

Interne audit 2022 Wet Politiegegevens

1 januari 2022 tot en met 15 november 2022

Gemeente Nijmegen

Datum:	9 december 2022
Rapportnummer:	Wpg-intern-2022
Versie:	1.0
Status:	Definitief

Versiebeheer

Versie	Datum	Status	Naam
0.1	15 november 2022	Initiële versie	2-Control B.V.
0.9	24 november 2022	Concept	2-Control B.V.
1.0	9 december 2022	Definitief	2-Control B.V.

Inhoud

1	Algemeen	5
1.1	Achtergrond en doelstelling	5
1.2	Scope	5
1.3	Auditplanning	5
1.4	Auditor en aanpak	6
1.5	Verspreiding en gebruik	6
1.6	Conclusies	6
2	Normenkader	8
3	Bevindingen en aanbevelingen	14
3.1	Algemene bevindingen en aanbevelingen	14
3.2	Bevindingen domein Leerplicht	15
3.3	Bevindingen domein Toezicht en handhaving	16
3.4	Detailbevindingen en aanbevelingen (Wpg beheersingsmaatregelen) domein Sociale recherche	17
3.5	Detailbevindingen en aanbevelingen (technische en organisatorische beheersingsmaatregelen)	34

Management samenvatting

Alle organisaties met boa's in dienst moeten, voor verwerkingen in het kader van opsporing, voldoen aan de Wet Politiegegevens (Wpg) en het Besluit Politiegegevens. Onderdeel van deze Wet is het vierjaarlijks uitvoeren van een externe privacy audit en het jaarlijks uitvoeren van een interne audit.

De jaarlijkse interne audit heeft tot doel op systematische wijze toetsen of voor één, dan wel een aantal onderdelen van de wet op adequate wijze uitvoering is gegeven aan de bepalingen van de wet. Hiervoor heeft een beoordeling plaatsgevonden van de opzet, bestaan en de werking van maatregelen en procedures die in naleving van de wettelijke eisen moeten voorzien.

Dit rapport is het resultaat van de uitgevoerde interne audit bij Gemeente Nijmegen over de periode 1 januari 2022 tot en met 15 november 2022. Scope van het onderzoek betrof de verwerkingen in het kader van handhaving door boa's in de domeinen I, III en V. Het gehanteerde normenkader betreft alle eisen zoals gesteld in de Wpg (zie hoofdstuk 2).

Het onderzoek is uitgevoerd door interne auditor 5.1.2e in samenwerking met extern auditbureau 2-Control B.V.

Conclusies

Het gehanteerde normenkader betreft 36 normen. Op deze normen zijn de volgende conclusies van toepassing:

1. Voldoet: 7 normen;
2. Voldoet deels: 15 normen;
3. Voldoet niet: 7 normen;
4. Niet van toepassing: 7 normen.

Zie voor de detailconclusies per norm en de andere domeinen paragraaf 3.2 tot en met 3.5. Zie daarnaast hieronder een aantal algemene bevindingen.

Algemene bevindingen en aanbevelingen

1. **Verbeterplan en borging naar de toekomst:** De organisatie heeft naar aanleiding van de externe audit geen concreet verbeterplan opgesteld. Hiermee is de uitvoering van verbeteracties niet gecoördineerd en ontbreekt een bewaking hierop. De organisatie heeft geen centraal aanspreek- en coördinatiepunt aangesteld voor de uitvoering van het verbeterplan (een zogenaamde "kartrekker"). Momenteel wordt deze taak waargenomen door de privacy officer, deze heeft echter onvoldoende capaciteit. Wij adviseren om een concreet verbeterplan op te stellen en om een kartrekker aan te stellen om de borging in de toekomst van maatregelen om te voldoen aan de Wpg verder vorm te geven.
2. **Locaties met politiegegevens:** Op dit moment is het niet overal helder waar allemaal politiegegevens worden verwerkt. Dit betreft met name netwerkschijven en de applicatie Corsa. Wij adviseren om per domein inzichtelijk te maken waar politiegegevens worden verwerkt en waar mogelijk het gebruik van netwerkschijven of persoonlijke schijven (aantoonbaar) uit te faseren en op te schonen. Inzake Corsa adviseren wij om na te gaan óf hier Wpg gegevens worden verwerkt en zo ja, hoe binnen Corsa aan normen als autorisaties, bewaartermijnen en logging wordt voldaan.
3. **Toetsing werking en auditdossier:** De organisatie moet op dit moment nog een aantal processen en maatregelen beschrijven en formaliseren. Een deel van de processen en geïmplementeerde maatregelen worden al wel uitgevoerd maar zijn niet beschreven (hier wordt op dit moment aan gewerkt). Daarnaast ontbreekt een centraal, gestructureerd auditdossier. Om die reden hebben wij op veel normen de werking niet kunnen toetsen. Wij adviseren bij het beschrijven van processen en maatregelen direct na te denken over hoe de werking van die de maatregelen in die processen in de toekomst kan worden aangetoond.

1 Algemeen

1.1 Achtergrond en doelstelling

Alle organisaties met boa's in dienst moeten, voor verwerkingen in het kader van opsporing, voldoen aan de Wet Politiegegevens (Wpg) en het Besluit Politiegegevens. Onderdeel van deze wet is het vierjaarlijks uitvoeren van een externe privacy audit en het jaarlijks uitvoeren van een interne audit.

De jaarlijkse interne audit heeft tot doel op systematische wijze toetsen of voor één, dan wel een aantal onderdelen van de wet op adequate wijze uitvoering is gegeven aan de bepalingen van de wet. Hiervoor heeft een beoordeling plaatsgevonden van de opzet, bestaan en de werking van maatregelen en procedures die in naleving van de wettelijke eisen moeten voorzien.

Dit rapport is het resultaat van de uitgevoerde interne audit bij Gemeente Nijmegen over de periode 1 januari 2022 tot en met 15 november 2022.

Een opdracht tot het uitvoeren van een interne audit is geen controle-, beoordelings- of andere assurance-opdracht en heeft niet als doel, in welke vorm dan ook, een oordeel te geven of een assurance-conclusie te trekken. Het doel van het interne audit rapport is om de organisatie inzicht te verschaffen in of de organisatie op adequate wijze uitvoering heeft gegeven aan de bepalingen van de wet en op basis daarvan verbeteracties uit te voeren.

1.2 Scope

De scope van de uitgevoerde interne audit bij Gemeente Nijmegen bestond uit de hierna genoemde verwerkingen van politiegegevens:

#	Organisatieonderdeel	Domein	Processen/verwerkingen	Applicaties
1	Toezicht & Handhaving	I	Opsporing strafbare feiten in domein I (openbare ruimte)	CityControl, Corsa, Brickyard netwerkschijf
3	Leerplicht	III	Opsporing strafbare feiten in domein III (leerplicht)	JVS
4	Opsporing sociaal domein	V	Opsporing strafbare feiten in domein V (sociaal domein)	Netwerkschijf

Tijdens de interne audit is geen onderzoek uitgevoerd naar hierboven niet genoemde verwerkingen van politiegegevens.

1.3 Auditplanning

Conform de wet dient jaarlijks voor één, dan wel een aantal onderdelen van de wet systematisch te worden getoetst of op adequate wijze uitvoering is gegeven aan de bepalingen van de wet. Bij Gemeente Nijmegen wordt de volgende auditplanning gehanteerd:

Jaar	Onderdeel
2022	Domein V
2023	Domein I
2024	Domein III
2025	Overkoepelende normen

Daarnaast wordt jaarlijks voor alle onderwerpen een inventarisatie naar de stand van zaken gedaan.

1.4 Auditor en aanpak

De interne audit is uitgevoerd door 5.1.2e als interne auditor van Gemeente Nijmegen in samenwerking met 2-Control B.V. De IT-auditors van 2-Control B.V. voldoen aan de bekwaamheidseisen voor de interne auditor zoals gesteld in de handreiking voor Wpg audits van de NOREA en leiden de interne auditor van Gemeente Nijmegen tijdens dit traject op tot zelfstandig intern auditor.

Wij hebben voor het uitvoeren van de interne audit de volgende activiteiten uitgevoerd:

1. Bestuderen van beschikbare documentatie;
2. Interviewen van onderstaande personen;
3. Waarnemingen in systemen.

Datum	Naam	Functie
4-11-2022	5.1.2e	Manager Sociale recherche
4-11-2022	5.1.2e	Sociaal rechercheur
10-11-2022	5.1.2e	Jurist Toezicht & handhaving
15-11-2022	5.1.2e	Staffunctionaris leerplicht
15-11-2022	5.1.2e	Staffunctionaris leerplicht
15-11-2022	5.1.2e	Functionaris gegevensbescherming
15-11-2022	5.1.2e	Privacy officer
15-11-2022	5.1.2e	Sociaal rechercheur
15-11-2022	5.1.2e	Bedrijfsinformatieadviseur

De interne auditor maakt bij het uitvoeren van deze activiteiten gebruik van de volgende criteria.

Opzet	De organisatie heeft de beheersingsmaatregelen beschreven die voorzien in de borging van de wettelijke eisen met betrekking tot de verwerking van politiegegevens door boa's.
Bestaan	De organisatie heeft de beheersingsmaatregelen overeenkomstig de opzet daadwerkelijk geïmplementeerd en toegepast.
Werking	De organisatie heeft de beheersingsmaatregelen gedurende de verslaggevingsperiode volgens de opzet toegepast, ingeval van handmatige beheersingsmaatregelen zijn deze toegepast door competente en bevoegde personen.

