Ministerie van Financiën

Onderzoeksrapport Wpg Douane 2021-2024

Definitief

Colofon

Titel	Wpg Douane 2021-2024
Uitgebracht aan	Persoonsgegevens
Datum	25 februari 2026
Kenmerk	2026-0000040894
Referentienummer	2025-FIN-021

Inlichtingen
Auditdienst Rijk
Persoonsgegevens

Inhoud

Hoofdboodschap

Deze privacy audit heeft tot doel om met een redelijke mate van zekerheid een oordeel te geven of de Douane aan de bepalingen van de Wet politiegegevens (Wpg) heeft voldaan over de periode 2021-2024. Hiertoe heeft een beoordeling plaatsgevonden van de opzet, bestaan en werking van maatregelen die in de borging van de wettelijke eisen moeten voorzien.

Oordeel met beperking

Naar ons oordeel voldoet de Douane niet volledig in de borging van de wettelijke eisen van de Wpg betreft de verwerking van politiegegevens in opzet, bestaan en werking gedurende de controleperiode 2021-2024.

De basis voor ons oordeel met beperking

Wij hebben vastgesteld dat de Douane ten opzichte van de vorige privacy audit over de controleperiode 2019-2021 stappen heeft gezet naar een betere beheersing van privacyrisico's. Echter zijn een aantal onderwerpen binnen de Douane nog niet (rood) of niet volledig (oranje) opgezet, bestaan en/of effectief hebben gewerkt gedurende de controleperiode 2021-2024. Dit had onder andere betrekking op:

- Gegevensbescherming door standaardinstellingen
- Data Protection Impact Assessment (DPIA)
- Bijzondere categorieën van politiegegevens
- Autorisaties en toegang tot politiegegevens
- Ter beschikking stellen van politiegegevens binnen het WPG-domein
- Logging
- Audits

Bij het lezen en interpreteren van onze bevindingen dient rekening te worden gehouden met de aard en omvang van de politiegegevens die binnen de Douane worden verwerkt. Veruit het merendeel betreft art. 8 politiegegevens en slechts een klein gedeelte art. 9. Bij het bepalen van het restrisico voor betrokkenen hebben wij hier rekening mee gehouden.

Op basis van de Regeling Periodieke Audits bevelen wij de Douane aan om binnen één jaar na rapportdatum van deze audit een hercontrole te laten uitvoeren. Het volledige overzicht van bevindingen en een aanvullende toelichting per onderwerp is te vinden in hoofdstuk 2.

1 Inleiding

1.1 Aanleiding onderzoek en opdrachtgever

1.1.1 Aanleiding

De Wet Politiegegevens (Wpg) is sinds 2007 van toepassing verklaard op de verwerking van persoonsgegevens die in het kader van de politietaak worden verwerkt. Naar aanleiding van het in werking treden van de Algemene verordening gegevensbescherming (AVG) in 2018, is de Wpg in 2019 aangepast en is het Besluit politiegegevens buitgewoon opsporingsambtenaar (Bpg boa) in werking getreden. Vanaf dat moment vallen buitengewone opsporingsambtenaren (boa's) die voor hun opsporingstaak persoonsgegevens verwerken onder de Wpg. De Wpg is daarmee van toepassing op de taken van de Douane.

De Wpg schrijft voor dat de verwerkingsverantwoordelijke de naleving van de regels gesteld in de Wpg controleert door middel van periodieke audits, zowel intern als extern. Werkgevers van boa's zijn verplicht om elk jaar een interne Wpg-audit te doen en elke 4 jaar een externe Wpg-audit. Het resultaat van de externe Wpg-audit dient te worden gedeeld met de Autoriteit Persoonsgegevens (AP) als de bij wet aangestelde toezichthouder in Nederland in dit geval voor 1 maart 2026.

1.1.2 Opdrachtgever

Door de Douane is in opdracht van Persoonsgegevens aan de Auditdienst Rijk (ADR) gevraagd de externe Wpg-audit uit te voeren over de controleperiode 2021-2024. Gedelegeerd opdrachtgever is Persoonsgegevens

1.2 Doelstelling en materieel belang

1.2.1 Doelstelling

Het doel van dit assurance-onderzoek is om met een redelijke mate van zekerheid een oordeel geven of de Douane aan de bepalingen van de Wpg op adequate wijze uitvoering heeft gegeven in de periode 2021-2024. Om dit oordeel te geven is er door de ADR gekeken naar:

- De opzet en het bestaan van maatregelen en procedures die in de borging van de wettelijke eisen moeten voorzien;
- De werking van de getroffen maatregelen en procedures.

Concreet betekent dit het beantwoorden van de vraag of door de Douane als boa-werkgever in voldoende mate is geborgd dat voldaan wordt aan wetsartikelen van de Wpg die terugkomen in de NOREA Handreiking Wpg audit Boa (versie sep 2024).

1.2.2 *Materieel belang*

De ADR heeft een oordeel gegeven of het onderzoeksobject vrij is van een verschil van materieel belang ten opzichte van de normen, afzonderlijk of gezamenlijk. Professionele oordeelsvorming is hierbij noodzakelijk om te concluderen of de entiteit de Wpg als geheel heeft nageleefd.

Wanneer het onderzoeksobject vrij is van een verschil van materieel belang, is een goedkeurend oordeel gegeven. Een afkeurend oordeel is gegeven wanneer bij 10 of meer beheersingsmaatregelen in opzet, bestaan en/of werking niet is voldaan aan de door de wetgever gestelde eisen. In dat geval zijn deze aangelegenheden materieel en van diepgaande negatieve invloed op het beschermen van de privacy van betrokkenen.

1.3 Object van onderzoek, afbakening en criteria

1.3.1 *Object van onderzoek*

Het object van onderzoek van deze audit bestond uit de verwerkingen van politiegegevens die binnen de Douane gedurende de controleperiode zijn verwerkt. Het onderzoek richtte zich hierbij op de beheersingsmaatregelen in de processen en de systemen die zijn gebruikt bij de opsporing van strafbare feiten en de vastlegging van politiegegevensgegevens hieromtrent. Dit betekent dat verwerkingen in het kader van toezichttaken niet binnen scope van onderzoek vielen. Hiervoor geldt de AVG.

De redelijke mate van zekerheid die gegeven is of aan de bepalingen van de Wpg op adequate wijze uitvoering is gegeven, gaat over de vastgestelde wettelijke controleperiode van onderzoek van 01-01-2021 tot en met 31-12-2024.

- Toetsing opzet en bestaan: gelegen binnen de controleperiode van 12 maanden (1 januari 2024 – 31 december 2024);
- Toetsing werking, maatregelen niet zijnde toezichtmaatregelen (TZM): een aaneengesloten periode van 12 maanden (1 januari 2024 – 31 december 2024);
- Toetsing werking toezichtmaatregelen (TZM): de controleperiode 1 januari 2021 - 31 december 2024);

De ADR heeft in paragraaf 2.3 ontwikkelingen meegenomen die zich hebben voorgedaan na de controleperiode.

