

**Assurance-rapport
NOREA Richtlijn 3000D**

Hercontrole

o.g.v. artikel 4 Regeling periodieke audit politiegegevens (artikel 6:5, vierde lid
Besluit Politiegegevens en artikel 33 vijfde lid Wet politiegegevens)

Privacy-audit Wet politiegegevens

Gemeente Nijmegen

Uitgebracht door:	2-Control B.V.
Onderzoeker(s):	5.1.2e
Uitgebracht aan:	Gemeente Nijmegen
Contactpersoon:	5.1.2e
Datum:	30 maart 2023
Rapportnummer:	2C-2023-479
Versie:	1.0
Status:	Definitief

Versiebeheer

Versie	Datum	Status	Naam
0.1	29-3-2023	Gereed voor OKB	2-Control B.V.
0.2	30-3-2023	Conceptversie voor management reactie	2-Control B.V.
1.0	30-3-2023	Definitieve versie	2-Control B.V.

Inhoud

1	Assurance-rapport van de onafhankelijke auditor	5
1.1	Opdracht	5
1.2	Object van onderzoek	5
1.3	Scope	6
1.4	Verantwoordelijkheden Gemeente Nijmegen	6
1.5	Onze onafhankelijkheid en kwaliteitsbeheersing	6
1.6	Verantwoordelijkheden van de auditor	7
1.7	Gehanteerde criteria	7
1.8	Overige informatie verstrekt door Gemeente Nijmegen	7
1.9	Beperkingen	7
1.10	Ons oordeel met beperking	8
1.11	De basis voor ons oordeel met beperking	8
1.12	Beperkingen in gebruik en verspreidingskring	13
2	Beschrijving privacy-doelstellingen	14
3	Overige informatie Gemeente Nijmegen	20
3.1	Inleiding	20
3.2	Overige informatie	20
4	Bijlage 1 – Beschrijving van de beheersingsmaatregelen en testresultaten (Wpg beheersingsmaatregelen)	22
5	Bijlage 2 – Beschrijving van de beheersingsmaatregelen en testresultaten (technische en organisatorische beheersingsmaatregelen)	32

Colofon

Voor u ligt het assurance-rapport inzake de hercontrole van de externe privacy audit op de politiegegevens die de buitengewoon opsporingsambtenaren (boa's) van Gemeente Nijmegen verwerken en die in een bestand zijn opgenomen, of die bestemd zijn daarin te worden opgenomen. Deze verwerkingen vallen onder de reikwijdte van de Wet politiegegevens (Wpg) en het Besluit politiegegevens voor buitengewoon opsporingsambtenaren (Bpgboa). Dit rapport is gebaseerd op de NOREA Handreiking Privacy audit Wpg voor boa's, versie 1.0 d.d. 24 juni 2021, de Richtlijn 3000D van de NOREA (Assurance-opdrachten door IT-auditors) en is opgesteld door 2-Control B.V. In dit rapport zijn de door ons vastgestelde bevindingen, conclusies en aanbevelingen beschreven.

Ons rapport wordt uitgebracht in twee versies: Het 'short form' rapport bevat de basiselementen en is bedoeld voor de toezichthouder. Het 'long form' rapport bevat in Bijlagen 1 en 2 aanvullende informatie die in beginsel uitsluitend bedoeld is voor Gemeente Nijmegen, zoals een overzicht van de getoetste interne beheersmaatregelen en de door ons vastgestelde bevindingen en aanbevelingen. Het voorliggende rapport is de 'long form' versie van ons rapport.

1 Assurance-rapport van de onafhankelijke auditor

Aan het college van B&W van Gemeente Nijmegen
Korte Nieuwstraat 6
6511 PP Nijmegen

Referentie: 2C-2023-479

1.1 Opdracht

Ingevolge de opdracht van Gemeente Nijmegen hebben wij een hercontrole uitgevoerd naar de opzet en het bestaan van de beheersingsmaatregelen die in het privacy audit rapport 2C-2022-336 van 2-Control B.V. als 'voldoet deels' of 'voldoet niet' zijn beoordeeld.

In de Wpg en het Bpgboa zijn vereisten en regels opgenomen voor het verwerken van persoonsgegevens die nodig zijn om de opsporing van strafbare feiten rechtmatig te kunnen uitvoeren. De wetgever heeft met de Wpg een evenwicht aangebracht tussen de belangen die met het uitvoeren van de opsporing van strafbare feiten gemoeid zijn en het beschermen van de privacy van burgers.

Om te kunnen beoordelen of dit evenwicht wordt gehandhaafd, is in artikel 33 van de Wpg bepaald dat de verwerkingsverantwoordelijke voor het verwerken van politiegegevens periodiek, door middel van het uitvoeren van audits door een onafhankelijke auditor, moet laten vaststellen of de bij of krachtens deze wet gegeven regels worden nageleefd. Een dergelijke controle moet volgens de Regeling periodieke audit politiegegevens twee jaar na inwerkingtreding van de wet en vervolgens elke vier jaar plaatsvinden. In artikel 33 lid 3 is bepaald dat indien uit de controleresultaten blijkt dat niet wordt voldaan aan het bij of krachtens de Wet politiegegevens bepaalde, de verwerkingsverantwoordelijke binnen een jaar een onafhankelijke hercontrole uit laat voeren op die onderdelen die niet voldeden aan de gestelde voorwaarden. In het externe auditrapport is aangegeven dat de externe auditor de hercontrole zou moeten uitvoeren.

De verwerkingsverantwoordelijke zendt een afschrift van de hercontrolerapport aan de Autoriteit Persoonsgegevens.

Gemeente Nijmegen maakt gebruik van serviceorganisaties Sigmax, Brickyard en MetaObjects voor het beheer en onderhoud van de applicaties waarin Wpg gegevens worden verwerkt en van ICT Rijk van Nijmegen (IRvN) voor het beheer en onderhoud van netwerkschijven en het zaakstelsel. Een deel van de beheersingsdoelstellingen kunnen enkel worden gerealiseerd door, of in samenhang met, interne beheersingsmaatregelen bij deze serviceorganisaties. Wij hebben bij onze werkzaamheden gebruik gemaakt van de uitsluitingmethode ('carve-out method'). Onze werkzaamheden strekken zich dan ook niet uit tot de interne beheersingsmaatregelen van deze serviceorganisaties.