1.5 Verspreiding en gebruik

Dit rapport is vertrouwelijk, alleen bestemd voor intern gebruik en mag niet worden verspreid naar derden partijen zonder uitdrukkelijke toestemming van de interne auditor. Dit rapport dient te worden gebruikt om intern te rapporteren aan het verantwoordelijk management en dit rapport geeft op geen enkele wijze assurance naar derden.

1.6 Conclusies

Wij hebben vastgesteld dat de hierna volgende Wpg onderwerpen niet (rood) of niet volledig (oranje) zijn opgezet, bestaan en/of effectief werken. Zie hoofdstuk 3 voor detailbevindingen en aanbevelingen.

Voor de volledigheid zijn de onderwerpen die afdoende zijn opgezet, geïmplementeerd en effectief werkten ook vermeld (groen). Dit geldt eveneens voor de onderwerpen die niet zijn onderzocht (grijs).

De redenen waarom normen niet zijn onderzocht zijn als volgt aangeduid:

*) Bestaan en/of werking bij betreffende norm niet kunnen toetsen wegens non-occurrence;

**) Norm geheel niet van toepassing omdat het betreffend proces zich niet voordoet bij Gemeente Nijmegen

Domein V: Opsporing strafbare feiten in domein V (sociaal domein)

Onderwerpen	Conclusie		
	Opzet	Bestaan	Werking
1. Reikwijdte			
2. Doelbinding			
3. Noodzakelijkheid en rechtmatigheid, vermelding herkomst			
4. Juistheid en volledigheid politiegegevens			
5. Onderscheid feiten en oordeel			
6. Gegevensbescherming door beveiliging en ontwerp			
7. Gegevensbescherming door standaardinstellingen			
8. Gegevensbeschermingseffectbeoordeling/ Data protection impact assessment (DPIA)			
9. Bijzondere categorieën van politiegegevens			
10. Autorisaties en toegang tot politiegegevens			
11. Autorisaties: aanwijzen functionarissen			
12. Onderscheid tussen verschillende categorieën van betrokkenen (*)			
13. Verwerker en Verwerkersovereenkomst			
14. Geheimhoudingsplicht			
15. Geautomatiseerde individuele besluitvorming (**)			
16. Uitvoering van de dagelijkse politietaak (**)			
17. Ter beschikking stellen van politiegegevens binnen het WPG-domein (*)			
18. Geautomatiseerd vergelijken en in combinatie zoeken (**)			
19. Ondersteunende taken (**)			
20. Bewaartermijnen, verwijderen en vernietigen			
21. Verstrekking van politiegegevens aan anderen dan politie en Koninklijke marechaussee			
22. Doorgiften aan derde landen (**)			
23. Verstrekking aan derden structureel voor samenwerkingsverbanden (**)			
24. Rechtstreekse verstrekking aan inlichtingen- of veiligheidsdiensten (**)			
25. Informatie aan de betrokkene, recht op inzage, rectificatie en verwijdering			
26. Register			
27. Documentatie			
28. Logging			
29. Audits			
30. Melding datalekken			
31. Functionaris voor gegevensbescherming			

Technische en organisatorische maatregelen	Conclusie		
	Opzet	Bestaan	Werking
1. Wijzigingenbeheer			
2. Logische toegangsbeveiliging			
3. Beheer van kwetsbaarheden (patchmanagement)			
4. Cryptografie			
5. Vulnerability scans en Penetratietesten			

2 Normenkader

Om de privacy van de verwerkte politiegegevens ten behoeve van de wettelijke taak te kunnen waarborgen en te kunnen voldoen aan de eisen die de wet daaraan stelt, heeft Gemeente Nijmegen beheersingsmaatregelen getroffen in lijn met de illustratieve beheersingsmaatregelen uit de NOREA Handreiking Privacy audit Wpg (boa). Die illustratieve beheersingsmaatregelen zijn gebaseerd op de Wet politiegegevens en het Besluit politiegegevens buitengewoon opsporingsambtenaren en omvatten de te verwachten onderwerpen en -beheersingsmaatregelen, gericht op beheersing van privacy in gegevensverwerkende processen en indicatieve controles, in lijn met de geldende wet- en regelgeving.

Onderstaand zijn deze onderwerpen en illustratieve beheersingsmaatregelen weergegeven.

Onderwerpen en beheersingsmaatregelen
1. Reikwijdte De verwerkingsverantwoordelijke heeft bestanden met politiegegevens binnen de organisatie geïdentificeerd en gedocumenteerd.
2. Doelbinding Politiegegevens worden alleen verwerkt als dat nodig is voor de in de wet genoemde doeleinden. Geborgd is 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. Noodzakelijkheid en rechtmatigheid, vermelding herkomst Er wordt geborgd dat de politiegegevens daartoe toereikend, ter zake dienend en beperkt zijn tot wat noodzakelijk is (niet bovenmatig) en dat de herkomst van gegevens voor art 9 verwerkingen wordt vermeld.
4. Juistheid en volledigheid politiegegevens <ul style="list-style-type: none">De verwerkingsverantwoordelijke heeft controles op de kwaliteit ingericht ten behoeve van de borging van de juistheid en nauwkeurigheid van politiegegevens.Er zijn procedures opgesteld voor het vernietigen en rectificeren van politiegegevens.
5. Onderscheid feiten en oordeel Er zijn maatregelen genomen om politiegegevens die op feiten zijn gebaseerd, voor zover mogelijk, te onderscheiden van politiegegevens die op een persoonlijk oordeel zijn gebaseerd.
6. Gegevensbescherming door beveiliging en ontwerp <ul style="list-style-type: none">Er is (aantoonbaar) een risicoanalyse uitgevoerd waaruit het risiconiveau blijkt en identificeert, evalueert en mitigeert systematisch en periodiek factoren die het beschermen van politiegegevens tegen ongeoorloofde of onrechtmatige verwerking en tegen opzettelijk verlies, vernietiging of beschadiging in gevaar brengen en past de maatregelen hierop aan.De organisatie heeft gegevensbeschermingsbeleid en procedures ontwikkeld en vastgesteld. De verwerkingsverantwoordelijke heeft de maatregelen die nodig zijn om het risico te beperken (passende technische en organisatorische maatregelen) aantoonbaar geïmplementeerd.Privacy by design wordt toegepast/geborgd (bijv. bij ontwikkelingen/ wijzigingen).De verwerkingsverantwoordelijke kan aantonen dat de verwerking van politiegegevens wordt verricht in overeenstemming met wat bepaald is in de wet.
7. Gegevensbescherming door standaardinstellingen De verwerkingsverantwoordelijke treft passende technische en organisatorische maatregelen om te waarborgen dat standaard: <ul style="list-style-type: none">alleen die politiegegevens worden verwerkt die noodzakelijk zijn voor elk specifiek doel van de verwerking;politiegegevens niet zonder tussenkomst van een natuurlijke persoon voor een onbeperkt aantal natuurlijke personen toegankelijk worden gemaakt.

Onderwerpen en beheersingsmaatregelen	
8. Gegevensbeschermingseffectbeoordeling / Data protection impact assessment (DPIA)	<ul style="list-style-type: none"> • Indien een verwerking waarschijnlijk een hoog risico voor de rechten en vrijheden van personen oplevert worden binnen de organisatie de risico's systematisch geïdentificeerd, beoordeeld en aangepakt door middel van een DPIA die ten minste aan de eisen gesteld in de wet voldoet. • De verwerkingsverantwoordelijke beoordeelt, indien nodig of wanneer sprake is van een verandering van het risico, of de verwerking in overeenstemming met de DPIA wordt uitgevoerd en past de DPIA zo nodig aan.
9. Bijzondere categorieën van politiegegevens Er vindt geen verwerking van bijzondere categorieën van politiegegevens plaats, tenzij:	<ul style="list-style-type: none"> • Dat onvermijdelijk is voor het doel van de verwerking. • Dit in aanvulling is op de verwerking van andere politiegegevens betreffende de persoon. • De gegevens afdoende zijn beveiligd.
10. Autorisaties en toegang tot politiegegevens	<ul style="list-style-type: none"> • Er is een systeem van autorisaties dat voldoet aan de vereisten van zorgvuldigheid en evenredigheid. Dit houdt in dat: De verwerkingsverantwoordelijke heeft die personen die vanuit hun functie en de wet toegang mogen hebben tot bepaalde politiegegevens geautoriseerd voor alleen die gegevens (need-to-know). • Er is een proces voor het toewijzen, wijzigen en intrekken van autorisaties t.b.v. de toegang tot politiegegevens. • Er zijn maatregelen vastgesteld en geïmplementeerd die de identiteit en de toegangsrechten van een gebruiker controleert en rechtmatige toegang tot de gegevens borgt.
11. Autorisaties: aanwijzen functionarissen Er is een actuele lijst van, door de verwerkingsverantwoordelijke aangewezen, bevoegde functionarissen.	
12. Onderscheid tussen verschillende categorieën van betrokkenen De verwerkingsverantwoordelijke heeft geborgd dat, voor zover mogelijk, duidelijk onderscheid wordt gemaakt in de verschillende categorieën van betrokkenen.	
13. Verwerker en Verwerkersovereenkomst	<ul style="list-style-type: none"> • De verwerker stelt de verwerkingsverantwoordelijke alle informatie ter beschikking die nodig is om aantoonbaar te maken dat de verplichtingen in de Verwerkersovereenkomst en de Wpg worden nageleefd en die nodig is om audits mogelijk te maken. • De verwerking door een verwerker vindt alleen plaats als een verwerkingsverantwoordelijke afdoende garanties heeft over de toereikendheid van de geïmplementeerde technische en organisatorische maatregelen. • Bij elke uitvoering van een gegevensverwerking door een verwerker zijn de taken en afspraken schriftelijk vastgesteld en vastgelegd in een (toereikende) overeenkomst of andere rechtshandeling. • Er zijn afspraken vastgesteld en vastgelegd m.b.t. de handelswijze bij een inbreuk op de beveiliging. • Een andere partij is alleen ingeschakeld bij de uitvoering van de verwerking met toestemming van de verwerkingsverantwoordelijke. Aan deze andere verwerker (subverwerker) is bij een overeenkomst dezelfde verplichtingen inzake gegevensbescherming opgelegd.
14. Geheimhoudingsplicht Er is geborgd dat de ambtenaar van politie of de persoon aan wie politiegegevens ter beschikking zijn gesteld formeel bekend is met de plicht tot geheimhouding en de consequenties bij schending van deze plicht.	

