Auditdienst Rijk
Ministerie van Financiën

Eindrapport
Privacy audit Wet politiegegevens boa's ILT 2021

Definitief

Colofon

Titel	Privacy audit Wet politiegegevens boa’s ILT 2021
Uitgebracht aan	Inspecteur-Generaal Inspectie Leefomgeving en Transport (ILT)
Datum	30 juni 2023
Kenmerk	2023-0000159024

Inlichtingen
Auditdienst Rijk
070-342 7700

Inhoud

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 in het kader van strafrechtelijke handhaving van de Inspectie Leefomgeving en Transport (ILT), als toezichthouder van het ministerie van Infrastructuur en Waterstaat (IenW). De opsporingstaken van buitengewoon opsporingsambtenaren (boa's) van de ILT, 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 ILT 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 aan te bieden. Eind mei 2022 is door de Auditdienst Rijk (ADR) de audit bij de ILT opgestart om aan deze wettelijke verplichting te voldoen. Dit betekent concreet dat de ILT tot uiterlijk 31-12-2022 had 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. Vanwege een verlate start van de privacy audit door de ADR in combinatie met het niet tijdig aanleveren van benodigde informatie over derden door de ILT, is het niet gelukt om aan deze rapportageverplichting te voldoen en wordt het rapport van de externe audit alsnog en zo snel als mogelijk in 2023 aangeleverd bij de AP.

Deze assurance-opdracht is door de ADR uitgevoerd in opdracht van de inspecteur-generaal (IG) ILT. De privacy audit heeft betrekking op de wijze waarop bij de ILT het verwerken van politiegegevens door boa's 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 ILT 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.

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[3]:

- Algemene bepalingen (artikelen 1-7);

[1] Besluit Politiegegevens, artikel 6:5, lid 2.
[2] Regeling periodieke audit politiegegevens
[3] Behoudens de uitzonderingen zoals openomen in artikel 2 van het Besluit politiegegevens buitengewoon opsporingsambtenaren.

- 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).

Omdat de ILT 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 qua controleperiode in ieder geval het jaar 2021 volledig omvatten. In afwijking op de controleperiode in de oorspronkelijke opdracht voor het toetsen van de werking, is in overleg met ILT besloten in deze audit niet verder terug te gaan in de tijd dan 2021. In 2021 is voor het eerst een interne audit op de naleving van de Wpg uitgevoerd en is eveneens voor het eerst een toezicht jaarverslag van de FG voor 2021 opgesteld. Beide rapportages zijn voor deze audit als basis genomen voor de status van Wpg verbetermaatregelen in 2021. Het ontbreken van een intern toezicht- en controlesysteem voor toepassing van de wet in 2021 alsook het grotendeels ontbreken van andere maatregelen in opzet en bestaan in 2021, maken dat het niet goed mogelijk en zinvol is om in de externe audit voor de werking verder terug in de tijd te gaan dan 2021. Ontwikkelingen en verbeteringen die na 2021 hebben plaatsgevonden zijn niet in dit oordeel over 2021 betrokken.

Afbakening

De privacy audit heeft betrekking op de artikelen van de Wpg die van toepassing[4] zijn op de ILT bij de verwerking[5] van politiegegevens[6] in het kader van de opsporingstaken van boa's[7]. Het onderzoek richt zich op de beheersingsmaatregelen in de processen en de systemen die gebruikt worden bij de uitvoering van deze taken, de vastlegging van persoonsgegevens hierbij en alleen op de procedures en maatregelen die de ILT in het kader van de Wpg moet treffen.
De ADR heeft geen zelfstandig onderzoek uitgevoerd naar door derden aan de ILT geleverde faciliteiten, voor zover de verantwoordelijkheid is belegd bij anderen dan de ILT. 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 ILT gericht op de realisatie van de afspraken (zie 3.1.11). In overleg met ILT hebben wij wel geprobeerd om een aantal organisatorische en technische maatregelen te toetsen op aantoonbare implementatie bij SSC-ICT en DICTU. Vanwege onvoldoende medewerking en informatie is dat slechts in heel beperkte mate mogelijk gebleken.

Omdat het vanwege de omvang onmogelijk is om bij de ILT alle processen waarin Wpg-verwerkingen plaatsvinden te toetsen aan uitvoering van de Wpg, is na overleg met contactpersonen van de ILT voor de scope van deze audit op basis van risico's, omvang en aard van de werkzaamheden van boa's door de ADR een selectie gemaakt van te onderzoeken afdelingen, modaliteiten en teams. 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

[4] Zie Besluit politiegegevens bijzondere opsporingsambtenaren en Besluit politiegegevens.
[5] 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.
[6] Elk persoonsgegeven van een geïdentificeerde of identificeerbare natuurlijke persoon dat wordt verwerkt in het kader van de uitvoering van de politietaak.
[7] De verwerking van persoonsgegevens door de algemeen opsporingsambtenaren vanuit de bijzondere opsporingsdienst van de ILT (ILT-IOD), valt buiten de scope van dit onderzoek.

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

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 redelijke 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 ILT voldoet in 2021 in belangrijke mate niet aan de Wpg voor de uitvoering van opsporingstaken door boa's. Het daadwerkelijk en aantoonbaar bestendigen en borgen van geconstateerde verbeteringen vraagt om structurele aandacht en inzet.

2.1 Oordeel met afkeuring

Wij hebben voor de uitvoering van opsporingstaken door boa's bij de ILT 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 ILT 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 van de Wpg. 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 daar niet aan wordt voldaan. Het gaat hier in de basis om het ontbreken van een goed functionerend systeem voor interne controle en toezicht op de naleving van de Wpg waaronder ook door verwerkers. Ook ontbreekt een goede risicoanalyse voor alle Wpg verwerkingen door boa's en verwerkers inclusief inzicht in de benodigde beveiligingsmaatregelen voor de daarbij gebruikte systemen, voorzieningen en bestanden. Daarnaast is de aantoonbaarheid van het naleven van privacy maatregelen doorgaans onvoldoende. Dit maakt dat het veelal niet goed mogelijk is te controleren of organisatorische en technische maatregelen ter bescherming van de privacy daadwerkelijk conform de Wpg zijn geïmplementeerd en passend zijn. Dit is essentieel om goed verantwoording te kunnen afleggen over het nakomen van verplichtingen uit de Wpg en het aantoonbaar in control zijn. Voor een overzicht van de afwijkingen van de norm wordt verwezen naar Tabel 1 en 2: Overzicht conclusie per norm.

Ten opzichte van de interne audit van de ILT op de naleving van de Wpg over 2021 (rapportage juli 2021) zijn er in 2021 nauwelijks vorderingen gemaakt in het daadwerkelijk doorvoeren van destijds geconstateerde verbetermogelijkheden[8]. In

[8] Overigens zijn niet alle Wpg maatregelen in de interne audit van de ILT over 2021 object van onderzoek geweest. De aard en diepgang van deze audit was ook anders dan nu: het betrof geen assurance audit. Met deze (externe) assurance audit zijn ook andere en nieuwe verbetermogelijkheden geconstateerd.

de tweede helft, en met name eind 2021 zijn wel enkele verbeteracties door het interne Wpg boa project (dat is gestart in oktober 2021) 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 in de loop van 2022 gedeeltelijk effect gehad en/of moet in veel gevallen het daadwerkelijk en aantoonbaar bestendigen en borgen in de organisatie op moment van onderzoek nog plaatsvinden. In 2021 heeft er niet veel tijd gezeten tussen het opgeleverde rapport van de interne audit en het oppakken van de verbetermaatregelen waardoor de ruimte die er toen in 2021 nog was voor het daadwerkelijk effectueren van verbetermaatregelen beperkt was. Veel van deze maatregelen vergen immers aanzienlijk wat tijd om deze met structurele aandacht en inzet (voldoende gekwalificeerde capaciteit) te bestendigen en borgen in de organisatie. Dat neemt echter niet weg dat de Wpg en de Baseline Informatiebeveiliging Overheid (BIO), waar het gaat om beveiligingsmaatregelen ter bescherming van de privacy, al eerder (begin 2019) van toepassing waren. Wij hebben geconstateerd dat het lopende interne project Wpg boa inmiddels een behoorlijk aantal verbeterpunten heeft opgepakt die volgens de aangegeven planning in 2023 verder gerealiseerd zullen worden.

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 ILT moet treffen voor naleving van de Wpg-eisen. De ADR heeft geen zelfstandig onderzoek verricht naar door derden aan de ILT geleverde faciliteiten, voor zover de verantwoordelijkheid is belegd bij een andere overheidsorganisatie dan de ILT. In dergelijke gevallen is wel gekeken naar de gemaakte afspraken tussen de partijen en de regie vanuit de ILT gericht op de realisatie van de afspraken (zie 3.1.11). Met de uitzondering dat, vanwege het ontbreken van regie door ILT op het aantoonbaar naleven van gemaakte afspraken en maatregelen, in overleg met ILT toch geprobeerd is een aantal organisatorische en technische maatregelen te toetsen op aantoonbare implementatie bij SSC-ICT en DICTU. Dat is vanwege onvoldoende medewerking en informatie slechts in heel beperkte mate mogelijk gebleken.

