2-Control B.V.
Haagsemarkt 1
4813 BA Breda
The Netherlands

T: +31 (0)76 50 194 70
www.2-control.nl
info@2-control.nl

Assurance-rapport
NOREA Richtlijn 3000D

Privacy-audit 2025 Wet politiegegevens

1 januari 2021 tot en met 31 december 2024

Gemeente Nijmegen

Uitgebracht door:	2-Control B.V.
Onderzoeker(s):	J. Dictus MSc RE
Uitgebracht aan:	Gemeente Nijmegen
Contactpersoon:	FG van de Gemeente Nijmegen
Datum:	26 november 2025
Rapportnummer:	2C-2025-759
Versie:	1.0
Status:	Definitief

Versiebeheer

Versie	Datum	Status	Naam
0.1	8 augustus 2025	Gereed voor OKB	2-Control B.V.
0.2	19 augustus 2025	Conceptversie voor afstemming met klant	2-Control B.V.
1.0	26 november 2025	Definitieve versie na managementreactie	2-Control B.V.

Inhoud

1	Assurance-rapport van de onafhankelijke auditor	5
1.1	Ons afkeurend oordeel	5
1.2	De basis voor ons afkeurend oordeel	5
1.3	Criteria	9
1.4	Aangelegenheden met betrekking tot de reikwijdte van ons onderzoek	9
1.5	Beoogde gebruikers en doel	10
1.6	Verantwoordelijkheden Gemeente Nijmegen	10
1.7	Verantwoordelijkheden van de IT-auditor	10
1.8	Overige informatie verstrekt door Gemeente Nijmegen	11
1.9	Aanbeveling met betrekking tot de hercontrole	11
2	Beschrijving privacy-doelstellingen	12
3	Overige informatie Gemeente Nijmegen	17
3.1	Inleiding	17
3.2	Overige informatie	17
4	Bijlage 1 – Beschrijving van de beheersingsmaatregelen en testresultaten (Wpg beheersingsmaatregelen)	18
5	Bijlage 2 – Beschrijving van de beheersingsmaatregelen en testresultaten (technische en organisatorische maatregelen)	19

Colofon

Voor u ligt het assurance-rapport inzake 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 2024, versie 1.0 d.d. 3 september 2024, de Richtlijn 3000D van de NOREA (Assurance-opdrachten door IT-auditors) en is opgesteld door 2-Control B.V.

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 short form versie van ons rapport.

1 Assurance-rapport van de onafhankelijke auditor

Aan het college van B&W van Gemeente Nijmegen
Postbus 9105
6500 HG Nijmegen

Referentie: 2C-2025-759

1.1 Ons afkeurend oordeel

Naar ons oordeel voldoen de door Gemeente Nijmegen getroffen beheersingsmaatregelen om te voorzien in de borging van de wettelijke eisen met betrekking tot de verwerking van politiegegevens in opzet, bestaan en werking gedurende de controleperiode (zie sectie 1.4.3) in belangrijke mate niet aan de gestelde criteria (zie sectie 1.3). Vanwege het belang en de omvang van de aangelegenheden die hierna zijn beschreven, geven wij een afkeurend oordeel. Het overzicht met oordelen per beheersingsmaatregel is hierna in paragraaf 1.2 'De basis voor ons afkeurend oordeel' weergegeven.

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 beheersingsmaatregelen en testresultaten (Wpg beheersingsmaatregelen) en Bijlage 2 – Beschrijving van de beheersingsmaatregelen en testresultaten (technische en organisatorische maatregelen).

1.2 De basis voor ons afkeurend oordeel

Wij hebben vastgesteld dat een aanzienlijk deel van de hiernavolgende Wpg onderwerpen niet (rood) of niet volledig (oranje) zijn opgezet, bestaan en/of effectief werken. Omdat bij 10 of meer beheersingsmaatregelen in opzet, bestaan en/of werking niet wordt voldaan aan de door de wetgever gestelde eisen, zijn deze aangelegenheden materieel en van diepgaande negatieve invloed op het beschermen van de privacy van betrokkenen.

Wij hebben ons onderzoek uitgevoerd volgens Nederlands recht, waaronder de NOREA Richtlijn 3000D 'Assurance-opdrachten door IT-auditors (Directe-opdrachten)'. Deze opdracht is gericht op het verkrijgen van een redelijke mate van zekerheid. Onze verantwoordelijkheden op grond hiervan zijn beschreven in de sectie 'Verantwoordelijkheden van de IT-auditor'.

Wij zijn onafhankelijk van Gemeente Nijmegen en hebben voldaan aan de overige vereisten van het Reglement Gedragscode ('Code of Ethics') van NOREA.

Wij zijn van mening dat de door ons verkregen assurance-informatie voldoende en geschikt is als basis voor onze oordelen.

Toelichting gebruikte kleuren:
Groen - De beheersingsmaatregelen voldoen;
Oranje - De beheersingsmaatregelen voldoen deels. Om geheel aan de beheersingsmaatregelen te voldoen dien(t)(en) de geconstateerde afwijking(en) te worden opgelost;
Rood - De beheersingsmaatregelen voldoen niet. Om aan de beheersingsmaatregelen te voldoen dien(t)(en) de geconstateerde afwijking(en) te worden opgelost;
Grijs - Niet onderzocht.