1.2 Object van onderzoek

Deze hercontrole heeft alleen betrekking op het onderdeel of de onderdelen van de wet ten aanzien waarvan tekortkomingen zijn geconstateerd tijdens het initiële onderzoek, zoals vastgelegd in het initiële externe auditrapport 2C-2022-336 d.d. 30 maart 2022 van 2-Control B.V. en heeft tot doel op systematische wijze te toetsen of door de verantwoordelijke zodanige maatregelen zijn getroffen dat aan de uitvoering van het onderdeel of de betreffende onderdelen van de wet thans op adequate wijze uitvoering is gegeven.

1.3 Scope

De scope van ons onderzoek 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, Netwerkschijf, C1 (Brickyard), Scanauto (ACI)
2	Leerplicht	III	Opsporing strafbare feiten met betrekking tot de leerplichtwet	JVS
3	Sociale Recherche	V	Opsporing strafbare feiten met betrekking tot de Wet maatschappelijke ondersteuning (Wmo)	Netwerkschijf

Wij hebben uitsluitend onderzoek uitgevoerd naar de bij de initiële privacy audit als ‘deels’ of ‘niet voldoende’ in opzet en bestaan beoordeelde beheersingsmaatregelen. Wij hebben geen onderzoek gedaan naar de bij de initiële audit niet beoordeelde normen en doen daar derhalve ook geen uitspraak over. Tevens doen wij geen uitspraak over de werking van de gerealiseerde verbetermaatregelen¹.

1.4 Verantwoordelijkheden Gemeente Nijmegen

Gemeente Nijmegen is verantwoordelijk voor de opzet en het bestaan van de aanvullende beheersingsmaatregelen om alsnog te kunnen voldoen aan het bij of krachtens de Wpg bepaalde binnen een jaar na de initiële externe privacy audit.

Gemeente Nijmegen is ook verantwoordelijk om binnen drie maanden na afronding van de initiële externe privacy audit een verbeterrapport op te stellen waarin de maatregelen worden beschreven die getroffen zijn ter verbetering van de geconstateerde tekortkomingen. Tijdens de hercontrole wordt beoordeeld of een verbeterrapport (verbeterplan) is opgesteld om de verbeteringen op te stellen.

1.5 Onze onafhankelijkheid en kwaliteitsbeheersing

Wij hebben de vereisten van het Reglement Gedragscode (‘Code of Ethics’) van NOREA nageleefd, welke is gebaseerd op de fundamentele beginselen van integriteit, objectiviteit, vakbekwaamheid en zorgvuldigheid, vertrouwelijkheid en professioneel gedrag.

Wij passen het Reglement Kwaliteitsbeheersing NOREA (RKBN) toe en bijgevolg onderhouden wij een uitgebreid systeem van kwaliteitscontrole met inbegrip van gedocumenteerd beleid en de procedures met betrekking tot de naleving van de ethische voorschriften, professionele standaarden en de van toepassing zijnde wet- en regelgeving.

Wij voldoen aan de specifieke vereisten voor de uitvoering van de externe privacy audit, zoals bepaald in artikel 5 van de Regeling periodieke audit politiegegevens².

¹ De hercontrole heeft in beginsel alleen betrekking op opzet en bestaan, omdat de tijdspanne om een gewogen oordeel te geven over de werking in veel gevallen te kort zal zijn.

² Zie hiervoor de Regeling van de Minister van Justitie, de Minister van Binnenlandse Zaken en de Minister van Defensie van 9 december 2008, nr. 5578598/08, houdende nadere regels ten aanzien van het toezicht op de naleving van de bij of krachtens de Wet politiegegevens gegevens voorschriften (Regeling periodieke audit politiegegevens).

1.6 Verantwoordelijkheden van de auditor

Wij hebben onze opdracht uitgevoerd in overeenstemming met de Richtlijn 3000D (Herzien) 'Assurance-opdrachten door IT-auditors' van NOREA.

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

De werkzaamheden zijn afhankelijk van de door de IT-auditor toegepaste professionele oordeelsvorming en bestonden uit een combinatie van inspectie van documentatie, het houden van interviews, het evalueren van de resultaten van de uitgevoerde interne controles en het verrichten van eigen (aanvullende) testwerkzaamheden. Onze bevindingen zijn opgenomen in de bijlagen 1 en 2.

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

1.7 Gehanteerde criteria

De (generieke) algehele beheersingsdoelstelling voor de privacy audit Wpg voor boa's is het voorzien in de borging van de wettelijke eisen met betrekking tot de verwerking van politiegegevens door boa's. Hiertoe heeft de organisatie beheersingsmaatregelen getroffen die in opzet en bestaan door de IT-auditor worden getoetst. De IT-auditor maakt bij deze hercontrole gebruik van de volgende criteria:

Opzet	De organisatie heeft de beheersingsmaatregelen beschreven die, indien deze werken zoals beschreven, een redelijke mate van zekerheid bieden dat voorzien is aan 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.

1.8 Overige informatie verstrekt door Gemeente Nijmegen

De informatie uit hoofdstuk 3 met de titel "Overige informatie Gemeente Nijmegen" is opgenomen door Gemeente Nijmegen om additionele informatie te verschaffen. Deze informatie is geen onderdeel van ons onderzoek en wij brengen daarover geen oordeel tot uitdrukking.

1.9 Beperkingen

Zoals hierboven staat vermeld, hebben wij bij deze hercontrole geen werkzaamheden uitgevoerd met betrekking tot de werking van de interne beheersmaatregelen die binnen de scope van ons onderzoek vallen. Wij achten de periode waarin de onderzochte beheersingsmaatregelen effectief hebben gewerkt daarvoor te kort. Wij brengen derhalve daarover geen oordelen tot uitdrukking.

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

Bovendien is de projectie van oordelen naar de toekomst onderhevig aan het risico dat interne beheersmaatregelen ineffectief kunnen worden.

