Interne audit Wpg
derde cyclus 2015-2018

2018

Concernaudit
Definitief
Assurance rapport
versie 1.0
19 september 2019

« waakzaam en dienstbaar »

Documentinformatie

Versiegeschiedenis

Versie	Versie datum	Samenvatting van de aanpassing	Gemarkeerde wijzigingen
0.6	21 februari 2019	Auditors 10.2.e en 10.2.e	
0.7	8 maart 2019	Opmerkingen kwaliteitscontrole verwerkt	
0.8	19 juli 2019	Concept definitief ter review	
0.9	2 september 2019	Opmerkingen / aanvullingen verwerkt	
1.0	19 september 2019	Versie definitief	

Distributie

Versie	Verzend datum	Naam	Afdeling / Functie
1.0	30-01-20	Dhr. H.G. Geveke	Lid Korpsleiding
1.0	30-01-20	Dhr. 10.2.e	Gegevensautoriteit / Dir. IV
1.0	30-01-20	Dhr. 10.2.e	Vz Stuurgroep Wpg en IB
1.0	30-01-20	Dhr. T. Visscher	Functionaris Gegevensbescherming
1.0	30-01-20	Dhr. 10.2.e	Ministerie J&V / DGPOL
1.0	30-01-20	Mevr. 10.2.e Mevr. 10.2.e	Auditdienst Rijk
1.0	30-01-20	Mevr. 10.2.e	Secretaris Auditcommissie Politie

Inhoudsopgave

1. Samenvatting / belangrijkste bevindingen

Concernaudit (CA) heeft conform wet en regelgeving een onderzoek uitgevoerd naar de Wet politiegegevens (Wpg). Het doel van het onderzoek is vaststellen in hoeverre de Politie voldoet aan de Wpg.

De centrale onderzoeksvraag van deze audit is:

Geeft de Politie in opzet, bestaan en werking op adequate wijze uitvoering aan de bepalingen bij of krachtens de Wpg?

Het antwoord op deze vraag luidt:

Alleen op het onderwerp Rechten van de Betrokkene zijn verbeteractiviteiten volledig afgerond waardoor de Politie in opzet en bestaan voldoet aan de wet. Voor de andere onderwerpen geldt dat deze niet of niet geheel voldoen aan de wet. Dit brengt met zich mee dat de uitvoerbaarheid en de beheersbaarheid van naleving van de bepalingen bij of krachtens de Wpg niet of niet geheel is geborgd.

Wij hebben waargenomen dat de laatste jaren veel inspanningen zijn verricht om gegevens betrouwbaar en in lijn met de Wpg vast te leggen en te beheersen. Aan de andere kant hebben wij gezien dat de executiekracht van de organisatie om hierin volwassener te worden beperkt is. In onderstaande figuur is de status per onderwerp ultimo 2018 weergegeven. De onderbouwing van ieder onderwerp is opgenomen in hoofdstuk 4.

Wpg art.	Het management is in control conform Wpg	Opzet	Bestaan	Oordeel opzet en bestaan op basis van bevindingen uit cyclus	
6	Autoriseren	Or	Rd		3 (2015-2018)
16-24	Verstrekken	Gr	Gs		3 (2015-2018)
32	Protocolleren	Gr	Gs		3 (2015-2018)
8-14	Bewaartermijnen	Rd	Gs	2 (2011-2014)	
25-31	Rechten van de Betrokkene	Gr	Gr		3 (2015-2018)
3-4	Kwaliteitsaspecten van politiegegevens	Rd	Gs	2 (2011-2014)	
5	Gevoelige gegevens	Rd	Gs	2 (2011-2014)	
11	Geautomatiseerd vergelijken en in combinatie zoeken	Rd	Gs	2 (2011-2014)	
15	Ter beschikking stellen	Rd	Gs	2 (2011-2014)	
33	Audits	Rd	Rd		3 (2015-2018)
34	Privacy Functionaris	Gr	Rd		3 (2015-2018)
----	Governance / beheersing	Or	Or		3 (2015-2018)

Wpg art.	Onderwerpen behorende tot de Wpg vanaf 1 januari 2019 alsmede randvoorwaarden behorende tot de Wpg	Opzet	Bestaan	Oordeel opzet en bestaan op basis van bevindingen uit cyclus	
36	Functionaris Gegevensbescherming	Gr	Gr		3 (2015-2018)
----	Implementatie PSbD	Gr	Gr		3 (2015-2018)
----	ITGC	Rd			3 (2015-2018)

Rd	Voldoet niet
Or	Voldoet niet geheel
Gr	Voldoet
Gs	Geen oordeel

Figuur 1 Samenvattend overzicht Wpg ultimo 2018

2. Context

2.1. Aanleiding audit

Centrale en lokale overheden, uitvoeringsorganisaties en bijvoorbeeld ook Politie en ministerie van Justitie en Veiligheid beschikken over een grote hoeveelheid, vaak gevoelige, persoonsgegevens. De Politie verzamelt persoonsgegevens van burgers zonder dat zij daar toestemming voor geven. Zij moeten er dan op kunnen vertrouwen dat de overheid zich bij de verwerking van de persoonsgegevens aan de regels houdt. Sinds januari 2008 is de Wet politiegegevens (Wpg) van kracht. In deze wet is geregeld waaraan de Politie moet voldoen bij het verwerken van persoonsgegevens voor de politietaak. Eén van de wettelijke eisen is het periodiek (laten) uitvoeren van interne en externe audits.

De interne audit moet per jaar voor een deel van de Wpg, of een deel van de organisatie worden uitgevoerd. De voor u liggende rapportage is in dit kader opgesteld.

2.2. Doelstelling en onderzoeksvragen

De jaarlijkse interne audit heeft tot doel op systematische wijze toetsen of op adequate wijze uitvoering is gegeven aan de bepalingen van de wet. Hiervoor heeft een beoordeling plaatsgevonden van de opzet en bestaan van maatregelen en procedures die in naleving van de wettelijke eisen moeten voorzien. De onderzoeksvraag voor deze audit luidt:

Geeft de Politie in opzet, bestaan en werking op adequate wijze uitvoering aan de bepalingen bij of krachtens de Wpg?

2.3. Werkwijze

2.3.1. Scope audit

De ***opzet*** is het ontwerp op papier en is onder andere het ‘beleid’ dat de organisatie heeft opgesteld. Hierbij gaat het onder meer om de processen en beheersingsmaatregelen die zijn ontworpen en beschreven om aan de Wpg te voldoen. Als de opzet is bepaald kan in de praktijk bij de eenheden worden vastgesteld of de beschreven processen en beheersingsmaatregelen zijn geïmplementeerd. Hierbij is het zo dat bij een geïmplementeerde beheersingsmaatregel, het ***bestaan*** vaststaat als een ontworpen proces/maatregel minimaal één keer heeft gewerkt. De ***werking*** kan worden vastgesteld wanneer het bestaan gedurende een bepaalde periode in ogenschouw wordt genomen.

Bij dit onderzoek is gekeken naar de ‘opzet’ en het ‘bestaan’. Werking is buiten de scope gebleven omdat in audit cyclus twee 2011 - 2014[i] het bestaan niet is vastgesteld. Daarnaast geldt dat werking pas kan worden vastgesteld als opzet en bestaan over langere periode aan de wet voldoet. Voor resterende onderwerpen is dat niet het geval. Bovendien heeft de opdrachtgever bij sommige onderwerpen aangegeven dat niet alle verbeteractiviteiten zijn afgerond. Hierdoor komen deze onderwerpen ook niet in aanmerking voor een onderzoek om vast te stellen of deze onderwerpen gedeeltelijk of volledig voldoen aan de Wpg. Voor deze onderwerpen zijn wij uitgegaan van de resultaten zoals die zijn vastgesteld in audit cyclus 2. Zie figuur 1 voor welke onderwerpen dit betreft.

Voor de Wpg onderwerpen Rechten van de Betrokkene en Autoriseren, zijn wél verbetermaatregelen afgerond die zouden kunnen leiden tot het gedeeltelijk of volledig voldoen aan de Wpg. Op deze Wpg onderwerpen hebben wij een audit uitgevoerd. In de afgelopen periode is veel geïnvesteerd binnen de opzet van Rechten van de Betrokkene en Autorisaties. Ook in het bestaan zijn stappen gezet, echter deze hebben nog niet hun effect gehad tijdens de gehele Wpg cyclus van vier jaar. De periode om de werking te kunnen toetsen gedurende deze audit over de derde cyclus is korter dan vier jaar en daarom te kort.

In 2015 is destijds de werking van een aantal onderdelen nog wel vastgesteld. De eenheden konden worden getoetst aan de eigen ontwikkelde of uit een oud korps geadopteerde opzet. In 2015 was er nog geen centrale opzet ontwikkeld.

Voor de audit van cyclus 3, beschouwen wij de politie als één organisatie waarbij beleid (opzet) centraal is vastgesteld. Het bestaan is vastgesteld in de eenheden op lokaal niveau (zoals de privacydesk). De werking vastgesteld wanneer dit centraal (zoals autoriseren) is geïmplementeerd.

Volgens de Wpg is de Politie verplicht ieder jaar een deel van de Wpg te onderzoeken welke bestaat uit een lijst van 12 onderwerpen, waarvan er 11 expliciet in de wet worden genoemd.

De Wpg is in 2008 opgedeeld in 11 onderwerpen plus het onderwerp Governance/beheersing. In de tweede cyclus is daar het onderwerp IT-General Controls (ITGC) aan toegevoegd omdat dit iets zegt over de mate van IT-beheersing. In de huidige derde cyclus is ook de Functionaris Gegevens bescherming toegevoegd aan de lijst omdat in mei 2018 de verplichting van een functionaris gegevensbescherming (FG) is voorgeschreven door de Algemene Verordening Gegevensbescherming (AVG) en de FG in de Wpg wordt genoemd. Ook is alvast in deze cyclus meegenomen Privacy en Security by Design (PSbD). Dit onderwerp is overigens pas verplicht vanaf 1 januari 2019.

Met de opdrachtgever is afgesproken dat de audit zich richt op Rechten van de Betrokkene, Autoriseren en PSbD. Reden hiervoor is dat *alleen* op deze drie onderwerpen zodanig vooruitgang is gerealiseerd dat het zinvol was de status te onderzoeken. Voor de andere onderwerpen was dat niet nodig omdat volgens de opdrachtgever verbeteractiviteiten niet of niet volledig waren afgerond.

Resume
Hieronder zijn de onderwerpen opgenomen waar het oordeel op is gebaseerd. Een visuele weergave is opgenomen in figuur 1.

CA beperkt zich in dit rapport tot een samenvatting van de bevindingen van Rechten van de Betrokkene omdat dit onderwerp dermate omvangrijk is dat dit een eigen rapport verdient. Voor de details verwijzen wij naar het parallel uitgebrachte rapport Rechten van de Betrokkene. [ii] Dit is een rapport dat gaat over de het bestaan in de eenheden.

Voor de onderwerpen Autoriseren, Rechten van de Betrokkene en PSbD is opdracht gegeven voor het onderzoeken van de opzet en het bestaan. Het oordeel is gebaseerd op de uitgevoerde werkzaamheden in cyclus 3.