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 ILT 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			
12.	Geheimhoudingsplicht				
13.	Gegevensbeschermingseffectbeoordeling (GEB)	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			

Nr.	Norm	Key control	Conclusie		
			Opzet	Bestaan	Werking
29.	Logging	X			
30.	Audits	X			
31.	Privacyfunctionaris	X			
32.	Functionaris voor gegevensbescherming	X			

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

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/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 Het doel van de in het register vermelde verwerkingen met status "in bewerking" is vastgelegd. Het register is nog niet compleet en vastgesteld voor alle verwerkingen door boa's en een proces dat toeziet op naleving doelbinding ontbreekt.

De ILT verwerkt politiegegevens in het kader van de opsporingstaak en strafrechtelijke afdoening. Hierbij worden persoonsgegevens en de aard van de overtreding door boa's verwerkt met name in processen-verbaal (PV) en daarna een vastlegging hiervan in het inspectiesysteem Holmes. Het doel van de in het register vermelde Wpg verwerkingen is in opzet vastgelegd in het AVG register van het ministerie van IenW. De artikel 8 Wpg verwerking door boa's is ten tijde van het onderzoek verwijderd uit en later weer toegevoegd met status "in bewerking" aan het register. De reden hiervan is ons niet bekend.

Toepassing en instemming voor verdere verwerking van politiegegevens volgens art. 9 Wpg is nog niet bepaald en uitgewerkt voor alle verwerkingen door boa's van de ILT, terwijl dit volgens enkele geïnterviewde boa's in praktijk wel voorkomt. Het register met de daarin vermelde Wpg verwerkingen is zodoende nog niet volledig, actueel en formeel vastgesteld. De ADR heeft geen proces in opzet en bestaan aangetroffen dat op navolgbare wijze toeziet dat bij het verwerken van politiegegevens altijd sprake is van doelbinding en dat de gegevens niet op een met die doeleinden onverenigbare wijze worden verwerkt.

3.1.2 Noodzakelijkheid en rechtmatigheid verwerking persoonsgegevens is niet aantoonbaar en procesmatig geborgd

Op welke manier ILT 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 over 2021 naar voren, alsook welke organisatorische en technische maatregelen zijn getroffen om dit te borgen. Doordat naast of buitenom Holmes ook andere voorzieningen en netwerkschijven voor opslag van Wpg gegevens op ongecontroleerde wijze worden gebruikt, bestaat het risico dat bij de verwerking van gegevens niet volgens de Wpg wordt gehandeld. Een systeem voor intern toezicht en controles op de naleving van Wpg maatregelen w.o. ook bij verwerkers ontbreekt en daardoor is niet met zekerheid vast te stellen dat Wpg maatregelen daadwerkelijk zijn geïmplementeerd en functioneren.
Indien er artikel 9 gegevens worden verwerkt door boa's, dient de ILT aan te geven in welk informatiesysteem dit moet gebeuren. Waar artikel 9 gegevens worden vastgelegd is nu niet duidelijk. Wij hebben niet met zekerheid kunnen vaststellen dat de herkomst van gegevens voor artikel 9 verwerkingen wordt vermeld.

3.1.3 Controle op juistheid en volledigheid politiegegevens niet aantoonbaar volgens uitgewerkt proces geborgd

Er zijn in opzet geen beschreven procedures en werkinstructies aangetroffen waaruit voor 2021 blijkt dat de ILT controles heeft ingericht op de kwaliteit ten behoeve van de borging van de juistheid en nauwkeurigheid van persoonsgegevens. Uit de interviews met boa's is gebleken dat dit in praktijk wordt vormgegeven door een collegiale toets op de juistheid en volledigheid van proces-verbalen (PV) middels een 4 ogen-principe. Wij hebben niet kunnen vaststellen of de collegiale toets structureel

en op dezelfde wijze wordt uitgevoerd door boa’s, mede doordat hier in de basis geen handreikingen of werkinstructies voor zijn.

3.1.4 *Instructies en controle verwerking bijzondere categorieën van persoonsgegevens ontbreken en beschermingsmaatregelen zijn niet aantoonbaar*

Wij hebben geen werkinstructie en/of procedure aangetroffen voor het verwerken van bijzondere categorieën van politiegegevens. In het register met Wpg verwerkingen is voor art. 8 aangegeven dat bijzondere politiegegevens bijvoorbeeld over de gezondheid van individuen in de verwerkingen kunnen voorkomen. In een interview met boa's is aangegeven dat gezondheidsgegevens van chauffeurs in een PV kunnen staan ten behoeve van bewijsvoering. Het daadwerkelijk voorkomen van bijzondere persoonsgegevens hebben wij niet met zekerheid aan de hand van enkele voorbeelden kunnen vaststellen, alsook of deze gegevens adequaat zijn beveiligd. Controle op de juiste verwerking alsook een overzicht met de technische en organisatorische maatregelen ontbreken.

3.1.5 *Er is geen sprake van geautomatiseerde individuele besluitvorming*

Er zijn geen geautomatiseerde verwerkingen aangetroffen. Volgens het register en geïnterviewden komt op geautomatiseerde verwerking gebaseerde besluitvorming of geautomatiseerd vergelijken niet voor bij de Wpg verwerkingen en in het daarbij gebruikte systeem Holmes.

3.1.6 *Instructies onderscheid feiten en oordeel waren in 2021 nog niet beschreven. Structurele controle op naleving waarborgen en richtlijnen moet nog aantoonbaar geborgd worden.*

Opleiding, kennis en ervaring zijn zoals in de interviews is aangegeven belangrijke voorwaarden om het werk goed en zo feitelijk mogelijk uit te voeren. Dit is onderdeel van de professionaliteit van de boa. Het systeem en de instructies ondersteunen daarbij evenals een collegiale toetsing waarbij door een andere collega wordt gecontroleerd of de vastleggingen juist en objectief zijn. De concept werkinstructie “onderscheid feiten en oordelen” (augustus 2022) geeft aan dat een duidelijk onderscheid gemaakt moet worden bij het vastleggen van feiten en eventuele oordelen.

3.1.7 *Onduidelijkheid over van toepassing zijn artikel 9 verwerkingen door boa’s en instemming door bevoegde functionarissen*

Toepassing en instemming voor verdere verwerking van politiegegevens volgens art. 9 en 13 is, voor zover daar voor boa’s in praktijk sprake van is of kan zijn, nog niet bepaald en uitgewerkt voor alle verwerkingen door boa's van de ILT. Het merendeel van de verwerkingen van een boa betreft artikel 8, uitvoering van de dagelijkse politietaak. Uit de interviews blijkt dat sommige boa's ook volgens artikel 9 en mogelijk artikel 13 gegevens verwerken, maar wij hebben het daadwerkelijk voorkomen van dergelijke verwerkingen niet met zekerheid kunnen vaststellen. Volgens de concept werkinstructie 8, 9 en 13 en contactpersonen van ILT worden art. 13 gegevens nog niet verwerkt. Gebleken is dat er wel behoefte bestaat artikel 13 gegevens te verwerken in de vorm van risicoprofielen. Gekeken zal worden of dit separaat van de artikel 8 verwerkingen in Holmes kan worden verwerkt, zodat rekening kan worden gehouden met de verschillende bewaartermijnen. Zodra dit is ingeregeld, zal de werkinstructie hierop worden aangevuld. Indien boa’s in bepaalde gevallen ook artikel 9 gegevens verwerken, dan moet er volgens de Wpg een actuele lijst zijn van, door de verantwoordelijke aangewezen, bevoegde functionarissen. Een dergelijke lijst is er momenteel niet.

3.1.8 *Onderscheid verschillende categorieën van betrokkenen moet nog aantoonbaar in proces en gebruikte voorzieningen geborgd worden*

In het AVG Register en de daarin vermelde Wpg verantwoordelijke verwerkingen zijn de verschillende categorieën van betrokkenen vermeld (Verdachten, Slachtoffers, Veroordeelden en Derden). Er is een concept werkinstructie categorieën van betrokkenen (augustus 2022). Deze was er nog niet in 2021. Een

beschrijving van getroffen systeem maatregelen moet op moment van onderzoek nog worden opgesteld.

3.1.9 Reikwijdte: nog niet alle verwerkingen van politiegegevens zijn geïdentificeerd en gedocumenteerd

ILT heeft in 2021 nog niet alle Wpg verwerkingen van politiegegevens door boa's en de daarbij binnen de organisatie gebruikte systemen en devices geïdentificeerd en gedocumenteerd. Voor artikel 9 (onderzoek in verband met de handhaving van de rechtsorde in een bepaald geval) is nog niet bepaald of en in hoeverre dit (ook) van toepassing is op de Wpg verwerkingen door boa's van de ILT. Er is in 2021 nog geen compleet beeld of overzicht van voor verwerking van Wpg gegevens gebruikte voorzieningen en bestanden. Er is voor 2021 geen Wpg Data Protection Impact Assessment (DPIA) of andersoortige risicoanalyse uitgevoerd voor de betreffende verwerkingen en daarbij gebruikte systemen en voorzieningen zoals voor Holmes, Alfresco (DMS), devices zoals laptops en smartphones en de gebruikte netwerkschijven. Daarom is er onvoldoende beeld of de risico's worden beheerst met een passend stelsel van organisatorische en technische maatregelen.