1.3.2 *Afbakening*

Het onderzoek richt zich alleen op de procedures en maatregelen die de Douane moet treffen. De ADR verricht geen onderzoek naar door derden aan de Douane geleverde faciliteiten, voor zover de verantwoordelijkheid is belegd bij anderen dan de Douane. In dergelijke gevallen wordt wel gekeken naar de gemaakte afspraken

tussen de partijen en de regie vanuit de Douane gericht op de realisatie van de afspraken.

1.3.3 *Criteria*

Als toetsingskader is gebruik gemaakt van de NOREA Handreiking Privacy Audit Wpg voor boa's 2024. Deze handreiking is 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.

De (generieke) algehele beheersingsdoelstelling voor de privacy audit Wpg voor boa's is het voorzien in de borging van de wettelijke eisen met betrekking tot de verwerking van politiegegevens door boa's. Hiertoe heeft de Douane beheersingsmaatregelen getroffen die in opzet, bestaan en werking door de ADR zijn getoetst. De ADR maakte bij deze toetsing gebruik van de volgende criteria:

Opzet	De organisatie heeft de interne beheersingsmaatregelen 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 controleperiode volgens de opzet toegepast. In het geval van handmatige beheersingsmaatregelen zijn deze toegepast door competente én bevoegde personen.

Om tot een beoordeling te komen is bij elke norm uit het toetsingskader de bevindingen en eventuele (rest)risico's gewogen door middel van professionele oordeelsvorming. Hierbij is rekening gehouden met mitigerende maatregelen en de risico's voor de rechten van betrokkenen. Bij de beoordeling van de opzet, het bestaan en de werking van een norm zijn de volgende oordelen gehanteerd:

	De beheersingsmaatregelen voldoen.
	De beheersingsmaatregelen voldoen deels. Om geheel te voldoen dien(t)(en) de geconstateerde afwijking(en) te worden opgelost.
	De beheersingsmaatregelen voldoen niet. Om te voldoen dien(t)(en) de geconstateerde afwijking(en) te worden opgelost.
	Niet onderzocht of niet van toepassing (toegelicht).

1.4 Leeswijzer

In het volgende hoofdstuk vindt u een overzicht van de bevindingen die het ADR-onderzoekteam heeft. We hebben de bevindingen per Wpg-onderwerp geordend. In hoofdstuk 3 vindt u informatie over de onderzoeksmethode en de gehanteerde standaarden. Hoofdstuk 4 beslaat de ondertekening van het rapport en in hoofdstuk 5 is de managementreactie op dit rapport gevoegd.

2 Oordeel en bevindingen

2.1 Oordeel Douane 2021-2024

Naar ons oordeel voldoet de Douane niet volledig in de borging van de wettelijke eisen van de Wpg betreffende de verwerking van politiegegevens in opzet, bestaan en werking gedurende de controleperiode 2021-2024.

Wij hebben vastgesteld dat de Douane ten opzichte van de vorige privacy audit over de controleperiode 2019-2021 stappen heeft gezet naar een betere beheersing van privacyrisico's. Echter, hebben wij vastgesteld dat een aantal onderwerpen binnen de Douane nog steeds niet (rood) of niet volledig (oranje) zijn opgezet, bestaan en/of effectief hebben gewerkt.

Hieronder is grafisch ons oordeel per onderwerp weergegeven. In de volgende paragraaf wordt per onderwerp onze bevinding tekstueel toegelicht waar wij ons oordeel hebben gebaseerd.

Onderwerpen	Oordeel		
	O	B	W
1. Reikwijdte			
2. Doelbinding			
3. Noodzakelijkheid en rechtmatigheid, vermelding herkomst			
4. Juistheid en volledigheid politiegegevens			
5. Onderscheid feiten en oordeel			
6. Gegevensbescherming door beveiliging en ontwerp			
7. Gegevensbescherming door standaardinstellingen			
8. Data Protection Impact Assessment (DPIA)			
9. Bijzondere categorieën van politiegegevens			
10. Autorisaties en toegang tot politiegegevens			
11. Autorisaties: aanwijzen functionarissen			
12. Onderscheid tussen verschillende categorieën van betrokkenen			
13. Verwerker en Verwerkersovereenkomst			
14. Geheimhoudingsplicht			
15. Geautomatiseerde individuele besluitvorming			
16. Uitvoering van de dagelijkse politietaak			
17. Ter beschikking stellen van politiegegevens binnen het WPG-domein			
18. Geautomatiseerd vergelijken en in combinatie zoeken			
19. Ondersteunende taken			
20. Bewaartermijnen, verwijderen en vernietigen			
21. Verstrekking van politiegegevens aan anderen dan politie en KMar			
22. Doorgiften aan derde landen			
23. Verstrekking aan derden structureel voor samenwerkingsverbanden			

Onderwerpen	Oordeel		
	O	B	W
24. Rechtstreekse verstrekking			
25. Informatie aan de betrokkene, recht op inzage, rectificatie en verwijdering			
26. Register			
27. Documentatie			
28. Logging			
29. Audits			
30. Melding datalekken			
31. Functionaris voor gegevensbescherming			

Technische en organisatorische maatregelen	O	B	W
1. Wijzigingenbeheer			
2. Logische toegangsbeveiliging			
3. Beheer van kwetsbaarheden (patchmanagement)			
4. Cryptografie			
5. Vulnerability scans en Penetratietesten			

Bevindingen op bovengenoemde onderwerpen hebben geleid tot een oordeel met beperking. Bij het lezen en interpreteren van onze bevindingen dient rekening te worden gehouden met de aard en omvang van de politiegegevens die worden verwerkt binnen de Douane. Veruit het merendeel betreft art. 8 politiegegevens en een klein gedeelte art. 9. Bij het bepalen van ons oordeel en restrisico voor betrokkenen hebben wij hier rekening mee gehouden.

Op basis van ons oordeel en Regeling Periodieke Audits bevelen wij de Douane aan om binnen één jaar na rapportdatum van deze audit een hercontrole uit te voeren.

2.2 Bevindingen

2.2.1 Reikwijdte

De Douane heeft middels een Wpg Kwaliteitshandboek uit 2023 beschreven op welke manier uitvoering wordt gegeven aan de Wpg. Binnen de Douane zijn verwerkingen van art. 8, 9 en 13-politiegegevens geïdentificeerd en gedocumenteerd. Voor deze verwerkingen is een entry opgenomen in het register van verwerkingsactiviteiten. Bij de Douane ligt de nadruk op het verwerken van art. 8 politiegegevens. De werkzaamheden op het gebied van art. 9 zijn beperkt.