Onderwerpen en beheersingsmaatregelen	
15. Geautomatiseerde individuele besluitvorming	<ul style="list-style-type: none"> Besluiten gebaseerd uitsluitend op geautomatiseerde verwerking dat voor de betrokkene nadelige rechtsgevolgen heeft of hem in aanmerkelijke mate treft, worden niet genomen tenzij voorzien is in de voorwaarden genoemd in de wet. Het verbod op het gebruik van profilering die leidt tot discriminatie van personen op grond van de bijzondere categorieën van politiegegevens (art 5) is bekend binnen de organisatie. Dit beperkte verbod op profilering is onderwerp van de bewustwordingssessies binnen de organisatie.
16. Uitvoering van de dagelijkse politietaak	<ul style="list-style-type: none"> Geborgd is dat art 8 politiegegevens één jaar na de datum van de eerste verwerking zodanig worden opgeslagen (achter een schot worden geplaatst) dat ze alleen nog beschikbaar komen voor verdere verwerking op basis van de vergelijking van gegevens (hit-no-hit basis). Geborgd is voor zover dat noodzakelijk is met het oog op de uitvoering van de dagelijkse politietaak politiegegevens ten aanzien waarvan in art 8 lid 1 genoemde termijn is verstrekt geautomatiseerd worden vergeleken met politiegegevens die worden verwerkt op grond van art 8 lid 1 teneinde vast te stellen of verbanden bestaan tussen de betreffende gegevens. De gerelateerde gegevens kunnen verder worden verwerkt met het oog op de uitvoering van de dagelijkse politietaak.
17. Ter Beschikking stellen (voor verdere verwerking)	<ul style="list-style-type: none"> Geborgd is dat de verdere verwerking van art 9 gegevens alleen plaats vindt na toestemming (aantoonbaar) van de daartoe bevoegde functionaris. Geborgd is dat de 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 art 1, onderdeel a conform de richtlijnen gesteld in de wet plaatsvindt.
18. Geautomatiseerd vergelijken en in combinatie zoeken	<ul style="list-style-type: none"> Geborgd is dat gegevens alleen geautomatiseerd worden vergeleken met andere politiegegevens of met andere dan politiegegevens binnen de richtlijnen gesteld in art 11. Geborgd is dat gegevens alleen in combinatie met elkaar worden verwerkt binnen de richtlijnen gesteld in art 11 lid 4. Geborgd is dat het in combinatie verwerken van art 8 politiegegevens beperkt is tot de ambtenaren van politie die daarvoor geautoriseerd zijn. Geborgd is dat de ambtenaren die geautomatiseerd vergelijken en ambtenaren die in combinatie zoeken over voldoende kennis en vaardigheden beschikken.
19. Ondersteunende taken	Geborgd is dat voor de verwerkingen bedoeld in art 13 lid 1 t/m 3, van tevoren is voldaan aan de schriftelijke vereisten (art 13 lid 4).
20. Bewaartermijnen, verwijderen en vernietigen	<ul style="list-style-type: none"> Politiegegevens worden niet langer bewaard dan de minimale tijd die nodig is, zoals vereist door de toepasselijke wet- en regelgeving, of voor de doeleinden waarvoor deze zijn verwerkt. De verwerkingsverantwoordelijke voorziet in voldoende waarborgen om te bewerkstelligen dat de gegevens conform de wet worden gecontroleerd, verwijderd en vernietigd. Geborgd is dat Politiegegevens na verwijdering maximaal vijf jaar worden bewaard. Indien van cultureel of historisch belang kan worden afgezien van vernietiging van de gegevens. Er wordt dan aan de bewaareisen zoals genoemd in de Archiefwet voldaan.

Onderwerpen en beheersingsmaatregelen
<p>21. Verstrekking van politiegegevens aan anderen dan politie en Koninklijke marechaussee</p> <ul style="list-style-type: none"> • Geborgd is dat politiegegevens alleen worden verstrekt aan personen of instanties buiten het politiedomein, voor zover dit noodzakelijk is voor de doeleinden zoals deze in de Wet politiegegevens en het Besluit politiegegevens zijn genoemd. • Geborgd is dat wanneer gegevens verstrekt worden er wordt voldaan aan de documentatieplicht (conform 6 lid 4 Bpg). • Geborgd is dat verstrekking alleen plaatsvindt in overeenstemming met het bevoegd gezag indien dit vereist is in de wet. • Bij verstrekkingen is geborgd dat de ontvangende partij wordt gewezen op zijn geheimhoudingsplicht. • De juistheid, volledigheid, actualiteit en betrouwbaarheid van politiegegevens bij verstrekking wordt, voor zover mogelijk, gecontroleerd en inzichtelijk gemaakt voor de ontvangende partij. • Er is een procedure voor het onverwijd in kennis stellen van de ontvanger van politiegegevens indien geconstateerd wordt dat onjuiste politiegegevens zijn verstrekt of dat politiegegevens op onrechtmatig wijze zijn verstrekt.
<p>22. Doorgiften aan derde landen</p> <ul style="list-style-type: none"> • De doorgifte van gegevens aan verwerkingsverantwoordelijke in derde landen vindt alleen plaats indien er een adequaatsheidsbesluit is van de Commissie van de Europese Unie of indien één van de uitzonderingsgronden zoals genoemd in de wet van toepassing is. • De doorgifte van gegevens aan derde landen wordt vastgelegd (documentatieplicht). • Indien doorgifte plaatsvindt op basis van art 17a lid 2 onderdeel a of b, lid 3 of lid 5 is (aantoonbaar) voldaan aan de gestelde eisen in de wet. • Indien politiegegevens van een andere lidstaat afkomstig worden doorgegeven aan derde landen is de toestemming van de verantwoordelijke autoriteit van deze lidstaat beschikbaar.
<p>23. Verstrekking aan derden structureel voor samenwerkingsverbanden</p> <ul style="list-style-type: none"> • De verwerkingsverantwoordelijke heeft inzicht in de samenwerkingsverbanden waarbij politiegegevens worden verstrekt. • In de beslissing voor het verstrekken van politiegegevens t.b.v. een samenwerkingsverband wordt vastgelegd: <ul style="list-style-type: none"> ○ Ten behoeve van welk zwaarwegend algemeen belang de verstrekking noodzakelijk is, ○ Ten behoeve van welk samenwerkingsverband de politiegegevens worden verstrekt, ○ Het doel waartoe dit is opgericht, ○ Welke gegevens worden verstrekt, ○ De voorwaarden onder welke de gegevens worden verstrekt en ○ Aan welke personen of instanties de gegevens worden verstrekt. • De daadwerkelijke verstrekking van gegevens wordt vastgelegd.
<p>24. Rechtstreekse verstrekking</p> <ul style="list-style-type: none"> • De organisatie heeft geborgd dat rechtstreekse verstrekking uitsluitend plaatsvindt voor zover noodzakelijk op grond van art 23 en alleen voor zover voldaan kan worden aan de beveiligingseisen. • De rechtstreekse verstrekking op basis van art 23 lid 2 vindt alleen plaats aan de aangewezen personen.

Onderwerpen en beheersingsmaatregelen	
25. Informatie aan de betrokkene, recht op inzage, rectificatie en verwijdering	<ul style="list-style-type: none"> De verwerkingsverantwoordelijke biedt de betrokkene informatie over de verwerking van persoonsgegevens en doet dit beknopt, toegankelijk en duidelijk, zodat de betrokkene zijn rechten kan uitoefenen. De informatievoorziening voldoet aan de eisen gesteld in art 24b lid 1 en 2. Bij uitstel, beperking of achterwege laten van de verstrekking van informatie bedoeld in 24b lid 2 is de uitstel, beperking of achterwege laten alsmede de duur van deze maatregel onderbouwd. Verzoeken tot inzage, rectificatie, vernietiging van betrokkenen worden - met inachtneming van het gestelde in artikel 27 - tijdig en adequaat afgehandeld. De organisatie borgt dat bij een verzoek tot inzage (art 25 lid 1) of rectificatie (art 28 lid 1) dat de betrokkene zonder onnodige vertraging in kennis wordt gesteld van de ontvangst van het verzoek, de termijn voor uitsluitel en de mogelijkheid een klacht in te dienen bij de AP. Een weigering gevolg te geven aan het verzoek conform art 24a lid 4 is onderbouwd. Elke weigering of beperking van de inzage wordt aan de betrokkene toegelicht, met vermelding van de feitelijke of juridische gronden die aan het besluit ten grondslag liggen.
26. Register	<ul style="list-style-type: none"> De verwerkingsverantwoordelijke houdt een register bij dat de gegevens bevat zoals aangegeven in art 31d lid 1. De verwerker houdt een register bij dat de gegevens bevat zoals aangegeven in art 31d lid 2.
27. Documentatie	<ul style="list-style-type: none"> De verwerkingsverantwoordelijke borgt een volledige en toegankelijke schriftelijke vastlegging (documentatieplicht) van de onderdelen genoemd in art 32 lid 1. De bedoelde politiegegevens worden conform art 32 lid 4 bewaard. De verwerkingsverantwoordelijke borgt een volledige en toegankelijke schriftelijke vastlegging (documentatieplicht) van de doorgifte van politiegegevens aan een verwerkingsverantwoordelijke in een derde land of aan een internationale organisatie. De schriftelijke melding van een gemeenschappelijke verwerking van politiegegevens aan de AP is geborgd.
28. Logging	<ul style="list-style-type: none"> De verwerkingsverantwoordelijke en de verwerker dragen zorg voor de logging van verwerkingen zoals opgenomen in art 32a lid 1. De organisatie gebruikt de logging uitsluitend ter controle van de rechtmatigheid van de gegevensverwerkingen, interne controles, ter waarborging van de integriteit en de beveiliging van politiegegevens en voor strafrechtelijke procedures.
29. Audits	Er wordt uitvoering gegeven aan de eisen zoals gesteld in de Regeling periodieke audit politiegegevens.
30. Melding datalekken	<ul style="list-style-type: none"> De organisatie detecteert en behandelt privacy gerelateerde incidenten op gepaste wijze om de gevolgen te beperken en maatregelen te nemen om toekomstige inbreuken te voorkomen. De verantwoordelijkheden van de behandeling van datalekken zijn belegd in de organisatie, de daadwerkelijke uitvoering wordt beheerst, gedocumenteerd en geëvalueerd. De melding van een datalek aan de Autoriteit Persoonsgegevens vindt tijdig en volledig plaats. Betrokkenen worden, indien vereist, tijdig en volledig in kennis gesteld van een inbreuk op de beveiliging als deze inbreuk waarschijnlijk een hoog risico voor hun rechten en vrijheden betekent.

