duidelijk. Wij hebben niet aan de hand van voorbeelden uit de registratie kunnen vaststellen of het doorgeven van politiegegevens aan Europese Lidstaten via Napels II volgens de norm en art. 17a plaatsvindt.

3.1.24 *Verstrekking aan derden structureel voor samenwerkingsverbanden is inzichtelijk*

De Douane heeft inzicht in de verstrekkingen die op vordering verstrekt kunnen worden.

3.1.25 *Rechtstreekse verstrekking moet nog op werking getoetst worden*

Voor rechtstreekse verstrekkingen van politiegegevens is een proces beschreven en eind 2021 ingericht. De werking van dit proces moet nog blijken uit het (interne) toezicht op de naleving van de Wpg door de PF en/of pFG dat nog cyclisch moet plaatsvinden. De werking van het beschreven en ingerichte proces kan pas goed vastgesteld worden als dit proces enige tijd functioneert.

3.1.26 *Informatie aan de betrokkene, recht op inzage, rectificatie en verwijdering behoeft aandacht in uitwerking volgens de Wpg*

De Douane geeft aan, net zoals in de nulmeting over 2020, nog geen uitspraken te kunnen doen over de toereikendheid van deze procedures om de Wpg-verzoeken van betrokkenen tijdig en adequaat af te handelen, omdat er nog geen verzoeken zijn gedaan en er dus nog geen overzicht van is.

Er is een procesbeschrijving voor verzoeken van betrokkenen. Dit document beschrijft hoe verzoeken van betrokkenen dienen te worden behandeld. Procedureel wordt zoveel mogelijk aangesloten bij de procedure zoals die geldt voor de behandeling van inzageverzoeken AVG. Er is ook een instructie rechten van betrokkenen AVG en Wpg. Dit is een groeidocument. Op de websites van het ministerie van Financiën en de Belastingdienst is een privacyverklaring inclusief toelichting opgenomen. De privacyverklaring van de Belastingdienst is een verbijzondering van de privacyverklaring van het Ministerie van Financiën. Beide websites zijn nog niet aangepast aan de Douane en de Wpg en er is geen mogelijkheid opgenomen voor het doen van verzoeken met betrekking tot de Wpg bij de Douane.

3.1.27 *Vulling register behoeft aandacht en moet vastgesteld worden*

Er is een register waarin de relevante Wpg verwerkingen van de Douane worden bijgehouden. Voor het invoeren van nieuwe en gewijzigde verwerkingen is een werkwijze opgesteld. Er is op moment van onderzoek een navraag of de actualisering van het register compleet is. De Persoonsgegevens geeft aan dat er nog een discussie loopt over de invulling van het register. De status van de verschillende Wpg verwerkingen in het register is "In bewerking". Het register voldoet nog niet aan alle eisen gesteld in de wet (1a, d, h en j van art. 31d).

3.1.28 *Documentatie moet op onderdelen verbeterd worden*

Een aantal onderdelen van art. 32 lid 1-4 hebben wij niet kunnen verifiëren, dat wil zeggen dat wij niet hebben kunnen vaststellen dat in praktijk aan de volgende bepalingen voor schriftelijke vastlegging wordt voldaan, omdat:

- wij voor verstrekkingen of doorgiften niet over een aantal voorbeelden uit de registratie konden beschikken;
- een afwijzing zoals bedoeld in art 27 lid 1 zich nog niet heeft voorgedaan;
- Incidenten/datalekken met persoonsgegevens zo weinig voorkomen en zo divers zijn dat Douane daar niet op kan sturen. Onduidelijk is welke incidenten Wpg gerelateerd zijn.
- in DFB en ATD geen bewaartermijnen zijn opgenomen, waardoor niet in alle gevallen geborgd kan worden dat vereiste schriftelijke vastleggingen conform art. 32 lid 1 nog beschikbaar zijn voor controles volgens art. 33.

Verder hebben wij geen centraal overzicht aangetroffen met alle geregistreerde verstrekkingen.