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

Doordat er in 2021 geen Wpg DPIA’s door ILT zijn uitgevoerd en opgesteld, is het beeld voor 2021 voor benodigde Wpg-maatregelen niet toereikend. Het ontbreekt aantoonbaar aan voldoende adequate technische en organisatorische maatregelen om verwerkingen van persoonsgegevens te beschermen. Een functionerend systeem voor intern toezicht en controle op basis van voor alle Wpg verwerkingen en daarbij gebruikte voorzieningen geïdentificeerde risico's en maatregelen ontbreekt. De principes van privacy by design worden daardoor niet aantoonbaar toegepast.

3.1.11 Verwerkersovereenkomsten aanwezig, maar onbekend en geen aantoonbaar houvast dat afspraken en Wpg maatregelen worden nageleefd

Het register met Wpg verwerkingen bevat niet alle op basis van analyse geïdentificeerde en vastgestelde verwerkers inclusief de daarbij behorende verwerkingsovereenkomsten c.q. -afspraken. In de ontvangen contractuele afspraken met verwerkers (SSC-ICT en DICTU) is geen specifieke aandacht voor het verwerken van persoonsgegevens in overeenstemming met de Wpg. Er wordt in algemene zin gesproken over het verwerken en beveiligen van persoonsgegevens. Het ‘right to audit’ en het ter beschikking stellen van alle benodigde informatie die nodig is om te kunnen aantonen dat aan de verplichtingen wordt voldaan, is in de verwerkersovereenkomsten opgenomen, echter hier is nog niet eerder dan in deze audit gebruik van gemaakt. ILT kan op moment van onderzoek niet aantonen op basis van intern toezicht en controles dat de verwerking van persoonsgegevens bij verwerkers overeenkomstig de vastgelegde afspraken en Wpg plaatsvindt. Er kan dus niet met zekerheid worden vastgesteld dat verwerkingsverantwoordelijke afdoende garanties heeft over de toereikendheid van de geïmplementeerde technische en organisatorische maatregelen bij de betreffende verwerkers.

3.1.12 Geheimhoudingsplicht ingeregeld, mate van aandacht verschilt per modaliteit en team. Aantoonbaarheid naleving verwerkers heeft aandacht nodig.

In het privacybeleid is aandacht voor het privacy bewust werken en opleiden van medewerkers (AVG en Wpg). Verder is in de eed en belofte nadrukkelijk aandacht voor de geheimhouding alsook in het Praktijkhandboek Wpg voor boa's. Dit zijn documenten die in de loop van 2022 zijn opgesteld en er in 2021 nog niet waren.

Er is een generiek proces voor indiensttreding nieuwe medewerker en een specifiek proces voor aanstelling van boa’s.

In de ontvangen verwerkingsovereenkomsten en afspraken met verwerkers is aandacht voor de geheimhouding in het kader van het verwerken van persoonsgegevens. Wij hebben niet kunnen vaststellen of en in hoeverre daar intern

bij de betreffende verwerkers (SSC-ICT en DICTU) op actieve wijze aandacht aan wordt besteed. Het toezicht op de naleving van de Wpg, ook door verwerkers, is daar niet op ingericht.

In het kader van bewustwording, training en opleiding is er volgens een aantal geïnterviewde boa's en teamleiders aandacht voor het zorgvuldig omgaan met Wpg gegevens. Niet alle geïnterviewde boa's vinden dat er in praktijk voldoende (actieve) aandacht o.a. door de leidinggevende is voor geheimhouding en het zorgvuldig omgaan met Wpg gegevens en daar ook daadwerkelijk naar handelen. De mate waarin aandacht is voor de Wpg verschilt in de organisatie per modaliteit en team.

3.1.13 Proces gegevensbeschermingseffectbeoordeling (GEB) / DPIA in opzet beschreven maar in 2021 geen Wpg DPIA(s) uitgevoerd

In opzet is er aandacht voor het uitvoeren van DPIA's inclusief de rollen en verantwoordelijkheden en een proces voor het monitoren van maatregelen die uit de vastgestelde DPIA's komen. Uit het overzicht met DPIA's uit het Toezichtjaarverslag over 2021 blijkt dat er in 2021 geen Wpg DPIA rapporten voor advies en beoordeling werden voorgelegd aan de Functionaris Gegevensbescherming (FG). Zodoende is er voor 2021 geen volledig en aantoonbaar beeld of en in hoeverre wordt voldaan aan de technische en organisatorische maatregelen om verwerkingen van persoonsgegevens te beschermen. Doordat er geen specifieke GEB's of DPIA's voor Wpg verwerkingen door boa’s zijn uitgevoerd, hebben wij voor de werking niet kunnen vaststellen of de risico’s volgens een systematisch proces worden geïdentificeerd, beoordeeld en aangepakt en of de in de GEB of DPIA vastgestelde risico's en maatregelen worden geëvalueerd.

3.1.14 Melding datalekken procedureel beschreven en ingericht, er zijn nog geen specifieke Wpg datalekken gemeld

Het Interne audit rapport over 2021 geeft aan dat over 2021 geen documentatie aanwezig is waarin aangetoond wordt dat het herkennen van datalekken actief onder de aandacht van boa's wordt gebracht met het doel om toekomstige datalekken te voorkomen. Ondanks dat op het intranet informatie te vinden is over datalekken en hoe hiermee moet worden omgegaan (passief), is het niet vanzelfsprekend dat alle medewerkers zich hiervan bewust zijn.
Verder wordt in het interne audit rapport over 2021 aangegeven dat er geen rapportage plaatsvindt aan het IG-team van de ILT over hoeveel datalekken plaatsvinden per periode.

Uit de registratie van gemelde datalekken blijkt dat er in 2021 geen Wpg datalekken zijn gemeld. Daardoor hebben wij nog niet kunnen vaststellen of aan alle vereisten van de Wpg voor het melden van datalekken wordt voldaan zoals het tijdig melden aan de AP en indien relevant betrokkene(n).

3.1.15 Gegevensbescherming door standaardinstellingen op aantoonbare wijze uitwerken en implementeren

Bij ILT is geen vastgesteld beleid aangetroffen waarin conform de Wpg specifiek aandacht is voor gegevensbescherming door standaardinstellingen. Ook in de verwerkingsafspraken met SSC-ICT en DICTU is geen specifieke aandacht voor de Wpg. In 2021 zijn geen adequate risicoanalyses uitgevoerd voor de Wpg verwerkingen door boa’s en de daarbij gebruikte systemen, voorzieningen en bestanden alsook voor de verwerkingen door genoemde dienstverleners. Daardoor is niet aantoonbaar of en in hoeverre passende organisatorische en technische maatregelen zijn getroffen waarbij en waarmee ook de gegevensbescherming door standaardinstellingen is geborgd.

3.1.16 Autorisaties en toegang tot politiegegevens niet aantoonbaar ingericht volgens need-to-know

Eind december 2021 heeft de ILT een wijziging van de autorisatiestructuur voor opsporingsambtenaren doorgevoerd in het systeem Holmes. In opzet is het autorisatieproces in 2021 beperkt beschreven en de ontvangen autorisatie documenten zijn niet gedateerd en vastgesteld. Wij hebben het bestaan van deze norm niet goed kunnen vaststellen vanwege het ontbreken van de beoogde opzet voor autorisaties en/of functiescheidingen voor het systeem Holmes en toegang tot gegevens op basis van het need-to-know principe. Omdat de autorisatiewijziging pas eind december 2021 is doorgevoerd, hebben wij voor 2021 geen bestaansbewijs aangetroffen waaruit blijkt dat periodieke controles op autorisaties plaatsvinden (zowel voor boa's, niet boa's als voor toegang door verwerkers zoals DICTU en SSC-ICT). Het ontbreken van een structureel autorisatieproces met periodieke controles werd ook geconstateerd in de interne audit over 2021. Dit heeft als risico dat ongeautoriseerde en ongewenste toegang tot Wpg gegevens mogelijk is en dat ongewenste toegang en combinaties van functies, rollen en autorisaties niet goed inzichtelijk zijn.