Onderwerpen en beheersingsmaatregelen

31. Functionaris voor gegevensbescherming

- Er is een functionaris voor gegevensbescherming aangesteld die toezicht houdt op:
 - het naleven van de Wpg;
 - het beleid van de verwerkingsverantwoordelijke met betrekking tot de bescherming van persoonsgegevens;
 - de toewijzing van de autorisaties, bedoeld in art 6;
 - de bewustmaking en opleiding van de ambtenaren van politie betrokken bij de verwerking van politiegegevens;
 - de audits;
 - de uitvoering van de DPIA's.
- De Functionaris Gegevensbescherming stelt jaarlijks een verslag op van zijn bevindingen en stelt het ter beschikking aan de verwerkingsverantwoordelijke.
- De Functionaris voor Gegevensbescherming is aangemeld bij de Autoriteit Persoonsgegevens.

3 Bevindingen en aanbevelingen

3.1 Algemene bevindingen en aanbevelingen

3.1.1 *Verbeterplan en borging naar de toekomst*

De organisatie heeft naar aanleiding van de externe audit geen concreet verbeterplan opgesteld. Hiermee is de uitvoering van verbeteracties niet gecoördineerd en ontbreekt een bewaking hierop. De organisatie heeft geen centraal aanspreek- en coördinatiepunt aangesteld voor de uitvoering van het verbeterplan (een zogenaamde “kartrekker”). Momenteel wordt deze taak waargenomen door de privacy officer, deze heeft echter onvoldoende capaciteit. Wij adviseren om een concreet verbeterplan op te stellen en om een kartrekker aan te stellen om de borging in de toekomst van maatregelen om te voldoen aan de Wpg verder vorm te geven.

3.1.2 *Locaties met politiegegevens*

Op dit moment is het niet overal helder waar allemaal politiegegevens worden verwerkt. Dit betreft met name netwerkschijven en de applicatie Corsa. Wij adviseren om per domein inzichtelijk te maken waar politiegegevens worden verwerkt en waar mogelijk het gebruik van netwerkschijven of persoonlijke schijven (aantoonbaar) uit te faseren en op te schonen. Inzake Corsa adviseren wij om na te gaan of hier Wpg gegevens worden verwerkt en zo ja, hoe binnen Corsa aan normen als autorisaties, bewaartermijnen en logging wordt voldaan.

Voor één onderdeel (opsporing sociaal domein) is het gebruik van netwerkschijven (voorlopig) onvermijdelijk. Om hier te kunnen voldoen aan normen als logging gaat de organisatie onderzoeken met de IRvN hoe dit technisch kan worden gerealiseerd. Hier is al een start mee gemaakt waarbij is aangegeven dat vanaf het tweede kwartaal in 2023 de situatie met betrekking tot netwerkschijven gaat wijzigen. Bij deze wijziging worden de eisen van de Wpg meegenomen. Wij adviseren om te bewaken dat dit daadwerkelijk gebeurt zodat dit naar de toekomst toe geborgd is.

3.1.3 *Toetsing werking en auditdossier*

De organisatie moet op dit moment nog een aantal processen en maatregelen beschrijven en formaliseren. Een deel van de processen en geïmplementeerde maatregelen worden al wel uitgevoerd maar zijn niet beschreven (hier wordt op dit moment aan gewerkt). Daarnaast ontbreekt een centraal, gestructureerd auditdossier. Om die reden hebben wij op veel normen de werking niet kunnen toetsen. Wij adviseren bij het beschrijven van processen en maatregelen direct na te denken over hoe de werking van die de maatregelen in die processen in de toekomst kan worden aangetoond.

3.2 Bevindingen domein Leerplicht

Domein Leerplicht heeft een aantal verbeteracties uitgevoerd, met name met betrekking tot het upgraden naar JVS3 en het verbeteren van de autorisatieprocedures. Hiermee heeft de afdeling deels uitvoering gegeven aan de uit te voeren verbeteracties. Een aantal zaken moeten nog verder worden opgepakt. Wij adviseren om:

1. Met de leverancier van JVS in overleg te treden over de volgende onderwerpen:
 - a. Autorisaties (norm 10): hoe kan aangetoond (en gecontroleerd) worden dat de rechten zijn ingericht zoals beschreven in de autorisatiematrix? Focus hierbij moet liggen op controle van:
 - i. Juiste toepassing van het nieuwe proces;
 - ii. Juiste gebruikers per team;
 - iii. Juiste rechten per team;
 - b. Achter 't schot plaatsen / bewaartermijnen (norm 16 en 20): het is momenteel niet duidelijk of JVS deze functionaliteit biedt en of dit is ingericht. Wij adviseren om te bespreken met de leverancier hoe aan deze normen kan worden voldaan;
 - c. Logging (norm 28): JVS biedt logging, het is op dit moment niet duidelijk of deze logging bruikbaar is voor een controle. Wij adviseren om te bespreken met de leverancier hoe de logging op een bruikbare manier aan de gemeente kan worden aangeleverd;
2. Autorisaties (norm 10): de procedure voor het toekennen en intrekken van autorisaties is in opzet opgesteld in combinatie met een autorisatiematrix. Wij adviseren om een (minimaal halfjaarlijks) controleproces in te richten op de juistheid van de toegekende autorisaties (zie ook hierboven) en de bevindingen hiervan te rapporteren aan de teamleider;
3. Logging (norm 28): wij adviseren om op basis van de beschikbare logging (zie ook hierboven) een (minimaal halfjaarlijks) controleproces in te richten op atypische raadplegingen en de bevindingen hiervan te rapporteren aan de teamleider;
4. Samenwerkende gemeenten: de regiogemeenten moeten in staat worden gesteld om controles uit te voeren óf zij moeten het uitvoeren van de controles (al dan niet deels) uitbesteden aan de gemeente Nijmegen. Wij adviseren om in overleg te treden met de regiogemeenten en gezamenlijk af te stemmen hoe de controle op de autorisaties en de logging kan worden geïmplementeerd;
5. Handboek (norm 2 tot en met 5): het handboek waarin de diverse maatregelen en onderwerpen rondom de Wpg worden beschreven is nog niet geformaliseerd en afgemaakt. Wij adviseren om het handboek af te ronden, een formele status te geven en uit te dragen in de organisatie.

3.3 Bevindingen domein Toezicht en handhaving

Binnen het domein Toezicht en handhaving hebben veel personeelswisselingen plaatsgevonden. Hierdoor is weinig voortgang geboekt in de verbeteracties voor de Wpg. Wij adviseren om:

1. Voldoende capaciteit voor het implementeren van Wpg maatregelen beschikbaar te maken;
2. Handboek (norm 2 tot en met 5): het handboek waarin de diverse maatregelen en onderwerpen rondom de Wpg worden beschreven is nog niet (af)gemaakt. Wij adviseren om het handboek af te ronden, een formele status te geven en uit te dragen in de organisatie.
3. Met de leverancier van CityControl in overleg te treden over de volgende onderwerpen:
 - a. Autorisaties (norm 10): hoe kan aangetoond (en gecontroleerd) worden dat de rechten zijn ingericht zoals beschreven in de autorisatiematrix?
Focus hierbij moet liggen op controle van:
 - i. Juiste toepassing van het proces;
 - ii. Juiste gebruikers per team;
 - iii. Juiste rechten per team;
 - b. Logging (norm 28): CityControl biedt logging, het is op dit moment niet duidelijk of deze logging bruikbaar is voor een controle. Wij adviseren om te bespreken met de leverancier hoe de logging op een bruikbare manier aan de gemeente kan worden aangeleverd;
4. Autorisaties (norm 10): de procedure voor het toekennen en intrekken van autorisaties is in opzet opgesteld in combinatie met een autorisatiematrix. Wij adviseren om een (minimaal halfjaarlijks) controleproces in te richten op de juistheid van de toegekende autorisaties (zie ook hierboven) en de bevindingen hiervan te rapporteren aan de teamleider;
5. Logging (norm 28): wij adviseren om op basis van de beschikbare logging (zie ook hierboven) een (minimaal halfjaarlijks) controleproces in te richten op atypische raadplegingen en de bevindingen hiervan te rapporteren aan de teamleider.