3.1.29 *Logging is nog niet conform de daaraan te stellen eisen ingericht. De Wpg geeft formeel nog ruimte tot 2023.*

Formeel hoeft nog niet voldaan te worden aan art. 32a van de Wpg, echter vanuit het oogpunt van beveiliging is de BIO ook en al langer van toepassing. Daarin worden specifieke eisen aan de logging en monitoring gesteld. Daarbij wordt onderscheid gemaakt in logging en monitoring ten behoeve van informatiebeveiligingsgebeurtenissen en voor activiteiten van gebruikers zoals wie heeft wat en wanneer opgeslagen, geraadpleegd, gewijzigd en verwijderd. Met dat laatste wordt de zogenaamde applicatieve logging bedoeld. Logging en monitoring op applicatieniveau is niet ingericht in bestaande systemen zoals DFB en ATD/Caseware. DFB wordt binnen afzienbare tijd uitgefaseerd maar bij het beschikbaar houden van de gegevens moet ook aan de WPG-eisen w.o. voor logging en monitoring worden voldaan (uiterlijk 2023). Dit laatste geldt ook voor andere bestaande systemen zoals ATD/Caseware die voor Wpg verwerkingen gebruikt worden. Het nieuwe systeem DON dat DFB gaat vervangen is op moment van onderzoek nog niet operationeel. Bij de inrichting van DON is er aandacht voor logging en monitoring conform de Wpg. Zodra DON operationeel is zal dit vastgesteld moeten worden.

Zelfbouw applicaties vallen voor wat betreft de logging en monitoring niet onder de standaard ICT-diensten die door de IV-organisatie (van de BD) geleverd worden. In de samenwerkingsafspraken en serviceovereenkomst met de Belastingdienst (BD) voor ICT-diensten zijn geen specifieke afspraken w.o. voor logging en monitoring vastgelegd over het borgen van de privacy conform de Wpg.

3.1.30 *Audits hebben nog niet volgens de Regeling periodieke Audit politiegegevens plaatsgevonden*

In 2021 hebben nog geen interne audits inclusief rapportage volgens de Regeling Periodieke Audit politiegegevens plaatsgevonden. Deze audit betreft de eerste volgens de cyclus voorgeschreven externe Wpg audit. Wij konden ter voorbereiding op deze vier jaarlijkse externe privacy audit dus niet steunen op resultaten van interne controles en audits. Er ligt inmiddels een verzoek om capaciteit voor interne audits te werven.

3.1.31 *Toezichttaken Privacyfunctionaris nog niet formeel belegd en uitgevoerd*

Voor het interne toezicht op de naleving van de Wpg conform art. 34 Wpg is binnen de Douane geen formele functionaris aangesteld, althans dit blijkt niet uit de ons aangeleverde stukken en de afgenomen interviews. Aan de eis van periodiek intern toezicht op de Wpg incl. rapportage wordt nog geen invulling gegeven door een formeel daarvoor aangestelde functionaris.

De Wpg art. 34 stelt dat de verwerkingsverantwoordelijke een of meer privacyfunctionarissen (PF'en) benoemt. De bijbehorende memorie van toelichting spreekt zelfs van een verplichte aanwijzing van een PF. Het Besluit politiegegevens buitengewoon opsporingsambtenaren art. 2 lid 1 daarentegen sluit art 34 Wpg voor boa's uit, maar stelt dat het gegeven de omstandigheden toch nuttig (verstandig) kan zijn om naast een FG één of meerdere PF'en aan te stellen. Vanwege de aard en omvang van de organisatie denken wij dat het verstandig is om toch een privacyfunctionaris conform art. 34 Wpg aan te stellen.

3.1.32 *Toezicht door de Functionaris voor gegevensbescherming heeft nog niet plaatsgevonden*

Er is sinds eind oktober 2020 op het niveau van het kerndepartement van het ministerie van Financiën formeel een plaatsvervangend functionaris voor gegevensbescherming (pFG) aangesteld die conform art. 36 Wpg verantwoordelijk is voor het toezicht op de naleving van de Wpg. Vanwege verschillende redenen w.o. gebrek aan capaciteit en lopende verbeteringen bij de Douane, heeft de pFG in 2021 tot op heden een terughoudende positie c.q. rol ingenomen. Daardoor heeft het onafhankelijk toezicht incl. verslaglegging conform art. 36 Wpg nog niet plaatsgevonden. De pFG is in afwachting (toezichtpauze) van de resultaten van de lopende Wpg audit van de ADR. In 2021 is er dus nog geen sprake van een werkend controle en toezichtsysteem specifiek voor de naleving van de Wpg. Het jaarlijkse toezicht door de pFG incl. verslaglegging heeft nog niet plaatsgevonden conform art. 36 Wpg.