De opzet van de onderwerpen Verstrekken en Protocolleren is opnieuw onderzocht omdat deze in cyclus 2 als ‘voldoende in opzet’ waren beoordeeld. De opdrachtgever heeft aangegeven dat voor bestaan geen verbeteractiviteiten zijn afgerond en daarom is het oordeel gebaseerd op cyclus 2. Het oordeel over de opzet is gebaseerd op de uitgevoerde werkzaamheden in cyclus 3.

Van de onderwerpen Bewaartermijnen, Kwaliteit van Gegevens, Gevoelige Gegevens, Geautomatiseerd Vergelijken en in Combinatie Zoeken en Ter Beschikking stellen zijn volgens de opdrachtgever niet alle verbeteracties afgerond. Het gevolg hiervan is dat op het gebied van de opzet en/of bestaan geen gebreken zijn verholpen. Het oordeel is gebaseerd op de uitgevoerde werkzaamheden in cyclus 2.

Voor de onderwerpen Audit, privacyfunctionarissen en Control is geen onderzoeksopdracht gegeven. De onderwerpen zijn desondanks wel onderzocht in opzet en bestaan omdat deze onderwerpen uit het oogpunt van Concernaudit (CA) wel auditwaardig waren. Het oordeel is gebaseerd op de uitgevoerde werkzaamheden in cyclus 3.

CA heeft eveneens geen opdracht gekregen voor de onderwerpen FG en ITGC. Deze onderwerpen zijn tóch onderzocht ondanks het feit dat deze onderwerpen niet zijn verplicht in de Wpg 2018. Dit is gedaan omdat de FG in de Wpg wel wordt genoemd. Het onderwerp ITGC is onderzocht omdat de status van belang is voor de mate van IT-beheersing.

2.3.2. Onderzoeksmethoden

We hebben onze opdracht uitgevoerd overeenkomstig de NOREA Richtlijn 3000, “Richtlijn Assurance-opdrachten door IT-auditors”. Dit vereist dat wij voldoen aan de voor ons geldende ethische voorschriften en onze werkzaamheden zodanig plannen en uitvoeren dat een redelijke mate van zekerheid wordt verkregen over de vraag of de interne beheersingsmaatregelen, in alle van materieel belang zijnde aspecten, op afdoende wijze zijn opgezet en bestaan.

Voor de onderwerpen waarvan de opzet is beoordeeld (zie figuur 1) betekent dit dat (beleids) documenten zijn bestudeerd en afgezet tegen het normenkader ontleend aan de wet. Daarbij is een oordeel gegeven of de organisatie al dan niet in voldoende mate voldoet aan de wet.

Voor het toetsen van bestaan zijn interviews gehouden. Omdat Rechten van de Betrokkene wordt uitgevoerd in de eenheden, is door alle eenheden te bezoeken het bestaan vast gesteld.

Daarnaast zijn er op centraal niveau interviews gehouden met sleutelfiguren binnen de organisatie zoals de Functionaris Gegevensbescherming, de Gegevensautoriteit, de projectleider implementatie Wpg en de voorzitter van de stuurgroep Verbeterprogramma Wpg en IB.

2.3.3. Normenkader

Generiek
Per 1 januari 2019 is de nieuwe Wpg van kracht geworden. Omdat dit onderzoek betrekking heeft op 2018 wordt het normenkader gevormd door de óude Wpg zoals die tot 1 januari 2019 gold.

Specifiek
Aanvullend is een normenkader gehanteerd dat is gebaseerd op de centraal ontwikkelde handleidingen voor Autoriseren, Verstrekken, Protocolleren, Rechten van de Betrokkene en Privacy en Security by Design. De reden hiervoor is dat in de handleidingen meer duiding wordt gegeven aan het generieke normenkader, zodat het bestaan kan worden onderzocht/vastgesteld.

Criterium
Alle Wpg onderwerpen bestaan uit één of meerdere subonderwerpen. Dat betekent dat een eindoordeel voor een onderwerp een weergave is van deze subonderwerpen. Waar nodig is dit in de tekst uitgelegd. Wanneer één eenheid niet voldoet aan de Wpg, dan voldoet de Politie als geheel niet volledig aan de Wpg. Toelichting: als één eenheid tekortkomingen heeft, dan kan dit aanleiding zijn om het oordeel negatief voor de politie als geheel uit te laten vallen.

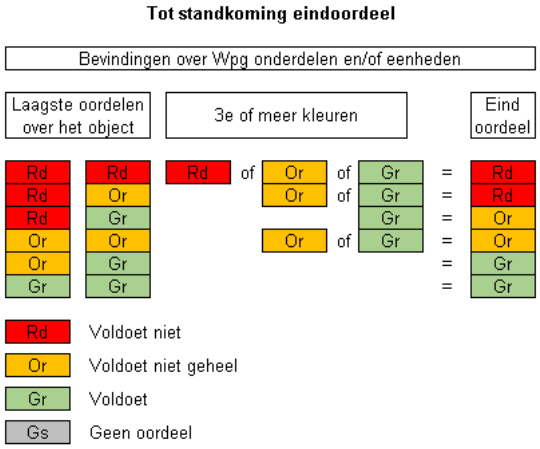
Beoordeling
De kleuren in de tabellen betekenen het volgende. De kleur rood betekent: voldoet niet aan de bepalingen uit de Wpg. Oranje staat voor: voldoet niet geheel. Groen wil zeggen dat het geheel voldoet aan de bepalingen uit de Wpg zoals die gold tot en met 31 december 2018. De kleur grijs is gehanteerd wanneer een onderwerp uit de Wpg leidt tot ‘geen oordeel’. De keus ‘geen oordeel’ komt voor als CA niet kon steunen op de uitkomst in cyclus 2 (2011-2014) omdat destijds het betreffende onderwerp niet is onderzocht.

In de onderstaande tabel is zichtbaar wanneer een bevinding over een Wpg onderwerp of een eenheid tot het oordeel rood, oranje of groen leidt. Om het gebruik van de tabel uit te leggen worden enkele regels toegelicht.

Eerste regel; Wanneer de *laagste* waarden, in dit geval tweemaal rood is gescoord, dan is het eind oordeel rood. Het maakt voor het eindoordeel niet uit of eventuele resterende kleuren positiever scoren, bijvoorbeeld 5 keer groen.

Derde regel: Wanneer de laagste twee kleuren een rood en een groen betreffen, dan is het eindoordeel oranje, ook al zijn er nog drie of meer groene kleuren aanwezig.

Vijfde regel: De laagste waarde is oranje en groen. Er zijn dus geen andere waardes van oranje. Anders waren er twee oranje waardes aanwezig en was regel 4 van toepassing. Er zijn dus voor de rest alleen groene waardes gescoord. Eén oranje en x groene waardes maakt dat het eindoordeel groen is.



Figuur 2 Beoordelingscriteria

2.3.4. Three Lines of Defense

Bij de politie is het model Three Lines of Defense geadopteerd. Het model ziet er als volgt uit. Eerste lijnsmanagement is de besturingslaag die verantwoordelijk is voor de uitvoering van effectieve en efficiënte bedrijfsprocessen, zowel op strategisch, tactisch als op operationeel niveau. Daarnaast is het eerste lijnsmanagement verantwoordelijk voor het ontwerpen, inrichten en (eventueel) toepassen van beheersingsmaatregelen bij gebeurtenissen die deze bedrijfsprocessen dreigen te verstoren. Doel hiervan is borgen dat organisatiedoelen worden bereikt.
De tweede lijn bestaat uit ‘Control & Riskmanagement’ en onder meer de privacyfunctionarissen. Deze tweede lijn ondersteunt de eerste lijn. De derde lijn is de interne auditfunctie die wordt uitgeoefend door Concernaudit. De Functionaris Gegevensbescherming (FG) geeft aan dat ook hij is gepositioneerd als derdelijnsfunctie. Een kleine toevoeging op het model zijn de volgende verdedigingslijnen. De vierde lijn is de externe auditfunctie die voor deze audit door de Auditdienst Rijk (ADR) is ingevuld. De vijfde lijn is de externe toezichthouder in de vorm van de Autoriteit Persoonsgegevens (AP). Iedere lijn steunt op de voorliggende lijn.

In dit onderzoek hebben we getoetst of de lijnmanagers hun eigen kwaliteit vaststellen en waar nodig bijsturen.

3. Wpg-audits

Dit hoofdstuk beschrijft de auditvoorschriften vanuit de Wpg en voor de herinnering de resultaten uit eerder uitgevoerde audits in cyclus 2.

3.1. Audits op grond van de Wpg

De interne audit moet minimaal één keer per jaar worden uitgevoerd, waarbij een deel van de organisatie wordt onderzocht of waarbij een deel van de Wpg in de gehele organisatie wordt onderzocht. Na 4 jaar moet de gehele organisatie op de gehele Wpg zijn onderzocht. Het voor u liggende rapport is de interne afronding van de derde 4-jaarlijkse cyclus.

De *externe* ofwel Privacy audit moet eens in de vier jaar worden verricht aan het einde van de cyclus. De Politie heeft hiervoor de Auditdienst Rijk (ADR) als externe auditor gevraagd een oordeel te geven over de mate waarin de Politie voldoet aan naleving van de bepalingen uit de Wpg.

Voor de herinnering volgt hieronder hoe het oordeel van de ADR over de tweede cyclus over de jaren 2011 tot en met 2014 luidde (citaat, zie [i]):

> …'Op grond van onze werkzaamheden concluderen wij dat het stelsel van maatregelen en procedures gericht op de bescherming van de politiegegevens, betrekking hebbende op de in de Wpg genoemde artikelen, naar de stand van ultimo december 2014, in opzet, bestaan en werking niet of niet geheel heeft voldaan aan de vereisten zoals genoemd in de Wpg.'…

Het eind 2017 en begin 2018 uitgevoerde jaarlijkse vooronderzoek Hercontrole Wpg[iii] dat door CA is uitgevoerd heeft geleid tot de volgende bevindingen:

De eerste vraag was: "Welke tijdens de privacy audit cyclus 2 geconstateerde gebreken op het gebied van de '*opzet*' conform de Wpg-bepalingen zijn per 1 maart 2017 verholpen door het Landelijk Verbeter Programma (LVP)?"

> Op basis van het verbeterrapport van het LVP en het gespreksverslag met de voorzitter LVP hebben wij vastgesteld dat een jaar na de start van het verbeterprogramma van geen enkel onderwerp alle acties zijn afgerond. Het gevolg hiervan is dat op het gebied van de 'opzet' geen gebreken zijn verholpen.
>
> Ten opzichte van de resultaten van de 2e auditcyclus zijn per 1 maart 2017 in 'opzet' alleen verbeteringen zichtbaar op het onderdeel 'Rechten van de Betrokkene'. De beleidsproducten hiervan waren tijdens Auditcyclus 2 reeds als 'voldoende' bevonden. In 2016 zijn deze beleidsproducten in samenspraak met de eenheden verbeterd en door de voorzitter van de stuurgroep LVP (thans stuurgroep Wpg en IB) opnieuw vastgesteld.