3.4 Detailbevindingen en aanbevelingen (Wpg beheersingsmaatregelen) domein Sociale recherche

In de onderstaande tabel hebben wij in de kolom 'Bevindingen' de resultaten van onze werkzaamheden gericht op het vaststellen van de opzet, het bestaan en/of de werking van de beheersingsmaatregelen vastgelegd. In de kolom 'Conclusie / aanbeveling' geven wij aan of aan de criteria voor de opzet, het bestaan en/of de werking wordt voldaan.

#	Onderwerp	Verwijzing Wpg	Beheersingsmaatregelen	Bevindingen	Conclusies / Aanbevelingen
1	Reikwijdte	Art 2 lid 1 en 2	De verwerkingsverantwoordelijke heeft bestanden met politiegegevens binnen de organisatie geïdentificeerd en gedocumenteerd.	<p>Vastgesteld dat gemeente een verwerkingsregister heeft opgesteld waarin Wpg verwerkingen zijn opgenomen inclusief de locaties van de bestanden</p> <p>Vastgesteld dat verwerkingsregister voldoet aan de eisen uit de Wpg. Daarnaast vastgesteld dat gemeente een instructie heeft voor het opnemen van nieuwe verwerkingen.</p> <p>Vastgesteld dat gemeente een proces heeft opgezet om de actualiteit van het verwerkingsregister te waarborgen. Hieronder valt een jaarlijkse uitvraag bij de afdelingsmanagers. De werking hiervan nog niet vast kunnen stellen.</p>	Voldoet deels

#	Onderwerp	Verwijzing Wpg	Beheersingsmaatregelen	Bevindingen	Conclusies / Aanbevelingen
2	Doelbinding	Art 3 lid 1, 3 en 4 Art 8 lid 1 Art 9 lid 1 en 2 Art 11 lid 1	Politiegegevens worden alleen verwerkt als dat nodig is voor de in de wet genoemde doeleinden. Geborgd is dat bij het verwerken van politiegegevens altijd sprake is van doelbinding en dat de gegevens niet op een onrechtmatige wijze, worden verwerkt.	<p>De organisatie heeft een opzet gemaakt voor het beschrijven van maatregelen voor het borgen van doelbinding, noodzakelijkheid en rechtmatigheid, vermelding herkomst, juistheid en volledigheid en onderscheid feiten en persoonlijk oordeel in een handboek. Dit handboek is nog in concept en dient nog af te worden gemaakt en vastgesteld.</p> <p>Vastgesteld dat in het handboek voor Sociale Recherche benoemd is wat de specifieke regels zijn voor artikel 9 verwerkingen, zoals het binnen een week vastleggen van het doel van het onderzoek.</p> <p>De gemeente heeft de afgelopen jaren een proces opgezet waarmee doelbinding wordt getoetst (door de FG) aan de hand van uitgevoerde DPIA's (controle van DPIA's). Voor de Wpg verwerkingen zijn op dit moment nog geen DPIA's uitgevoerd. Hiermee voldoet de opzet wel maar kan het bestaan en de werking niet worden vastgesteld.</p>	<p>Voldoet deels</p> <p>Wij adviseren om het beschrijven van de geïmplementeerde maatregelen verder af te ronden.</p> <p>Daarnaast adviseren wij om jaarlijks toezichthoudende maatregelen te ontwerpen en te implementeren en intern na te gaan wie deze kan uitvoeren (onder toezicht van de FG).</p>
3	Noodzakelijkheid & rechtmatigheid, vermelding herkomst	Art 3 lid 2 en 5	Er wordt geborgd dat de politiegegevens daartoe toereikend, ter zake dienend en beperkt zijn tot wat noodzakelijk is (niet bovenmatig) en dat de herkomst van gegevens voor art 9 verwerkingen wordt vermeld.	Zie 2.	<p>Voldoet deels</p> <p>Zie 2.</p>
4	Juistheid en volledigheid politiegegevens	Art 4 lid 1	<p>De verwerkingsverantwoordelijke heeft controles op de kwaliteit ingericht ten behoeve van de borging van de juistheid en nauwkeurigheid van politiegegevens.</p> <p>Er zijn procedures opgesteld voor het vernietigen en rectificeren van politiegegevens.</p>	Zie 2.	<p>Voldoet deels</p> <p>Zie 2.</p>

#	Onderwerp	Verwijzing Wpg	Beheersingsmaatregelen	Bevindingen	Conclusies / Aanbevelingen
5	Onderscheid feiten en persoonlijk oordeel	Art 4 lid 3	Er zijn maatregelen genomen om politiegegevens die op feiten zijn gebaseerd, voor zover mogelijk, te onderscheiden van politiegegevens die op een persoonlijk oordeel zijn gebaseerd.	Zie 2.	Voldoet deels Zie 2.
6	Gegevensbescherming door beveiliging en ontwerp	Art 4a lid 1 t/m 5	<p>Er is (aantoonbaar) een risicoanalyse uitgevoerd waaruit het risiconiveau blijkt en identificeert, evalueert en mitigeert systematisch en periodiek factoren die het beschermen van politiegegevens tegen ongeoorloofde of onrechtmatige verwerking en tegen opzettelijk verlies, vernietiging of beschadiging in gevaar brengen en past de maatregelen hierop aan.</p> <p>De organisatie heeft gegevensbeschermingsbeleid en procedures ontwikkeld en vastgesteld. De verwerkingsverantwoordelijke heeft de maatregelen die nodig zijn om het risico te beperken (passende technische en organisatorische maatregelen) aantoonbaar geïmplementeerd.</p> <p>Privacy by design wordt toegepast/geborgd (bijv. bij ontwikkelingen/ wijzigingen).</p> <p>De verwerkingsverantwoordelijke kan aantonen dat de verwerking van politiegegevens wordt verricht in overeenstemming met wat bepaald is in de wet.</p>	<p>Vastgesteld dat gemeente beleid heeft rondom privacy by design en default en dat aan de voorkant bij ieder nieuwe intake bij I&A geborgd is dat over privacy wordt nagedacht.</p> <p>Vastgesteld dat gemeente processen heeft om DPIA's uit te voeren en dat geborgd is in processen dat DPIA's aan de voorkant van het proces worden uitgevoerd. Vastgesteld dat voor Wpg verwerkingen nog geen DPIA's zijn uitgevoerd.</p>	<p>Voldoet deels</p> <p>Wij adviseren om na te gaan of voor de Wpg verwerkingen DPIA's moeten worden uitgevoerd en om deze waar nodig uit te voeren.</p>

#	Onderwerp	Verwijzing Wpg	Beheersingsmaatregelen	Bevindingen	Conclusies / Aanbevelingen
7	Gegevens- bescherming door standaard- instellingen	Art 4b lid 1a en lid 1b	De verwerkingsverantwoordelijke treft passende technische en organisatorische maatregelen om te waarborgen dat standaard: a) alleen die politiegegevens worden verwerkt die noodzakelijk zijn voor elk specifiek doel van de verwerking; b) politiegegevens niet zonder tussenkomst van een natuurlijke persoon voor een onbeperkt aantal natuurlijke personen toegankelijk worden gemaakt.	Zie 6.	Voldoet deels Zie 6.
8	Gegevens- beschermings- effectbeoordeling/ Data protection- impact assessment (DPIA)	Art 4c	Indien een verwerking waarschijnlijk een hoog risico voor de rechten en vrijheden van personen oplevert worden binnen de organisatie de risico's systematisch geïdentificeerd, beoordeeld en aangepakt door middel van een DPIA die ten minste aan de eisen gesteld in de wet voldoet. De verwerkingsverantwoordelijke beoordeelt, indien nodig of wanneer sprake is van een verandering van het risico, of de verwerking in overeenstemming met de DPIA wordt uitgevoerd en past de DPIA zo nodig aan.	Zie 6.	Voldoet deels Zie 6.
9	Bijzondere categorieën van politiegegevens	Art 5	Er vindt geen verwerking van bijzondere categorieën van politiegegevens plaats, tenzij: • dat onvermijdelijk is voor het doel van de verwerking; • dit in aanvulling is op de verwerking van andere politiegegevens betreffende de persoon; • de gegevens afdoende zijn beveiligd.	Vastgesteld dat de bijzondere categorieën zijn vastgelegd in het verwerkingsregister per domein.	Voldoet

#	Onderwerp	Verwijzing Wpg	Beheersingsmaatregelen	Bevindingen	Conclusies / Aanbevelingen
10	Autorisaties en toegang tot politiegegevens	Art 6 lid 1 t/m 6 Art 6a	<p>Er is een systeem van autorisaties dat voldoet aan de vereisten van zorgvuldigheid en evenredigheid. Dit houdt in dat: De verwerkingsverantwoordelijke heeft die personen die vanuit hun functie en de wet toegang mogen hebben tot bepaalde politiegegevens geautoriseerd voor alleen die gegevens (need-to-know) .</p> <p>Er is een proces voor het toewijzen, wijzigen en intrekken van autorisaties t.b.v. de toegang tot politiegegevens.</p> <p>Er zijn maatregelen vastgesteld en geïmplementeerd die de identiteit en de toegangsrechten van een gebruiker controleert en rechtmatige toegang tot de gegevens borgt.</p>	Vastgesteld dat domein uitgangspunten rondom autorisaties heeft beschreven in het handboek inclusief een matrix. Controle op rechten is nog niet uitgevoerd en ingericht. Niet-boa's zijn geautoriseerd middels een verklaring van verantwoordelijke.	<p>Voldoet deels</p> <p>Wij adviseren de gevolgde processen concreter te beschrijven in het handboek en om een halfjaarlijks controleproces in te richten.</p>
11	Autorisaties: aanwijzen functionarissen	Art 6 lid 7	Er is een actuele lijst van, door de verantwoordelijke aangewezen, bevoegde functionarissen.	Vastgesteld dat de Teamleider Sociale recherche is aangesteld als Bevoegd Functionaris. De aanstelling is nog niet formeel bekrachtigd.	<p>Voldoet deels</p> <p>Wij adviseren om zo snel mogelijk de aanstelling van de bevoegd functionaris te laten bekrachtigen door verantwoordelijke (of gemandateerde).</p>
12	Onderscheid tussen verschillende categorieën van betrokkenen	Art 6b	De verwerkingsverantwoordelijke heeft geborgd dat, voor zover mogelijk, duidelijk onderscheid wordt gemaakt in de verschillende categorieën van betrokkenen.	Vastgesteld op basis van interview dat onderscheid wordt gemaakt in categorieën van betrokkenen als dit zich voordoet.	Voldoet