Binnen de primaire applicaties geldt dat er duidelijk zicht is op politiegegevens die worden verwerkt. Binnen kleinere robuuste tijdelijke voorzieningen is dit zicht er minder. De Douane dient de sfeerovergang tussen AVG en Wpg verder uit te kristalliseren, in het bijzonder de bestanden en systemen met politiegegevens waarin beide privacy regimes aanwezig zijn; persoonsgegevens die worden verwerkt als toezichthouder (AVG) en persoonsgegevens – in dit geval politiegegevens - die worden verwerkt als opsporingsambtenaar (Wpg). Het inventariseren van processen

waarin Wpg-gegevens worden verwerkt is nog één van de speerpunten in de Wpg-actielijst 2025.

2.2.2 *Doelbinding*

De Douane heeft in het Wpg Kwaliteitshandboek bij de verwerking van politiegegevens het doel (en de grondslag) beschreven. Dit komt ook terug bij de entries in het register van verwerkingsactiviteiten. De Douane verwerkt een klein aantal art. 9-gegevens. Het merendeel (80%-90%) betreft art. 8. De Douane beschikt over een lijst van, door de verwerkingsverantwoordelijke aangewezen, bevoegde functionarissen. De taak om het doel van art. 9-verwerkingen te omschrijven en vast te leggen is niet beschreven. Wij hebben het bestaan en de werking van deze vastlegging ook niet vastgesteld.

2.2.3 *Noodzakelijkheid & rechtmatigheid, vermelding herkomst*

De Douane heeft in het Wpg Kwaliteitshandboek beschreven dat enkel politiegegevens mogen worden verwerkt die toereikend, ter zake dienend en beperkt zijn tot wat noodzakelijk is. Beschreven is dat de Douane hiervoor technische en organisatorische maatregelen treft. In de onderliggende werkinstructies op het gebied van de organisatorische maatregelen worden echter geen handvatten meegegeven op welke manier dit in de praktijk uitgevoerd dient te worden. Aangegeven is dat het wel is meegegeven in de boa-opleiding en dat er in de dagelijkse werkzaamheden collegiale toetsing plaatsvindt. Wij hebben de vastlegging hiervan echter niet geconstateerd.

2.2.4 *Juistheid en volledigheid politiegegevens*

De Douane heeft in het Wpg Kwaliteitshandboek beschreven dat de Douane maatregelen treft zodat politiegegevens, gelet op de doeleinden waarvoor zij worden verwerkt, juist en nauwkeurig zijn. Beschreven is dat hiervoor een toetsing op het proces-verbaal met bijbehorende stukken is ingericht ten behoeve van de bewaking van de juistheid en volledigheid van de gegevens, door een daarvoor geautoriseerd persoon. In de onderliggende werkinstructies worden echter geen handvatten meegegeven op welke manier dit in de praktijk uitgevoerd dient te worden. Aangegeven is dat het wel is meegegeven in de boa-opleiding en dat er in de dagelijkse werkzaamheden collegiale toetsing plaatsvindt. Wij hebben de vastlegging hiervan echter niet geconstateerd.

2.2.5 *Onderscheid feiten en persoonlijk oordeel*

De Douane heeft in het Wpg Kwaliteitshandboek beschreven dat de Douane politiegegevens die worden verwerkt zoveel mogelijk gebaseerd zijn op feiten; het pv bevat slechts feiten waarbij sprake is van objectiviteit en geen persoonlijke conclusies worden getrokken. Beschreven is dat de Douane hiervoor maatregelen heeft ingericht. In de onderliggende werkinstructies worden echter geen handvatten meegegeven op welke manier dit in de praktijk uitgevoerd dient te worden. Aangegeven is dat het wel is meegegeven in de boa-opleiding en dat er in de

dagelijkse werkzaamheden collegiale toetsing plaatsvindt. Wij hebben de vastlegging hiervan echter niet geconstateerd.

2.2.6 *Gegevensbescherming door beveiliging en ontwerp*

De Douane heeft in het Wpg Kwaliteitshandboek middels vijf bullet-points beschreven op welke manier zij privacy by design vormgeeft binnen de organisatie. In het informatiebeveiligingsbeleid wordt meer uitvoerig beschreven welke technische en organisatorische maatregelen concreet zijn ingericht. Dit wordt echter hoofdzakelijk vanuit informatiebeveiligings-oogpunt beschreven en in mindere mate vanuit privacy. Dit geldt ook voor de uitgevoerde risicoanalyses op de processen en systemen (waaronder de primaire applicatie DON) binnen de Douane waardoor informatiebeveiliging is meegenomen maar privacy onderbelicht blijft.

Wel is er een epic opgesteld voor DON en voor overige Wpg-systemen om de gebruikersbehoefte in kaart te brengen. Deze epics beschrijven echter vooral het 'wat' en minder het 'hoe'. Daarnaast In 2024 is onder leiding van Deloitte samen met het Competence Centre een project gestart om te komen tot één "compliance by design" waarin alle wensen en behoeftes vanuit verschillende IT-domeinen worden gebundeld. Het Competence Centre is anno 2025 aan het verkennen hoe zij compliancy by design op eigen titel verder kunnen voltooien en realiseren in 2026.

2.2.7 *Gegevensbescherming door standaardinstellingen*

Beschreven is dat om te zorgen dat politiegegevens rechtmatig en slechts worden verwerkt voor specifieke doelen, de Douane technische en organisatorische (beveiligings-)maatregelen treft zoals een systeem van autorisaties tot de gegevens. De Douane heeft echter geen nadere en concrete uitgangspunten alsmede een uitwerking daarvan beschreven aangaande privacy by default.

2.2.8 *Data Protection Impact Assessment (DPIA)*

De Douane heeft in het Privacy Playbook DPIA uitvoerig het DPIA-proces beschreven, ondersteund door een DPIA-flowchart, DPIA Pre-scan en het DPIA Rijksmodel. De Douane heeft DPIA's uitgevoerd op AVG-verwerkingen, maar niet op Wpg-verwerkingen van art. 8, 9 en 13-gegevens. In het register is bij één entry beschreven dat een DPIA noodzakelijk is. Los van deze verwerking zou de Douane, kijkend naar de aard van art. 8, 9 en 13-gegevens, (moeten heroverwegen) ook voor deze verwerkingen alsnog een DPIA uit te voeren.

2.2.9 *Bijzondere categorieën van politiegegevens*

De Douane heeft in het Wpg Kwaliteitshandboek beschreven dat bijzondere politiegegevens alleen worden verwerkt wanneer dit onvermijdelijk is voor het doel van de verwerking en onder toezicht en goedkeuring van de betreffende BFC. In het register van verwerkingsactiviteiten staat aangegeven dat er geen bijzondere persoonsgegevens worden verwerkt. Echter, staat veelal bij opmerkingen dat er toch wel een mogelijk is. Uit interviews is gebleken dat binnen de Douane–

weliswaar op kleine schaal – gevoelige dan wel bijzondere persoonsgegevens worden verwerkt zoals het burgerservicenummer (bsn) en een kopie ID/rijbewijs. Zowel in digitale als fysieke vorm.