1.10 **Ons oordeel met beperking**

Naar ons oordeel, uitgezonderd de aangelegenheden die hierna zijn beschreven in paragraaf 1.11 'De basis voor ons oordeel met beperking', zijn de door de Gemeente Nijmegen getroffen beheersingsmaatregelen om te voorzien in de borging van de wettelijke eisen met betrekking tot de verwerking van politiegegevens door boa's, in alle van materieel belang zijnde aspecten, op afdoende wijze opgezet en bestaan deze per 1 maart 2023.

Ons oordeel is gevormd op basis van de aangelegenheden die in dit assurance-rapport zijn uiteengezet. De specifieke, getoetste beheersingsmaatregelen en de aard, timing en resultaten van die toetsingen zijn opgenomen in Bijlage 1 – Beschrijving van de beheersingsdoelstellingen, beheersmaatregelen en testresultaten (Wpg) en Bijlage 2 - Beschrijving van de beheersingsdoelstellingen, beheersmaatregelen en testresultaten (technische en organisatorische maatregelen).

1.11 **De basis voor ons oordeel met beperking**


Wij hebben de hiernavolgende beheersingsmaatregelen, die tijdens de initiële privacy audit als 'voldoet deels' of 'voldoet niet' zijn beoordeeld, opnieuw beoordeeld. Tijdens deze hercontrole hebben wij vastgesteld dat de hiernavolgende Wpg onderwerpen niet (rood) of niet geheel (oranje) zijn opgezet en / of bestaan.


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


Ons oordeel is gevormd op basis van de aangelegenheden die in dit assurance-rapport zijn uiteengezet. Wij hebben geconstateerd dat door Gemeente Nijmegen niet tijdig (dat wil zeggen binnen drie maanden na de initiële privacy audit) een verbeterrapport is opgesteld.

Omdat binnen Gemeente Nijmegen meerdere verwerkingen van politiegegevens plaatsvinden, waarbij de oordelen per onderwerp onderling afwijken, hebben we ons oordeel per verwerking weergegeven.

Toelichting gebruikte kleuren:

 **Groen** - Voldoet aan de beheersingsmaatregel.

 **Oranje** - Voldoet deels aan de beheersingsmaatregel. Om geheel aan de beheersingsmaatregel te voldoen dien(t)(en) de aanbeveling(en) te worden opgevolgd.

 **Rood** - Voldoet niet aan de beheersingsmaatregel.

 **Grijs** – Niet onderzocht.

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

*) Bestaan bij betreffende norm niet kunnen toetsen wegens non-occurrence

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

***) Norm niet in scope voor hercontrole

Domein I: Opsporing strafbare feiten in domein I (openbare ruimte)

Onderwerpen	Initiële audit			Hercontrole	
	Opzet	Bestaan	Werking	Opzet	Bestaan
1. Reikwijdte (***)					
2. Doelbinding					
3. Noodzakelijkheid & rechtmatigheid, vermelding herkomst					
4. Juistheid en volledigheid politiegegevens					
5. Onderscheid feiten en persoonlijk 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 (***)					
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	Initiële audit			Hercontrole	
	Opzet	Bestaan	Werking	Opzet	Bestaan
1. Wijzigingenbeheer					

Technische en organisatorische maatregelen	Initiële audit			Her-controlle	
	Opzet	Bestaan	Werking	Opzet	Bestaan
2. Logische toegangsbeveiliging					
3. Beheer van kwetsbaarheden (patchmanagement)					
4. Cryptografie					
5. Vulnerability scans en Penetratietesten					

Domein III: Opsporing strafbare feiten met betrekking tot de leerplichtwet

Onderwerpen	Initiële audit			Her-controlle	
	Opzet	Bestaan	Werking	Opzet	Bestaan
1. Reikwijdte (***)					
2. Doelbinding					
3. Noodzakelijkheid & rechtmatigheid, vermelding herkomst					
4. Juistheid en volledigheid politiegegevens					
5. Onderscheid feiten en persoonlijk 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 (***)					
25. Informatie aan de betrokkene, recht op inzage, rectificatie en verwijdering. (***)					
26. Register (***)					
27. Documentatie					

Onderwerpen	Initiële audit			Her-controle	
	Opzet	Bestaan	Werking	Opzet	Bestaan
28. Logging					
29. Audits					
30. Melding datalekken (***)					
31. Functionaris voor gegevensbescherming					

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

Domein V: Opsporing strafbare feiten met betrekking tot de Wmo

Onderwerpen	Initiële audit			Her-controle	
	Opzet	Bestaan	Werking	Opzet	Bestaan
1. Reikwijdte (***)					
2. Doelbinding					
3. Noodzakelijkheid & rechtmatigheid, vermelding herkomst					
4. Juistheid en volledigheid politiegegevens					
5. Onderscheid feiten en persoonlijk 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					

Onderwerpen	Initiële audit			Hercontrole	
	Opzet	Bestaan	Werking	Opzet	Bestaan
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 (***)					
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	Initiële audit			Hercontrole	
	Opzet	Bestaan	Werking	Opzet	Bestaan
1. Wijzigingenbeheer					
2. Logische toegangsbeveiliging					
3. Beheer van kwetsbaarheden (patchmanagement)					
4. Cryptografie					
5. Vulnerability scans en Penetratietesten					

1.12 Beperkingen in gebruik en verspreidingskring

Gemeente Nijmegen dient ingevolge artikel 33 2e lid van de Wpg een afschrift van de controleresultaten van deze hercontrole aan de Autoriteit persoonsgegevens te zenden. In eerste instantie betreft dit het 'short form' rapport (rapport exclusief bijlagen). De Autoriteit persoonsgegevens kan, in het kader van haar toezichthoudende taak, het 'long form' rapport (rapport inclusief bijlagen) zonder opgaaf van redenen bij Gemeente Nijmegen opvragen. Voor de verstrekking van beide rapportages geldt als voorwaarde dat de rapportage origineel, volledig en ongewijzigd ter inzage wordt aangeboden.

Het is, zonder onze uitdrukkelijke voorafgaande schriftelijke toestemming, niet toegestaan de rapportages met anderen dan de Autoriteit persoonsgegevens te delen. Het verstrekken van deze toestemming kan omgeven zijn met nadere voorwaarden. Het is niet toegestaan deze rapportage te gebruiken in juridische conflicten tussen gemeente Nijmegen en andere (rechts)personen.