3.2 Bevindingen per norm - organisatorische en technische beheersingsmaatregelen

3.2.1 *Wijzigingenbeheer, Logische toegangsbeveiliging en Beheer van kwetsbaarheden*

Omdat het belangrijkste voor de Wpg verwerkingen gebruikte systeem DFB van voor de Wpg is en dit systeem binnen afzienbare tijd wordt uitgefaseerd en vervangen door een nieuwe systeem DON, is het ons inziens nu niet opportuun om in de externe privacy audit naar het wijzigingenbeheer, de logische toegangs-beveiliging en het beheer van kwetsbaarheden te kijken. DFB wordt in principe niet meer aangepast. De geadviseerde aanpassingen voor de Wpg worden in DON gerealiseerd. De WPG-vereisten voor wijzigingsbeheer en het beheer van kwetsbaarheden moeten op een nog nader te bepalen moment na implementatie van DON worden getoetst.

In het normenkader met de Wpg beheersingsmaatregelen hebben wij de norm met betrekking tot de autorisaties en toegang tot politiegegevens getoetst (zie 3.1.16). Als onderdeel daarvan is de logische toegangsbeveiliging aan bod geweest. Daarom verwijzen wij in het kader met de organisatorische en technische beheersingsmaatregelen hiernaar.

3.2.2 *Toepassing van cryptografie voor opslag en transport van gegevens behoeft aantoonbare controle*

Vanuit het oogpunt van beveiliging hebben wij als onderdeel van de organisatorische en technische beheersingsmaatregelen apart gekeken naar het gebruik van cryptografische beheersingsmaatregelen.

Geïnterviewden gaan ervan uit dat Cryptografie voor opslag en transport van gegevens wordt toegepast en dat dit een standaard voorziening is die door de IV-organisatie (voor BBN2)[7] is ingericht. Ze weten het echter niet zeker. Uit navraag bij IV blijkt dat er wordt gewerkt met encrypted FTP. Er is echter nog geen rapportage over toepassing en naleving van dergelijke beveiligingseisen door verwerkers of dienstverleners.

[7] basis beveiligingsniveau 2, uitgangspunt voor alle informatiesystemen.

3.2.3 *Vulnerability scans en penetratietesten zijn nog niet uitgevoerd op DFB of daarvoor gebruikte platformen*

Vanuit het oogpunt van beveiliging hebben wij als onderdeel van de organisatorische en technische beheersingsmaatregelen apart gekeken naar het uitvoeren van vulnerability scans en penetratietesten.

Uit het onderzoek blijkt dat er geen pentesten op DFB of daarvoor gebruikte platformen zijn uitgevoerd.

4 Aanbevelingen en/of vervolgstappen

4.1 Overzicht aanbevelingen en/of vervolgstappen per norm

Hierna volgen per norm onze aanbevelingen en/of vervolgstappen op basis van de geconstateerde bevindingen zoals weergegeven in hoofdstuk 3.