In de onderliggende werkinstructies worden geen handvatten meegegeven op welke manier met deze gegevens in de praktijk omgegaan dienen te worden. Ook in het beveiligingsbeleid hebben wij geen concrete maatregelen aangetroffen om deze gegevens (aanvullend) te beveiligen. Wij hebben het toezicht en goedkeuring van de BFC niet vastgesteld. Wel hebben wij een speciale afgesloten papierbak vastgesteld waarin fysieke kopieën van ID/rijbewijs kunnen worden vernietigd.

2.2.10 Autorisaties en toegang tot politiegegevens

De Douane heeft in het Wpg Kwaliteitshandboek geen uitgangspunten beschreven aangaande autorisaties. Het Landelijke Toegangsbeheer (LTB), als onderdeel van het Douane Diensten Centrum (DDC), richt de autorisaties binnen de primaire systemen van de Douane in middels een Identity and Access Managementsysteem (IAMS). Voor het inrichten en uitvoeren van de IAMS is een werkinstructie opgesteld alsmede een algemene LTB-procedure.

De basisautorisaties worden verleend door het LTB. Hierbij wordt gebruik gemaakt van een toetsingsdocument voor DON. Voor de Q:\-schijf is er geen toetsingsdocument. Binnen DON kan men specifieker autorisaties toekennen dan voor de samenwerkingsgebieden op de Q:\-schijf. Voor dit laatste geldt dat iemand toegang heeft of niet. Er kan niet gedifferentieerd worden naar sub-mappen. Autorisaties binnen DON dienen de boa's aan te vragen bij de teamleider die een bepaalde rol toekent. Voor het toewijzen, wijzigen en intrekken van autorisaties binnen DON hebben wij geen concreet beschreven proces aangetroffen. Voor fysieke politiegegevens zijn er persoonlijke kluizen en afgesloten brievenbussen.

In het kader van controle en monitoring op autorisaties is beschreven dat de Douane een overzicht zou bijhouden van alle autorisaties die zijn verleend voor de toegang tot politiegegevens binnen het Wpg-domein. De privacyfunctionaris zou toezicht houden op dit overzicht om te waarborgen dat alle verleende autorisaties in overeenstemming zijn met de vereisten van de Wpg en dat alleen geautoriseerde personen toegang hebben tot de gegevens. Dit omvat het periodiek controleren en actualiseren van de autorisaties om ervoor te zorgen dat deze nog steeds relevant en gerechtvaardigd zijn. Wij hebben echter het bestaan en werking van de controle niet vastgesteld.

2.2.11 Autorisaties: aanwijzen functionarissen

De Douane beschikt over een lijst van, door de verwerkingsverantwoordelijke aangewezen, bevoegde functionarissen. Hiervoor is er een mandaat afgegeven. Beschreven is dat de bevoegd functionaris toestemming dient te geven en toetst of bij een verstrekking de onderzoeksbelangen in het geding komen. De taak om het

doel van art. 9-verwerkingen te omschrijven en vast te leggen is niet beschreven. Aangegeven is dat dit wel de taak is van de bevoegd functionaris. Wij hebben de vastlegging hiervan in bestaan en werking niet vastgesteld (zie ook 2.2.2)

2.2.12 *Onderscheid tussen verschillende categorieën van betrokkenen*

De Douane heeft in het Wpg Kwaliteitshandboek beschreven dat er onderscheid wordt gemaakt tussen verdachten, veroordeelden (bij recidive) en derden, namelijk getuigen en melders. Beschreven is dat de categorie van betrokkenen in DON kan worden aangemerkt bij het opmaken van een dossier. Deze technische mogelijkheid in DON hebben wij ook vastgesteld. Wij hebben echter geen werkinstructie aangetroffen die het onderscheid maken tussen verschillende categorieën van betrokkenen uitwerkt. Daarnaast is de controle hierop niet aangetoond. De categorieën van betrokkenen zijn ook vastgelegd bij de entries in het register van verwerkingsactiviteiten.

2.2.13 *Verwerker en verwerkersovereenkomst*

De Douane heeft in het Wpg Kwaliteitshandboek geen uitgangspunten beschreven aangaande verwerkers en verwerkersovereenkomsten. De Douane heeft aangegeven dat er bij de verwerkingen van politiegegevens geen sprake is van verwerkers. Dit is ook vastgelegd bij de entries in het register van verwerkingsactiviteiten.

2.2.14 *Geheimhoudingsplicht*

De Douane heeft in het Wpg Kwaliteitshandboek beschreven dat eenieder is gehouden tot geheimhouding wanneer aan hem/haar politiegegevens worden verstrekt. Wij hebben verschillende documenten ontvangen waaruit blijkt dat de geheimhoudingsplicht (actief en blijvend) onder de aandacht wordt gebracht in de boa-opleiding, bewustwordingsacties en andere informatieverstrekkingen.

De Douane benadrukt het belang om bij verstrekkingen de ontvanger altijd te wijzen op de geheimhoudingsplicht die op de gegevens rust en daarbij aan te geven dat ook een eventuele volgende ontvanger hiervan op de hoogte dient te worden gesteld.

2.2.15 *Geautomatiseerde individuele besluitvorming*

De Douane heeft in het Wpg Kwaliteitshandboek geen uitgangspunten beschreven over geautomatiseerde individuele besluitvorming. De Douane heeft aangegeven dat de Douane als boa-werkgever niet bevoegd is tot het verwerken van gegevens t.b.v. art. 11. Geautomatiseerde individuele besluitvorming vindt daarom niet plaats. Dit is ook vastgelegd bij de entries in het register van verwerkingsactiviteiten.

2.2.16 *Uitvoering van de dagelijkse politietaak*

De Douane heeft in het Wpg Kwaliteitshandboek beschreven dat voor art. 8 gegevens vanaf het eerste moment van verwerking 1 jaar ruime toegang is. Daarna

dienen de gegevens 4 jaar alleen beschikbaar te zijn voor verdere verwerking op basis van de vergelijking van gegevens (hit-no-hit basis). Het achter schot plaatsen art. 8 politiegegevens is grafisch ondersteund. De exacte praktische uitvoering hiervan alsmede de controle hierop, waaronder in DON, is echter niet beschreven.

Wij hebben vastgesteld dat in het primaire systeem DON is geautomatiseerd dat art. 8 politiegegevens één jaar na eerste moment van verwerking achter schot worden geplaatst. Uit interviews is naar voren gekomen dat het achter schot plaatsen in DON dermate goed werkt, dat het de dagelijkse operatie kan hinderen gezien een zaak veelal langer dan een jaar loopt. Voor art. 9 gegevens, wat slechts een klein deel beslaat, is het automatisch achter schot plaatsen niet als zodanig ingericht. Dit geldt ook voor kleinere robuuste tijdelijke voorzieningen en de Q-schijf. Er is geen zicht of fysieke politiegegevens ook tijdig achter schot worden geplaatst.