Breda, 30 maart 2023

30 Mar 2023 16:15 +0200

Breda

5.1.2e
QUALIFIED SIGNATURE

2-Control B.V.

5.1.2e

2 Beschrijving privacy-doelstellingen

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
<p>1. Reikwijdte De verwerkingsverantwoordelijke heeft bestanden met politiegegevens binnen de organisatie geïdentificeerd en gedocumenteerd.</p>
<p>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.</p>
<p>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.</p>
<p>4. Juistheid en volledigheid politiegegevens</p> <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.
<p>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.</p>
<p>6. Gegevensbescherming door beveiliging en ontwerp</p> <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.
<p>7. Gegevensbescherming door standaardinstellingen De verwerkingsverantwoordelijke treft passende technische en organisatorische maatregelen om te waarborgen dat standaard:</p> <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
<p>8. Gegevensbeschermings-effectbeoordeling / Data protection impact assessment (DPIA)</p> <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.
<p>9. Bijzondere categorieën van politiegegevens</p> <p>Er vindt geen verwerking van bijzondere categorieën van politiegegevens plaats, tenzij:</p> <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.
<p>10. Autorisaties en toegang tot politiegegevens</p> <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.
<p>11. Autorisaties: aanwijzen functionarissen</p> <p>Er is een actuele lijst van, door de verwerkingsverantwoordelijke aangewezen, bevoegde functionarissen.</p>
<p>12. Onderscheid tussen verschillende categorieën van betrokkenen</p> <p>De verwerkingsverantwoordelijke heeft geborgd dat, voor zover mogelijk, duidelijk onderscheid wordt gemaakt in de verschillende categorieën van betrokkenen.</p>
<p>13. Verwerker en Verwerkersovereenkomst</p> <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 handelwijze 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.
<p>14. Geheimhoudingsplicht</p> <p>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>

Onderwerpen en beheersingsmaatregelen
<p>15. Geautomatiseerde individuele besluitvorming</p> <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.
<p>16. Uitvoering van de dagelijkse politietaak</p> <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 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>17. Ter Beschikking stellen (voor verdere verwerking)</p> <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.
<p>18. Geautomatiseerd vergelijken en in combinatie zoeken</p> <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.
<p>19. Ondersteunende taken</p> <p>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).</p>
<p>20. Bewaartermijnen, verwijderen en vernietigen</p> <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

21. Verstrekking van politiegegevens aan anderen dan politie en Koninklijke marechaussee

- 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 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.

22. Doorgiften aan derde landen

- 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.

23. Verstrekking aan derden structureel voor samenwerkingsverbanden

- 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:
 - 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.

24. Rechtstreekse verstrekking

- 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
<p>25. Informatie aan de betrokkene, recht op inzage, rectificatie en verwijdering</p> <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.
<p>26. Register</p> <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.
<p>27. Documentatie</p> <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.
<p>28. Logging</p> <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.
<p>29. Audits</p> <p>Er wordt uitvoering gegeven aan de eisen zoals gesteld in de Regeling periodieke audit politiegegevens.</p>
<p>30. Melding datalekken</p> <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.

De bijlagen van dit rapport zijn vertrouwelijk en uitsluitend bestemd voor Gemeente Nijmegen.

3 Overige informatie Gemeente Nijmegen

3.1 Inleiding

De informatie is opgenomen door Gemeente Nijmegen om additionele informatie te verschaffen. Deze informatie is geen onderdeel van het onderzoek door 2-Control B.V. en zij brengen daarover geen oordeel tot uitdrukking.

3.2 Overige informatie

Wij herkennen ons in het 'oordeel met beperkingen', zoals weergegeven in tabel 1.11 voor de drie onderzochte domeinen:

- Domein I: Opsporing strafbare feiten in domein I (openbare ruimte);
- Domein III: Opsporing strafbare feiten met betrekking tot de leerplichtwet;
- Domein V: Opsporing strafbare feiten met betrekking tot de Wmo;

De externe auditeur '2-Control B.V.' stelt in haar rapportage:

Ons oordeel met beperking

Naar ons oordeel, uitgezonderd de aangelegenheden die hierna zijn beschreven in paragraaf 1.11 'De basis voor ons oordeel met beperking', in alle van materieel belang zijnde aspecten, zijn de door de Gemeente Nijmegen getroffen beheersingsmaatregelen om te voorzien in de borging van de wettelijke eisen met betrekking tot de verwerking van politiegegevens door boa's op afdoende wijze opgezet en bestaan deze per 1 maart 2023.

Ons oordeel is gevormd op basis van de aangelegenheden die in dit assurance-rapport zijn uiteengezet. De specifieke, getoetste beheersingsmaatregelen en de aard, timing en resultaten van die toetsingen zijn opgenomen in Bijlage 1 – Beschrijving van de beheersingsdoelstellingen, beheersmaatregelen en testresultaten (Wpg) en Bijlage 2 - Beschrijving van de beheersingsdoelstellingen, beheersmaatregelen en testresultaten (technische en organisatorische maatregelen).

De basis voor ons oordeel met beperking

Wij hebben de hiernavolgende beheersingsmaatregelen, die tijdens de initiële privacy audit als 'voldoet deels' of 'voldoet niet' zijn beoordeeld, opnieuw beoordeeld. Tijdens deze hercontrole hebben wij vastgesteld dat de hiernavolgende Wpg onderwerpen niet (rood) of niet geheel (oranje) zijn opgezet en / of bestaan.

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

Ons oordeel is gevormd op basis van de aangelegenheden die in dit assurance-rapport zijn uiteengezet. Wij hebben geconstateerd dat door Gemeente Nijmegen niet tijdig (dat wil zeggen binnen drie maanden na de initiële privacy audit) een verbeterrapport is opgesteld.

Omdat binnen Gemeente Nijmegen meerdere verwerkingen van politiegegevens plaatsvinden, waarbij de oordelen per onderwerp onderling afwijken, hebben we ons oordeel per verwerking weergegeven.