3.1.17 Uitvoering van de dagelijkse politietaak verder uitwerken in beleid en procedures en aantoonbaar borgen in de gebruikte systemen en voorzieningen

Een beschrijving van systeem maatregelen is niet aanwezig. De ontvangen documenten met betrekking tot deze norm zijn vaak niet gedateerd en vastgesteld of nog in concept. Wij hebben verder geen bestaansbewijs ontvangen waardoor het niet inzichtelijk is dat artikel 8 politiegegevens één jaar na de datum van de eerste verwerking achter een schot worden geplaatst en dat deze maximaal 5 jaar na eerste datum van verwerking beschikbaar zijn voor raadplegen en daarna nog 5 jaar afgeschermd worden bewaard en waarna de gegevens vernietigd worden. Daarbij worden Wpg gegevens niet alleen in Holmes opgeslagen maar ook op diverse netwerkschijven en andere gebruikte voorzieningen.

Uit de interviews is gebleken dat niet alle ILT inspecteurs, boa's en teamleiders bekend zijn met de Wpg bewaartermijnen (ook vanwege het tijdig schonen van politiegegevens die buiten Holmes worden opgeslagen w.o. op netwerkschijven), waarbij eveneens is opgemerkt dat de ILT nog dient te bepalen op welke wijze artikel 9 en artikel 13 gegevens moeten worden verwerkt. De overgang van controle naar opsporingsactiviteiten is in praktijk lastig te duiden in de werkzaamheden en de daarbij gebruikte systemen en voorzieningen.

3.1.18 Geautomatiseerd vergelijken en in combinatie zoeken is niet van toepassing

In de interviews alsook in het Interne Wpg audit rapport over 2021 is aangegeven dat er in Holmes geen sprake is van geautomatiseerd vergelijken en in combinatie zoeken. Het gebruikte systeem biedt daarvoor geen functionaliteit of geautomatiseerd mechanisme. Dit hebben wij verder niet onderzocht.

3.1.19 Ondersteunende taken artikel 13 volgens opgaaf niet van toepassing voor boa's van ILT maar niet goed aan te tonen

Volgens opgaaf contactpersonen ILT en de concept werkinstructie artikel 8, 9 en 13, worden artikel 13 gegevens nog niet verwerkt. Gebleken is dat er wel behoefte bestaat artikel 13 gegevens te verwerken in de vorm van risicoprofielen. Gekeken zal worden of dit separaat van de artikel 8 verwerkingen in Holmes kan worden verwerkt, zodat rekening kan worden gehouden met de verschillende bewaartermijnen. Zodra dit is ingeregeld, zal de werkinstructie hierop worden aangevuld.

In het kader van opsporing hebben de boa's van ILT doorgaans alleen met artikel 8 Wpg verwerkingen te maken. Wij hebben echter niet met zekerheid kunnen vaststellen of boa's in praktijk ook ondersteunende taken volgens artikel 13 Wpg (kunnen) verrichtten.

3.1.20 Het ter Beschikking stellen (voor verdere verwerking) is niet aantoonbaar volgens de Wpg ingericht

Omdat de ILT nog geen artikel 9 heeft bepaald, zijn er geen maatregelen getroffen voor het ter beschikking stellen voor verdere verwerking door een bevoegd functionaris. Ook heeft de ILT nog geen bevoegde functionarissen aangewezen.

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

Vanwege het ontbreken van bestaansbewijs zoals maatregelen gebruikte systemen zijn de bewaartermijnen van de Wpg gegevens in praktijk niet inzichtelijk. Voor het verwijderen van gegevens was in 2021 nog niets ingeregeld. De vernietigingstermijn van 10 jaar is opgenomen in de selectielijst (conform Archiefwet) van het ministerie van IenW. Hiervoor is een proces ingeregeld.

3.1.22 Verstrekking van politiegegevens aan anderen dan politie en Koninklijke marechaussee werd in 2021 nog niet vastgelegd

Het proces van verstrekken van politiegegevens buiten het Wpg domein is geïmplementeerd in juli 2022. In 2021 waren er nog geen vastleggingen en controles van dergelijke verstrekkingen. Zodoende kon het bestaan en de werking van dit proces nog niet worden vastgesteld.

3.1.23 Doorgiften aan derde landen werd in 2021 nog niet vastgelegd

In de interviews alsook in het interne Wpg audit rapport over 2021 is aangegeven dat er geen gegevens worden verstrekt aan derde landen. De documentatieplicht voor doorgifte van gegevens aan derde landen is geïmplementeerd vanaf juli 2022. Omdat vastlegging van eventuele doorgiften ontbreekt hebben wij niet kunnen vaststellen of er in 2021 ook daadwerkelijk doorgiften aan derde landen hebben plaatsgevonden.

3.1.24 Verstrekking aan derden structureel voor samenwerkingsverbanden werd in 2021 nog niet vastgelegd

Vastlegging van verstrekkingen aan derden structureel voor samenwerkingsverbanden vindt vanaf juli 2022 plaats. Daardoor kon voor 2021 het bestaan en de werking van dit proces nog niet worden vastgesteld.

3.1.25 Er is geen sprake van rechtstreeks via geautomatiseerde weg verstrekken van gegevens

De ILT heeft vanuit boa's geen register/ gegevensleveringen geautomatiseerd opengesteld voor diverse partijen waar zij van buitenaf op gegevensvelden kunnen meekijken. Er vindt geen geautomatiseerde rechtstreekse verstrekking plaats aan het OM. Het OM vereist een uitgeprint PV. Het uitprinten van een dossier en opsturen naar het OM door een boa valt daarmee niet in de definitie van rechtstreeks verstrekken, dat immers noch geautomatiseerd noch zonder menselijke tussenkomst is. Rechtstreekse verstrekking van gegevens zonder menselijke tussenkomst vindt zodoende niet plaats bij ILT.

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

Nog niet alle procesbeschrijvingen en instructies zijn aangepast op de Wpg. Voor 2021 is er geen overzicht met verzoeken tot inzage, rectificatie, vernietiging van betrokkenen. Daardoor kon nog niet vastgesteld worden of uitvoering van het proces en de instructies toereikend en conform Wpg zijn.

3.1.27 Vulling register behoeft aandacht en moet vastgesteld en periodiek gecontroleerd worden

In 2021 en op moment van onderzoek is de registratie van Wpg verwerkingen in het AVG register van ILT nog niet volledig en actueel. De in het register vermelde Wpg verwerkingen zijn in 2021 en op moment van onderzoek nog niet vastgesteld.

In het register zijn niet alle optionele gegevens vermeld, te weten: de beoogde termijnen waarbinnen de verschillende categorieën van gegevens worden verwijderd of vernietigd. Dit is niet verplicht volgens de wet, maar geeft aan “zo mogelijk”.

De DPIA's en afspraken/overeenkomsten met verwerkers ontbreken in het register. Verder ontbreekt bij diverse onderdelen van de Wpg verwerkingen een korte motivatie of toelichting waarom iets wel of niet van toepassing is. Dit kan bijvoorbeeld ook een verwijzing zijn naar een ander document of vastlegging ter onderbouwing. Verder hebben wij voor 2021 geen vastgestelde procedure aangetroffen voor het opstellen en bijhouden van een verwerkingenregister alsook een aantoonbare controle voor het periodiek vaststellen van de juistheid en volledigheid van het register.

3.1.28 De documentatie- en bewaarplicht is niet aantoonbaar volgens artikel 32 Wpg ingericht

Op basis van de opgeleverde documenten kan over 2021 geen uitspraak worden gedaan over het bestaan en de werking van de documentatie- en bewaarplicht. Ook is geen documentatie aangeleverd waaruit blijkt dat in 2021 de schriftelijke vastlegging conform de Wpg is geborgd.
De wijze van vastlegging, het bewaken van de juistheid en volledigheid van de vastlegging en het naleven van de documentatie- en bewaarplicht kan op basis van de aangeleverde informatie niet worden vastgesteld.

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

Formeel hoeft nog niet voldaan te worden (uiterlijk 2023) aan art. 32a van de Wpg, echter vanuit het oogpunt van beveiliging is de BIO (norm 12.4.1) 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.
Er zijn geen logoverzichten en -beleid aangetroffen voor systemen zoals Holmes die gebruikt worden voor verwerking en vastlegging van Wpg-gegevens. Alleen op basis van mededelingen in enkele interviews is aangegeven dat er in beperkte mate gelogd wordt door de beheerder van Holmes (DICTU). Daarom hebben wij niet kunnen vaststellen in welke mate de logging is ingericht volgens de bestaande en breed gedragen normen van de BIO voor alle voor de Wpg verwerkingen gebruikte systemen en voorzieningen.

Uit recente mailwisseling tussen DICTU en ILT blijkt dat logbestanden van Holmes in 2021 niet volledig zijn omdat logbestanden eerder werden verwijderd dan gewenst. In 2021 werden logbestanden niet langer dan één maand bewaard. Deze bewaartermijn is eind 2022 aangepast naar 10 jaar.