2.2.17 *Ter beschikking stellen van politiegegevens binnen het Wpg-domein*

De Douane heeft in het Wpg Kwaliteitshandboek beschreven dat ten aanzien van ter beschikking stellen de Wpg uitgaat van een systeem van free flow of information binnen het Wpg-domein; ambtenaren van de politie, Rijksrecherche, Koninklijke Marechaussee, bijzondere opsporingsdiensten en boa's. De Douane is verplicht om politiegegevens aan personen binnen het Wpg-domein ter beschikking te stellen voor zover zij deze gegevens nodig hebben voor een goede uitvoering van hun taak. Er zijn echter geen concrete werkinstructies met uitgangs- en aandachtspunten bij het ter beschikking stellen van politiegegevens.

Wel is beschreven dat de bevoegde functionaris de taak heeft om (aantoonbaar) instemming te geven voor verdere verwerking. De bevoegd functionaris dient te toetsen of de onderzoeksbelangen in het geding komen. Ook is beschreven dat de Douane centraal een overzicht zou bijhouden van verstrekkingen en doorgiften van persoonsgegevens binnen het Wpg-domein in het Wpg-verwerkingsregister. De privacyfunctionaris zou toezicht houden op dit overzicht waarbij controle wordt gehouden op de vereisten uit de Wpg. Wij hebben echter het bestaan en de werking hiervan niet vastgesteld.

2.2.18 *Geautomatiseerd vergelijken en in combinatie zoeken*

De Douane heeft in het Wpg Kwaliteitshandboek beschreven dat de mogelijkheid voor geautomatiseerd vergelijken en in combinatie zoeken enkel is voorbehouden aan personen en instanties met een publieke taak en die zijn aangewezen in artikel 4:6 Bpg en artikel 24 Wpg. De Douane valt hier niet onder waardoor er geen sprake is van geautomatiseerd vergelijken in combinatie zoeken binnen de Douane.

2.2.19 *Ondersteunende taken*

De Douane heeft in het Wpg Kwaliteitshandboek beschreven dat binnen de Douane verwerkingen plaatsvinden die gebaseerd zijn op artikel 13 van de Wpg. Hiervoor is ook een entry opgenomen in het register van verwerkingsactiviteiten. Echter is

aangegeven dat er geen verwerkingen gebaseerd op art. 13 gedurende de controleperiode hebben plaatsgevonden.

2.2.20 *Bewaartermijnen, verwijderen en vernietigen*

De Douane heeft in het Wpg Kwaliteitshandboek beschreven dat voor art. 8 gegevens vanaf het eerste moment van verwerking 1 jaar ruime toegang is. Daarna dienen de gegevens 4 jaar alleen beschikbaar te zijn voor gericht zoeken, waarna de gegevens verwijderd dienen te worden. De gegevens worden na die 1 + 4 jaar vernietigd. De termijnen betreft bewaren en vernietigen zijn grafisch ondersteund. De exacte praktische uitvoering hiervan alsmede de controle hierop, waaronder in DON, is echter niet beschreven.

Wij hebben vastgesteld dat in het primaire systeem DON is geautomatiseerd dat art. 8 politiegegevens één jaar na eerste moment van verwerking achter schot worden geplaatst, vervolgens vier jaar daarna worden verwijderd en vijf jaar daarna wordt vernietigd. Uit interviews is naar voren gekomen dat deze automatische bewaartermijnen in DON dermate goed werken, dat het de dagelijkse operatie kan hinderen gezien een zaak veelal langer dan een jaar loopt. Voor art. 9 gegevens, wat slechts een klein deel beslaat, is het automatisch achter schot plaatsen alsmede verdere verwijdering en vernieitiging niet als zodanig ingericht. Dit geldt ook voor kleinere applicaties en de Q-schijf. Er is geen zicht of fysieke politiegegevens ook tijdig worden verwijderd en vernietigd.

2.2.21 *Verstrekking van politiegegevens aan anderen dan politie en Koninklijke marechaussee*

De Douane heeft in het Wpg Kwaliteitshandboek summier beschreven hoe de Douane omgaat met het verstrekken van politiegegevens. Een verstrekking van politiegegevens dient volgens de beginselen van proportionaliteit en subsidiariteit plaats te vinden wat inhoudt dat voorafgaand aan elke verstrekking een zorgvuldige afweging moet worden gemaakt.

In veel gevallen is toestemming nodig van de bevoegd functionaris en/of van het bevoegd gezag. De bevoegd functionaris toetst of onderzoeksbelangen in het geding komen en het bevoegd gezag toetst of het vervolgingsbelang in het geding komt. Voor het verstrekken dient gebruik gemaakt te worden van een verstrekkingentabel. De concrete praktische uitvoering en vastlegging van een verstrekking is echter niet beschreven.

Aangegeven is dat er geen verstrekkingen van politiegegevens aan anderen dan politie en Koninklijke marechaussee hebben plaatsgevonden gedurende de controleperiode.

2.2.22 *Doorgiften aan derde landen*

De Douane heeft in het Wpg Kwaliteitshandboek beschreven dat de doorgifte aan derde landen of internationale organisaties alleen plaatsvindt, voor zover dit noodzakelijk is voor de doeleinden zoals opsporing, handhaving van de openbare orde of de hulpverlening en in beginsel alleen van het derde land of de internationale organisatie die een toereikend beschermingsniveau voor de voorgenomen gegevensverwerking verzekert. Daartoe onderscheidt artikel 17a Wpg drie situaties. Verwezen wordt naar een nadere uitwerking van die drie situaties alsmede een werkinstructie. Dit hebben wij echter niet aangetroffen.

Aangegeven is dat er geen doorgifte van gegevens aan derde landen hebben plaatsgevonden gedurende de controleperiode.

2.2.23 *Verstrekking aan derden structureel voor samenwerkingsverbanden*

De Douane heeft in het Wpg Kwaliteitshandboek beschreven dat de Douane ten behoeve van een samenwerkingsverband met personen of instanties in overeenstemming met het bevoegd gezag (OM) op grond van artikel 20 Wpg kan beslissen politiegegevens te verstrekken. Daartoe zou de Douane een artikel 20 Wpg beslissing opmaken – een document waarin het zwaarwegend algemeen belang, het samenwerkingsverband en het doel daarvan, het soort politiegegeven, de voorwaarde(n) waaronder wordt verstrekt en de -ontvanger(s) van de politiegegevens omschreven staan. Het concept wordt ter accordering voorgelegd aan het bevoegd gezag Persoonsgegevens Namens het College van PG's zou het Parket- Generaal een overzicht bijhouden van alle beschikbare artikel 20 Wpg beslissingen

Aangegeven is dat er geen verstrekkingen aan derden structureel voor samenwerkingsverbanden hebben plaatsgevonden gedurende de controleperiode.