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.

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

Verwerking 1 (Openbare Ruimte)

Onderwerpen	Conclusie		
	Opzet	Bestaan	Werking
5.1.2h			

Technische en organisatorische maatregelen	Conclusie		
	Opzet	Bestaan	Werking
5.1.2h			

Verwerking 2 (Leerrecht)

Onderwerpen	Conclusie		
	Opzet	Bestaan	Werking
5.1.2h			

Technische en organisatorische maatregelen	Conclusie		
	Opzet	Bestaan	Werking
5.1.2h			

Verwerking 3 (Sociale Recherche)

#	Onderwerp	Conclusie		
		Opzet	Bestaan	Werking
5.1.2h				

Technische en organisatorische maatregelen	Conclusie		
	Opzet	Bestaan	Werking
5.1.2h			

1.3 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, bestaan en werking door de IT-auditor worden getoetst. De IT-auditor maakt bij deze toetsing gebruik van de volgende criteria.

Opzet	De organisatie heeft de beheersingsmaatregen beschreven die, indien deze werken zoals beschreven, een redelijke mate van zekerheid bieden dat voorzien is in de borging van de wettelijke eisen met betrekking tot de verwerking van politiegegevens door boa's.
Bestaan	De organisatie heeft de 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.

1.4 Aangelegenheden met betrekking tot de reikwijdte van ons onderzoek

1.4.1 Object van onderzoek

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)	5.1.2h
2	Leerplicht (Leerrecht)	III	Opsporing strafbare feiten in domein III (leerplicht)	
3	Opsporing sociaal domein	V	Opsporing strafbare feiten in domein V (sociaal domein)	

Wij hebben geen onderzoek uitgevoerd naar hierboven niet genoemde verwerkingen van politiegegevens en doen daar derhalve ook geen uitspraak over.

Gemeente Nijmegen verwerkt Wpg gegevens ook voor een ander bestuursorgaan, te weten: Gemeente Berg en Dal voor het onderdeel Leerplicht. Deze verwerking is in scope van ons onderzoek.

1.4.2 Serviceorganisaties

Gemeente Nijmegen maakt gebruik van serviceorganisatie(s) voor het onderhouden en het hosten van de applicatie(s) waarin politiegegevens worden verwerkt, zoals weergegeven in paragraaf 1.4.1. 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 uitsluitingsmethode ('carve-out method'). Onze werkzaamheden strekken zich dan ook niet uit tot de interne beheersingsmaatregelen van deze serviceorganisaties.

1.4.3 Specificatie van de controleperiode

Ons onderzoek ten aanzien van de opzet en het bestaan van beheersingsmaatregelen strekte zich uit tot de periode 1 januari 2021 tot en met 31 december 2024.

Ons onderzoek ten aanzien van de werking van beheersingsmaatregelen is beperkt tot de periode 1 januari 2024 tot en met 31 december 2024.

Uitzondering hierop vormen een aantal zogenaamde 'Toezichtmaatregelen'. Dit betreft de beheersingsmaatregelen:

- Planning, uitvoering, en rapportage van de interne audits (#29);
- Toezichttaken van de FG (#31).

Het onderzoeken van de hiervoor genoemde 'Toezichtmaatregelen' strekte zich uit tot de volledige controleperiode (1 januari 2021 tot en met 31 december 2024).

Hierbij merken wij op dat de controleperiode 1 januari 2021 tot en met 31 december 2021 bij een eerdere externe privacy audit (onder verwijzing naar kenmerk 2C-2022-336 en de rapportdatum 18 maart 2022) is onderzocht en aan de AP is gerapporteerd. Om "dubbeling" te voorkomen, maakt deze specifieke periode geen onderdeel uit van de thans onderzochte controleperiode. De controleperiode is daarmee beperkt tot 1 januari 2022 tot en met 31 december 2024.

1.4.4 Beperkingen

Wij kunnen niet uitsluiten dat, indien wij aanvullende beheersingsmaatregelen zouden hebben onderzocht, wellicht andere onderwerpen zouden zijn geconstateerd die voor rapportering in aanmerking zouden zijn gekomen. Bovendien is de projectie van oordelen naar de toekomst onderhevig aan het risico dat interne beheersingsmaatregelen ineffectief kunnen worden.

1.5 Beoogde gebruikers en doel

Gemeente Nijmegen dient ingevolge artikel 33 2e lid van de Wet politiegegevens een afschrift van de controleresultaten van de privacy audit 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.

1.6 Verantwoordelijkheden Gemeente Nijmegen

Gemeente Nijmegen is verantwoordelijk voor de opzet, het bestaan en de werking van de relevante beheersingsmaatregelen gedurende de controleperiode, om te voldoen aan de wettelijke eisen van de in de Wet Politiegegevens (Wpg) en het Besluit politiegegevens buitengewoon opsporingsambtenaren (Bpg boa) gestelde bepalingen.