1. **Doelbinding**: stel de verwerkingen vast in het register van verwerkingsactiviteiten en beschrijf een proces dat erop toeziet dat het doel wordt vastgelegd in de gehanteerde systemen evenals dat er vanuit bestaan controle op wordt uitgevoerd. Neem dit ook op in een Wpg kwaliteitshandboek.
2. **Noodzakelijkheid en rechtmatigheid**: beschrijf in opzet een Wpg kwaliteitshandboek waarin de noodzakelijkheid en rechtmatigheid van de verwerking van politiegegevens is opgenomen. Beschrijf tevens een werkinstructie betreft een controle hierop alsmede de technische en organisatorische maatregelen die hierbij horen.
3. **Juistheid en volledigheid**: beschrijf in opzet een Wpg kwaliteitshandboek waarin de juistheid en volledigheid van de verwerking van politiegegevens is opgenomen. Beschrijf tevens in een werkinstructie de controle hierop alsmede de technische en organisatorische maatregelen
4. **Bijzondere categorieën van persoonsgegevens**: beschrijf in opzet een Wpg kwaliteitshandboek waarin het verwerken van bijzondere persoonsgegevens is opgenomen en de manier waarop de Douane hiermee omgaat. Beschrijf tevens in een werkinstructie de controle hierop alsmede de technische en organisatorische maatregelen.
5. **Geautomatiseerde individuele besluitvorming**: beschrijf in opzet een Wpg kwaliteitshandboek waarin geautomatiseerde individuele besluitvorming dan wel profilering is opgenomen.
6. **Onderscheid feiten en oordeel**: beschrijf in opzet een Wpg kwaliteitshandboek waarin het onderscheid tussen feiten en oordeel is opgenomen. Beschrijf tevens in een werkinstructie de controle hierop alsmede de technische en organisatorische maatregelen.
7. **Aanwijzen bevoegd functionarissen**: houd de lijst van de verantwoordelijke aangewezen bevoegde functionarissen actueel.
8. **Onderscheid tussen verschillende categorieën van betrokkenen**: beschrijf in opzet een Wpg kwaliteitshandboek waarin het onderscheid tussen verschillende categorieën van betrokken is opgenomen.
9. **Reikwijdte**: realiseer het voornemen om de Wpg-verwerkingen verder in kaart te brengen. Maak de medewerkers bewust van de informatie die beschikbaar is om hen in de praktijk te helpen met de sfeerovergang en de daarbij behorende aandachtspunten.
10. **Gegevensbescherming door beveiliging en ontwerp**: Continueer het voornemen om het compliance rapport Wpg verder uit te werken om de risico's inzichtelijk te krijgen. Besteed hierbij tevens aandacht voor de benodigde maatregelen om deze risico's te mitigeren evenals het toepassen van privacy by design bij het verder ontwikkelen van DON.
11. **Verwerkers en verwerkersovereenkomsten**: breid de samenwerkingsafspraken met de Belastingdienst verder uit met concrete afspraken inzake het verwerken van politiegegevens.
12. **Geheimhouding**: kristalliseer de discussie uit over aanvullende screening voor boa's.
13. **Gegevensbeschermings-effectbeoordeling / DPIA**: Realiseer het voornemen om het compliance rapport verder uit te werken en af te ronden.
14. **Melding datalekken:**

- Zorg dat binnen de Douane meer aandacht wordt gegeven aan wat een datalek is, niet alleen gegevens maar ook de devices waarop de gegevens zijn vastgelegd. Zorg hierbij dat: de procedure meldplicht datalekken breder bekend wordt hoe wordt gemeld; hoe de betrokkenen in kennis worden gesteld van een inbreuken op hun gegevens; op juiste wijze de meldingen worden geregistreerd en aan de AP worden gemeld.
- Richt een procedure in waarmee voorkomen wordt dat datalekken bij de proces-verbalen ontstaan, door te checken of alle aangevraagde DFB-nummers ook daadwerkelijk resulteren in een binnengekomen proces-verbaal.
- Actualiseer de registratie van de datalekken met: risicoclassificatie, maatregelen ter voorkoming van herhaling van een datalek en neem het tijdstip van melding op aan de AP.