De tweede vraag was: "Welke tijdens de privacy audit cyclus 2 geconstateerde gebreken op het gebied van het '*bestaan*' conform de Wpg-bepalingen zijn per 1 maart 2017 verholpen door de eenheden?"

> Op het gebied van het 'bestaan' is van 5 eenheden vernomen dat zij van mening zijn dat het 'bestaan' van 'Rechten van de Betrokkene' gereed is voor hercontrole.

Voor de derde cyclus, die loopt van 1 januari 2015 t/m 31 december 2018, is het voornemen van de ADR het oordeel in het derde kwartaal van 2019 vast te stellen. De ADR steunt hierbij op de door de Politie aangeleverde jaarlijkse rapporten van de derde cyclus. Dit is conform afspraak en bovendien efficiënt omdat de jaarlijkse interne onderzoeken zodanig zijn uitgevoerd dat de externe auditor hierop maximaal kan steunen.

4. Bevindingen

De centrale onderzoeksvraag van deze audit is:

In welke mate voldoet de Politie in opzet en bestaan aan de bepalingen uit de Wet politiegegevens?

Deze vraag wordt beantwoord aan de hand van de onderwerpen uit de Wpg. In de paragrafen hierna worden deze onderwerpen toegelicht:

1. Autoriseren (art.6 Wpg);
2. Verstrekken (art.16-24 Wpg);
3. Protocolleren (art.32 Wpg);
4. Bewaartermijnen (art.14 Wpg);
5. Rechten van de Betrokkene (art.25-31 Wpg);
6. Kwaliteit van gegevens (art.3-4 Wpg);
7. Gevoelige gegevens (art.5 Wpg);
8. Geautomatiseerd vergelijken en in combinatie verwerken (art. 11 Wpg);
9. Ter beschikking stellen (art.15 Wpg);
10. Audits (art.33 Wpg);
11. Privacyfunctionaris (art.34 Wpg);
12. Beheersing (dit onderwerp is toegevoegd om de governance vast te kunnen stellen).

Aanvullende nog niet verplichte onderwerpen:

13. Functionaris Gegevensbescherming;
14. Privacy en Security by Design;
15. IT-technische zaken.

4.1. Autoriseren (artikel 6 Wpg 2018)

Wpg art.	*Het Autoriseren is in lijn met de Wpg (art.6)*	*Opzet*	*Bestaan*
	Autorisaties aanvragen en wijzigen (proces)	Gr	Gr
	Autorisaties intrekken (proces)	Or	Or
	Inrichting van het autorisatie systeem (kader)	Gr	Gr
	Controle en toezicht op het proces en het systeem	Or	Rd
	Ingerichte autorisaties in IT systemen	Gs	Gs
6	**Autoriseren**	Or	Rd

score is cyclus 3 (2015-2018)

Rd	Voldoet niet
Or	Voldoet niet geheel
Gr	Voldoet
Gs	Geen oordeel

Figuur 3 Te onderzoeken onderwerpen

Op basis van de verrichte werkzaamheden komen wij tot het volgende oordeel:

De in de Wpg genoemde verantwoordelijke onderhoudt in *opzet* een systeem van autorisaties dat niet geheel voldoet aan de vereisten van zorgvuldigheid en evenredigheid. Voor het bestaan geldt dat de-autoriseren van oude autorisaties niet voldoet.

Opzet
Er bestaat politiebreed beleid voor autorisaties. De uitgangspunten van het autorisatiebeleid bestaan uit richtinggevende principes. De-autoriseren is geen onderdeel van het landelijk autorisatie model (LAM).

Bestaan
De ATL en IAM zijn geïmplementeerd en ondersteunen de instroom, doorstroom en uitstroom van medewerkers. Het de-autoriseren van oude autorisaties is niet afgerond. Controle en toezicht op het proces en het systeem zijn nog niet ingericht.

De ATL en IAM zijn geïmplementeerd en ondersteunen de instroom, doorstroom en uitstroom van medewerkers. Punt van aandacht is dat nog niet alle autorisaties via IAM en ATL kunnen worden toegekend. De landelijk beheerde applicaties kunnen worden toegekend, Eigen Beheerde Omgevingen (EBO's) zijn hiervan uitgesloten. Extra toegekende autorisaties worden automatisch binnen maximaal één jaar ingetrokken.

Specifieke toegang, zoals de directe toegang tot databases die soms van toepassing is bij functioneel beheer, gaat via Privileged Access Management (PAM). Om dit te regelen is een project in juli 2019 gestart.

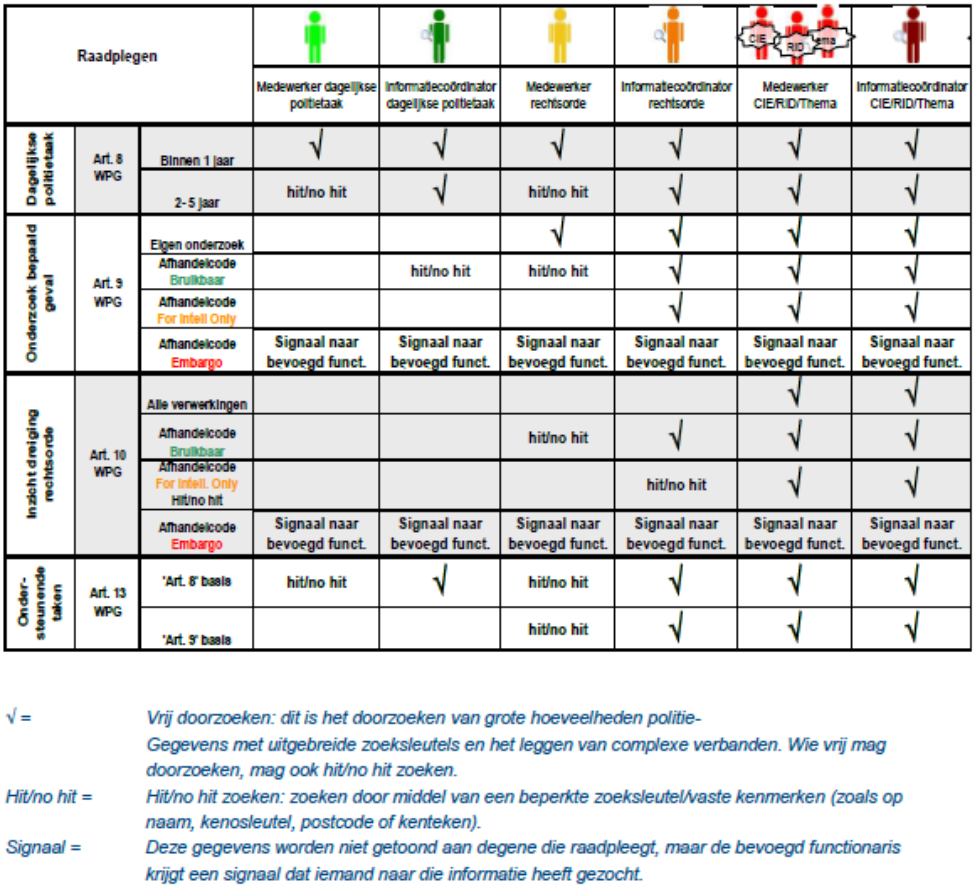
De-autoriseren was geen onderdeel van het landelijk autorisatie model (LAM). Oude autorisaties worden nu beoordeeld op validiteit maar dit heeft tot onvoldoende resultaat geleid. De nieuwe aanpak is om alle oude autorisaties die niet vernieuwd zijn batchgewijs uit te zetten. Deze activiteit is nog niet afgerond.

Via Datamart en BVI-IB zijn wel initiatieven in ontwikkeling om monitoring op een hoger volwassenheidsniveau te brengen.

Opzet
Om een beeld te krijgen van de *opzet* van autoriseren is documentatie bestudeerd. Dit heeft geleid tot de volgende bevindingen:

- Er bestaat politiebreed beleid voor autorisaties[iv]. De uitgangspunten van het autorisatiebeleid bestaan uit richtinggevende principes. Er is in voorzien dat een CISO is benoemd en dat deze toezicht houdt op het stelsel van autoriseren. De politie is verantwoordelijk voor iedereen aan wie zij een autorisatie geeft en voor iedere toegang tot informatie die zij in beheer heeft. Derden kunnen in opdracht van de politie gegevens verwerken.

  In de kern bevat de visie het volgende autorisatiemodel:



Figuur 4 Kern van het autorisatiemodel

- Beschreven is hoe medewerkers met behulp van Identity & Access Managementproces (IAM)[v] worden geautoriseerd. Hierdoor bestaat zicht op welke medewerker waarvoor is geautoriseerd. Het toekennen en intrekken van autorisaties gebeurt op basis van:
    - de instroom van nieuwe medewerkers;
    - de doorstroom van medewerkers;
    - de uitstroom van medewerkers;
    - het toekennen en intrekken van autorisaties voor politiemedewerkers die tijdelijk bij een andere afdeling of eenheid worden gedetacheerd. De leidinggevende van de afdeling waar de medewerker (tijdelijk) werkzaam is trekt de autorisaties in via ATL. Daarnaast kan een autorisatie automatisch worden ingetrokken als de einddatum van de TTW wordt overschreden.
- Er bestaat een beschrijving van het Autorisatie Tool Leidinggevend (ATL)[vi] dat als doel heeft leidinggevenden te ondersteunen bij het (de)autoriseren van eigen teamleden en medewerkers.
- Er is beschreven op welke wijze autorisatieprofielen via een gestructureerd proces worden beheerd[vii].
- Bevoegde functionarissen kunnen worden aangewezen. Hiervan is een Model Aanwijzingsbesluit bevoegd functionaris aangetroffen alsmede geformuleerde vakbekwaamheidseisen waaraan de bevoegd functionaris moet voldoen. Kanttekening hierbij is dat onduidelijk is in hoeverre deze documenten actueel zijn en door wie deze worden beheerd.

Bestaan

Op centraal niveau zijn profielen geanalyseerd en gekoppeld aan applicaties. Het resultaat hiervan is een functiegerichte applicatieboom. Het landelijk project (Landelijk project autoriseren/de-autoriseren) is gestart in 2016 om medewerkers autorisaties te geven die passen bij hun rol in de organisatie maar zonder de oude autorisaties in te trekken. Het was destijds niet duidelijk welke oude autorisaties nog actief werden gebruikt. Er is dus een situatie geweest dat medewerkers oude bestaande plus nieuwe autorisaties hadden. In de jaren 2015-2017 zijn alle profielen naar IAM

overgezet. Iedere medewerker is toen voorzien van minimaal één profiel. 2018 is het jaar van herstel, bijslijpen en schonen.