2.2.24 *Rechtstreekse verstrekking*

De Douane heeft in het Wpg Kwaliteitshandboek beschreven dat de Wpg en het Bpg een aantal personen en instanties aanwijzen waaraan politiegegevens rechtstreeks kunnen worden verstrekt - het bieden van zelfstandige toegang tot politiegegevens langs geautomatiseerde weg. Voor het OM, minister van Defensie en aan de korpschef is volledige toegang tot politiegegevens mogelijk. Voor ambtenaren van IND en Buitenlandse Zaken, personen werkzaam bij FIU, bepaalde nationale politiële contactpunten, de Passagiersinformatieeenheid, de AIVD en MIVD is het toegang mogelijk door middel van geautomatiseerde vergelijking (hit/no hit). Dit heeft echter niet plaatsgevonden gedurende controleperiode.

Beschreven is dat de Douane een overzicht zou bijhouden van verstrekkingen en doorgiften van persoonsgegevens binnen het Wpg-domein binnen het Wpg-verwerkingsregister. Beschreven is dat de privacyfunctionaris toezicht houdt op dit

overzicht waarbij controle wordt gehouden op de vereisten uit de Wpg. Aangegeven is dat dit als zodanig in de praktijk niet gebeurt.

2.2.25 *Informatie aan de betrokkene, recht op inzage, rectificatie en verwijdering.*

De Douane heeft in het Wpg Kwaliteitshandboek beschreven dat op grond van de artikelen 24a en 25 Wpg de verwerkingsverantwoordelijke aan eenieder op zijn/haar verzoek deelt of, en zo ja welke, politiegegevens over hem/haar zijn vastgelegd. Een verzoek op basis van artikel 25 Wpg wordt altijd door de privacyfunctionaris van het Ministerie van Financiën of het betreffende Dienstonderdeel in behandeling genomen, met consultatie van de FG.

Informatie over de verwerking van persoonsgegevens door de Douane is te vinden op www.douane.nl. Om aan verzoeken van betrokkenen uitvoering te geven beschikt de Douane over een werkinstructie. Als uitgangspunt geldt dat politiegegevens slechts ter inzage worden geboden aan de betrokkene en er geen kopie van de politiegegevens wordt verstrekt.

Aangegeven is dat er geen Wpg-verzoeken van betrokkenen hebben plaatsgevonden gedurende de controleperiode.

2.2.26 *Register*

De Douane heeft in het Wpg Kwaliteitshandboek beschreven dat de Douane een actueel verwerkingsregister zou onderhouden dat alle verwerkingen met betrekking tot de Wpg documenteert. Beschreven is dat de Privacyfunctionaris de Wpg-verwerkingen binnen de Douane monitort en zorgdraagt dat het Wpg-verwerkingsregister actueel is. Hier wordt echter nog geen uitvoering aan gegeven gezien er op het gebied van Wpg andere prioriteiten spelen.

Wij hebben vastgesteld dat de Douane beschikt over een register van verwerkingen waarin zes Wpg-verwerkingen als entries zijn opgenomen. Het register bevat de benodigde informatie per verwerking. Echter, hebben wij inderdaad vastgesteld dat de entries niet allemaal juist en actueel zijn. De Douane heeft aangegeven het register in 2026 te actualiseren.

2.2.27 *Documentatie*

De Douane heeft in het Wpg Kwaliteitshandboek geen uitgangspunten beschreven aangaande de documentatieplicht. De documentatieplicht komt terug bij andere normen, te wetende; documenteren van art. 9-doeleinden, documenteren van alle verstrekkingen, documenteren van alle weigeringen van inzageverzoeken en het documenteren van alle datalekken. Wij hebben bij die normen vastgesteld dat – indien van toepassing - niet altijd de benodigde informatie wordt gedocumenteerd.

2.2.28 *Logging*

De Douane heeft in het Wpg Kwaliteitshandboek beschreven dat in het kader van controle en monitoring de Douane zorgdraagt voor de logging van alle handelingen die met politiegegevens worden uitgevoerd. Deze logboeken moeten een volledig en nauwkeurig overzicht geven van wie, wanneer, welke gegevens heeft geraadpleegd, gewijzigd, toegevoegd of verwijderd. Het doel van deze loggingsplicht is om de integriteit en beveiliging van de gegevens te waarborgen, en om ongeautoriseerde toegang of gebruik van de gegevens te detecteren en te voorkomen. De Douane volgt hierbij het logging- en monitoringsbeleid van Financiën. Op welke manier dit concreet tot uiting komt binnen de Douane, in het bijzonder in de primaire applicatie DON is niet beschreven.

In DON is logging wel technisch ingericht. Logboeken zijn vijf jaar beschikbaar waarna ze geautomatiseerd worden verwijderd. De voorkeur heeft het om loggegevens voor wat betreft de medewerkergegevens te pseudonimiseren. De wijze waarop de loggegevens worden gepseudonimiseerd moet nog worden uitgewerkt. Aangegeven is dat de logboeken echter niet worden gebruikt t.b.v. controle en monitoring rondom de verwerking van Wpg-gegevens. Voor kleinere applicaties en de Q-schijf is dit niet geautomatiseerd.

2.2.29 *Audits*

De Douane heeft in het Wpg Kwaliteitshandboek beschreven dat ieder jaar een interne audit en iedere vier jaar een externe audit uitgevoerd dient te worden om te waarborgen dat de verwerking van politiegegevens binnen de Douane conform Wpg plaatsvinden. De Douane heeft echter niet een auditplan beschreven.

Wij hebben vastgesteld dat in de jaren 2021, 2022 en 2023 heeft er geen interne audit plaatsgevonden. Door het ontbreken van een eigen interne auditfunctie heeft in 2024 KPMG een interne audit uitgevoerd op de opzet. In 2025 voert de ADR de externe audit uit over 2021-2024.

2.2.30 *Melding Datalekken*

De Douane heeft niet in het Wpg Kwaliteitshandboek beschreven op welke manier zij omgaat met Wpg-gerelateerde datalekken. De Douane maakt gebruik van de datalekkenprocedure van het ministerie van Financiën. Deze procedure bevat een duidelijk stappenplan, ondersteund middels een flowchart.

De ADR heeft verschillende documenten ontvangen t.b.v. het verhogen van het privacy bewustzijn alsmede het melden van datalekken. Daarnaast hebben wij maandrapportages ontvangen vanuit de Melddesk Datalekken over (beveiligings-)incidenten en inbreuken met persoonsgegevens in het kader van AVG en Wpg. De rapportages maken geen expliciet onderscheid tussen AVG en Wpg-datalekken, maar biedt wel duidelijk inzicht in aantallen, trends en acties.

Aangegeven is dat er geen Wpg-gerelateerde datalekken hebben plaatsgevonden gedurende de controleperiode.