3.1.30 Audits zijn nog niet helemaal structureel volgens de regeling en met volledige cyclus en reikwijdte ingebed.

In de auditplanning 2021 is een kalender opgenomen met de geplande interne- en externe audits ILT voor 2021. Voor voorgaande jaren is geen planning aangeleverd. Volgens de door ons getoetste normen zijn de auditplanning en de auditrapportages zogenaamde ‘Toezichtmaatregelen’. Toezichtmaatregelen dienen over de gehele verslagperiode op hun werking te worden getoetst. Er is één interne auditrapportage aangeleverd, terwijl volgens de 'Regeling periodieke audit politiegegevens' er jaarlijks een audit dient te worden uitgevoerd. ILT heeft het zo gepland dat de interne audit start na de externe audit. In de aangeleverde Mavim producten worden Wpg- of interne privacy audits niet genoemd.

Hoewel de opzet niet volledig is, is door de ILT in 2021 een audit naar de verwerking van politiegegevens volgens de Wpg uitgevoerd. Dit heeft geresulteerd

in een auditrapport over 2021. Dit rapport bevat de minimaal vereiste onderdelen. Niet duidelijk is of de betreffende auditors voldeden aan de bekwaamheidseisen. Naar aanleiding van het auditrapport is een verbeterplan opgesteld. Binnen een jaar dient een hercontrole plaats te vinden, dit is niet gebeurd omdat in dezelfde periode de externe privacy-audit plaats zou vinden.

3.1.31 Privacyfunctionaris formeel niet verplicht voor boa's, maar intern toezicht heeft structurele aandacht en inzet nodig

Voor het interne toezicht binnen de ILT op de naleving van de Wpg conform art. 34 Wpg is geen formele privacyfunctionaris aangesteld. Volgens het Besluit politiegegevens boa is dat niet verplicht voor werkgevers van boa's. Het interne toezicht inclusief verslaglegging conform art. 34 Wpg heeft nog niet plaatsgevonden. De ILT heeft wel een privacycoördinator, echter deze komt in de praktijk niet toe aan het toezien op de verwerking van gegevens door boa's. Bovendien is er onduidelijkheid over het wel of niet toebehoren van de Wpg in de rol en het takenpakket van de privacy coördinator. In interviews is aangegeven dat er voor de Wpg te weinig awareness, kennis en capaciteit aanwezig is in de organisatie. Vanwege de aard en omvang van de organisatie en werkzaamheden van de boa's is het verstandig om het interne toezicht op de naleving van de Wpg formeel en met voldoende gekwalificeerde capaciteit (professionalisering en borging van Wpg functies) binnen de organisatie te beleggen.

3.1.32 Toezicht door de Functionaris voor gegevensbescherming vindt plaats, maar is nog in ontwikkeling. Er is nog onvoldoende houvast bij het aantoonbaar naleven en functioneren van Wpg maatregelen.

In 2021 was er formeel een FG en een plv. FG aangesteld. De rol en de taken van de FG zien zowel toe op de verwerkingen onder de AVG als die onder de Wpg. De rol, positie en taken van de FG zijn in opzet uitgewerkt. De in de norm vermelde onderwerpen maken onderdeel uit van het Toezichtjaarverslag van de FG over de naleving van de Wpg over 2021.

Voor 2021 wordt voor het eerst invulling gegeven aan de rapportage- verplichting van de FG over naleving van de Wpg. Het toezichtjaarverslag over 2021 is op moment van onderzoek (mede door vertrek FG per februari 2022 en recente aanstelling nieuwe FG) nog in concept en bepaalde cijfers/gegevens moeten nog op juistheid en volledigheid worden gecontroleerd. Het interne toezicht door ILT op de naleving van de Wpg voor de verwerkingen door boa's moet nog verder ontwikkeld en geborgd worden, zodat het toezicht door de FG van IenW hier op adequate wijze op kan steunen. De interne audit heeft eveneens voor het eerst in 2021 plaatsgevonden, maar nog niet voor alle onderdelen van de Wpg. De resultaten van de interne audit bevat belangrijke input voor het toezicht door de FG.

De functie/rol ten aanzien van het interne toezicht van buitenaf door de FG op de naleving van de Wpg door ILT is nog in ontwikkeling alsmede het interne toezicht door ILT zelf (zie 3.1.31). Er is nog onvoldoende beeld over de werking (het aantoonbaar naleven van) van de Wpg maatregelen. Systematische controles (in de lijn) waarmee aangetoond kan worden dat de Wpg wordt nageleefd (w.o. ook door verwerkers) heeft aandacht nodig. Dit vraagt om professionalisering en borging van Wpg functies en rollen met voldoende gekwalificeerde capaciteit. Als gevolg van personele wisselingen in van voor Wpg verantwoordelijke functies en rollen was er beperkte aandacht en capaciteit voor de Wpg in 2021.

3.2 Bevindingen per norm - organisatorische en technische beheersingsmaatregelen

Dit onderdeel bevat de getoetste normen uit bijlage 4 van de als toetsingskader gebruikte Norea handreiking Privacy audit Wpg voor boa's. 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 en de leveranciers (serviceorganisaties). De door ons getoetste normen bevatten een minimale set aan passende maatregelen, de zogenaamde 'General IT Controls' (GITC) die rand voorwaardelijk zijn voor de juiste verwerking van gegevens die onder de Wpg vallen.

Over het algemeen is gebleken dat de aantoonbaarheid van getroffen beheersmaatregelen onvoldoende is. Voor de dienstverlening door DICTU en SSC-ICT zijn verwerkingsafspraken gemaakt waarin een right to audit bepaling is opgenomen. Voor deze audit hebben wij daar echter onvoldoende op kunnen steunen, doordat er ondanks de gemaakte afspraken geen of beperkte medewerking was en informatie werd verstrekt.

3.2.1 Proces van wijzigingenbeheer, logische toegangsbeveiliging en beheer van kwetsbaarheden kan niet goed beoordeeld worden omdat informatie ontbreekt en getroffen beheersmaatregelen niet aantoonbaar zijn

Doordat geen documentatie ten aanzien van het wijzigingenbeheer zoals een formele procedure is aangeleverd, kan geen goed oordeel over opzet, bestaan en werking worden gegeven. De informatie die wel is aangeleverd is heel summier en niet vastgesteld en biedt in combinatie met wat in de interviews is aangegeven weinig aantoonbaar houvast om te kunnen vaststellen of en in hoeverre passende Wpg maatregelen zijn getroffen door ILT en verwerkers/leveranciers (in dit geval ook door DICTU in verband met IT-beheersing van Holmes en SSC-ICT in verband met beheersing en beveiliging netwerkschijven).
DICTU heeft uiteindelijk pas na maanden een ISO27001 auditrapport verstrekt aangaande een hercertificering van het eigen management systeem voor 2021. Dit rapport gaf ons onvoldoende houvast specifiek voor de beveiliging en beheersing van Holmes voor de Wpg. Omdat dit rapport ruim na de Wpg rapportage deadline van 31-12-2022 in de periode van uitstel is opgeleverd, is in overleg met ILT besloten nu niet verder onderzoek te doen.

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

Er is geen documentatie of voorbeeld over het toepassen van cryptografie aangeleverd voor het opslaan en transporteren van Wpg gegevens. Hierdoor kan geen oordeel over het bestaan en de werking van dit proces worden gegeven. Door het ontbreken van bestaansbewijs is niet inzichtelijk dat encryptie over de gehele (Wpg-)keten (conform BIO) is toegepast.

3.2.3 Uitvoering vulnerability scans en penetratietesten is niet aantoonbaar voor 2021

Er zijn voor 2021 geen documenten over vulnerability scans en pentesten aangeleverd. Hierdoor kan geen oordeel over het bestaan en de werking van dit proces worden gegeven.

Volgens mededeling van de FG, CISO en FB werden penetratietesten uitgevoerd in 2022 en ook al eerder, maar hebben wij van 2021 geen rapporten aangetroffen en/of ingezien.

Eind 2022 is een penetratietest op Holmes uitgevoerd. Daarin is ook het DMS Alfresco alsook de getroffen beveiligingsmaatregelen bij DICTU meegenomen. Toegang tot de netwerkschijven die worden beheerd bij SSC-ICT is geen onderdeel van de penetratietest of een ander beveiligingsonderzoek geweest.

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 Wpg verwerkingen door boa's en het doel van deze verwerkingen vast in het register van verwerkingsactiviteiten en beschrijf en borg een proces dat erop toeziet dat op navolgbare wijze controle wordt uitgevoerd dat de gegevens niet op een met die doeleinden onverenigbare wijze worden verwerkt. Neem dit ook op in een Wpg kwaliteitshandboek.

2. **Noodzakelijkheid en rechtmatigheid**:
   Stel een Wpg kwaliteitshandboek op waarin de noodzakelijkheid en rechtmatigheid van de verwerking van politiegegevens is opgenomen. Beschrijf tevens in een werkinstructie de controle hierop. Beschrijf ook de technische en organisatorische maatregelen die hierop van toepassing zijn en periodiek worden geëvalueerd.