De huidige autorisatiemethodiek heeft de volgende kenmerken:

- door de ATL tool kan de leidinggevende voor zijn personeel de autorisaties van een aantal applicaties zelf regelen;
- leidinggevenden zijn verantwoordelijk voor de uitgave van extra autorisaties; dit zijn autorisaties die niet standaard bij de functie van de medewerker hoort;
- extra autorisaties zijn beperkt (maximaal 12 maanden) houdbaar;
- autorisaties van landelijke beheerde applicaties kunnen worden gemonitord;
- Alle profielen zijn centraal vastgesteld. Veranderen van een profiel kan alleen centraal worden gedaan en dan geldt zo'n aangepast profielen meteen landelijk.

Leidinggevenden hebben o.a. als taak toezicht uitoefenen op de uitgegeven autorisaties van aan hem gelieerde medewerkers. Verantwoordelijkheden van de leidinggevenden worden echter niet volledig ingevuld onder meer omdat eenvoudige rapportage mogelijkheden ontbreken. Monitoring staat nog in de kinderschoenen. Via Datamart en BVI-IB zijn wel initiatieven in ontwikkeling.

Aan leidinggevenden wordt via ATL twee vragen voorgelegd:

- Werken deze mensen voor u?
- Oefenen zij deze functie uit?

Deze twee vragen geven voldoende input voor de realisatie van een standaard koppeling met autorisatierechten. Het is ook mogelijk dat de leidinggevende de medewerker autoriseert voor één of meerdere applicaties buiten zijn profiel om. Deze extra autorisaties zijn bijvoorbeeld nodig voor het uitvoeren van activiteiten in het kader van TTW, vervangen zieke collega's e.d. Deze zijn altijd tijdelijk en gelden maximaal een jaar.

De-autoriseren

- De-autoriseren was geen onderdeel van het landelijk autorisatie model (LAM).
- Omdat 'de-autoriseren' niet was meegenomen is dit binnen IM opgepakt voor de nog beschikbare uren 2018. In eerste instantie is aan alle leidinggevenden gevraagd welke oude autorisaties van de medewerkers nog valide waren. Dit heeft tot onvoldoende resultaat geleid. De nieuwe aanpak is om alle oude autorisaties die niet vernieuwd zijn batchgewijs uit te zetten. Wanneer een medewerker zich meldt kan deze als extra autorisatie door de leidinggevende via de ATL worden uitgedeeld.

<u>Relevante ontwikkelingen</u>

- Deze zogenaamde PAM's (Privileged Access Management) zijn beheeraccounts en hebben verschillende rollen op serverniveau. Het streven is het aantal beheeraccounts te verminderen; van 50 naar 5 voor lokale beheerders. Want hoe meer accounts, hoe minder inzicht. Planning gereed juli 2019.
- Er wordt gewerkt aan een two factor authentication (via een wachtwoord en een token/SMS). Planning gereed mei 2019. RSA (asymmetrisch encryptiealgoritme) wordt uitgefaseerd en er wordt overgegaan naar een Digipas voor toegang tot het systeem. Dit zal over het hele netwerk worden uitgerold. Het wachtwoord is al in 2018 van 6 naar minimaal 12 karakters opgehoogd.
- Afgesproken is dat landelijk autorisaties worden gemonitord en er wordt geanalyseerd hoe teamchefs binnen hun team omgaan met extra autorisaties en of er een landelijke trend zichtbaar is. Bijvoorbeeld of een bepaalde autorisatie mist in een profiel die vooraf niet bedacht was of die nieuw is.

<u>Knelpunten</u>

Geïnterviewden hebben knelpunten bij de huidige manier van werken aangegeven.

- Geïnterviewden geven aan dat de kans bestaat dat de medewerker gegevens die worden gebruikt uit BO4 om te autoriseren onbetrouwbaar zijn. De impact is dat personen ten onrechte over autorisaties beschikken.
- De medewerkers kunnen nog beschikken over oude autorisaties omdat de-autoriseren onvoldoende betrouwbaar wordt uitgevoerd.
- In IAM zijn de functies van Functioneel Beheer (FB) niet opgenomen, omdat deze niet in een applicatie werken maar rechtstreeks in de database. Deze situatie is onwenselijk. De reden is dat deze werkwijze met zich meebrengt dat applicationcontrols worden omzeild. Bovendien is de herleidbaarheid van een verandering naar een specifieke user een probleem.
- Bij functiewisselingen van medewerkers binnen de organisatie worden de autorisaties afgehandeld. Er is echter kans op fouten als er geen (juiste) organisatorische eenheid aan een medewerker wordt gekoppeld.

Risico
Het risico bestaat dat politiemedewerkers onrechtmatig gegevens kunnen verwerken en delen omdat zij ten onrechte autorisaties hebben.

4.2. Verstrekken (artikel 16-24 Wpg 2018)

Wpg art.	Het Verstrekken is in lijn met de Wpg (art.16-24)	Opzet	Bestaan
16	Verstrekking aan opsporingsambtenaren en gezagsdragers	Gr	Gs
17-24	Verstrekking aan inlichtingendiensten en buitenlandse opsporingsinstanties	Gr	Gs
18	Verstrekking aan derden structureel	Gr	Gs
19	Verstrekking aan derden incidenteel	Gr	Gs
20	Verstrekking aan derden structureel voor samenwerkingsverbanden	Gr	Gs
22	Verstrekking voor wetenschappelijk onderzoek en statistiek	Gr	Gs
16-24	**Verstrekken (totaal oordeel)**	Gr	Gs

score is cyclus 3 (2015-2018)

Rd	Voldoet niet
Or	Voldoet niet geheel
Gr	Voldoet
Gs	Geen oordeel

Figuur 5 Oordeel Verstrekken

Op basis van de verrichte werkzaamheden komen wij tot het volgende oordeel:

De in de Wpg genoemde verantwoordelijke onderhoudt in *opzet* een systeem van Verstrekken dat voldoet aan de vereisten van zorgvuldigheid en evenredigheid.

Opzet
De verstrekkingenwijzer beleefde eind 2018 de digitale status en is voor iedere politiemedewerker toegankelijk.

Bestaan
De opdrachtgever heeft aangegeven dat op dit punt geen verbeteractiviteiten zijn afgerond.

Opzet
In de vorige audit cyclus 2 is de opzet als voldoende beoordeeld, daarom is besloten met de externe auditor de opzet opnieuw te bepalen. De opzet is opnieuw beoordeeld en omdat deze niet gewijzigd is voldoet de Politie opnieuw aan de wet. De verstrekkingenwijzer beleefde eind 2018 de digitale status en is daarmee als handleiding voor iedere politiemedewerker toegankelijk.

Bestaan
De opdrachtgever heeft aangegeven dat op dit punt geen verbeteractiviteiten zijn afgerond.

Risico
Het risico bestaat dat medewerkers onrechtmatig gegevens verstrekken omdat zij teveel informatie aan een partij verstrekken of informatie aan een verkeerde partij verstrekken waardoor de kans op bijvoorbeeld datalekken aanwezig is.

4.3. Protocolleren (artikel 32 Wpg 2018)

Wpg art.	De Protocolplicht is in lijn met de Wpg (art.16-24)	Opzet	Bestaan
32,1A	Vastleggen doel verwerkingen, (art 9 lid 2)	Gr	Gs
32,1B	Vastleggen van een verwerking als bedoeld in artikel 13 lid 4 verwerking	Gr	Gs
32,1C	Protocolleren van de toekenning van autorisaties	Gr	Gs
32,1D	Protocolleren van geautomatiseerde vergelijking/combinatie verwerken	Gr	Gs
32,1E	Protocolleren hernieuwde verwerking	Gr	Gs
32,1F	Protocolleren van verstrekkingen	Gr	Gs
32,1G	Protocolleren onrechtmatige verwerkingen	Gr	Gs
32,1H	Protocolleren van geautomatiseerde vergelijkingen van politiegegevens met a	Gr	Gs
32	**Protocolplicht (totaal oordeel)**	Gr	Gs

score is cyclus 3 (2015-2018)

Rd Voldoet niet
Or Voldoet niet geheel
Gr Voldoet
Gs Geen oordeel

Figuur 6 Oordeel Protocolleren

Op basis van de verrichte werkzaamheden komen wij tot het volgende oordeel:

De in de Wpg genoemde verantwoordelijke onderhoudt in *opzet* een systeem van Protocolleren dat voldoet aan de vereisten van zorgvuldigheid en evenredigheid.

Opzet
Het geformuleerde beleid en de strategie is actueel.

Bestaan
De opdrachtgever heeft aangegeven dat op dit punt geen verbeteractiviteiten zijn afgerond.

Opzet
Er is in de vorige cyclus 2 een landelijke procedure opgesteld. Destijds is deze opzet als voldoende beoordeeld, daarom is besloten in overleg met de externe auditor de opzet opnieuw te bepalen. De opzet is opnieuw beoordeeld en omdat deze niet gewijzigd was voldoet de Politie opnieuw aan de wet.

Het geformuleerde beleid en strategie is nog steeds actueel volgens de opdrachtgever. Hierdoor voldoet de politie aan de wet. Er is op intranet een Toolkit waarmee de verschillende subartikelen van art 32 Wpg nader worden uitgelegd.

Bestaan
De opdrachtgever heeft aangegeven dat op dit punt geen verbeteractiviteiten zijn afgerond.

Risico
Het risico bestaat dat de politie niet volledig aan de protocolplicht voldoet omdat niet zeker is of in alle processen die worden genoemd in artikel 32 Wpg wordt geprotocolleerd.

4.4. Bewaartermijnen (artikel 14 Wpg 2018)

Wpg art.	De Bewaartermijnen zijn in lijn met de Wpg (art.8-14)	Opzet	Bestaan
8	Verwerken politiegegevens dagelijkse politietaak (art.8)	Rd	Gs
9	Verwerken van politiegegevens t.b.v een onderzoek in een bepaald geval (art.9)	Rd	Gs
10	Verwerken van politiegegevens ivm inzicht van de betrokkenheid van personen bij ernstige bedreiging rechtsorde.(art.10)	Rd	Gs
12	Verwerken politiegegevens ivm informantenbeheer (art.12)	Rd	Gs
13	Verwerken politiegegevens tbv ondersteunende taken (art.13)	Rd	Gs
14	Verwerken politiegegevens tbv klachten, verantwoording, RvB en hernieuwde verwerking (art.14)	Rd	Gs
8-14	**Bewaartermijnen (totaal oordeel)**	Rd	Gs

score is conform audit cyclus 2 (2011-2015)

Rd Voldoet niet
Or Voldoet niet geheel
Gr Voldoet
Gs Geen oordeel

Figuur 7 Oordeel Bewaartermijnen

Voor het onderwerp bewaartermijnen blijft het oordeel uit de tweede cyclus staan.

Opzet
De opdrachtgever heeft aangegeven dat in de opzet verbeteractiviteiten niet of niet volledig zijn afgerond.

Bestaan
De opdrachtgever heeft aangegeven dat voor bestaan verbeteractiviteiten niet of niet volledig zijn afgerond.

Opzet
In de cyclus 3 (2018) zijn opzet en bestaan opnieuw onderzocht. De opdrachtgever heeft aangegeven dat verbeteracties niet of niet volledig zijn afgerond. Daarom worden de resultaten van de vorige cyclus aangehouden. De consequentie hiervan is dat de opzet rood blijft.