Streven voor jaarschijf 2023

Wij – vanuit de gemeente Nijmegen - zien in de rapportage de tekortkomingen op de voortgang op - Domein I: Opsporing strafbare feiten in de openbare ruimte. Niettemin zien wij ook de positieve vooruitgang op de overige domeinen en onderschrijven dat. De komende jaarschijf willen wij inzetten op het op orde brengen van de achterstand op - Domein I: Opsporing strafbare feiten in de openbare ruimte waarbij de focus ligt op opzet en bestaan. Niettemin realiseren wij ons de beperkingen van dit streven vanwege de arbeidsmarkt binnen het BOA domein alsmede de personeelsproblematieken binnen het specifieke bureau.

In termen van de gehanteerde kleurscore: groen (voldoet aan de norm) of minimaal geel (voldoet deels aan de norm). Daarnaast willen we het 'bestaan' (streven score 'groen' of in uiterste gevallen minimaal 'geel') en de 'werking' (minimaal 'geel') verbeteren. Uiteindelijk is ons streven om in 2023 zoveel mogelijk 'aan de norm te voldoen' (kleurcode groen), voor zover dat mogelijk is vanuit afhankelijkheid van derde partijen en de personeelsproblematieken zoals hierboven besproken.

Wij zijn voornemens de genoemde aanbevelingen over te nemen voor het kalenderjaar 2023. Inmiddels werken wij met een interne auditor, die begeleid wordt door 2Control. In het voorjaar 2023 willen we de aanbevelingen vanuit deze hercontrole in de organisatie implementeren. Extra aandacht zal hierbij uitgaan naar het domein Opsporing strafbare feiten in de Openbare Ruimte.

4 Bijlage 1 – Beschrijving van de beheersingsmaatregelen en testresultaten (Wpg beheersingsmaatregelen)

In deze bijlage zijn de beheersingsmaatregelen opgenomen zoals die zijn overeengekomen met Gemeente Nijmegen. In de onderstaande tabel hebben wij in de kolom 'Bevindingen' de resultaten van onze werkzaamheden gericht op het vaststellen van de opzet en het bestaan van de beheersingsmaatregelen vastgelegd. In de kolom 'Conclusie en aanbeveling' geven wij aan of aan de criteria voor de opzet en het bestaan wordt voldaan (eventueel) aangevuld met een aanbeveling ter verbetering.

Zoals in paragraaf 1.3 is aangegeven, verwerkt Gemeente Nijmegen politiegegevens in onderstaande domeinen.

#	Organisatieonderdeel	Domein	Processen/verwerkingen	Applicaties
1	Toezicht & Handhaving	I	Opsporing strafbare feiten in domein I (openbare ruimte)	CityControl, Corsa, Netwerkschijf, C1 (Brickyard), Scanauto (ACI)
2	Leerplicht	III	Opsporing strafbare feiten met betrekking tot de leerplichtwet	JVS
3	Sociale Recherche	V	Opsporing strafbare feiten met betrekking tot de Wet maatschappelijke ondersteuning (Wmo)	Netwerkschijf

#	Onderwerp	Verwijzing Wpg	Beheersingsmaatregelen	Testwerkzaamheden / 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>Algemeen</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) [22, 24, 68 t/m 71]. De gemeente is op dit moment de DPIA's voor Wpg verwerkingen aan het afronden (zie 8). Bestaan vastgesteld aan de hand van de jaarrapportage privacy 2022 [21]. Hierin is geconstateerd dat de gemeente sneller en eerder DPIA's moet uitvoeren, dat is nu in gang gezet.</p> <p>Domeinen</p> <p>De domeinen hebben een handboek waarin regels en richtlijnen met betrekking tot doelbinding, noodzakelijkheid, rechtmatigheid, juistheid en volledigheid en onderscheid feiten en persoonlijk oordeel zijn opgenomen. Deze handboeken zijn in opzet akkoord [75]. Bestaan voor Leerrecht vastgesteld aan de hand van diverse voorbeelden [37, 39, 40, 42, 43]. Op</p>	<p>Toezicht & Handhaving: voldoet niet</p> <p>Leerrecht: voldoet</p> <p>Sociale recherche: voldoet</p>

#	Onderwerp	Verwijzing Wpg	Beheersingsmaatregelen	Testwerkzaamheden / Bevindingen	Conclusies / Aanbevelingen
				<p>basis van interview bestaan vastgesteld voor Sociale recherche: beide sociaal rechercheurs die bezig zijn met de onderzoeken (momenteel 2 onderzoeken) lezen en reviewen elkaars onderzoeken.</p> <p>Voor het domein Sociale recherche worden ook artikel 9 verwerkingen uitgevoerd. 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 [75].</p> <p>Voor domein Toezicht & Handhaving opzet en bestaan niet vast kunnen stellen wegens ontbreken van stukken. Door diverse personeelsswisselingen is in dit domein niet of nauwelijks aan verbetermaatregelen gewerkt en is opnieuw begonnen aan de opzet.</p> <p>Bestudeerde documenten: 37: FW 2e lezer 5.1.2e .msg 39: FW 2e lezer PV 5.1.2e .msg 40: FW 2e lezer PV 5.1.2e .msg 42: FW 2e lezer 5.1.2e Luxeverzuim.msg 43: FW tweede lezer proces-verbaal.msg 75: Handboek Wpg sociale recherche Nijmegen 2022_2025 getekend.pdf 21: Jaarrapportage privacy 2022 v1.0.docx 22: Opzet Controlplan FG 2022.docx 24: P31.Uitvoering Controlplan per afdeling.pptx 68: 31.1.Verantwoording uitvoering AVG v2.pptx 69: 31.2. Van aanvraag tot oordeel privacy impact (2).pptx 70: 31.3. Uitvoering Controlplan per afdeling.pptx 71: 31.4.Uitvoering Controlplan FG Bevindingen Naleving.DEF versie 140222.pdf</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.	Toezicht & Handhaving: voldoet niet Leerrecht: voldoet Sociale