15. **Gegevensbescherming door standaardinstellingen:** Regel alsnog dat een risicoanalyse wordt opgesteld voor de applicatie DFB waarin de gegevens inzake de WPG worden vastgelegd als de implementatie van DON, de opvolger van DFB, meer tijd vergt. De uitkomsten van deze risicoanalyse zijn de input voor "Autorisaties en Toegang tot politiegegevens".
16. **Autorisaties en Toegang tot politiegegevens:** Richt de logische toegangsbeveiliging waarvoor een proces is ingericht zodanig in dat ook voldaan wordt aan de eisen van de WPG:
    - Pas de autorisatiematrix / functiescheidingsmatrix voor DFB (Douane Fraude Bestrijding) of de opvolger DON aan dat voldaan wordt aan de eisen uit de WPG eisen. Hierbij wordt onderscheid gemaakt tussen artikel 8 en artikel 9 verwerkingen en wordt onderscheid gemaakt naar ouderdom van gegevens die op grond van de WPG dient te worden gemaakt.
    - Borg dat ook het dossiersysteem ATD/ Caseware voldoet aan de WPG-eisen.
    - Pas het Jaarlijks uitgevoerde controleprogramma Beveiliging aan zodat de controles ook zijn gericht op de eisen die de Wpg stelt aan de logische toegangsbeveiliging van de systemen.
17. **Uitvoering van de dagelijkse politietaak:** Implementeer richtlijnen voor het verwerken van politiegegevens volgens Wpg. Bepaal wanneer er sprake is van verwerking en houdt hierbij rekening met de overgang van controle naar opsporing.
    Pas DFB aan of richt de opvolger DON zodanig in dat aan de Wpg wordt voldaan: Volgens de Wpg dienen de gegevens in een artikel 8-omgeving na een jaar te worden gearchiveerd. Deze gearchiveerde gegevens mogen volgens de Wpg alleen na verkregen toestemming benaderbaar zijn.
18. **Geautomatiseerd vergelijken en in combinatie zoeken:** N.v.t. zie onder bevindingen.
19. **Ondersteunende taken:** Geen, zie onder bevindingen.
20. **Ter Beschikking stellen (voor verdere verwerking):** N.v.t. zie onder bevindingen
21. **Bewaartermijnen, verwijderen en vernietigen:** Voer procedures in waarmee bewaar- /vernietigingstermijnen van de Wpg gegevens worden gemonitord en geschoond op de binnen de Douane gebruikte opslagen: de gemeenschappelijke Q-schijf, de applicatie DFB, het dossiersysteem ATD/Caseware en de tijdelijke opslag op netwerkschijven (C:, N: en Q:) en e-mail.
22. **Verstrekking van politiegegevens aan anderen dan politie en Koninklijke marechaussee:** N.v.t. zie onder bevindingen.
23. **Doorgiften aan derde landen:** Pas het register met Wpg verwerkingen aan op het punt van doorgiften aan derde landen zodat duidelijk en eenduidig is in welk geval er sprake of geen sprake is van doorgiften aan derde landen. Maak het periodiek toetsen van de werking van ingerichte processen w.o. voor doorgiften van politiegegevens onderdeel van het periodiek toezicht door de PF en/of pFG. Het toezicht op de naleving van richtlijnen voor het verstrekken en doorgeven van politiegegevens kan ook

onderdeel uitmaken van een formele interne controle door een afdeling kwaliteitsbeheer.