3. **Juistheid en volledigheid**:
   Stel een Wpg kwaliteitshandboek op waarin de juistheid en volledigheid van de verwerking van politiegegevens is opgenomen. Beschrijf tevens in een werkinstructie de controle hierop. Beschrijf ook de technische en organisatorische maatregelen. Richt op aantoonbare wijze controles in op de kwaliteit ten behoeve van de borging van de juistheid en nauwkeurigheid van persoonsgegevens. Houd daarbij rekening met alle systemen, voorzieningen en bestanden die gebruikt worden bij opslag van politiegegevens elders dan in Holmes, op gemeenschappelijke netwerkschijven en gegevensdragers.

4. **Bijzondere categorieën van persoonsgegevens**:
   Stel een Wpg kwaliteitshandboek op waarin het verwerken van bijzondere persoonsgegevens is opgenomen en de manier waarop de ILT hiermee omgaat. Beschrijf tevens in een werkinstructie controle op de juiste verwerking. Beschrijf ook de technische en organisatorische maatregelen. Maak inzichtelijk welke beveiliging wordt toegepast bij ILT op bijzondere categorieën van persoonsgegevens (denk daarbij ook aan de Wpg gegevens die zijn verwerkt met andere voorzieningen dan Holmes en het aantoonbaar naleven van maatregelen bij SSC-ICT en DICTU). Controleer op basis van intern toezicht of de bijzondere categorie gegevens alleen worden gebruikt in aanvulling op andere politiegegevens of ook echt nodig zijn voor de strafrechtelijke interventies.

5. **Geautomatiseerde individuele besluitvorming**:
   N.v.t. zie onder bevindingen.

6. **Onderscheid feiten en oordeel**:
   Werk de in 2022 opgestelde werkinstructie onderscheid feiten en oordelen verder uit en formaliseer deze. Beschrijf en borg tevens de controle op het toepassen en naleven van de beschreven waarborgen en richtlijnen zoals het structureel toepassen van een collegiale toets door middel van het vier ogen principe.

7. **Aanwijzen bevoegde functionarissen**:
   Bepaal voor boa's van de ILT of en in welke situaties het (verder) verwerken van politiegegevens volgens art. 9 Wpg van toepassing is en wie daarbij als bevoegde functionaris verantwoordelijk is voor het op navolgbare wijze verlenen van toestemming voor het verder verwerken van gegevens. Indien dit van toepassing is of kan zijn voor boa's van de ILT, werkt dit dan procesmatig uit conform artikel 6 lid 7 en zorg ervoor dat op aantoonbare wijze functionarissen binnen ILT worden aangewezen (bv. bepaalde teamleiders/boa's) die volgens een vastgesteld overzicht bevoegd zijn om instemming te verlenen voor het onder bepaalde voorwaarden verder verwerken van gegevens. Leg de verleende instemming en het doel van het onderzoek nadrukkelijk vast, zodat dit achteraf te reconstrueren is.

8. **Onderscheid tussen verschillende categorieën van betrokkenen**:
   Borg in de gegevensverwerkingen en de daarbij gebruikte systemen, voorzieningen en richtlijnen dat op aantoonbare wijze duidelijk onderscheid wordt gemaakt in de verschillende categorieën van betrokkenen zoals ook opgenomen in het register van verwerkingen. Stel de in 2022 opgestelde conceptwerkinstructie categorieën van betrokkenen vast (incl. datum, versiebeheer en auteur) en toets of deze werkinstructie toereikend is voor het op een juiste wijze vastleggen van betrokkenen.

9. **Reikwijdte**:
   Identificeer en documenteer alle Wpg gegevensverwerkingen door boa's van de ILT inclusief de daarbij gebruikte systemen, voorzieningen en bestanden. Dit vormt de basis voor de uit te voeren Wpg DPIA of risicoanalyse. Completeer op basis hiervan het register van verwerkingen en stel dit vast. Bepaal en leg tevens duidelijk vast of artikel 9 en 13 (ook) van toepassing (kunnen) zijn op de Wpg verwerkingen door boa's van de ILT.

10. **Gegevensbescherming door beveiliging en ontwerp**:
    Voer op aantoonbare wijze voor alle Wpg verwerkingen door boa's inclusief de daarbij gebruikte systemen en voorzieningen alsook voor de verwerking bij derden een gedegen risicoanalyse (DPIA) uit en evalueer periodiek of het stelsel van getroffen organisatorische en technische maatregelen (nog) afdoende/ passend is. Maak volgens het in 2022 vastgestelde privacybeleid inzichtelijk dat aantoonbaar conform de wet wordt voldaan aan privacy by design, door op navolgbare wijze passende organisatorische en technische maatregelen te treffen en daar verantwoording over af te leggen.

11. **Verwerkers en verwerkersovereenkomsten**:
    Borg in de contractuele afspraken met verwerkers aangaande de afgenomen dienstverlening dat specifiek aandacht is voor het verwerken van persoonsgegevens in overeenstemming met de Wpg en dat de vigerende verwerkersafspraken in het register bij de betreffende geïdentificeerde verwerkers worden opgenomen. Borg tevens in de organisatie dat jaarlijks op aantoonbare wijze en volgens vastgelegde afspraken en het in 2022 vastgestelde privacybeleid wordt toegezien op de naleving van de Wpg door alle vastgestelde verwerkers door hiervoor een intern controleplan op te stellen. Draag zorg dat bij interne audits eveneens getoetst wordt of verwerkers technische en organisatorische maatregelen hebben getroffen zodat de ILT kan voldoen aan haar wettelijke plichten ten aanzien van de Wpg. ILT moet zich ten behoeve van verwerkingsverantwoordelijke over de toereikendheid van de door verwerkers geïmplementeerde technische en organisatorische maatregelen kunnen verantwoorden.

12. **Geheimhouding**:
    Borg dat met regelmaat actief aandacht op de werkvloer is voor het zorgvuldig en bewust omgaan met Wpg gegevens maar ook aan de consequenties van het niet naleven van geheimhouding. Zorg dat dit ook aantoonbaar in het toezicht

op de naleving van de Wpg is geborgd zowel voor boa's van de ILT alsook voor het nakomen van afspraken hierover met verwerkers.

13. **Gegevensbeschermingseffectbeoordeling/DPIA**:
    Zorg dat op aantoonbare wijze conform de eisen in de wet de privacyrisico's en de benodigde maatregelen in kaart worden gebracht voor alle Wpg verwerkingen door boa's en voor verwerkingen door derden inclusief de daarbij gebruikte systemen, voorzieningen en bestanden. Leg de opgestelde Wpg DPIA's vast in het register en evalueer periodiek of het stelsel van getroffen organisatorische en technische maatregelen afdoende is. Besteed daarbij nadrukkelijk aandacht aan de risico's die gepaard gaan met het verwerken van bijzondere categorieën van persoonsgegevens.

14. **Melding datalekken:**
    Stel een communicatieplan op voor meerdere jaren waarbij het actief communiceren naar medewerkers over Wpg datalekken herkennen, beperken en voorkomen centraal staat. Zorg ervoor dat datalekken (AVG en toekomstige Wpg) aantoonbaar binnen 72 uur worden gemeld bij de AP en indien relevant tijdig aan betrokkene(n).

15. **Gegevensbescherming door standaardinstellingen:**
    Wij bevelen aan om de maatregelen voor gegevensbescherming door standaardinstellingen van de Wpg meer expliciet uit te werken in een beleidskader en in de verwerkingsafspraken op te nemen en te laten accorderen door de daartoe bevoegde functionaris(sen).

16. **Autorisaties en Toegang tot politiegegevens:**
    Wij bevelen aan om een overzicht met functiescheiding en een bijbehorende autorisatiematrix conform Wpg voor alle gebruikte systemen en voorzieningen op te stellen en door bevoegd gezag te laten accorderen. Stel eerst een functiescheidingsmatrix op welke functies/rechten wel en niet mogen worden vermengd. Maak een IST-positie van Holmes en corrigeer onjuistheden o.b.v. (1) functiescheidingsmatrix en (2) bezettingsoverzichten (HR-lijsten). Dit is de nulmeting/beginstand/IST. Bij iedere periodieke controle vervolgens de onjuistheden eruit halen (dit wordt dan de delta op de IST-positie (nulmeting)) Ten slotte het vaststellen door een bevoegd functionaris (bv. afdelingsmanager) als nieuwe IST-positie.

    Verder bevelen wij aan de Holmes autorisatie documenten te actualiseren en te laten accorderen door de daartoe bevoegde functionaris(sen). Leg op aantoonbare wijze het aanmaken, wijzigen en intrekken van Holmes autorisaties vast, alsmede de periodieke controles hierop, zodat de werking van het proces vastgesteld kan worden.

17. **Uitvoering van de dagelijkse politietaak:**
    Actualiseer de procedures en werkinstructies conform de Wpg en stel deze documenten vast. Daarnaast is het aan te bevelen om het systeem met Wpg-registraties dusdanig in te richten dat aantoonbaar geborgd wordt dat artikel 8 politiegegevens één jaar na de datum van de eerste verwerking achter een schot worden geplaatst en maximaal 5 jaar beschikbaar zijn. Na het verstrijken van de bewaartermijn moet geborgd zijn dat de gegevens aantoonbaar worden verwijderd. Borg tevens in de gebruikte systemen en voorzieningen dat op aantoonbare wijze een duidelijk onderscheid te maken is in toezicht- en opsporingsactiviteiten.