Bestaan
Bestaan is grijs gemarkeerd omdat de opzet ontbreekt. De politie heeft de afgelopen jaren wel Privacy by Design in gang gezet waardoor nieuw ontwikkelde applicaties aan de voorzijde worden getoetst op het voldoen aan de Wpg.

Risico
Het risico bestaat dat gegevens in systemen niet tijdig worden verwijderd of vernietigd omdat met name oude systemen niet uit gefaseerd worden of omdat het teveel kosten met zich meebrengt om oude systemen aan te passen aan de Wpg-eisen.

Aanvulling
Wij hebben gezien dat in het document Uitvoerings-kader voor de omgang met gegevens, Versie 2.0, datum 23 april 2018 de opzet van bewaren en vernietigen inmiddels is beschreven.

4.5. Rechten van de Betrokkene (artikel 25 – 31 Wpg 2018)

Wpg art.	Rechten van de Betrokkene is in lijn met de Wpg (art.25-31)	Opzet	Bestaan
25-27	Verzoek tot kennisneming oordeel	Gr	Gr
28	Verzoek tot wijziging oordeel	Gr	Gr
31.1	Vergoeding kosten (niet van toepassing)	Gr	Gr
25-31	**Rechten van de Betrokkene (totaal oordeel)**	Gr	Gr

Rd	Voldoet niet
Or	Voldoet niet geheel
Gr	Voldoet
Gs	Geen Oordeel

Figuur 8 Rechten van de Betrokkene

In deze paragraaf is een samenvatting opgenomen van het door CA parallel uitgebrachte rapport Rechten van de Betrokkene 2018. De reden hiervoor is dat dit onderzoeksobject dermate omvangrijk is dat dit onderdeel een eigen rapport verdient. Omwille van het totaaloverzicht van de status van de gehele Wpg is in dit Wpg-brede rapport volstaan met de samenvatting. Voor de duidelijkheid, de in het separate rapport Rechten van de Betrokkene opgenomen risico's verdienen uiteraard ook de aandacht van het management.

De in de Wpg genoemde verantwoordelijke onderhoudt in *opzet en bestaan* een systeem om de Rechten van de Betrokkene te borgen dat voldoet aan de vereisten van zorgvuldigheid en evenredigheid.

Opzet
Voor de o*pzet* is vastgesteld dat de Handleiding 'Rechten van de Betrokkene' op een adequate wijze invulling geeft aan de bepalingen zoals die die zijn opgenomen in de Wpg.

Bestaan
Voor het b*estaan* hebben wij vastgesteld dat de Privacydesks in de eenheden invulling geven aan de bepalingen van de Wpg voor zover deze betrekking hebben op Rechten van de Betrokkene.

Opzet
Voor het bepalen van de opzet hebben wij documenten ontvangen van de GA, zoals het handboek Rechten van de Betrokkene en de door de eenheden gebruikte landelijk centraal vastgestelde brieven tbv de communicatie met de inzage verzoekers.

Bestaan
Voor het bestaan van Rechten van de Betrokkene heeft onderzoek plaatsgevonden in de eenheden. Alle eenheden hebben een Privacyloket. Dit loket heet soms Privacydesk en de inrichting en ophanging

verschilt per eenheid. Ook de werkzaamheden verschillen per eenheid, afhankelijk welke van de 3 opties, minimaal, maximaal of logisch de eenheid heeft gekozen. De keuze is afhankelijk van de werkzaamheden die dit loket verricht. De loketten zijn gevuld met medewerkers op tijdelijke basis waardoor de continuïteit niet gewaarborgd is. Ondanks deze bevindingen voldoet de politie hiermee wel aan de wet, op het onderdeel Rechten van de Betrokkene.

Risico
Het risico bestaat dat de continuïteit van de afhandeling van inzageverzoeken in gevaar komt omdat de Privacydesks grotendeels zijn bemenst met tijdelijke krachten.

4.6. Kwaliteitsaspecten (artikel 3-4 Wpg 2018)

Wpg art.	Kwaliteit politiegegevens is in lijn met Wpg (art.3-4)	Opzet	Bestaan
3-4	**Kwaliteitsaspecten van politiegegevens**	Rd	Gs

score is conform audit cyclus 2 (2011-2015)

Rd	Voldoet niet
Or	Voldoet niet geheel
Gr	Voldoet
Gs	Geen oordeel

Figuur 9 Kwaliteit van Gegevens

Voor het onderwerp Kwaliteitsaspecten blijft het oordeel uit de tweede cyclus staan.

Opzet
De opdrachtgever heeft aangegeven dat in opzet verbeteractiviteiten niet of niet volledig zijn afgerond.

Bestaan
De opdrachtgever heeft aangegeven dat voor bestaan verbeteractiviteiten niet vof niet volledig zijn afgerond.

Opzet
In de cyclus 3 (2018) is opzet opnieuw onderzocht. De opdrachtgever heeft aangegeven dat verbeteracties niet of niet volledig zijn afgerond. Daarom worden de resultaten van de vorige cyclus aangehouden. De consequentie hiervan is dat de opzet rood blijft.

Bestaan
Bestaan is grijs gemarkeerd omdat de opzet ontbreekt. Voor dit onderwerp is door de opdrachtgever aangegeven dat hier nog onvoldoende voortgang op gemaakt is om aan een audit te onderwerpen.

Risico
Het risico bestaat dat onbetrouwbare gegevens in de operatien worden gebruikt omdat de kwaliteit van de gegevens niet vast staat.

Aanvulling
Door de GA is aangegeven dat in opzet in de afgelopen periode de volgende documenten zijn gemaakt om de kwaliteit van politiegegevens te verhogen:

- Uitvoeringskader PSbD v2.0

- Eindrapport 0-metingen highrisk applicaties
- Specifieke rapporten mbt 0-metingen PSbD
- Verantwoordelijkheid van gegevens
- Toepassingsprofiel metagegevens politie
- Handreiking archivering email (bewaren en vernietigen)
- Beleidskader logging
- Factsheet pseudonimisering, anonimisering (privacy by default)
- Kaders en richtlijnen voor omgang met politiegegevens
- Praktijkhandboek Wet politiegegevens.
- Verstrekkingenwijzer.
- Werkinstructie poortwachter Wpg.

Er zijn hierbij ook nog punten in ontwikkeling denk hierbij aan:

- Pilot traject bewustwording belang van kwaliteit politiegegevens
- Concrete verbeteringen in kwaliteit van gegevens worden opgepakt, uitgewerkt en doorgevoerd: onder meer kwaliteit van strafrechtsketennummer en kwaliteit van PV.

4.7. Gevoelige gegevens (artikel 7 Wpg 2018)

Wpg art.	Gebruik van gevoelige gegevens is in lijn met Wpg (art.5)	Opzet	Bestaan
5	**Gevoelige gegevens**	Rd	Gs

score is conform audit cyclus 2 (2011-2015)

Rd	Voldoet niet
Or	Voldoet niet geheel
Gr	Voldoet
Gs	Geen oordeel

Figuur 10 Gevoelige Gegevens

Voor het onderwerp Gebruik van gevoelige gegevens blijft het oordeel uit de tweede cyclus staan.

Opzet
De opdrachtgever heeft aangegeven dat in opzet verbeteractiviteiten niet of niet volledig zijn afgerond.

Bestaan
De opdrachtgever heeft aangegeven dat voor bestaan verbeteractiviteiten niet of niet volledig zijn afgerond.

Opzet
In de cyclus 3 (2018) is de opzet opnieuw onderzocht. De opdrachtgever heeft aangegeven dat verbeteracties niet of niet volledig zijn afgerond. Daarom worden de resultaten van cyclus 2 aangehouden. De consequentie hiervan is dat de opzet rood blijft.

Bestaan
Bestaan is grijs gemarkeerd omdat de opzet ontbreekt. Voor dit onderwerp is aangegeven door de opdrachtgever dat daar nog onvoldoende voortgang op gemaakt is om aan een audit te onderwerpen.

Risico
Het risico bestaat dat de Politie onzorgvuldig omgaat met gevoelige gegevens omdat controlemogelijkheden niet ingericht zijn.

4.8. Geautomatiseerd vergelijken en in combinatie zoeken

Wpg art.	Geautomatiseerd vergelijken en in combinatie zoeken is in lijn met Wpg (art.11)	Opzet	Bestaan
11	Geautomatiseerd vergelijken en in combinatie zoeken	Rd	Gs

score is conform audit cyclus 2 (2011-2015)

Rd	Voldoet niet
Or	Voldoet niet geheel
Gr	Voldoet
Gs	Geen oordeel

Figuur 11 Geautomatiseerd vergelijken en in combinatie zoeken

Voor het onderwerp Geautomatiseerd vergelijken en in combinatie zoeken blijft het oordeel uit de tweede cyclus staan.

Opzet
De opdrachtgever heeft aangegeven dat in opzet verbeteractiviteiten niet of niet volledig zijn afgerond.

Bestaan
De opdrachtgever heeft aangegeven dat voor bestaan verbeteractiviteiten niet of niet volledig zijn afgerond.

Opzet
In de cyclus 3 (2018) is opzet en bestaan niet opnieuw onderzocht. Daarom worden de resultaten van de vorige cyclus aangehouden. De opdrachtgever heeft aangegeven dat verbeteracties niet of niet volledig zijn afgerond. De consequentie hiervan is dat de opzet rood blijft.

Bestaan
Voor dit onderwerp is aangegeven door de opdrachtgever dat nog onvoldoende voortgang is gemaakt om aan een audit te onderwerpen. Bestaan is grijs gemarkeerd omdat de opzet ontbreekt.

Risico
Het risico bestaat dat op basis van hun rol onbevoegde medewerkers gegevens verwerken waardoor de rechtsgrondslag van deze werkzaamheden betwist kan worden.

4.9. Ter beschikking stellen

Wpg art.	Ter beschikking stellen is in lijn met Wpg (art. 15)	Opzet	Bestaan
15	**Ter beschikking stellen**	Rd	Gs

score is conform audit cyclus 2 (2011-2015)

Rd	Voldoet niet
Or	Voldoet niet geheel
Gr	Voldoet
Gs	Geen oordeel

Figuur 12 Ter beschikking stellen

Voor het onderwerp Ter beschikking blijft het oordeel uit de tweede cyclus staan.

Opzet
De opdrachtgever heeft aangegeven dat in opzet verbeteractiviteiten niet of niet volledig zijn afgerond.

Bestaan
De opdrachtgever heeft aangegeven dat voor bestaan verbeteractiviteiten niet of niet volledig zijn afgerond.

Opzet
In de cyclus 3 (2018) is opzet en bestaan opnieuw onderzocht. De opdrachtgever heeft aangegeven dat verbeteracties niet of niet volledig zijn afgerond. De consequentie hiervan is dat de opzet rood blijft.

Bestaan
Bestaan is grijs gemarkeerd omdat de opzet ontbreekt. Voor dit onderwerp is door de opdrachtgever aangegeven dat nog onvoldoende voortgang is gemaakt om dit onderwerp aan een audit te onderwerpen.