2.2.31 *Functionaris voor Gegevensbescherming (FG)*

De Douane heeft in het Wpg Kwaliteitshandboek beschreven dat in het kader van controle en monitoring de FG en pFG gevraagd en ongevraagd toezicht houden op de Wpg-verwerkingen van de Douane, bijv. door middel van adviezen op DPIA's, datalekken, verzoeken betrokkenen, verwerkingsregister, verstrekkingen/doorgifte, lopende zaken en op verwerkingen van auditbevindingen.

Wij hebben vastgesteld dat een FG specifiek is aangemeld voor de Wpg bij de AP. Aangegeven is dat de FG zich vooralsnog richt op het adviseren bij de implementatie van de Wpg. Het daadwerkelijke toezicht geschiedt in aanvulling op de werkzaamheden van de privacyfunctionaris en (interne) audits. Dit is afhankelijk van de mate waarin de implementatie heeft plaatsgevonden en is afhankelijk van het volwassenheidsniveau.

2.2.32 *Privacyfunctionaris*[1]

De Douane heeft in het Wpg Kwaliteitshandboek beschreven dat binnen de Douane de Chief Privacy Officer (CPO) tezamen met Wpg Privacy deskundige door de verwerkingsverantwoordelijke zijn aangesteld als Privacyfunctionaris (artikel 34 Wpg). Beschreven is dat de privacyfunctionaris rapporteert op basis van artikel 32, lid 1 Wpg en volgt de privacyfunctionaris de rapportagelijnen. In de praktijk heeft dit in de controleperiode 2021-2024 niet plaatsgevonden. Die periode beschikte de Douane nog niet over een privacyfunctionaris. Controle en monitoring was die periode nog niet als zodanig ingericht en geborgd.

2.2.33 *Organisatorische en technische beheersingsmaatregelen*

De Wpg stelt, evenals de AVG, dat de verwerkingsverantwoordelijke 'passende' technische en organisatorische maatregelen moeten treffen voor o.a. de beveiliging en het ontwerp van informatiesystemen. Het is afhankelijk van de specifieke situatie wat passend zal zijn. Doorgaans zal dit worden bepaald aan de hand van een DPIA. Ook de BIO zal, in het geval van overheidsinstellingen, in acht moeten worden genomen door de verwerkingsverantwoordelijke. Het normenkader omvat een minimale set aan passende maatregelen die voor de onderwerpen 6, 7, 10, 13 en 24 zijn getest.

[1] Het Bpg boa schrijft geen privacyfunctionaris binnen boa-organisaties voor. In artikel 2, lid 1 van het Bpg boa staat namelijk dat artikel 34 Wpg is uitgezonderd. Een privacyfunctionaris naast een FG is volgens de wetgever een (te) zware belasting, zeker voor kleine organisaties. Dit neemt niet weg dat het verstandig kan zijn toch een privacyfunctionaris aan te stellen. Deze persoon kan een adviserende rol innemen bij bijvoorbeeld het inrichten van het verwerkingsregister, het aanwijzen van bevoegde functionarissen en andere Wpg-vraagstukken. We hebben daarom het onderwerp privacyfunctionaris wel meegenomen, maar er volgt geen oordeel uit.

GITC 1 - Wijzigingenbeheer

De Douane maakt gebruik van de verschillende IV-diensten van de Belastingdienst. Douane-specifieke informatiesystemen worden voornamelijk ontwikkeld en beheerd door de afdeling IBS (Integratie Business Services) Douane van de Belastingdienst. Wij hebben vastgesteld dat IBS verschillende kwaliteitschecks uitvoert op GITC-normen waaronder wijzigingenbeheer. De MD-teams binnen IBS Douane werken volgens gestelde normen en procedures. De functiescheiding tussen het aanvragen, goedkeuren en doorvoeren van wijzigingen wordt echter niet altijd strikt toegepast om ongeautoriseerde wijzigingen te voorkomen.

GITC 2 - Logische toegangsbeveiliging

Het Landelijke Toegangsbeheer (LTB), als onderdeel van het Douane Diensten Centrum (DDC), richt de autorisaties binnen de primaire systemen van de Douane in middels een Identity and Access Managementsysteem (IAMS). Voor het inrichten en uitvoeren van de IAMS is een werkinstructie opgesteld alsmede een algemene LTB-procedure. Het Raamwerk Integrale Beveiliging Douane beschrijft de doelstelling, kaders en uitgangspunten voor informatiebeveiliging binnen de Douane. De scope van LTB Douane betreft het autorisatieproces van individuele douane-medewerkers.

GITC 3 - Beheer van kwetsbaarheden (patch management)

De Douane heeft beschreven dat om kwetsbaarheden in software te verhelpen, updates snel en gecontroleerd aangebracht dienen te worden. Hiervoor wordt een proces ingericht dat updates voor software identificeert, test en installeert. De IBS voert verschillende kwaliteitschecks uit op GITC-normen waaronder patch management.

GITC 4 -Cryptografie

De Douane beschikt niet over een eigen cryptografiebeleid maar maakt gebruikt van standaarden van de Belastingdienst alsmede het Rijksbrede beleidskader cryptografie dat als raamwerk dient voor het opstellen van cryptografiebeleid. Wij hebben vastgesteld dat cryptografie, naast classificatie van gegevens, wordt meegenomen in de epics.

GITC 5 - Vulnerability scans en pentesten

De Douane heeft beschreven dat alle informatiesystemen, inclusief de extern-uitbestede diensten, periodiek gescand dienen te worden op kwetsbaarheden. Hiervoor dienen afspraken te worden gemaakt met het SOC. Aangegeven is dat in de controleperiode 2021-2024 vanuit de Douane niet altijd actief werd gestuurd op het uitvoeren van pentesten. De kaders komen vanuit IV CTO Office en de verantwoordelijkheid voor het uitvoeren ligt bij IV IBS Douane. De Douane heeft een achterstand opgelopen in de uitvoering die momenteel in een samenwerking tussen het CTO Office en het IB-cluster van Douane wordt ingehaald. Zo zijn er in

2025 bedrijf-kritische systemen in kaart gebracht waar uiteindelijk jaarlijks een pentesten op gevoerd moet worden. Dit zal ook resulteren in omvattend beleid.

2.3 Ontwikkelingen Douane 2025

Wij hebben vastgesteld dat de Douane de afgelopen jaren stappen heeft gezet om de Wpg beter te borgen. In 2023 is een privacy-breed programma "Privacy Op Orde" i.s.m. Deloitte gestart. Dit heeft een aantal basisproducten in opzet opgeleverd. Daarnaast heeft de Douane een Wpg Kwaliteitshandboek ontwikkeld met uitgangspunten. Het bestaan hiervan is groeiende, maar de werking is nog niet waar het zou moeten zijn is uit voorgaande paragrafen gebleken. Dit kost tijd en capaciteit. Dit komt ook omdat de privacy governance binnen de Douane nog niet helemaal is uitgekristalliseerd. Daarnaast is de ondersteunende inhuur niet altijd verlengbaar waardoor continuïteit een uitdaging is. Naast "Privacy Op Orde" was er ook een apart privacy projectteam vanuit een andere directie.