#	Onderwerp	Verwijzing Wpg	Beheersingsmaatregelen	Testwerkzaamheden / Bevindingen	Conclusies / Aanbevelingen
					recherche: voldoet
4	Juistheid en volledigheid politiegegevens	Art 4 lid 1	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.	Zie 2.	Toezicht & Handhaving: voldoet niet Leerrecht: voldoet Sociale recherche: voldoet
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.	Toezicht & Handhaving: voldoet niet Leerrecht: voldoet Sociale recherche: voldoet
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.	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 [17, 15]. Vastgesteld dat voor Wpg systemen DPIA's worden uitgevoerd [14, 16, 18, 19, 23] en dat bij de aanschaf van nieuwe systemen adviezen van de privacy officer worden gegeven en uitgevoerd [20, 25]. Bestudeerde documenten: 17: 1. intakeformulier.pdf 15: 2. sjabloon DPIA.docx 14: 3. DPIA's onder beheer 2 - stand mrt 2023.docx 16: DPIA - Dashboard Toezicht (WPG data).pdf 18: DPIA.bodycams.pilot.deel2.pdf 19: DPIA.sociale.recherche.gebruik.accounts.online.onderzoek.pdf 23: DPIA-Pilot.Bodycams.deel1.pdf 20: Intakes - Aanschaf BBM (WPG-veilige chatapp) voor Toezicht...pdf 25: voorbeeld intake Aanschaf bodycams voor Toezicht & handhaving...pdf	Voldoet

#	Onderwerp	Verwijzing Wpg	Beheersingsmaatregelen	Testwerkzaamheden / 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>	<p>Toezicht en handhaving Vastgesteld dat domein bezig is met een handboek en een autorisatiematrix, maar dit is nog niet afgerond voor alle onderdelen. Controle op rechten is nog niet uitgevoerd. Niet-boa's zijn nog niet geautoriseerd middels een verklaring van verantwoordelijke. Hiermee wordt niet voldaan aan deze norm.</p> <p>Leerrecht Vastgesteld op basis van waarneming en interview dat domein een procedure heeft beschreven in het handboek. Vastgesteld dat een opzet voor een autorisatiematrix is gemaakt. Het handboek is momenteel nog in concept (niet vastgesteld) en daarmee voldoet de opzet deels. Bestaan procedure gecontroleerd aan de hand van 2 voorbeelden [41, 44]. Controle op rechten is uitgevoerd [38, 51]. Advies is om de controle uitgebreider te beschrijven. Niet-boa's zijn nog niet geautoriseerd middels een verklaring van verantwoordelijke [53, 55].</p> <p>Sociale recherche Vastgesteld dat domein een procedure heeft beschreven in het handboek inclusief een matrix [75]. Controle op rechten is uitgevoerd door bevoegd functionaris door rechten op te vragen bij de IRvN [58]. Niet-boa's zijn geautoriseerd middels een verklaring van verantwoordelijke [32, 33].</p> <p>Bestudeerde documenten: 38: Export (Medewerkers) (5).xlsx 58: FW Oplossing melding nr M2303 1235.msg 41: FW Stopzetten autorisatie.msg 44: FW VRAAG Account 5.1.2e beëindigen.msg 75: Handboek Wpg sociale recherche Nijmegen 2022_2025 getekend.pdf 33: Modelverklaring autorisatie niet-BOA 5.1.2e .pdf 32: Modelverklaring autorisatie niet-BOA 5.1.2e .pdf 51: Rapportage logging WPG tbv concernmanager 15-03-2023.docx 53: Verklaring autorisatie niet BOA 5.1.2e .pdf 55: Verklaring autorisatie niet BOA 5.1.2e .pdf</p>	<p>Toezicht & Handhaving: voldoet niet Leerrecht: voldoet deels Sociale recherche: voldoet</p>
11	Autorisaties: aanwijzen functionarissen	Art 6 lid 7	Er is een actuele lijst van, door de verantwoordelijke aangewezen, bevoegde functionarissen.	Vastgesteld dat dit alleen van toepassing is bij Sociale recherche en dat de bevoegd functionaris is aangewezen (via vaststelling van het handboek) [75].	Voldoet

#	Onderwerp	Verwijzing Wpg	Beheersingsmaatregelen	Testwerkzaamheden / Bevindingen	Conclusies / Aanbevelingen
				Bestudeerde documenten: 75: Handboek Wpg sociale recherche Nijmegen 2022_2025 getekend.pdf	
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>Vastgesteld op basis van interview dat gemeenten generiek aandacht aan bewustwording besteden en mensen bij indiensttreden verplicht een geheimhoudingsverklaring laten tekenen en een bewustwordingscursus laten volgen in StudyTube [60, 61, 62, 64, 65]. Daarnaast moeten boa's een opleiding volgen voor zij beëdigd worden waarin aandacht wordt besteed aan dit soort onderwerpen. De gemeente beschikt verder over een sanctiebeleid [63]. Vastgesteld dat in handboek sociale recherche aandacht wordt besteed aan bewustwording [75].</p> <p>Bestaan voor Leerrecht vastgesteld aan de hand van indiensttreding 5.1.2e (Leerrecht) [34 t/m 36, 48]. Vastgesteld dat in teamoverleg aandacht is voor bewustwording [47, 49].</p> <p>Bestaan voor Toezicht & Handhaving niet vastgesteld, de afdeling is dit jaar helemaal opnieuw begonnen met het handboek, hier zijn nog geen voorbeelden van. Opzet voldoet deels door generieke gemeentebrede maatregelen.</p> <p>Bestudeerde documenten: 34: beediging 5.1.2e.pdf 35: bewijs van deelname LP v Beginners - 5.1.2e 17-1-2023.pdf 36: Certificaat 5.1.2e ambtseed.pdf 75: Handboek Wpg sociale recherche Nijmegen 2022_2025 getekend.pdf 48: IGD 22-0408 Introductiedossier Ingrado_V5.pdf 47: Kopie van Agenda LPO D-E 03-02-2022.xlsx 49: Kopie van Agenda LPO D-E 16-03-2023.xlsx 60: 14. Geheimhoudingsverklaring mei 2019.doc 61: 14. GMT voorstel 25-11-2020 i bewustijn programma NvD.docx 62: 14. instructie verwijderen fotos.pdf 63: 14. Proces sanctiebeleid en uittreksels personeelshandboek.docx 64: 14.AVG_flyer 7 stappen def.pdf 65: 14.Cursusoverzicht.studytube.02072021.PNG</p>	<p>Toezicht & Handhaving: voldoet niet Leerrecht: voldoet Sociale recherche: voldoet</p>