24. **Verstrekking aan derden structureel voor samenwerkingsverbanden:** Geen, zie onder bevindingen.
25. **Rechtstreekse verstrekking:** Pak het toezicht door de PF en pFG zo snel als mogelijk na afronding van deze audit en op basis van de resultaten op in samenhang met het nog in te richten systeem voor interne controle en audit. Maak het periodiek toetsen van de werking van ingerichte processen w.o. voor verstrekkingen onderdeel van dit toezicht.
26. **Informatie aan de betrokkene, Recht op inzage, rectificatie en verwijdering:** De werking van het proces en de instructies in wording kan nog niet getoetst worden omdat er nog geen verzoeken zijn gedaan. Actualiseer en completeer het beschreven proces en de instructies en toets dit op toereikendheid zodra er verzoeken zijn gedaan. Van belang daarbij is dat dit onderdeel wordt aangepast aan de Wpg.
27. **Register:** Actualiseer het register in overeenstemming met de eisen van art. 31d Wpg en betrek daarbij de uitkomst van de lopende discussie over de invulling van het register.
28. **Documentatie:** Maak een centraal overzicht van alle verstrekkingen en doorgiften van Wpg gegevens. Maak het periodiek toetsen van de werking van ingerichte processen w.o. voor verstrekkingen onderdeel van het periodiek toezicht door de PF en/of pFG.
29. **Logging:** Toets deze norm bij de eerstvolgende (interne) audit afhankelijk van de situatie op dat moment. Dat wil zeggen toepassen op DON als dit systeem dan operationeel is en/of op andere voor de Wpg gegevensverwerking gebruikte systemen w.o. DFB en ATD/Caseware, die nog operationeel zijn. Uiterlijk 2023 zal aan de Wpg eisen voor logging moeten worden voldaan. Uitgangspunten voor het inrichten van logging en monitoring zijn in de BIO (paragraaf 12.4) en het beleid voor Logging en monitoring van het ministerie van Financiën opgenomen.
30. **Audits:** Geef prioriteit aan het daadwerkelijk inrichten en borgen van een werkend proces voor controle en audit, waarbij interne controles en audits gebruikt kunnen worden ter voorbereiding op de vierjaarlijkse externe privacy audit en ten behoeve van het toezicht door de pFG en PF.
31. **Privacyfunctionaris:** Beleg het interne toezicht op de naleving van de Wpg conform art. 34 formeel en met voldoende gekwalificeerde capaciteit bij de Privacyfunctionaris, zodat invulling gegeven wordt aan een werkende cyclus voor interne toezicht.
32. **Functionaris voor gegevensbescherming:** Pak het externe toezicht door de pFG zo snel als mogelijk na afronding van deze audit en op basis van de resultaten op in samenhang met het nog in te richten systeem voor interne controle en audit.
33. **Cryptografie:** Richt een aantoonbaar proces in dat periodiek toeziet op het toepassen en naleven van het gebruik van cryptografische beheersmaatregelen door verwerkers en dienstverleners.
34. **Vulnerability scans en Penetratietesten:** Indien DFB binnen afzienbare tijd is uitgefaseerd bevelen wij aan periodiek volgens vastgesteld beleid pentesten uit te voeren op DON en ATD. Als DFB nog enige tijd operationeel blijft en/of de gegevens blijven nog beschikbaar, maak dan een aantoonbare afweging voor het alsnog uitvoeren van een penetratietest op deze omgeving.
35. **Wijzigingenbeheer en Beheer van kwetsbaarheden**
    Borg in het verbeterplan dat voor DON ook de WPG-vereisten voor wijzigingsbeheer en het beheer van kwetsbaarheden worden opgenomen. Als de implementatie van DON, de opvolger van DFB, meer tijd vergt, dan adviseren wij dat deze onderdelen tussentijds worden getoetst in de eerstvolgende interne audit.

5 Verantwoording onderzoek

5.1 Werkzaamheden en afbakening

Werkzaamheden

Zoals in de aanleiding is aangegeven is het doel van dit assurance-onderzoek om een redelijke mate van zekerheid te geven of door de Douane op adequate wijze uitvoering is gegeven aan de bepalingen van de Wpg. Hiertoe hebben wij in de periode april 2022 tot en met november 2022 werkzaamheden uitgevoerd om de opzet, het bestaan en de werking vast te stellen van de beheersingsmaatregelen die de Douane heeft getroffen en door deze te toetsen aan het normenkader.

Het normenkader voor deze privacy audit is gebaseerd op de NOREA Handreiking Privacy Audit Wpg (boa) versie 1.0 Definitief van 24 juni 2021. Deze handreiking is specifiek ontwikkeld om Nederlandse gekwalificeerde IT-auditors (Register IT-auditors, RE's) handvatten te bieden om een assurance rapport op te stellen in lijn met de Wet politiegegevens (Wpg) en het Besluit politiegegevens buitengewoon opsporingsambtenaren (Bpg boa), en relevante standaarden voor assurance-opdrachten. Dit kader bevat voor alle relevante artikelen van de Wpg de te toetsen beheersmaatregelen.

Dit onderzoek bestond uit de volgende werkzaamheden:

- Review werkzaamheden interne controle en audit: Uit de eerste waarnemingen bleek dat er bij de Douane nog geen werkend proces is ingericht voor interne controle en audit volgens de Regeling Periodieke Audit politiegegevens. Zodoende konden wij daar niet op steunen ter voorbereiding op deze eerste externe privacy audit. Wel konden wij als vertrekpunt voor deze audit gebruik maken van de resultaten van de in 2020 door de ADR uitgevoerde nulmeting naar de implementatie van de Wpg.
- Interviews met de plv. functionaris voor gegevensbescherming, privacyfunctionaris, projectleiders, beveiligingsfunctionaris en teamleiders en boa's van de geselecteerde en onderzochte onderdelen en locaties. De interviews zijn vastgelegd en afgestemd met de betreffende functionarissen.
- Documentanalyse: wij hebben documenten opgevraagd om inzicht te verkrijgen in de opzet, bestaan en/of werking van de beheersingsmaatregelen. Dit betreft bijvoorbeeld procedures en rapportages van de pFG en PF, werkinstructies, inzage in het register van verwerkingen, screenshots uit DFB van verwerkingen, interne audit rapporten en jaarverslagen.
- Waarneming: wij hebben door middel van waarneming van de uitvoering van een beheersingsmaatregel beoordeeld of de beheersingsmaatregel wordt toegepast zoals beschreven.