    Tevens bevelen wij aan om de operationele werkvloer te trainen en te instrueren aangaande de Wpg bewaartermijnen en het tijdig schonen c.q. verwijderen van Wpg gegevens. Ook omdat er naast Holmes verschillende systemen, voorzieningen en bestanden voor verwerking en opslag van Wpg gegevens worden gebruikt.

18. **Geautomatiseerd vergelijken en in combinatie zoeken:**
    Leg bij het identificeren van alle Wpg verwerkingen door boa's en het completeren van het register vast of er sprake is van geautomatiseerd vergelijken en in combinatie zoeken. Geef daarbij ook expliciet aan of in de voor de verwerking gebruikte systemen en voorzieningen functionaliteit bestaat die dit mogelijk maakt.

19. **Ondersteunende taken:**
    Leg een werkwijze vast voor de vastlegging van artikel 13 verwerkingen en neem dit als onderdeel van het intern toezicht op de naleving van de Wpg mee en laat dit tevens door de interne audit toetsen.

20. **Ter Beschikking stellen (voor verdere verwerking):**
    Bepaald de artikel 9 verwerkingen en wijs vervolgens de functionarissen binnen ILT aan die de bevoegdheid hebben om toestemming te kunnen verlenen voor de verdere verwerking van gegevens door boa's. Het verdient aanbeveling om hiervoor een centraal overzicht op te maken en vast te stellen met bevoegde functionarissen (en bijvoorbeeld toegankelijk op het Rijksportaal) zodat dit goed vindbaar is voor boa's.
    Maak het ter beschikking stellen van politiegegevens aan bevoegde autoriteiten in andere lidstaten van de Europese Unie of aan organen en instanties belast met de taken, bedoeld in artikel 1, onderdeel a conform de richtlijnen, onderdeel van het interne toezicht.

21. **Bewaartermijnen, verwijderen en vernietigen:**
    Maak inzichtelijk hoe de bewaar-, verwijder- en vernietigingstermijnen voor politiegegevens op grond 8, 9 en 13 zijn ingericht, leg dit vast en controleer op navolgbare wijze periodiek (bv. per kwartaal) of uitvoering ervan op de vastgestelde manier plaatsvindt.

22. **Verstrekking van politiegegevens aan anderen dan politie en Koninklijke marechaussee:**
    Het bestaan en de werking van het in 2022 beschreven en ingerichte proces van verstrekken kan pas goed vastgesteld worden als dit proces enige tijd aantoonbaar functioneert. Maak het periodiek toetsen van de werking van ingerichte processen w.o. voor verstrekkingen onderdeel van het toezicht en de interne audits.

    Inmiddels is er een werkinstructie gerealiseerd (2022) waarin de documentatieplicht is opgenomen in Holmes. Als er sprake is van gegevensverstrekking buiten het Wpg domein dan moeten de gegevens worden vastgelegd in Holmes.

23. **Doorgiften aan derde landen:**
    Eventuele doorgiften van gegevens werden nog niet vastgelegd in 2021. Zie onder bevindingen. Wij adviseren in de eerstvolgende audit vast te stellen of de in 2022 geïmplementeerde documentatieplicht voor doorgifte van gegevens aan derde landen toereikend is.

24. **Verstrekking aan derden structureel voor samenwerkingsverbanden:**
    Breidt de Leidraad gegevensuitwisseling ILT uit, breng dit actief onder de aandacht van boa's zodat het duidelijk is en er inzicht ontstaat in de samenwerkingsverbanden waarbij politiegegevens worden verstrekt. Leg de betreffende samenwerkingsverbanden tevens vast in het register.

25. **Rechtstreekse verstrekking:**
    N.v.t. zie onder bevindingen.

26. **Informatie aan de betrokkene, recht op inzage, rectificatie en verwijdering:**
    Om op ordelijke manier geldende wet- en regelgeving te kunnen naleven, de gewenste werkwijze uit te dragen en inzicht te geven in verantwoordelijkheden en bevoegdheden, bevelen wij aan om procedures die nu alleen voor de AVG zijn opgesteld aan te passen zodat deze ook voor de Wpg van toepassing zijn en deze te actualiseren en te laten accorderen door de verantwoordelijke manager. Toets zodra er verzoeken tot inzage zijn gedaan voor Wpg verwerkingen of het proces en de instructies toereikend en conform Wpg zijn.

27. **Register:**
    Completeer en documenteer het verwerkingenregister met alle voorkomende Wpg-verwerkingen door boa's (incl. DPIA's, verwerkersovereenkomsten en termijnen waarbinnen verschillende categorieën van gegevens worden verwijderd of vernietigd) en stel dit vast. Neem bij diverse onderdelen in het register een korte motivatie of toelichting op waarom iets wel of niet van toepassing is en/of verwijs naar betreffende documenten. Controleer op aantoonbare wijze periodiek dat het register volgens vastgestelde procedure wordt bijgehouden c.q. geactualiseerd en dat het register juist en volledig is.

    In het stappenplan privacy als onderdeel van het privacybeleid (2022) wordt inmiddels een proces incl. verantwoordelijkheden beschreven voor het onderhouden van het verwerkingenregister.

28. **Documentatie:**
    Maak op aantoonbare wijze inzichtelijk dat wordt voldaan aan de schriftelijke vastlegging van de onderdelen genoemd in art 32 lid 1 en dat de bedoelde politiegegevens conform art 32 lid 4 worden bewaard.

29. **Logging:**
    Formeel hoeft nog niet voldaan te worden (uiterlijk 2023) aan art. 32a van de Wpg, echter vanuit de Baseline Informatiebeveiliging Overheid (BIO), die al langer van toepassing is op de gehele overheid, is het vastleggen van gebruikersactiviteiten voorgeschreven.
    Zie voor logging onder meer: BIO, 12.4.1 Gebeurtenissen registreren.
    "Logbestanden van gebeurtenissen die gebruikersactiviteiten, uitzonderingen en informatiebeveiligingsgebeurtenissen registreren, behoren te worden gemaakt, bewaard en regelmatig te worden beoordeeld".

    Om zorg te dragen dat door of namens een belanghebbende achteraf op basis van administratieve vastleggingen de besluitvorming in processen en de administratieve verwerking van deze besluitvorming kan worden beoordeeld en op ordelijkheid worden getoetst, bevelen wij aan het loggen van gebruikersactiviteiten ten aanzien van de Wpg-gegevens structureel te borgen (in beleid en procedures) in de organisatie en de voor de Wpg verwerkingen gebruikte systemen.

    Aanbeveling is om deze norm bij de eerstvolgende (interne) audit te toetsen.

30. **Audits:**
    Om de kwaliteit van de verwerking van Wpg-gegevens naar een hoger niveau te brengen, raden wij aan om het auditproces structureel en met volledige reikwijdte te borgen en in te richten, zodanig dat de resultaten van de interne audits gebruikt kunnen worden voor verbeteringen intern ILT, het toezicht op de naleving van de Wpg en ter voorbereiding op de externe privacy-audit.

31. **Privacyfunctionaris:**
    Hoewel de privacyfunctionaris Wpg niet verplicht is gesteld volgens het Besluit politiegegevens boa, bevelen wij aan het interne toezicht op en de rapportage over de naleving van de Wpg door boa's conform art. 34 formeel en met voldoende gekwalificeerde capaciteit te beleggen binnen de organisatie, zodat op structurele wijze invulling gegeven wordt aan een werkende cyclus voor intern toezicht door ILT op de Wpg waar het toezicht door de FG goed op kan steunen. Wij denken dat het verstandig is om dit Wpg toezicht specifiek bij een aparte functionaris te beleggen en dit niet te combineren met het takenpakket van de PC.

32. **Functionaris voor gegevensbescherming:**
    Borg structureel dat de taken, verantwoordelijkheden en rapportagelijnen voor het toezicht en de controle (door ILT zelf en door de FG van buitenaf) op de naleving van de Wpg-verplichtingen voor de verwerkingen door boa’s zijn vastgelegd, ingericht en aantoonbaar met voldoende gekwalificeerde capaciteit functioneren volgens het vastgestelde privacybeleid. Dit vormt de basis om op een transparante en adequate wijze zowel in opzet als voor het bestaan en de werking van maatregelen verantwoording over het naleven van de Wpg te kunnen afleggen door de verwerkingsverantwoordelijke.