#	Onderwerp	Verwijzing Wpg	Beheersingsmaatregelen	Bevindingen	Conclusies / Aanbevelingen
13	Verwerker en Verwerkers-overeenkomst	Art 6c	<p>De verwerker stelt de verwerkingsverantwoordelijke alle informatie ter beschikking heeft die nodig is om aantoonbaar te maken dat de verplichtingen in de Verwerkersovereenkomst en de Wpg worden nageleefd en die nodig is om audits mogelijk te maken.</p> <p>De verwerking door een verwerker vindt alleen plaats als een verwerkingsverantwoordelijke afdoende garanties heeft over de toereikendheid van de geïmplementeerde technische en organisatorische maatregelen.</p> <p>Bij elke uitvoering van een gegevensverwerking door een verwerker zijn de taken en afspraken schriftelijk vastgesteld en vastgelegd in een (toereikende) overeenkomst of andere rechtshandeling.</p> <p>Er zijn afspraken vastgesteld en vastgelegd m.b.t. de handelswijze bij een inbreuk op de beveiliging.</p> <p>Een andere partij is alleen ingeschakeld bij de uitvoering van de verwerking met toestemming van de verwerkingsverantwoordelijke. Aan deze andere verwerker (sub verwerker) is bij een overeenkomst dezelfde verplichtingen inzake gegevensbescherming opgelegd.</p>	De afdeling Sociale recherche maakt geen gebruik van applicaties van derden. Gegevens worden opgeslagen op netwerkschijven gehost bij de IRvN. Het is niet bekend of hier een verwerkersovereenkomst mee is afgesloten.	Voldoet

#	Onderwerp	Verwijzing Wpg	Beheersingsmaatregelen	Bevindingen	Conclusies / Aanbevelingen
14	Geheimhoudingsplicht	Art 7	Er is geborgd dat de ambtenaar van politie of de persoon aan wie politiegegevens ter beschikking zijn gesteld formeel bekend is met de plicht tot geheimhouding en de consequenties bij schending van deze plicht.	<p>De organisatie heeft een procedure indienst waarin een VOG wordt vereist en aandacht aan privacy wordt besteed. Iedere medewerker moet een geheimhoudingsverklaring tekenen als onderdeel van de arbeidsovereenkomst. Daarnaast heeft de organisatie intern diverse activiteiten ter bevordering van bewustwording en geheimhouding en is de organisatie bezig om een specifieke e-learning voor de Wpg te implementeren.</p> <p>De generieke bewustwordingsactiviteiten op het gebied van informatiebeveiliging en privacy zijn beschreven in een bewustwordingsplan. Over de uitvoering wordt sinds dit jaar (auditplan IB) gerapporteerd. De eerste rapportage volgt aan het einde van dit jaar (over het jaar 2022).</p>	<p>Voldoet deels</p> <p>Wij adviseren om de uitgevoerde activiteiten rondom bewustwording en geheimhouding verder te beschrijven en de uitvoering hiervan aantoonbaar vast te leggen.</p>
15	Geautomatiseerde individuele besluitvorming	Art 7a	<p>Besluiten die uitsluitend zijn gebaseerd op geautomatiseerde verwerking die voor de betrokkene nadelige rechtsgevolgen (kunnen) hebben of hem in aanmerkelijke mate treft, worden niet genomen tenzij voorzien is in de voorwaarden genoemd in de wet.</p> <p>Het verbod op het gebruik van profilering dat leidt tot discriminatie van personen op grond van de bijzondere categorieën van politiegegevens (art 5) is bekend binnen de organisatie. Dit beperkte verbod op profilering is onderwerp van de bewustwordingssessies binnen de organisatie.</p>	Niet van toepassing.	Niet van toepassing.

#	Onderwerp	Verwijzing Wpg	Beheersingsmaatregelen	Bevindingen	Conclusies / Aanbevelingen
16	Uitvoering van de dagelijkse politietaak	Art 8 lid 1 en 2	<p>Geborgd is dat art 8 politiegegevens één jaar na de datum van de eerste verwerking zodanig worden opgeslagen (achter een schot worden geplaatst) dat ze alleen nog beschikbaar komen voor verdere verwerking op basis van de vergelijking van gegevens (hit-no-hit basis).</p> <p>Geborgd is voor zover dat noodzakelijk is met het oog op de uitvoering van de dagelijkse politietaak politiegegevens ten aanzien waarvan in art 8 lid 1 genoemde termijn is verstreken geautomatiseerd worden vergeleken met politiegegevens die worden verwerkt op grond van art 8 lid 1 teneinde vast te stellen of verbanden bestaan tussen de betreffende gegevens. De gerelateerde gegevens kunnen verder worden verwerkt met het oog op de uitvoering van de dagelijkse politietaak.</p>	Niet van toepassing.	Niet van toepassing.
17	Ter beschikking stellen van politiegegevens binnen het Wpg-domein	Art 4 lid 1 Art 8 lid 4 Art 9 lid 3 Art 15 lid 1 en 2 Art 15a lid 1 en 2	<p>Geborgd is dat de verdere verwerking van art 9 gegevens alleen plaats vindt na toestemming (aantoonbaar) van de daartoe bevoegde functionaris.</p> <p>Geborgd is dat de 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 art 1, onderdeel a conform de richtlijnen gesteld in de wet plaatsvindt.</p>	De organisatie verwerkt mogelijk gegevens onder grondslag artikel 9. Een bevoegd functionaris is aangewezen (maar nog niet bekrachtigd, zie norm 11).	Voldoet

#	Onderwerp	Verwijzing Wpg	Beheersingsmaatregelen	Bevindingen	Conclusies / Aanbevelingen
18	Geautomatiseerd vergelijken en in combinatie zoeken	Art 11 lid 1, 3, 4 en 5 Art 8 lid 3 Art 2:1 en 2:2 lid 1 Bpg	<p>Geborgd is dat gegevens alleen geautomatiseerd worden vergeleken met andere politiegegevens of met andere dan politiegegevens binnen de richtlijnen gesteld in art 11.</p> <p>Geborgd is dat gegevens alleen in combinatie met elkaar worden verwerkt binnen de richtlijnen gesteld in art 11 lid 4.</p> <p>Geborgd is dat het in combinatie verwerken van art 8 politiegegevens beperkt is tot de ambtenaren van politie die daarvoor geautoriseerd zijn.</p> <p>Geborgd is dat de ambtenaren die geautomatiseerd vergelijken en ambtenaren die in combinatie zoeken over voldoende kennis en vaardigheden beschikken.</p>	Niet van toepassing.	Niet van toepassing.
19	Ondersteunende taken	Art 13	Geborgd is dat voor de verwerkingen bedoeld in art 13 lid 1 t/m 3, van tevoren is voldaan aan de schriftelijke vereisten (art 13 lid 4).	Niet van toepassing.	Niet van toepassing.
20	Bewaartermijnen, verwijderen en vernietigen	Art 4 lid 2 Art 8 lid 6 Art 9 lid 4 Art 14	<p>Politiegegevens worden niet langer bewaard dan de minimale tijd die nodig is, zoals vereist door de toepasselijke wet- en regelgeving, of voor de doeleinden waarvoor deze zijn verwerkt.</p> <p>De verwerkingsverantwoordelijke voorziet in voldoende waarborgen om te bewerkstelligen dat de gegevens conform de wet worden gecontroleerd, verwijderd en vernietigd.</p> <p>Geborgd is dat Politiegegevens na verwijdering maximaal vijf jaar worden bewaard. Indien van cultureel of historisch belang kan worden afgezien van vernietiging van de gegevens. Er wordt dan aan de bewaareisen als genoemd in de Archiefwet voldaan.</p>	De organisatie verwerkt gegevens onder grondslag artikel 9 op netwerkschijven. Op dit moment zijn hier geen maatregelen voor ingericht om te waarborgen dat gegevens kunnen worden verwijderd en daarna vernietigd.	<p>Voldoet niet</p> <p>Wij adviseren om een tweede netwerkschijf waar alleen de bevoegd functionaris toegang toe heeft in te richten waar afgesloten dossiers handmatig naartoe worden verplaatst (en vervolgens na vijf jaar worden vernietigd).</p>