Risico
Het risico bestaat dat informatie onrechtmatig aan derden binnen het politie-domein ter beschikking wordt gesteld door politiemedewerkers.

4.10. Audits

Wpg art.	Audit in lijn met Wpg (art. 33)	Opzet	Bestaan
33.1	Periodiek doen verrichten van privacy audits.	Or	Or
33.2	Privacy audits aangeboden aan het Cbp. (nu AP)	Gr	Gr
33.3	Uitvoeren hercontrole	Rd	Rd
33.4	Geheimhoudingsplicht	Gs	Gs
33.5	AMvB inhoud en wijze van uitvoering van de controles	Gs	Gs
33	**Audits (totaal oordeel)**	Rd	Rd

score is cyclus 3 (2015-2018)

Rd	Voldoet niet
Or	Voldoet niet geheel
Gr	Voldoet
Gs	Geen oordeel

Figuur 13 Oordeel audits

Op basis van de verrichte werkzaamheden komen wij tot het volgende oordeel:

De in de Wpg genoemde verantwoordelijke onderhoudt in o*pzet en bestaan* een systeem van Audits dat niet voldoet aan de vereisten van zorgvuldigheid en evenredigheid.

Opzet
De auditfunctie is voor wat betreft de eenheden niet meegenomen in de Blauwdruk. Voor Concernaudit geldt dat de auditfunctie in beperkte mate is meegenomen.

Bestaan
In de eenheden zijn geen eenheidsauditors aangesteld. CA kan hierdoor moeilijk in haar rol van de derdelijns auditfunctie komen omdat zij niet kan steunen op werkzaamheden die in het kader van de Wpg moeten zijn uitgevoerd.

Opzet
In de Wpg is opgenomen dat ieder jaar een interne audit moet plaatsvinden over een deel van de organisatie of over een deel van de wet zodanig dat na 4 jaar de hele organisatie op de hele wet is onderzocht.

Hoewel de kennis op het gebied van politieprocessen en Wpg in de eenheden voldoende aanwezig is ontbreekt het aan onderzoekscapaciteit in de vorm van FTE's. Oorzaak is dat in de eenheden de 2e Line of Defense niet is ingericht terwijl het aanbod van te verrichten Wpg-werk groeit. Belangrijke groeifactor hierbij is de toenemende hoeveelheid te onderzoeken objecten op het vlak van werking. Het gevolg van het ontbreken van de 2e Line of Defense in de eenheden is dat 1e lijnsmanagement niet wordt ondersteund met het geven van aanvullende zekerheid en advies op basis van onderzoek.

CA kan in haar derdelijns rol, waarbij de focus ligt op de aanwezigheid van adequate beheersingsmaatregelen, niet steunen op werkzaamheden verricht door de 2e Line of Defense. Dit belemmert adequate uitvoering van interne Wpg audits.

Bestaan
In deze periode is nauw samengewerkt met de externe auditor, de Auditdienst Rijk (ADR). Er is gezamenlijk opgetrokken om de eenheden zo min mogelijk te belasten met het Wpg-onderzoek.

Werkzaamheden die te maken met Three Lines of Defense - waarbij de focus ligt op de mate waarin de KL in control is - zijn in beperkte mate uitgevoerd.

Op concernniveau is de afgelopen 4 jaar wel één maal een Vooronderzoek hercontrole Wpg uitgevoerd en is aan het einde van de derde cyclus onderhavige audit gehouden. Concernaudit heeft al in 2016 de externe auditor gecontracteerd om in 2018 de privacy audit uit te voeren. Binnen de afdeling is er nog weinig capaciteit gestoken in het volledig uitvoeren van de verplichte interne audit. Het feit dat de politieorganisatie nog onvoldoende op orde is, heeft hieraan bijgedragen. In 2018 is door Concernaudit een vierjaars kalender opgesteld voor de 4e periode (2019-2022). De start kan echter pas eind 2019 plaatsvinden omdat het verbeterprogramma tot eind 2019 doorloopt. In de planning zal rekening moeten worden gehouden met extra (eventueel in te huren) capaciteit.

Risico
Het risico is dat de Politie niet vooruitkomt omdat het eerste lijnsmanagement geen kennis kan nemen van bevindingen die aanleiding geven tot bijsturen.

4.11. Privacyfunctionaris

Wpg art.	Privacyfunctionarissen werken in lijn met Wpg (art. 34)	Opzet	Bestaan
34.1	Er zijn één of meerdere PF(en) benoemt binnen de eenheid	Gr	Gr
34.1	De PF geeft advies over de Wpg aan de verantwoordelijke	Gr	Gr
34.2	De PF houdt een overzicht bij van de schriftelijke vastleggingen	Gr	Rd
34.3	De PF stelt jaarlijks een verslag op van bevindingen	Gr	Rd
34.4	De PF is door de verantwoordelijke aangemeld bij de AP	Gr	Or
34	**Privacy Functionaris (totaal oordeel)**	Gr	Rd

score is cyclus 3 (2015-2018)

Rd	Voldoet niet
Or	Voldoet niet geheel
Gr	Voldoet
Gs	Geen oordeel

Figuur 14 Privacyfunctionarissen

Op basis van de verrichte werkzaamheden komen wij tot het volgende oordeel:

De in de Wpg genoemde verantwoordelijke onderhoudt in *opzet* een systeem van toezicht met inzet van privacyfunctionarissen dat voldoet aan de vereisten van zorgvuldigheid en evenredigheid. Het bestaan van het systeem van toezicht voldoet niet aan de Wpg.

Opzet
In het inrichtingsplan zijn privacyfunctionarissen voorzien.

Bestaan
De in de Wpg genoemde verantwoordelijke heeft in iedere eenheid één of meerdere privacyfunctionarissen aangesteld. De rollen van de privacyfunctionarissen verschillen per eenheid. Een overzicht van vastlegging van gegevens wordt niet in alle eenheden bijgehouden evenals het maken en publiceren van een jaarverslag.

In alle eenheden zijn één of meerdere privacyfunctionarissen aangesteld. Nog niet in alle eenheden worden de privacyfunctionarissen ingezet om toezicht te houden en werkzaamheden uit te voeren die de

wet aan hen stelt. Het privacyplatform is een gremium waar naast informatiedeling landelijke onderwerpen worden gecoördineerd en standpunten worden uitgewisseld. Het is tevens de verbinding tussen de privacyfunctionarissen en de (staf) KL.

Opzet
In het inrichtingsplan zijn privacyfunctionarissen voorzien.

Bestaan
In alle eenheden zijn één of meerder privacyfunctionarissen aangesteld en aangemeld bij de AP. De rollen van de verschillende privacyfunctionarissen verschilt per eenheid. Zo is er een adviesrol en een toezichtrol. Deze twee rollen worden gezamenlijk door een privacyfunctionaris uitgevoerd of door verschillende functionarissen.

Niet in alle eenheden houden de privacyfunctionarissen een overzicht bij van de vastlegging van gegevens. O.a. art 9 onderzoeken moeten worden aangemeld. Ook maakt niet iedere privacyfunctionaris een jaarverslag dat wel zou moeten volgens de wet.

Risico
Het risico bestaat dat inbreuken op de Wpg niet worden opgemerkt door een functionaris omdat onvoldoende toezicht wordt gehouden.

4.12. Governance (beheersing)

Wpg art.	Het management is in control conform Wpg	Opzet	Bestaan	Oordeel opzet en bestaan op basis van bevindingen uit cyclus	
6	Autoriseren	Or	Rd		3 (2015-2018)
16-24	Verstrekken	Gr	Gs		3 (2015-2018)
32	Protocolleren	Gr	Gs		3 (2015-2018)
8-14	Bewaartermijnen	Rd	Gs	2 (2011-2014)	
25-31	Rechten van de Betrokkene	Gr	Gr		3 (2015-2018)
3-4	Kwaliteitsaspecten van politiegegevens	Rd	Gs	2 (2011-2014)	
5	Gevoelige gegevens	Rd	Gs	2 (2011-2014)	
11	Geautomatiseerd vergelijken en in combinatie zoeken	Rd	Gs	2 (2011-2014)	
15	Ter beschikking stellen	Rd	Gs	2 (2011-2014)	
33	Audits	Rd	Rd		3 (2015-2018)
34	Privacy Functionaris	Gr	Rd		3 (2015-2018)
----	Governance / beheersing	Or	Or		3 (2015-2018)

Wpg art.	Onderwerpen behorende tot de Wpg vanaf 1 januari 2019 alsmede randvoorwaarden behorende tot de Wpg	Opzet	Bestaan	Oordeel opzet en bestaan op basis van bevindingen uit cyclus	
36	Functionaris Gegevensbescherming	Gr	Gr		3 (2015-2018)
----	Implementatie PSbD	Gr	Gr		3 (2015-2018)
----	ITGC	Rd			3 (2015-2018)

Rd	Voldoet niet
Or	Voldoet niet geheel
Gr	Voldoet
Gs	Geen oordeel

Figuur 15 Governance

Opzet

Na de rapportage van 2015 is door de GA een Verbeterplan in samenwerking met de eenheden gemaakt. Het verbeterplan van de GA loopt nog tot eind 2019. Het plan is daarna de verbeterwerkzaamheden over te dragen aan de lijnorganisatie.

Het resultaat van de governance is uiteindelijk terug te zien in de mate waarin Wpg compliant wordt gewerkt. Er is de afgelopen tijd veel inspanning geleverd in de vorm van beleidsstukken en verbeterplannen gericht om gegevens betrouwbaar en in lijn met de Wpg vast te leggen en te beheersen. Aan de andere kant hebben wij gezien dat de executiekracht van de politie om hierin volwassener te worden beperkt is.

Bestaan

Binnen de Politie is een stuurgroep Wpg en IB opgericht en is er meer aandacht gekomen om centraal zaken te ontwikkelen. Hiervan zien we op een aantal Wpg-onderwerpen voortgang. Op een deel van de Wpg onderwerpen is er minder voortgang of zijn de ingezette acties niet geheel of gedeeltelijk afgerond.

De voorzitter van de stuurgroep Wpg en IB geeft aan dat de Wpg structureel in de organisatie belegd zou moeten worden en als integraal onderdeel zou moeten worden opgenomen bij Intelligence i.p.v. bij de CIO. De vraag is wel of er voldoende ruimte is om de Wpg onderdeel te laten worden van Intelligence. De Wpg hoort volgens de voorzitter uiteindelijk thuis bij de Operatie en niet bij de bedrijfsvoering.

In 4 jaar tijd is op een gering aantal onderwerpen vooruitgang geboekt. Eenheden geven aan op instructies van het concern te wachten. Ook hebben de eenheden aangegeven dat zij alleen op de speerpunten van het Verbeterprogramma Wpg en IB hebben geïnvesteerd en niet op de bevindingen uit het Wpg-rapport van 2015.