Afbakening

De beoordeling van de opzet, het bestaan en de werking omvatte de maatregelen en procedures die in de borging van de wettelijke eisen van de Wpg moeten voorzien. Het bestaan is beoordeeld, voor zover mogelijk, aan de hand van procedures, werkwijze en vastleggingen op peildatum 31-12-2021. De werking van procedures en maatregelen is, voor zover mogelijk, beoordeeld over de periode 01-01-2020 tot en met 31-12-2021. De werking van de controle en toezicht (art. 32-34) maatregelen is, voor zover mogelijk, beoordeeld over heel 2021. Dit betreft bijvoorbeeld de uitvoering van interne audits en de toezichtwerkzaamheden (inclusief opstellen jaarverslag) van de privacyfunctionaris.

Onder coördinatie van een interne projectgroep voor implementatie van de Wpg zijn eind 2021 al een aantal verbeteracties opgepakt en in gang gezet. Het merendeel van de verbetermaatregelen moet op moment van onderzoek echter nog geëffectueerd worden. Voor de audit betekende dit dat op 31-12-2021 in opzet en voor het bestaan o.a. is gekeken naar de status van de (verbeter)maatregelen. Voor de werking betekende dit dat dit alleen is gecontroleerd indien de opzet en het bestaan eind 2021 als voldoende is beoordeeld en het mogelijk was het functioneren van een maatregel over 2021 te toetsen. Dat bleek voor veel van de toezichtmaatregelen nog niet mogelijk in verband met het ontbreken van een ingericht en werkend toezicht- en controlesysteem voor de Wpg. Het aparte onderdeel van het gehanteerde normenkader met de organisatorisch en technische beheersmaatregelen is marginaal getoetst. Redenen hiervoor zijn het ontbreken van een systeem voor toezicht en controle en het binnen afzienbare tijd uitfaseren van het Douane Fraude Bestrijding (DFB) systeem. De aandacht en prioriteit voor het Wpg compliant inrichten wordt thans gelegd bij het nieuwe systeem Douane Onregelmatigheden (DON), dat DFB binnen afzienbare tijd gaat vervangen. Daarom achten wij het nu niet opportuun om voor DFB uitgebreid in deze privacy audit in te gaan op de bedoelde organisatorische en technische maatregelen, mede ook omdat in de audit is vastgesteld dat de voor de Wpg verwerkingen gebruikte bestaande systemen van voor de Wpg zijn.

Verbetermaatregelen en nieuwe procedures die zijn opgestart na 31-12-2021 zijn, voor zover relevant, meegenomen in het onderzoek en de rapportage, maar zijn niet in het oordeel over de voorliggende controleperiode betrokken.

Scope onderdelen Douane
Omdat het vanwege de omvang onmogelijk is om bij de Douane alle processen waarin Wpg verwerkingen plaatsvinden te toetsen aan uitvoering van de Wpg, is na overleg met contactpersonen van de Douane voor de scope van deze Wpg audit een selectie gemaakt van te onderzoeken onderdelen en locaties van de Douane. De onderbouwing voor de selectie is onder meer gebaseerd op het document "Scope audit Wpg 2021-2022 uitwerking Douane 220204". Alsook op de vermelde verwerkingen in het Wpg-register. Voor deze Wpg audit zijn wij uitgegaan van een combinatie van een audit op de werkzaamheden door boa's op de regiokantoren Rotterdam Haven en Schiphol Passagiers. Daarnaast hebben wij de verwerkingen van team POSS (Precursoren, Strategische goederen en Sanctiewetgeving) en van de meldkamer apart meegenomen, omdat POSS artikel 9 verwerkingen heeft en de meldkamer een aparte verwerking volgens het register heeft. Bij de verschillende onderdelen en locaties zijn interviews afgenomen en zijn de verslagen middels hoor en wederhoor afgestemd met de betrokkenen.