33. **Wijzigingenbeheer, logische toegangsbeveiliging en beheer van kwetsbaarheden:**
    Voor het juist en nauwkeurig verwerken van Wpg-gegevens is het belangrijk dat de systemen die hiervoor worden gebruikt zoveel mogelijk vrij zijn van kwetsbaarheden en fouten en betrouwbaar en integer zijn. General IT Controls (GITC), waartoe het wijzigingenbeheer, de logische toegangsbeveiliging en het patchmanagement behoren, zijn rand voorwaardelijk voor de juiste verwerking van (Wpg-)gegevens. Wij adviseren dan ook het wijzigingsbeheer, de logische toegangsbeveiliging en het beheer van kwetsbaarheden structureel en aantoonbaar conform de GITC eisen van het toetsingskader in te bedden in de organisatie. Ook de aantoonbaarheid van getroffen Wpg maatregelen bij SSC-ICT en DICTU is van groot belang om adequaat de kunnen sturen en verantwoorden. Ons advies is om deze maatregelen bij de eerstvolgende audit met volle reikwijdte te toetsen en daar voorafgaand aan de audit goede afspraken over te maken en vast te leggen met betrokken partijen.

34. **Cryptografie:**
    Beschrijf in het cryptografiebeleid welke gegevens op basis van een classificatieschema versleuteld dienen te worden en op welke wijze, waarbij de focus ligt op zowel opslag als transport van politiegegevens.
    Richt een aantoonbaar proces in dat periodiek toeziet op het toepassen en naleven van het gebruik van cryptografische beheersmaatregelen door verwerkers en dienstverleners.

35. **Vulnerability scans en Penetratietesten:**
    Borg dat periodiek volgens vastgesteld beleid penetratietesten worden uitgevoerd op voor Wpg verwerkingen gebruikte systemen en voorzieningen.

    Omdat er ook Wpg gegevens buiten Holmes worden opgeslagen zoals op diverse netwerkschijven en mogelijk op andere voorzieningen en devices, bevelen wij aan dit eveneens in het kader van beveiliging en bescherming van Wpg-gegevens te onderzoeken.

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 ILT op adequate wijze uitvoering is gegeven aan de bepalingen van de Wpg. Hiertoe hebben wij in de periode augustus 2022 tot en met februari 2023 werkzaamheden uitgevoerd om de opzet, het bestaan en de werking vast te stellen van de beheersingsmaatregelen die de ILT 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 ILT nog geen werkend proces is ingericht voor intern toezicht voor naleving van de Wpg. 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 2021 door ILT uitgevoerde interne audit naar de implementatie van de Wpg.
- Interviews met de plv. functionaris voor gegevensbescherming (tevens waarnemend FG), privacycoördinator, projectleider, beveiligingsfunctionaris (CISO) en teamleiders en boa’s van de geselecteerde en onderzochte onderdelen. 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, werkinstructies, inzage in het register van verwerkingen, screenshots uit Holmes van verwerkingen, intern audit rapport en toezichtjaarverslag.
- Waarneming: wij hebben, waar dat kon, 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 functionaris voor de gegevensbescherming.

Onder coördinatie van een interne projectgroep voor implementatie van de Wpg zijn vanaf eind 2021 al een aantal verbeteracties naar aanleiding van de interne audit 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 maatregelen voor het interne toezicht nog niet mogelijk in verband met het ontbreken van een intern 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. Reden hiervan is dat beide dienstverleners (SSC-ICT en DICTU), waar het technisch beheer van de voor de gegevensverwerking gebruikte systemen en voorzieningen is belegd, geen informatie hebben aangeleverd waaruit blijkt dat Wpg maatregelen aantoonbaar zijn getroffen en worden beheerst. Wij hebben als basis wel gekeken naar de sturing en regie door ILT op het nakomen van de gemaakte afspraken tussen de partijen.

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 ILT
Omdat het vanwege de omvang onmogelijk is om bij de ILT alle processen waarin Wpg verwerkingen plaatsvinden te toetsen aan uitvoering van de Wpg, is na overleg met contactpersonen van de ILT voor de scope van deze Wpg audit door de ADR een selectie gemaakt van te onderzoeken modaliteiten en teams van de ILT. De onderbouwing voor de selectie is onder meer gebaseerd op het Jaarverslag BOA ILT over 2021, alsook op de vermelde Wpg verwerkingen door boa's in het register. Bij de ILT zijn per 31 december 2021 in totaal 163 boa's werkzaam. De boa's van de ILT zijn formatief geplaatst bij verschillende teams en bevinden zich daardoor verspreid door de organisatie. De 163 boa's zijn verdeeld over twee directies, zes afdelingen en vijfentwintig teams. Uit opgave in het Jaarverslag blijkt dat in 2021 verreweg de meeste boa's (122) werkzaam zijn binnen de afdelingen Keten gevaarlijke stoffen en organismen en Marktordening en dat daar ook de meeste processen-verbaal (486) en strafbeschikkingen (252) zijn opgeleverd. Daarom is besloten de focus binnen deze audit te richten op de opsporingswerkzaamheden van boa's op de afdelingen Keten gevaarlijke stoffen en organismen en Marktordening. Bij de verschillende afdelingen en teams 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, de inspecteur-generaal ILT, 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, 30 juni 2023

Bijlage 1 Managementreactie ILT

Inspectie Leefomgeving en Transport
Ministerie van Infrastructuur en Waterstaat

Auditdienst Rijk

ILT
Informatie, Netwerken en Programmering
ICT
[redacted]

Kenmerk
ILT-2023-CIO-boa02

Datum 21 juni 2023
Betreft Managementreactie bij het Assurancerapport Privacy Audit Wet politiegegevens boa's ILT 2021

De Inspectie Leefomgeving en Transport (ILT) dankt de Auditdienst Rijk (ADR) voor het uitgebreide onderzoek naar het voldoen aan de Wet politiegegevens (Wpg) door haar buitengewoon opsporingsambtenaren (boa's). Het betreft de eerste privacy audit die de Regeling periodieke audit politiegegevens voorschrijft, na de inwerkingtreding van het Besluit politiegegevens buitengewoon opsporingsambtenaren. Door uitloop als gevolg van late start en vertraagde oplevering van gegevens was het niet gelukt om de door de Autoriteit Persoonsgegevens gestelde uiterste deadline van 31 december 2022 te halen. Door de oplevering van dit assurancerapport kan de ILT alsnog aan deze verplichting voldoen.

De ILT herkent zich in het afgegeven oordeel dat de ILT in 2021 in belangrijke mate niet voldoet aan de Wpg en dat het daadwerkelijk bestendigen en aantoonbaar borgen van geconstateerde verbeteringen om structurele aandacht en inzet vraagt. De ILT neemt de aanbevelingen uit dit rapport onverwijld over.

Het afgegeven oordeel is overeenkomstig het beeld dat eerder uit het interne auditrapport uit juli 2021 naar voren kwam, op basis waarvan de ILT in het laatste kwartaal van 2021 een verbeterproject is gestart. Dit project heeft reeds een groot aantal verbeteracties uitgevoerd in 2022 en de eerste helft van 2023, die buiten de periode van toetsing door de ADR vallen.
Zo zijn in het automatiseringssysteem Holmes verbeteringen doorgevoerd ten aanzien van de afscherming van informatie, zijn bewaartermijnen geautomatiseerd ingesteld en zijn er functionaliteiten toegevoegd ten behoeve van de documentatieplicht bij verstrekkingen en kunnen categorieën van betrokkenen worden toegekend.
Ook is er al veel in gang gezet om de kennis en bewustwording omtrent Wpg te vergroten, o.a. door bewustwordingssessies te geven, het aanbieden van e-learningmodules en het opzetten van een kennisbank Wpg op het intranet van ILT waar hulpmiddelen en werkinstructies voor boa's beschikbaar zijn. Vanaf de tweede helft 2023 krijgen alle boa's van de ILT een maatwerktraining voor het werken onder de Wpg aangeboden.
In het nieuwe Privacybeleid ILT uit 2022 is de Wpg voor zowel voor boa's als voor de Inlichtingen- en Opsporingsdienst nu expliciet opgenomen. In aanvulling op dit generieke beleid is een specifiek operationeel werkkader opgesteld waarin afspraken worden gemaakt over de sturing en zijn de taken en

verantwoordelijkheden voor de Wpg verdeeld. Verder is het verwerkingsregister aangevuld voor de Wpg en zijn de procedures voor datalekken en rechten van betrokkene voor de afhandeling conform de Wpg uitgewerkt.

Bovenstaand inzet vanuit het project heeft ertoe geleid dat de ILT al goed op weg is met het oplossen van bevindingen die nu door de ADR zijn geconstateerd. Hierdoor is de ILT beter in staat om dit onderwerp te beheersen. Daarnaast biedt het uitgevoerde onderzoek ook nieuwe en aanvullende inzichten, die de ILT zullen helpen om de eerder genomen maatregelen te verbeteren of nieuwe maatregelen door te gaan voeren. De ILT zal hiertoe binnen drie maanden na ontvangst van dit rapport een nieuw verbeterplan opstellen en ook deze aanbevelingen met grote urgentie oppakken. De ILT zal vervolgens binnen een jaar vanuit de interne auditcyclus een hercontrole uitvoeren.

Auditdienst Rijk
Postbus 20201
2500 EE Den Haag
(070) 342 77 00