#	Onderwerp	Verwijzing Wpg	Beheersingsmaatregelen	Bevindingen	Conclusies / Aanbevelingen
21	Verstrekking van politiegegevens aan anderen dan politie en Koninklijke marechaussee	Art 16 Art 18 Art 19 Art 21 Art 22 Art 7 lid 1 Art 4	<p>Geborgd is dat politiegegevens alleen worden verstrekt aan personen of instanties buiten het politiedomein, voor zover dit noodzakelijk is voor de doeleinden zoals deze in de Wet politiegegevens en het Besluit politiegegevens zijn genoemd.</p> <p>Geborgd is dat wanneer gegevens verstrekt worden er wordt voldaan aan de documentatieplicht (conform 6 lid 4 Bpg).</p> <p>Geborgd is dat verstrekking alleen plaatsvindt in overeenstemming met het bevoegd gezag indien dit vereist is in de wet.</p> <p>Bij verstrekkingen is geborgd dat de ontvangende partij wordt gewezen op zijn geheimhoudingsplicht.</p> <p>De juistheid, volledigheid, actualiteit en betrouwbaarheid van politiegegevens bij verstrekking wordt, voor zover mogelijk, gecontroleerd en inzichtelijk gemaakt voor de ontvangende partij.</p> <p>Er is een procedure voor het onverwijld in kennis stellen van de ontvanger van politiegegevens indien geconstateerd wordt dat onjuiste politiegegevens zijn verstrekt of dat politiegegevens op onrechtmatig wijze zijn verstrekt.</p>	De organisatie verstrekt gegevens aan diverse partijen (waaronder het OM). De organisatie heeft de verstrekkingen gedocumenteerd een verstrekkingenwijzer waarin is beschreven wanneer aan wie verstrekt kan worden en onder welke voorwaarden.	Voldoet

#	Onderwerp	Verwijzing Wpg	Beheersingsmaatregelen	Bevindingen	Conclusies / Aanbevelingen
22	Doorgiften aan derde landen	Art 17a	<p>De doorgifte van gegevens aan verwerkingsverantwoordelijke in derde landen vindt alleen plaats indien er een adequaatsheidsbesluit is van de Commissie van de Europese Unie of indien één van de uitzonderingsgronden zoals genoemd in de wet van toepassing is.</p> <p>De doorgifte van gegevens aan derde landen wordt vastgelegd (documentatieplicht).</p> <p>Indien doorgifte plaatsvindt op basis van art 17a lid 2 onderdeel a of b, lid 3 of lid 5 is (aantoonbaar) voldaan aan de gestelde eisen in de wet.</p> <p>Indien politiegegevens van een andere lidstaat afkomstig worden doorgegeven aan derde landen is de toestemming van de verantwoordelijke autoriteit van deze lidstaat beschikbaar.</p>	Niet van toepassing.	Niet van toepassing.
23	Verstreking aan derden structureel voor samenwerkingsverbanden	Art 20	<p>De verantwoordelijke heeft inzicht in de samenwerkingsverbanden waarbij politiegegevens worden verstrekt.</p> <p>In de beslissing voor het verstrekken van politiegegevens t.b.v. een samenwerkingsverband wordt vastgelegd:</p> <ul style="list-style-type: none"> • Ten behoeve van welk zwaarwegend algemeen belang de verstreking noodzakelijk is, • Ten behoeve van welk samenwerkingsverband de politiegegevens worden verstrekt, • Het doel waartoe dit is opgericht, • Welke gegevens worden verstrekt, • De voorwaarden onder welke de gegevens worden verstrekt en • Aan welke personen of instanties de gegevens worden verstrekt. <p>De daadwerkelijke verstreking van gegevens wordt vastgelegd.</p>	Niet van toepassing.	Niet van toepassing.

#	Onderwerp	Verwijzing Wpg	Beheersingsmaatregelen	Bevindingen	Conclusies / Aanbevelingen
24	Rechtstreekse verstrekking	Art 23	<p>De organisatie heeft geborgd dat rechtstreekse verstrekking uitsluitend plaatsvindt voor zover noodzakelijk op grond van art 23 en alleen voor zover voldaan kan worden aan de beveiligingseisen.</p> <p>De rechtstreekse verstrekking op basis van art 23 lid 2 vindt alleen plaats aan de aangewezen personen.</p>	Niet van toepassing.	Niet van toepassing.
25	Informatie aan de betrokkene, recht op inzage, rectificatie en verwijdering.	Art 24a lid 1 t/m 4 Art 24b Art 25 Art 26 Art 27 Art 28	<p>De verwerkingsverantwoordelijke biedt de betrokkene informatie over de verwerking van persoonsgegevens en doet dit beknopt, toegankelijk en duidelijk, zodat de betrokkene zijn rechten kan uitoefenen. De informatievoorziening voldoet aan de eisen gesteld in art 24b lid 1 en 2.</p> <p>Bij uitstel, beperking of achterwege laten van de verstrekking van informatie bedoeld in 24b lid 2 is de uitstel, beperking of achterwege laten alsmede de duur van deze maatregel onderbouwd.</p> <p>Verzoeken tot inzage, rectificatie, vernietiging van betrokkenen worden - met inachtneming van het gestelde in artikel 27 - tijdig en adequaat afgehandeld.</p> <p>De organisatie borgt dat bij een verzoek tot inzage (art 25 lid 1) of rectificatie (art 28 lid 1) dat de betrokkene zonder onnodige vertraging in kennis wordt gesteld van de ontvangst van het verzoek, de termijn voor uitsluitel en de mogelijkheid een klacht in te dienen bij de AP.</p> <p>Een weigering gevolg te geven aan het verzoek conform art 24a lid 4 is onderbouwd. Elke weigering of beperking van de inzage wordt aan de betrokkene toegelicht, met vermelding van de feitelijke of juridische gronden die aan het besluit ten grondslag liggen.</p>	De organisatie beschikt over een procedure voor het uitvoeren van rechten van betrokkenen) en een openbare privacyverklaring (in het kader van de Wpg). Vastgesteld dat deze procedure zoals beschreven wordt uitgevoerd.	Voldoet

26	Register	Art 31d lid 1 en 2	<p>De <u>verwerkingsverantwoordelijke</u> houdt een register bij dat de volgende gegevens bevat:</p> <ul style="list-style-type: none"> a) de naam en de contactgegevens van de verwerkingsverantwoordelijke, de gezamenlijk verwerkingsverantwoordelijken en de functionaris voor gegevensbescherming; b) de doelen van de verwerking; c) de categorieën van ontvangers aan wie politiegegevens zijn of zullen worden verstrekt, met inbegrip van ontvangers in derde landen of internationale organisaties; d) een beschrijving van de categorieën van betrokkenen en van de categorieën van persoonsgegevens; e) in voorkomend geval, het gebruik van profilering; f) in voorkomend geval, de categorieën van doorgiften van politiegegevens aan een derde land of een internationale organisatie; g) een aanwijzing van de rechtsgrondslag van de verwerking, met inbegrip van doorgiften, waarvoor de politiegegevens bedoeld zijn; h) zo mogelijk, de beoogde termijnen waarbinnen de verschillende categorieën van gegevens worden verwijderd of vernietigd; i) zo mogelijk, een algemene beschrijving van de technische en organisatorische maatregelen ter beveiliging, bedoeld in artikel 4a; j) de toekenning van de autorisaties, bedoeld in artikel 6. <p>De <u>verwerker</u> houdt een register bij dat de volgende gegevens bevat:</p> <ul style="list-style-type: none"> a) de naam en de contactgegevens van de verwerker of verwerkers en van iedere verwerkingsverantwoordelijke ten behoeve van wie de verwerker handelt en, in voorkomend geval, van de functionaris voor gegevensbescherming; b) de categorieën van verwerkingen die namens iedere verwerkingsverantwoordelijke zijn uitgevoerd; c) indien van toepassing, doorgiften van politiegegevens aan een derde land of een internationale organisatie, 	Zie 1.	Voldoet deels
----	----------	--------------------	--	--------	---------------

#	Onderwerp	Verwijzing Wpg	Beheersingsmaatregelen	Bevindingen	Conclusies / Aanbevelingen
			<p>onder vermelding van dat derde land of die internationale organisatie, indien door de verwerkingsverantwoordelijke uitdrukkelijk daartoe geïnstrueerd</p> <p>d) indien mogelijk, een algemene beschrijving van de technische en organisatorische maatregelen, bedoeld in artikel 4a.</p>		
27	Documentatie	Art 32 lid 1 t/m 4	<p>De verwerkingsverantwoordelijke borgt een volledige en toegankelijke schriftelijke vastlegging (documentatieplicht) van de onderdelen genoemd in art 32 lid 1. De bedoelde politiegegevens worden conform art 32 lid 4 bewaard.</p> <p>De verwerkingsverantwoordelijke borgt een volledige en toegankelijke schriftelijke vastlegging (documentatieplicht) van de doorgifte van politiegegevens aan een verwerkingsverantwoordelijke in een derde land of aan een internationale organisatie.</p> <p>De schriftelijke melding van een gemeenschappelijke verwerking van politiegegevens aan de AP is geborgd.</p>	<p>De organisatie registreert de gevraagde gegevensverzamelingen op de volgende locaties:</p> <ol style="list-style-type: none"> 1. Verstrekkingen: zie 21. 2. Artikel 9 doeleinden: in het dossier; 3. Datalekken: zie 30. 4. Weigeringen van inzageverzoeken: zie 25. 	Voldoet deels