Ons oordeel is gebaseerd op bevindingen over de controleperiode 2021-2024. Gezien de audit in 2025 heeft plaatsgevonden, hebben wij ook een beeld gekregen over de stappen die de Douane na de controleperiode heeft gezet dan wel aan het zetten is. We zien dat de Wpg steeds verder belegd wordt in de lijn en uiteindelijk zal controle en monitoring vanuit de tweede lijn volgen in de komende periode. We zien ook dat de Persoonsgegevens in 2025 wel een rapportage heeft opgesteld op basis van stramien van de politie. Het rapport bevat cijfers en inzicht omtrent stand van zaken Wpg, datalekken, inzageverzoeken etc. Met dit inzicht kan de Douane grotere en snellere stappen zetten die aanvankelijk nog niet mogelijk waren. Ook de stappen die Competence Centre in 2025 heeft gezet en voornemens is om te zetten in 2026 belooft goeds als het gaat om de manier om privacy by design en default beter te borgen binnen de organisatie.

3 Verantwoording onderzoek

3.1 Werkzaamheden

De ADR heeft in de periode augustus 2025 tot en met december 2025 de audit uitgevoerd conform de overeengekomen werkzaamheden zoals beschreven in opdrachtbevestiging 2025-0000485897. De werkzaamheden omvatten onder andere het bestuderen en analyseren van de vooraf aangeleverde documentatie conform PBC-lijst, het analyseren van dossiers en uitkomsten van interne audits, het afnemen van interviews met betrokken functionarissen en directe waarnemingen van verwerkingen/vastleggingen in informatiesystemen. Interviews zijn met de geïnterviewde(n) afgestemd met hoor-wederhoor.

De inhoudelijke afstemming van dit rapport heeft plaatsgevonden met contactpersoon Douane alsmede de opdrachtgever. In de bijgevoegde managementreactie heeft de opdrachtgever zijn visie op de onderzoeksresultaten verwoord.

3.2 Gehanteerde standaard en kwaliteitsborging

Dit rapport is gebaseerd op de NOREA Handreiking Privacy audit Wpg voor boa's en de Richtlijn 3000D van de NOREA (Assurance-opdrachten door IT-auditors).

De opdracht is uitgevoerd conform de algemene uitgangspunten voor de uitoefening van de interne auditfunctie bij de rijksdienst. Daarbij hoort ook een stelsel van kwaliteitsborging. Een onderdeel daarvan is dat er een onafhankelijke kwaliteitstoetsing heeft plaatsgevonden op deze onderzoeksopdracht.

3.3 Verspreiding 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 van door de ADR uitgebrachte rapporten naar de Tweede Kamer.

4 Ondertekening

Den Haag, 25 februari 2026

Persoonsgegevens

Auditdienst Rijk

5 Managementreactie Douane

Het voorliggende assurance-rapport betreft de tweede verplichte periodieke privacy-audit naar het voldoen aan de Wet politiegegevens (Wpg). Deze privacy-audit gaat over de controleperiode 1 januari 2021 tot en met 31 december 2024. De Douane dankt de Auditdienst Rijk (ADR) voor het uitgevoerde onderzoek.

Resultaat van de privacy-audit
De bescherming van politiegegevens is een fundamentele voorwaarde bij de uitvoering van ons werk. De Douane heeft kennisgenomen van de inhoud van het assurance-rapport over de Opzet, het Bestaan en de Werking van de beheersmaatregelen die de Douane heeft getroffen. De ADR constateert dat de Douane ten opzichte van de vorige privacy-audit, over de periode 2019-2021, en de hercontrole in 2023 stappen heeft gezet naar een betere beheersing van de privacy-risico's.

De Douane onderschrijft de conclusies van de ADR en herkent zich in het afgegeven 'oordeel met beperkingen'. De Douane beschouwt dit oordeel als een realistische weergave van de huidige stand van de implementatie van de Wpg.

Doorontwikkeling privacy
Zoals vastgelegd in de Stand van zakenbrief van 12 december 2024, heeft de Douane in 2023 en 2024 via een projectmatige verbeteraanpak de 'Opzet en Bestaan' van privacy beheersings-maatregelen verbeterd. De resultaten van de interne audit Wet politiegegevens van 2024 en de privacy-audit 2025 bevestigen dit. De privacy-audit toont eveneens aan dat de 'Werking' van privacy beheersmaatregelen nog niet voldoende concrete resultaten heeft opgeleverd.
Op basis van het privacy-audit 2025 stelt de Douane een verbeterplan op, en geeft in 2027 de ADR de opdracht voor een hercontrole op de hoog risicobevindingen. De nadruk hierbij ligt op het verbeteren van de aantoonbaarheid en de dagelijkse uitvoering.

Deze verbeteringen worden doorgevoerd in een periode waarin de Douane over gaat van regiosturing naar processturing. Gegevensbescherming wordt als onderdeel opgenomen in het Organisatie & Formatieplan en wordt in 2027 integraal geïmplementeerd.

Daarnaast zijn IT-aanpassingen nodig. Complicerend daarbij zijn de afhankelijkheden van aanpassingen aan andere systemen, schaarse capaciteit en keuzes binnen het overvolle IT-portfolio van de Douane. Prioriteiten (zoals het

implementeren van Europese douanewetgeving en vervanging van IT om continuïteit te borgen) moeten daarbij continu integraal worden afgewogen.

De Douane voelt zich gesteund door de observaties van de ADR over de wijze waarop de Douane in 2025 verder heeft gewerkt aan borging van de Wpg binnen de organisatie, en zet hierop onverminderd in. De Douane is inmiddels gestart met de doorontwikkeling van het privacyframework om risico's direct te adresseren en het privacyonderwerp staat structureel op de bestuurlijke agenda. De Douane steunt hierbij op de in 2024 ingerichte privacy organisatie die de projectmatige aanpak van 2023/24 vervangt, waarbij is ingezet op een risicomanagement-cyclus, waarin risico's continu worden gemonitord en de risicobereidheid helder wordt gekaderd. De eerste resultaten daarvan zijn al zichtbaar, maar vallen buiten scope van deze audit.

Daarnaast wordt de effectiviteit van beheersmaatregelen periodiek getoetst. De Douane voert jaarlijks interne Wpg audits uit om tekortkomingen te signaleren en de organisatie verder te professionaliseren, waarbij onder andere de inzichten van de privacyfunctionaris en de functionaris gegevensbescherming leidend zijn.

Auditdienst Rijk
Postbus 20201
2500 EE Den Haag
Persoonsgegevens