#	Onderwerp	Verwijzing Wpg	Beheersingsmaatregelen	Testwerkzaamheden / 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>	<p>Toezicht en handhaving Vastgesteld dat gemeente op de laatste versie van CityControl zit waarmee aan deze norm voldaan kan worden. Voor andere systemen is dit nog onduidelijk. Voor wat betreft de netwerkschijf en Corsa, hier is momenteel nog geen proces voor ingericht om te kunnen voldoen aan deze eisen. Hiermee voldoet dit domein niet aan de norm.</p> <p>Leerplicht Vastgesteld dat gemeente op recente versie van JVS zit waarin bewaartermijnen door een gebeurtenissenautomaat kunnen worden geborgd. Vastgesteld tijdens audit dat dit voor oude dossiers nog niet was toegepast. Dit was een bug volgens leverancier, en dit wordt hersteld. Ten tijde van de hercontrole was dit nog niet gerealiseerd, hiermee wordt niet voldaan aan deze norm.</p> <p>Sociale recherche Vastgesteld dat gemeente een handmatige procedure heeft ingericht om bewaartermijnen op netwerkschijven te waarborgen [75 t/m 77]. Gezien het geringe aantal dossiers en de strakke toegangsbeveiliging op de netwerkschijven akkoord.</p> <p>Bestudeerde documenten: 75: Handboek Wpg sociale recherche Nijmegen 2022_2025 getekend.pdf 76: Terugkerend agendapunt Controle archivering en vernietiging mei.GIF 77: Terugkerend agendapunt Controle archivering en vernietiging november.GIF</p>	<p>Toezicht & Handhaving: voldoet niet Leerrecht: voldoet niet Sociale recherche: voldoet</p>
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>	Zie 16.	<p>Toezicht & Handhaving: voldoet niet Leerrecht: voldoet niet Sociale recherche: voldoet</p>

#	Onderwerp	Verwijzing Wpg	Beheersingsmaatregelen	Testwerkzaamheden / Bevindingen	Conclusies / Aanbevelingen
			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.		
21	Verstreking 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>	<p>Vastgesteld dat de gemeente over een verstrekkingenwijzer beschikt waarin alle relevante verstrekkingen zijn opgenomen, inclusief hoe verstrekt wordt en waar geregistreerd wordt ten behoeve van de documentatieplicht [66].</p> <p>Bestaan vast kunnen stellen door waarneming in CityControl en Brickyard (Toezicht en handhaving), waarneming in JVS (Leerrecht) en door een voorbeeld van Sociale recherche [31].</p> <p>Bestudeerde documenten: 31: Aangetekend verstuurd verzendstatus.pdf 66: 21. Verstrekkingenwijzer.WPG.BOA.2022.pdf</p>	Voldoet

#	Onderwerp	Verwijzing Wpg	Beheersingsmaatregelen	Testwerkzaamheden / Bevindingen	Conclusies / Aanbevelingen
23	Verstrekking 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 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. <p>De daadwerkelijke verstrekking van gegevens wordt vastgelegd.</p>	Zie 21.	Voldoet
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>Zie voor deze norm ook de volgende normen:</p> <ol style="list-style-type: none"> 1. Registratie artikel 9 doeleinden: 2 2. Registratie verstrekkingen: 21 3. Registratie afwijzingen: 25 4. Registratie datalekken: 30 <p>Vastgesteld op basis van waarneming en interview dat doeleind voor artikel 9 onderzoeken worden vastgelegd in dossier en dat hier controle op wordt uitgeoefend [78, 79].</p> <p>Bestudeerde documenten:</p> <p>78: Terugkerend agendapunt Controle registratie mei.GIF</p> <p>79: Terugkerend agendapunt Controle registratie november.GIF</p>	Voldoet

#	Onderwerp	Verwijzing Wpg	Beheersingsmaatregelen	Testwerkzaamheden / 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 de meest gebruikte applicaties de logging niet op het gewenste niveau kunnen bieden [75]. Alleen CityControl en JVS bieden logging. Vastgesteld dat voor JVS een controle (steekproef) is uitgevoerd op de logging [51]. Advies is om deze logging / controle uitgebreider te beschrijven (wie doet wat wanneer) en om de rapportage zichtbaar te delen met de verantwoordelijk manager.</p> <p>Bestudeerde documenten: 75: Handboek Wpg sociale recherche Nijmegen 2022_2025 getekend.pdf 51: Rapportage logging WPG tbv concernmanager 15-03-2023.docx</p>	<p>Toezicht & Handhaving: voldoet niet Leerrecht: voldoet Sociale recherche: voldoet niet</p>
29	Audits	Art 33	Er wordt uitvoering gegeven aan de eisen zoals gesteld in de Regeling Periodieke Audit politiegegevens.	<p>De gemeente heeft in 2022 een interne audit uitgevoerd [67]. De gemeente heeft intern iemand benoemd als interne auditor en heeft voor de eerste 4 jaar een samenwerking met 2-Control B.V. voor het uitvoeren van de interne audits (in het kader van opleiding en overdracht).</p> <p>Bestudeerde documenten: 67: Wpg-intern-2022 Interne audit Wet Politiegegevens Gemeente Nijmegen - DEFINITIEF.pdf</p>	Voldoet
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>Vastgesteld dat de gemeente een FG heeft aangesteld [72]. Vastgesteld dat de FG jaarlijks toezicht houdt op diverse onderdelen [68, 69, 70, 71]. Bestaan vastgesteld aan de hand van jaarrapportage privacy 2022 [21].</p> <p>Bestudeerde documenten: 21: Jaarrapportage privacy 2022 v1.0.docx 68: 31.1.Verantwoording uitvoering AVG v2.pptx 69: 31.2. Van aanvraag tot oordeel privacy impact (2).pptx 70: 31.3. Uitvoering Controlplan per afdeling.pptx 71: 31.4.Uitvoering Controlplan FG Bevindingen Naleving.DEF versie 140222.pdf 72: 31.aanmelding FG (Nijmegen).pdf</p>	Voldoet

#	Onderwerp	Verwijzing Wpg	Beheersingsmaatregelen	Testwerkzaamheden / Bevindingen	Conclusies / Aanbevelingen
			De functionaris voor gegevensbescherming is aangemeld bij de Autoriteit Persoonsgegevens en de contactgegevens van de FG zijn openbaar gemaakt.		