#	Onderwerp	Verwijzing Wpg	Beheersingsmaatregelen	Bevindingen	Conclusies / Aanbevelingen
28	Logging	Art 32a	<p>De verwerkingsverantwoordelijke en de verwerker dragen zorg voor de logging van verwerkingen zoals opgenomen in art 32a lid 1.</p> <p>De organisatie gebruikt de logging uitsluitend ter controle van de rechtmatigheid van de gegevensverwerkingen, interne controles, ter waarborging van de integriteit en de beveiliging van politiegegevens en voor strafrechtelijke procedures.</p>	<p>Vastgesteld dat Wpg gegevens op netwerkschijven worden opgeslagen. Vastgesteld dat logging op deze schijven momenteel ontbreekt.</p> <p>De organisatie heeft als gevolg van het ontbreken van adequate logging nog geen controleproces ingericht waarmee de rechtmatigheid van het gebruik van Wpg gegevens wordt gecontroleerd.</p>	<p>Voldoet niet</p> <p>Wij adviseren om na te gaan of Wpg gegevens op netwerkschijven noodzakelijk is en indien mogelijk deze op te schonen. Indien het gebruik van netwerkschijven onvermijdelijk is, adviseren wij om de logging met IRvN te implementeren.</p> <p>Daarnaast adviseren wij een controleproces te beschrijven en in te richten, deze controles uit te voeren en te rapporten aan de eindverantwoordelijke. Wij adviseren hierbij om te focussen op atypische verwerkingen en uitzonderingen.</p>
29	Audits	Art 33	Er wordt uitvoering gegeven aan de eisen zoals gesteld in de Regeling Periodieke Audit politiegegevens.	De organisatie heeft een eigen interne auditor aangesteld die opgeleid wordt in samenwerking met een externe partij. De interne audit in 2022 is uitgevoerd door de interne auditor met de externe partij.	<p>Voldoet deels</p> <p>Wij adviseren om voor de komende jaren voldoende capaciteit te borgen om de interne audit functie goed te beleggen in de organisatie.</p>

#	Onderwerp	Verwijzing Wpg	Beheersingsmaatregelen	Bevindingen	Conclusies / Aanbevelingen
30	Melding datalekken	Art 33a	<p>De organisatie detecteert en behandelt privacy gerelateerde incidenten op gepaste wijze om de gevolgen te beperken en maatregelen te nemen om toekomstige inbreuken te voorkomen.</p> <p>De verantwoordelijkheden van de behandeling van datalekken zijn belegd in de organisatie, de daadwerkelijke uitvoering wordt beheerst, gedocumenteerd en geëvalueerd.</p> <p>De melding van een datalek aan de AP vindt tijdig en volledig plaats.</p> <p>Betrokkenen worden, indien vereist, tijdig en volledig in kennis gesteld van een inbreuk op de beveiliging als deze inbreuk waarschijnlijk een hoog risico voor hun rechten en vrijheden betekent.</p>	Vastgesteld dat de gemeente over een procedure datalekken beschikt (ook van toepassing op Wpg) en een register bijhoudt. Vastgesteld dat de procedure zoals beschreven wordt uitgevoerd.	Voldoet

#	Onderwerp	Verwijzing Wpg	Beheersingsmaatregelen	Bevindingen	Conclusies / Aanbevelingen
31	Functionaris voor gegevensbescherming	Art 36	<p>Er is een functionaris voor gegevensbescherming aangesteld die toezicht houdt op:</p> <ul style="list-style-type: none"> o het naleven van de Wpg; o het beleid van de verwerkingsverantwoordelijke met betrekking tot de bescherming van persoonsgegevens; o de toewijzing van de autorisaties, bedoeld in art 6; o de bewustmaking en opleiding van de ambtenaren van politie betrokken bij de verwerking van politiegegevens; o de audits; o de uitvoering van de DPIA's. <p>De FG stelt jaarlijks een verslag op van zijn bevindingen en stelt het ter beschikking aan de verwerkingsverantwoordelijke.</p> <p>De functionaris voor gegevensbescherming is aangemeld bij de Autoriteit Persoonsgegevens en de contactgegevens van de FG zijn openbaar gemaakt.</p>	Vastgesteld dat de gemeente een FG heeft aangesteld. Vastgesteld dat de FG jaarlijks toezicht houdt op diverse onderdelen. Toezicht houden op de Wpg is nog in opzet, mede door het ontbreken van DPIA's op Wpg verwerkingen.	<p>Voldoet deels</p> <p>Wij adviseren om het toezicht op naleving van de Wpg verder te ontwerpen en te implementeren.</p>

3.5 Detailbevindingen en aanbevelingen (technische en organisatorische beheersingsmaatregelen)

#	Onderwerp	Beheersingsmaatregelen	Testwerkzaamheden / Bevindingen	Conclusies / Aanbevelingen
1	Wijzigingenbeheer	<p>Wijzigingenbeheer is procesmatig en procedureel zodanig uitgevoerd dat wijzigingen in de ICT-voorzieningen van webapplicaties tijdig, geautoriseerd en getest worden doorgevoerd.</p> <p>Doelstelling: Zeker stellen dat wijzigingen op een correcte en gecontroleerde wijze worden doorgevoerd waardoor de veilige werking van ICT-voorziening wordt gegarandeerd.</p> <p>Scope: Applicatie-, hosting (verwerker)- of SAAS leverancier van de Wpg-geclassificeerde verwerkende systemen.</p>	Het beheer van de netwerkschijven ligt bij de IRvN. Wij hebben op basis van interview vastgesteld dat de gemeente een procedure heeft voor dit onderwerp. Bestaan en werking hebben wij niet kunnen vaststellen.	<p>Voldoet niet</p> <p>Wij adviseren om bij de hercontrole de IRvN in detail mee te nemen in de audit en om afspraken rondom uitbesteed beheer helder te krijgen.</p>
2	Logische toegangsbeveiliging	<p>De inzet van identiteit- en toegangsmiddelen levert betrouwbare en effectieve mechanismen voor het vastleggen en vaststellen van de identiteit van gebruikers, het toekennen van de rechten aan gebruikers, het controleerbaar maken van het gebruik van deze middelen en het automatiseren van arbeidsintensieve taken.</p> <p>Doelstelling: Het efficiënter maken van het identiteit- en toegangsbeheer en zorgen dat functies en gegevens uitsluitend beschikbaar worden gesteld aan diegenen waarvoor deze bedoeld zijn als waarborg voor vertrouwelijkheid en integriteit.</p> <p>Scope: Hosting, leverancier van de Wpg-geclassificeerde verwerkende systemen.</p>	Het beheer van de netwerkschijven ligt bij de IRvN. Wij hebben op basis van interview vastgesteld dat de gemeente een procedure heeft voor dit onderwerp. Bestaan en werking hebben wij niet kunnen vaststellen.	<p>Voldoet niet</p> <p>Wij adviseren om bij de hercontrole de IRvN in detail mee te nemen in de audit en om afspraken rondom uitbesteed beheer helder te krijgen.</p>

#	Onderwerp	Beheersingsmaatregelen	Testwerkzaamheden / Bevindingen	Conclusies / Aanbevelingen
3	Beheer van kwetsbaarheden (patchmanagement)	<p>Informatie over technische kwetsbaarheden van informatiesystemen die worden gebruikt behoort tijdig te worden verkregen, de blootstelling van de organisatie aan dergelijke kwetsbaarheden te worden geëvalueerd en passende maatregelen te worden genomen om het risico dat ermee samenhangt aan te pakken.</p> <p>Doelstelling: Zeker stellen dat technische en software kwetsbaarheden tijdig en effectief worden aangepakt en zo een stabiele omgeving wordt gecreëerd.</p> <p>Scope: Hosting, leverancier van de Wpg-geclassificeerde verwerkende systemen.</p>	Het beheer van de netwerkschijven ligt bij de IRvN. Wij hebben op basis van interview vastgesteld dat de gemeente een procedure heeft voor dit onderwerp. Bestaan en werking hebben wij niet kunnen vaststellen.	<p>Voldoet niet</p> <p>Wij adviseren om bij de hercontrole de IRvN in detail mee te nemen in de audit en om afspraken rondom uitbesteed beheer helder te krijgen.</p>
4	Cryptografie	<p>Ter bescherming van politiegegevens behoort een beleid voor het gebruik van cryptografische beheersmaatregelen te worden ontwikkeld en geïmplementeerd.</p> <p>Doelstelling: Zorgen voor correct en doeltreffend gebruik van cryptografie om de vertrouwelijkheid, authenticiteit en/of integriteit van politiegegevens te beschermen.</p> <p>Scope: Hosting, leverancier van de Wpg-geclassificeerde verwerkende systemen.</p>	Het beheer van de netwerkschijven ligt bij de IRvN. Wij hebben op basis van interview vastgesteld dat de gemeente een procedure heeft voor dit onderwerp. Bestaan en werking hebben wij niet kunnen vaststellen.	<p>Voldoet niet</p> <p>Wij adviseren om bij de hercontrole de IRvN in detail mee te nemen in de audit en om afspraken rondom uitbesteed beheer helder te krijgen.</p>

#	Onderwerp	Beheersingsmaatregelen	Testwerkzaamheden / Bevindingen	Conclusies / Aanbevelingen
5	Vulnerability scans en Penetratietesten	<p>Penetratietesten en vulnerability scans worden procesmatig en procedureel, ondersteund door richtlijnen, uitgevoerd op de infrastructuur van de systemen waarin politiegegevens verwerkt worden.</p> <p>Doelstelling: Het verkrijgen van inzicht in de weerstand die de systemen kunnen bieden aan pogingen om het te compromitteren.</p> <p>Scope: Hosting, leverancier van de Wpg-geclassificeerde verwerkende systemen.</p>	Het beheer van de netwerkschijven ligt bij de IRvN. Wij hebben op basis van interview vastgesteld dat de gemeente een procedure heeft voor dit onderwerp. Bestaan en werking hebben wij niet kunnen vaststellen.	<p>Voldoet niet</p> <p>Wij adviseren om bij de hercontrole de IRvN in detail mee te nemen in de audit en om afspraken rondom uitbesteed beheer helder te krijgen.</p>

Legenda toegepaste uitzonderingsgrondslagen

In dit document zijn gegevens geanonimiseerd op grond van:

Wet	Artikel	Omschrijving	Pagina's
Wet open overheid	Art. 5.1 lid 2 sub e	De eerbiediging van de persoonlijke levenssfeer	4, 6