Voor veel onderdelen moeten wij ons beroepen op de score van de vorige periode. Documentatie waaruit blijkt dat activiteiten zijn afgerond, hebben wij niet aangetroffen. Van de 3 onderwerpen die we van de opdrachtgever hebben meegekregen zijn er 2 duidelijk verbeterd, te weten: Autoriseren en Rechten van de Betrokkene. PsBD is naar verluidt ook op orde maar is nog niet relevant in deze periode, pas vanaf 1 januari 2020. Van het onderwerp toezicht kunnen we stellen dat er op gebied van audit (te) weinig heeft plaatsgevonden. De privacyfunctionarissen en de Functionaris Gegevensbescherming zijn aangesteld waarbij de privacyfunctionarissen nog niet helemaal doen waarvoor ze in de wet worden genoemd. De FG richt zich meer op privacy-breed toezicht. Of beide functies zich settelen en tot wasdom komen binnen de organisatie kan pas in de volgende cyclus worden bekeken.

Risico

Het risico bestaat dat door onvoldoende toezicht, verantwoording en sturing op de Wpg door eerste lijnsmanagement, Wpg-compliant werken in onvoldoende mate bij de Politie wordt nageleefd.

5. Aanvullende onderwerpen

5.1. Functionaris Gegevensbescherming

Wpg art.	De Functionaris Gegevensbescherming werkt conform Wpg (art 36)	Opzet	Bestaan
	Aanwijzen Functionaris Gegevensbescherming	Gr	Gr
	Er is minimaal 1 FG	Gr	Gr
	De FG is aangewezen op grond deskundigheid	Gr	Gr
	De FG is bekend in de organisatie	Gr	Gr
	De FG heeft toegang tot personeelsgegevens	Gr	Gr
	De FG heeft toegang tot verwerkingsactiviteiten	Gr	Gr
	De FG informeert de verwerkingsverantwoordelijke	Gr	Gr
	De FG informeert de verwerker	Gr	Gr
	Toezien op de naleving	Gr	Gr
	Adviseren over de GEB	Gr	Gr
	Samenwerken met de toezichthouder	Gr	Gr
	Contactpunt zijn met de toezichthouder	Gr	Gr
	De FG houdt rekening met risico's o.h.g.v. Privacy	Gr	Gr
36	**Functionaris Gegevensbescherming**	Gr	Gr

score is cyclus 3 (2015-2018)

Rd	Voldoet niet
Or	Voldoet niet geheel
Gr	Voldoet
Gs	Geen oordeel

Figuur 16 Functionaris gegevensbescherming

Op basis van de verrichte werkzaamheden komen wij tot het volgende oordeel:

De in de Wpg genoemde verantwoordelijke onderhoudt in *opzet en bestaan* een systeem van toezicht met inzet van Functionaris gegevensbescherming dat voldoet aan de vereisten van zorgvuldigheid en evenredigheid.

Opzet
De komst van de AVG op 25 mei 2018 was voor de Politie de aanleiding een Functionaris voor Gegevensbescherming aan te stellen. Deze functionaris legt rechtstreeks verantwoordelijkheid af aan de verantwoordelijke (KC).

Bestaan
De in de Wpg genoemde verantwoordelijke heeft een Functionaris Gegevensbescherming aangesteld. Deze Functionaris Gegevensbescherming (art 34 Wpg) functioneert binnen een systeem van toezicht en advies omtrent naleving Wpg en AVG waarmee wordt voldaan aan de vereisten van zorgvuldigheid en evenredigheid.

Opzet
De functionaris voor de gegevensbescherming is niet nieuw en staat al sinds de eerste Wpg in 2008 in de wet. Het is geen *verplichting* volgens de wet maar een mogelijkheid. De functie was echter nooit door de Politie ingevuld. De komst van de AVG op 25 mei 2018, waardoor het onderwerp gegevensbescherming op de agenda kwam, was de aanleiding voor de Politie om een FG te benoemen.

Bestaan

Deze FG houdt toezicht op de privacy in het korps en brengt advies uit. De FG heeft daarbij 1 fte ondersteuning. In mei 2018 heeft de Politie een FG voor zowel de AVG en de Wpg aangesteld. Deze functionaris is tevens de FG voor de Politieacademie. De FG wordt ondersteund door een bedrijfsvoeringspecialist Veiligheid & Integriteit sinds augustus 2018. Per 1 januari 2019 krijgt de FG ondersteuning van een beleidsadviseur. De FG heeft een eigen budget onder meer om capaciteit in te huren. Belangrijke opdracht voor de FG als kwartiermaker is het maken van een onderbouwd voorstel voor inrichting van de FG-functie. De FG heeft als voornaamste activiteit de beheersing van de interne weerbaarheid t.a.v. Privacy. Dat doet de FG samen met andere functionarissen en afdelingen zoals de CISO, CA, GA en de Privacydesk. Deze signalerende taak bestaat primair uit het doen van voorstellen voor te nemen beheersingsmaatregelen op basis van een risico inventarisatie (i.p.v. achteraf van individuele gevallen). De FG bewaakt bovendien de overlap en de verschillen tussen de Wpg en de AVG.

De FG signaleert dat voor de Wpg een portefeuillehouder ontbreekt. Dit helpt de Politiechefs niet om in hun rol te komen die zij hebben m.b.t. de Wpg. Omdat een portefeuillehouder Wpg ontbreekt, bestaat er spanning tussen de verschillende stakeholders die zich bezig houden met de Wpg. Zoals het Verbeterprogramma en de Implementatiemanager, de stuurgroep Wpg en IB, e.d.

Overleg met de eenheden gebeurt op Politiechefs-niveau die zich laten ondersteunen door de privacyfunctionaris. Naar de mening van de FG is de Politiechef zelf verantwoordelijk voor de inrichting van monitoring op tweedelijns niveau. De FG geeft aan te acteren op het niveau van de Third line of Defense.

De FG heeft direct contact met de stuurgroep Wpg en IB. De stuurgroep neemt nu de impact van de *nieuwe* Wpg (geldig per 1-1-2019) bij de implementatie mee. De FG heeft daarnaast ook overleg met het privacyfunctionaris platform.

Risico

Het risico bestaat dat de FG in onvoldoende mate toezicht houdt door de grootte en complexiteit van de organisatie.

5.2. Privacy en Security by Design (artikel 4a nieuwe Wpg 2019)

Wpg art.	Privacy and Security by Design is in lijn met de Wpg	Opzet	Bestaan
	Implementatie PSbD	Gr	Gr

score is cyclus 3 (2015-2018)

Rd	Voldoet niet
Or	Voldoet niet geheel
Gr	Voldoet
Gs	Geen oordeel

Figuur 17 Privacy and Security by Design

Opzet

In 2015 heeft de politie een eerste versie van Privacy by Design ontwikkeld. Privacy by Design betekent dat in het stadium van het maken van ontwerpkeuzes en tijdens het ontwikkelen van de informatievoorziening mechanismen worden ingebouwd voor de bescherming van persoonsgegevens. Met de komst van nieuwe privacywetgeving in 2018 is versie 1.0 Uitvoeringskader Privacy & Security by Design geactualiseerd tot versie 2.0[viii]. Er zijn nog steeds twaalf principes. Het principe ‘voldoen aan de

wet' is komen te vervallen; de inhoud is verdeeld over een aantal andere principes. Anderzijds is een nieuw principe geïntroduceerd: 'privacy by default'.

De basis voor het uitvoeringskader voor de omgang met gegevens is de informatiearchitectuur en de informatiebeveiligingsarchitectuur. Daarbij zijn tevens de kaders vanuit wet- en regelgeving en ketenstandaarden meegenomen. Er bestaan in totaal twaalf principes waarvan drie principes betrekking hebben op de besturing van het gegevensmanagement, zoals de PDCA-cyclus en het beleggen van verantwoordelijkheden. De overige zijn inrichtingsprincipes, bijvoorbeeld hoe moet de gegevenshuishouding ingericht worden. Elk principe bestaat uit een omschrijving en een ratio, inhoudelijke onderwerpen, met zoveel mogelijk concrete handvatten en praktijkvoorbeelden, en tot slot een aantal handreikingen. De handreikingen beschrijven voor verschillende doelgroepen verschillende activiteiten en aandachtspunten.

In april 2018 was het voornemen om de zesendertig highrisk applicaties aan een nulmeting te onderwerpen. Doel hiervan is vaststellen in hoeverre de applicaties voldoen aan Privacy en Security by Design (PSbD) kaders en richtlijnen. Uiteindelijk zijn alle high-risk applicaties in 2018 onderzocht.

Highrisk applicaties	
ANPR	Agora
BOSZ	Internet Aangifte
BVH	MEOS
BVI-Blueview 4.0	PSH-TM / Digibon (backoffice)
I-Base	Servicemodule
Live Journaal Politie	LSV
Mappen standaard	AVR
Raffinaderij	Hansken
SUMMIT	FCM
Amazone	HAVANK
DCS	SBV
Kantoorautomatisering	TRIS
Verificatiemodule	VROS
BVO-Bruto	Orion
BVID 2.0	Personenserver
BVI-BlueSpotMonitor	PSH-V
BVI-IB	PSH-VM
SMC	ZUIS

Figuur 18 High Risk applications

Bestaan

In februari 2019 is de laatste rapportage opgeleverd in een rapport '0-meting Privacy & Security by Design' voor de raffinaderij. Dit was de laatste van alle high-risk applicaties van de politie die zijn onderzocht. In de eindscore van het onderzoek is aangegeven dat het merendeel van de applicaties niet voldoet. Er is wel specifiek aandacht op het gebied van PSbD, maar dit is vooralsnog niet toereikend om te voldoen aan het politiebeleid. Het onderzoek wordt niet periodiek herhaald. Het oplossen van de geconstateerde gebreken wordt gemonitord. Daarnaast wordt PSbD in de bestaande lijnsturing gebracht. PSbD geldt ook voor oude applicaties. In nieuwe applicaties en bij nieuwe ontwikkelingen wordt PSbD meegenomen. Het is onduidelijk of PSbD ook wordt toegepast op oude applicaties, of dat oude applicaties worden uitgefaseerd.

Risico
Het risico bestaat dat er onvoldoende aandacht is om met name oude systemen nog te laten voldoen aan de wettelijke vereisten.

5.3. ITGC

De IT General Controls zijn in lijn met de Wpg	O, B, W
Change Management	Or
Incident Management	Or
Problem Management	Gr
Configuration Management	Or
Security Management	Or
Logical Access Management	Or
Infrastructure Management (Windows, SQL & Oracle)	Rd
Physical Access Management	Rd
Continuity Management	Rd
Operations Management (Back-up & restore)	Or
ITGC (totaal oordeel)	Rd

score is cyclus 3 (2015-2018)

Rd Voldoet niet
Or Voldoet niet geheel
Gr Voldoet
Gs Geen oordeel

Figuur 19 IT General Controls

In bovenstaande tabel is geen onderscheid gemaakt tussen opzet, bestaan en werking. Het onderzoek is uitgevoerd in het kader van de jaarrekening controle 2018. De afgesproken werkwijze die afgestemd is met de accountant was dat hier een totaal oordeel gegeven wordt, in plaats van een apart oordeel voor opzet, bestaan en werking. Elk onderdeel van de ITGC heeft een eigen normenkader en de onderzoeken zijn los van elkaar in 2018 uitgevoerd.