5 Bijlage 2 – Beschrijving van de beheersingsmaatregelen en testresultaten (technische en organisatorische beheersingsmaatregelen)

Zoals in paragraaf 1.3 is aangegeven, verwerkt Gemeente Nijmegen politiegegevens in domeinen I, III en V.

Gemeente Nijmegen maakt voor deze verwerkingen gebruik van de volgende informatiesystemen:

Processen/verwerkingen	Informatiesysteem	Beheerorganisatie	Leverancier
Opsporing strafbare feiten in domein I (openbare ruimte)	CityControl	Sigma	Sigma
Opsporing strafbare feiten in domein I (openbare ruimte)	Corsa	IRvN	BCT Software
Opsporing strafbare feiten in domein I (openbare ruimte)	Netwerkschijf	IRvN	IRvN
Opsporing strafbare feiten in domein I (openbare ruimte)	C1	Brickyard	Brickyard
Opsporing strafbare feiten in domein I (openbare ruimte)	Scanauto	ACI	ACI
Opsporing strafbare feiten met betrekking tot de leerplichtwet	JVS	MetaObjects	MetaObjects
Opsporing strafbare feiten met betrekking tot de Wet maatschappelijke ondersteuning (Wmo)	Netwerkschijf	IRvN	IRvN

#	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>	<p>Vastgesteld dat de IRvN een procedure Wijzigingsbeheer heeft [81]. Bestaan vastgesteld aan de hand van twee voorbeelden (Corsa en een technische wijziging) [83, 87].</p> <p>Vastgesteld aan de hand van de TPM van JVS dat voor Leerrecht wordt voldaan aan deze norm [90].</p> <p>Vastgesteld voor de overige onderdelen van Toezicht & Handhaving (waaronder Brickyard) dat hier nog geen TPM voor beschikbaar is. Hiermee wordt niet voldaan aan deze norm. Voor Sigma voldoet deze norm, vastgesteld in de initiele audit door middel van een TPM.</p>	<p>Toezicht & Handhaving: voldoet deels</p> <p>Leerrecht: voldoet</p> <p>Sociale recherche: voldoet</p>

#	Onderwerp	Beheersingsmaatregelen	Testwerkzaamheden / Bevindingen	Conclusies / Aanbevelingen
			Bestudeerde documenten: 81: 10.1.2 Procedure Wijzingsbeheer.docx 90: 220505 TPM Wpg Metaobjects (1.0).pdf 83: W2107 1421 upgrade Corsa testomgevingpdf.pdf 87: W2303 0490 update citrix license server.pdf	
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>	<p>Vastgesteld dat IRvN procedures heeft voor instroom, doorstroom en uitstroom van medewerkers [88, 89]. Bestaan vastgesteld aan de hand van voorbeelden indienst 5.1.2e [84], uit dienst 5.1.2e [85] en mutatie 5.1.2e [86].</p> <p>Vastgesteld aan de hand van de TPM van JVS dat voor Leerrecht wordt voldaan aan deze norm [90].</p> <p>Vastgesteld voor de overige onderdelen van Toezicht & Handhaving (waaronder Brickyard) dat hier nog geen TPM voor beschikbaar is. Hiermee wordt niet voldaan aan deze norm. Voor Sigmax voldoet deze norm, vastgesteld in de initiele audit door middel van een TPM.</p> <p>Bestudeerde documenten: 90: 220505 TPM Wpg Metaobjects (1.0).pdf 88: Instroom medewerker processtappen.docx 89: Uitstroom medewerker processtappen.docx 84: W2203 1465 account IRVN aanmaken.pdf 85: W2210 1424 account irvn verwijderen.pdf 86: W2301 0024 account mutatie 5.1.2e .pdf</p>	<p>Toezicht & Handhaving: voldoet deels Leerrecht: voldoet Sociale recherche: voldoet</p>
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:</p>	<p>Vastgesteld aan de hand van de TPM van JVS dat voor Leerrecht wordt voldaan aan deze norm [90].</p> <p>Vastgesteld voor de overige onderdelen van Toezicht & Handhaving (waaronder Brickyard) dat hier nog geen TPM voor beschikbaar is. Hiermee wordt niet voldaan aan deze norm. Voor Sigmax voldoet deze</p>	<p>Toezicht & Handhaving: voldoet deels Leerrecht: voldoet Sociale recherche: voldoet niet</p>

#	Onderwerp	Beheersingsmaatregelen	Testwerkzaamheden / Bevindingen	Conclusies / Aanbevelingen
		<p>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>	<p>norm, vastgesteld in de initiele audit door middel van een TPM.</p> <p>Bestudeerde documenten: 90: 220505 TPM Wpg Metaobjects (1.0).pdf</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>	<p>Vastgesteld aan de hand van de TPM van JVS dat voor Leerrecht wordt voldaan aan deze norm [90].</p> <p>Vastgesteld voor de overige onderdelen van Toezicht & Handhaving (waaronder Brickyard) dat hier nog geen TPM voor beschikbaar is. Hiermee wordt niet voldaan aan deze norm. Voor Sigmax voldoet deze norm, vastgesteld in de initiele audit door middel van een TPM.</p> <p>Bestudeerde documenten: 90: 220505 TPM Wpg Metaobjects (1.0).pdf</p>	<p>Toezicht & Handhaving: voldoet deels</p> <p>Leerrecht: voldoet</p> <p>Sociale recherche: voldoet niet</p>
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>	<p>Vastgesteld aan de hand van de TPM van JVS dat voor Leerrecht wordt voldaan aan deze norm [90].</p> <p>Vastgesteld voor de overige onderdelen van Toezicht & Handhaving (waaronder Brickyard) dat hier nog geen TPM voor beschikbaar is. Hiermee wordt niet voldaan aan deze norm. Voor Sigmax voldoet deze norm, vastgesteld in de initiele audit door middel van een TPM.</p> <p>Bestudeerde documenten: 90: 220505 TPM Wpg Metaobjects (1.0).pdf</p>	<p>Toezicht & Handhaving: voldoet deels</p> <p>Leerrecht: voldoet</p> <p>Sociale recherche: voldoet niet</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	1, 13, 23, 25, 26, 33