5.2 Gehanteerde Standaard

Deze opdracht is uitgevoerd volgens de Richtlijn voor assurance-opdrachten door IT-auditors (NOREA Richtlijn 3000D).

5.3 Verspreiding rapport

De opdrachtgever, Persoonsgegevens, is eigenaar van dit rapport.

De ADR is de interne auditdienst van het Rijk. Dit rapport is primair bestemd voor de opdrachtgever met wie wij deze opdracht zijn overeengekomen. Voor openbaarmaking door het opdrachtgevende ministerie van door de ADR aan dit ministerie uitgebrachte rapporten gelden de voorschriften uit de Wet open overheid. De minister van Financiën stuurt elk halfjaar een overzicht met de titels van door de ADR uitgebrachte rapporten naar de Tweede Kamer en plaatst dit overzicht op de website.

Volgens artikel 33 lid 2 van de Wet politiegegevens dient de verantwoordelijke tevens een afschrift van de controleresultaten van de privacy audit aan de Autoriteit Persoonsgegevens beschikbaar te stellen.

6 Ondertekening

Den Haag, 22 december 2022

Persoonsgegevens

Auditdienst Rijk

Bijlage 1 Managementreactie Douane

Managementreactie Douane bij audit Wpg 2021

De Douane dankt de Auditdienst Rijk (ADR) voor het uitgebreide onderzoek naar het voldoen aan de Wet politiegegevens (Wpg). Het betreft de eerste periodieke privacy audit die de Wpg voorschrijft nadat de Douane onder de werking van de Wpg is komen te vallen per maart 2019. Het onderzoek geeft de Douane een waardevolle inkijk in toepassing van de vereisten vanuit de Wpg binnen de Wpg-verwerkingen binnen haar processen, zoals het vraaggestuurde onderzoek uit 2020 dat eerder ook heeft gedaan.

De ADR komt op basis van de privacy audit tot het oordeel dat de Douane in belangrijke mate niet voldoet aan de Wpg en dat het daadwerkelijk bestendigen en borgen van geconstateerde verbeteringen vraagt om structurele aandacht en inzet.

De Douane herkent zich in deze geconstateerde tekortkomingen en zal alle aanbevelingen met grote urgentie oppakken. De Douane is daarom inmiddels gestart met het opstellen van een verbeterrapport, waarin alle geconstateerde tekortkomingen opgenomen zijn en de daarbij behorende acties in de vorm van beheersmaatregelen die de Douane gaat instellen. De Douane draagt daarbij zorg voor structurele aandacht en inzet. In de rapportage die voortkomt uit de hercontrole op de uitvoering van het verbeterrapport verantwoorden wij ons nader op de gerealiseerde voortgang in 2023. De oplevering van deze rapportage is voorzien in het eerste kwartaal van 2024.

Hierbij wordt opgemerkt, dat de onderzochte periode een jaar geleden is geweest en een aantal bevindingen na deze periode al zijn opgelost. Op het gebied van bewustwording is bijvoorbeeld in 2022 een bewustwordingscampagne gestart en deze gaat in het eerste kwartaal van 2023 geïntensiveerd door. En tegelijkertijd zijn er ook punten die hardnekkig zijn en meer tijd en aandacht nodig hebben om tot een uitwerking te komen. Het gaat dan om het aanpassen van de automatiseringssystemen en het uitwerken van de te volgen procedures in de werkinstructies van de teams die Wpg-informatie verwerken. Ook zijn er niet eerder geconstateerde tekortkomingen naar voren gekomen. Zo is nu advies geformuleerd op de werkwijze binnen het Meldpunt Datalekken en op de procedure Rechten van betrokkenen.

Met deze rapportage werkt de Douane met grote voortvarendheid verder aan de aanbevelingen.

Persoonsgegevens

Auditdienst Rijk
Postbus 20201
2500 EE Den Haag
Persoonsgegevens