De in de Wpg genoemde verantwoordelijke onderhoudt in *opzet en bestaan en werking* een systeem van toezicht dat niet voldoet aan de vereisten van zorgvuldigheid en evenredigheid.

Opzet / bestaan / werking
De in de Wpg genoemde verantwoordelijke heeft een jaarlijkse audit laten uitvoeren naar de mate van IT-beheersing. Gebleken is dat alleen Problemmanagement voldoet aan de vereisten van zorgvuldigheid en evenredigheid.

Opzet
De Wpg schrijft de politie voor hoe moet worden omgegaan met gegevens die binnen de organisatie worden verwerkt om aan de organisatiedoelen te voldoen. De *manier* van verwerken laat de wet vrij maar in de praktijk is dit overwegend digitaal.

Om politiegegevens digitaal te kunnen verwerken maakt de Politie gebruik van infrastructuur, systemen en applicaties. Kritieke aspecten voor *betrouwbare* verwerking van gegevens zijn: vertrouwelijkheid, integriteit en beschikbaarheid.

Een belangrijke steunpilaar voor betrouwbare verwerking is de inrichting van IT General Controls (naast application controls). Vandaar dat onderzoek is verricht naar de dominante beheersingsmaatregelen binnen tien processen, te weten:

1. Change Management,
2. Incident Management,
3. Problem Management,
4. Configuration Management,
5. Security Management,
6. Logical Access Management,
7. Infrastructure Management (Windows, SQL & Oracle),
8. Physical Access Management,
9. Continuity Management,
10. Operations Management (Back-up & restore).

Er is ultimo 2018 geen politiebreed ITGC onderzoek beschikbaar dat kan dienen in het kader van het beoordelen van de ITGC van de Wpg. Hiervoor is gebruikt gemaakt als tweede optie, het ITGC onderzoek dat is uit gevoerd in het kader van de jaarrekening controle over 2018[ix]. Op basis van dit onderzoek zijn wij gekomen tot de volgende waarderingen.

De doelstelling van het onderzoek is het in opzet en bestaan toetsen van de beheersingsmaatregelen in 2018 om een beeld te geven van de mate waarin de beheersingsmaatregelen functioneren.

Status IT General Controls
De vraag is in welke mate de IT General Controls functioneren om de vertrouwelijkheid, integriteit en beschikbaarheid van gegevensverwerking te borgen?

Het antwoord op deze vraag luidt:

De mate waarin de IT General Controls functioneren, voldoet in redelijke mate aan de vereisten van zorgvuldigheid en evenredigheid. Continu blijft aandacht voor (verbetering van) de werking nodig omdat de ICT voortdurend verandert om de zich verder ontwikkelende organisatiedoelstellingen beter te ondersteunen.

Bij de politie zijn tien processen ingericht om de IT General Controls te beheersen. Bezien is in opzet en bestaan of de in figuur 16 genoemde processen zijn ingericht, de samenhang met andere processen duidelijk is, de procedures, rollen, functiescheidingen en ondersteunende systemen zijn beschrevenen periodiek worden geëvalueerd en door management geaccordeerd.

<u>Risico</u>
Het risico bestaat dat door beperkt onderzoek naar de status van ITGC er onvoldoende zicht is op de beheersingsmaatregelen die moeten borgen dat de gegevens overeenkomstig de Wpg worden verwerkt.

Proces	Belangrijkste geïdentificeerde aanvullende risico's
Change Management	Het risico bestaat dat RFC's niet efficiënt (op tijd, op maat, met de gevraagde kwaliteit) op worden geleverd omdat binnen afzonderlijke processen wordt gewerkt (change-, incident-, problemmanagement) waardoor overzicht ontbreekt op de koppelvlakken en samenhang van deze processen.
Incident Management	Er is geen aanvullend risico geïdentificeerd.

	Aangegeven is dat de procesmanager de processen evalueert en de procesgang, indien nodig, verbetert in samenspraak met de lijn.
Problem Management	Het risico bestaat dat niet alle issues worden opgelost omdat niet alle issues worden geregistreerd waardoor deze niet worden opgepakt om een oplossing te implementeren.
Configuration Management	Het risico bestaat dat wijzigingen onbeheerst worden doorgevoerd omdat de configuration management database (CMDB) niet volledig is waardoor geen zicht is op de componenten die tot een dienst behoren.
Security Management	Het risico bestaat dat de beveiliging niet voldoende breed en diepgaand wordt bewaakt en gecontroleerd omdat een geactualiseerd structureel proces met bijbehorende monitoringcyclus ontbreekt waardoor er grotere kans is op beveiligingsincidenten.
Logical Access Management	Het risico bestaat dat vertrouwelijkheid, integriteit en beschikbaarheid van systemen in gevaar komt omdat geautomatiseerde ondersteuning van IAM niet is ingericht voor beheeromgevingen.
Physical Access Management	Het risico bestaat dat medewerkers onjuiste/onvolledige en niet actuele rollen/verantwoordelijkheden hebben omdat niet inzichtelijk is wie waartoe toegang zou moeten hebben en of dit past bij de functie die deze persoon uitvoert.
Infrastructure Management	Er is geen aanvullend risico geïdentificeerd. Er is een uitvoeringsregeling Informatiebeveiliging en blauwdrukken zijn beschikbaar.
Continuity Management	Er is geen aanvullend risico geïdentificeerd. De inrichting van de crisisorganisatie wordt gelijk aan die van een SGBO, dus ook met een knoppenstructuur. Er zijn nu 4 teams die “piket” kunnen draaien, waarbij de wens is dat het zes teams worden.
Operations Management	Er is geen aanvullend risico geïdentificeerd. De backup methodiek is beschreven en geldt als standaard voor de hele organisatie

Figuur 20 Aanvullende risico’s

6. Ondertekening

Tot het geven van een nadere toelichting zijn wij graag bereid.

Den Haag, datum 29-01-2020

Projectleider 10.2.e 10.2.e

10.2.g

Senior Auditor
Concernaudit

7. Managementreactie

Het rapport Interne audit Wpg, derde cyclus 2015-2018 van 19 september jl. heb ik met belangstelling gelezen. Zoals gevraagd geef ik u hierbij mijn reactie.

Reactie op bevindingen
Bij het in gang zetten van de verbeteringen na de vorige audit is prioriteit gegeven aan de onderwerpen rechten van de betrokkene en autoriseren. Het is dan ook waardevol bevestigd te zien dat we ten aanzien van rechten van de betrokkene op de goede weg zijn en dat de inspanningen op dit onderwerp hebben geleid tot een positief resultaat.

Ook op het onderwerp autoriseren zijn flinke stappen gezet. Helaas komt dit nauwelijks tot uitdrukking in de bevindingen. Verschillende documenten beschrijven de wijze waarop het proces van het intrekken van autorisaties is ingericht en hoe het stelsel van monitoring en toezicht is vormgegeven. In opzet zou dit onderwerp naar mijn idee tot een positievere score moeten leiden. Deze bevindingen geven aanleiding daar nogmaals kritisch naar te kijken.

Overigens ben ik me er bewust van dat er ook op deze twee onderwerpen verbeterpunten zijn en dat deze processen continu aandacht nodig hebben, zeker ook om tot een positief resultaat ten aanzien van de werking te komen.

Daarnaast is door het Verbeterprogramma Wpg veel energie gestoken in de voorbereiding van nieuwe verplichtingen die per 1 januari 2019 zijn gaan gelden, zoals de eis van privacy by design. Hoewel dit strikt genomen niet binnen de auditperiode van 2015-2018 viel, is door Concernaudit toch naar opzet en bestaan gekeken, met een positief resultaat. Dat stemt mij optimistisch.

Relatie Verbeterprogramma Wpg en audit
Het voorliggende auditrapport beslaat de periode 2015-2018. Terugkijkend betekent dit dat eind 2015 het vorige auditrapport is ontvangen, dat in 2016 het verbeterprogramma is opgestart en dat gedurende 2017 en 2018 aan de verbetermaatregelen is gewerkt. Het auditproces dat heeft geleid tot uw rapportage is in 2017 gestart met de eerste hercontrole, dit betekent dat de bevindingen in uw auditrapport zijn gebaseerd op documentatie en interviews in 2017/2018.

Inmiddels is het januari 2020 en het Verbeterprogramma Wpg werkt zoals gepland naar een afronding toe. Gelet op het voorgaande kan het beeld ontstaan dat het Verbeterprogramma Wpg meent haar werkzaamheden te kunnen afronden terwijl de auditresultaten daar geen aanleiding toe geven. Echter, het Verbeterprogramma Wpg heeft ondertussen verschillende resultaten opgeleverd die ten minste wat betreft 'opzet' te beoordelen zijn en zal tot maart 2020 nog meer onderwerpen afronden. In aanloop naar de afronding zal vooral ook aandacht besteed worden aan de borging in de lijn en de inrichting van een systeem van monitoring en control. De audit kwam dus – in die zin – te vroeg om de resultaten van het Verbeterprogramma Wpg te toetsen.

Verbeterrapport
Aan de hand van deze interne auditrapportage zal overeenkomstig art. 4, lid 1 van de Regeling periodieke audit politiegegevens in april 2020 een verbeterrapport worden opgeleverd. Het betreft een verbeterrapport waarin de maatregelen worden beschreven die op dat moment getroffen zijn ter verbetering van de geconstateerde tekortkomingen. Aangezien een groot aantal onderdelen niet is onderzocht, zijn ten aanzien van die onderdelen ook geen tekortkomingen geconstateerd. Het verbeterrapport zal dan ook niet op alle onderwerpen ingaan.

Den Haag, datum: 30-01-2020

10.2.g

Dhr H.G. Geveke

Lid Korpsleiding

Refertes

i Privacy audit Wpg 2015 Politie; 29 oktober 2015; Kenmerk ADR 2015 1306; Auditdienst Rijk

ii Audit Wpg 2018 Rechten van de Betrokkene; Definitief versie 1.0; 19 september 2019; Concernaudit

iii Vooronderzoek Hercontrole Wpg; 1 maart 2018, 1.0 definitief; Concernaudit

[iv] Autorisatiebeleid politie 2016-2020; Auteur: project autorisatiemodel politie (team beleid en implementatie) Status: definitief; Versie 2.0; 21 april 2016

[v] Procesbeschrijving IAM: Autoriseren; Auteur: 10.2.e ; Status: Definitief; Versie 1.0; 26 september 2017

[vi] Korte beschrijving ATL Tool; Auteurs: 10.2.e , 10.2.e ; Status: Definitief Versie 1.6; 28/06/2018.

[vii] Procesbeschrijving autorisatieprofielen beheer; Auteur: 10.2.e Status: Definitief; Versie 1.0; 26 september 2017

[viii] Privacy & Security by Design, Uitvoerings-kader voor de omgang met gegevens; Definitief Versie 2.0; versiedatum 23 april 2018; Directie Informatievoorziening, Staf korpsleiding

[ix] Rapportage onderzoek CRC opzet , bestaan en werking over de periode 1 januari tot en met 31 december 2018. Versie 1.0