1.7 Verantwoordelijkheden van de IT-auditor

Onze verantwoordelijkheid is het zodanig plannen en uitvoeren van ons onderzoek dat wij daarmee voldoende en geschikte assurance-informatie verkrijgen voor het door ons af te geven oordeel. Ons onderzoek is uitgevoerd met een hoge mate maar geen absolute mate van zekerheid waardoor het mogelijk is dat wij tijdens ons onderzoek niet alle materiële afwijkingen als gevolg van fraude of fouten ontdekken.

Wij passen het 'Reglement Kwaliteitsbeheersing NOREA' (RKBN) toe. Op grond daarvan beschikken wij over een samenhangend stelsel van kwaliteitsmanagement inclusief vastgelegde richtlijnen en procedures inzake de naleving van de ethische voorschriften, professionele standaarden en andere relevante 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 politiegegevens[1].

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.

1.8 Overige informatie verstrekt door Gemeente Nijmegen

De informatie met de titel "Overige Informatie verstrekt door 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 Aanbeveling met betrekking tot de hercontrole

Wij hebben vastgesteld dat Gemeente Nijmegen niet (geheel) voldoet aan het bij of krachtens de wet bepaalde. Inzake de uitvoering van de hercontroles, bevelen wij Gemeente Nijmegen aan om deze door een externe auditor te laten uitvoeren. Wij baseren deze aanbeveling op het feit dat deze privacy-audit leidt tot een afkeurend oordeel.

Breda, 26 november 2025
26 Nov 2025
Breda

J. Dictus MSc RE

2-Control B.V.
Haagsemarkt 1
4813 BA Breda

[1] 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 politiegegegevens).

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
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 onrechtmatige 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 De verwerkingsverantwoordelijke heeft controles op de kwaliteit ingericht ten behoeve van de borging van de juistheid en nauwkeurigheid 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 • Er is (aantoonbaar) een risicoanalyse uitgevoerd waaruit het risiconiveau blijkt m.b.t. ongeoorloofde of onrechtmatige verwerking en tegen opzettelijk verlies, vernietiging of beschadiging. • De verwerkingsverantwoordelijke 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).
7. Gegevensbescherming door standaardinstellingen De verwerkingsverantwoordelijke treft passende technische en organisatorische maatregelen om te waarborgen dat standaard: • 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.
8. Gegevensbeschermings-effectbeoordeling / Data protection impact assessment (DPIA) • 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.

Onderwerpen en beheersingsmaatregelen
9. Bijzondere categorieën van politiegegevens 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.
10. Autorisaties en toegang tot politiegegevens • 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 • 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. • 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.
15. Geautomatiseerde individuele besluitvorming • 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. • 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.
16. Uitvoering van de dagelijkse politietaak • 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 (hitno-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.

Onderwerpen en beheersingsmaatregelen
17. Ter Beschikking stellen (voor verdere verwerking) • 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 • 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 boa's 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 • 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.
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.

Onderwerpen en beheersingsmaatregelen

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.
25. Informatie aan de betrokkene, recht op inzage, rectificatie en verwijdering • 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 uitsluitsel 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 De **verwerkingsverantwoordelijke** houdt een register bij dat de volgende gegevens bevat: 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. De **verwerker** houdt een register bij dat de volgende gegevens bevat: 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, onder vermelding van dat derde land of die internationale organisatie, indien door de verwerkingsverantwoordelijke uitdrukkelijk daartoe geïnstrueerd

Onderwerpen en beheersingsmaatregelen
d) indien mogelijk, een algemene beschrijving van de technische en organisatorische maatregelen, bedoeld in artikel 4a.
27. Documentatie • 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 • De verwerkingsverantwoordelijke en de verwerker dragen zorg voor de vastlegging langs elektronische weg (logging) van ten minste de volgende verwerkingen van politiegegevens in geautomatiseerde systemen: het verzamelen, wijzigen, raadplegen, verstrekken onder meer in de vorm van doorgiften, combineren of vernietigen van politiegegevens (32a lid1). • De organisatie gebruikt de logging uitsluitend ter controle van de rechtmatigheid van de gegevensverwerkingen, voor interne controles, ter waarborging van de integriteit en de beveiliging van politiegegevens en voor strafrechtelijke procedures (32a lid 2).
29. Audits Er wordt uitvoering gegeven aan de eisen zoals gesteld in de Regeling periodieke audit politiegegevens.
30. Melding datalekken • 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 AP 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.

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 en de contactgegevens van de FG zijn openbaar gemaakt.

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 wij brengen daarover geen oordeel tot uitdrukking.

3.2 Overige informatie

Reactie gemeente Nijmegen op conceptrapport audit Wpg van 19 augustus 2025:

'Onze inspanningen zijn erop gericht om alle beheersmaatregelen volledig op groen te hebben staan. Wij constateren dat we nog geen goedkeurend oordeel hebben en binnen het domein openbare ruimte, waar de meeste politiegegevens worden verwerkt, het meest voldoen aan de normen.'

'De beheersmaatregelen zijn verdeeld over drie verschillende BOA-domeinen en IT-beheer- en overkoepelende onderdelen. Wanneer er voor één domein een beheersmaatregel op rood staat, heeft dit een negatieve uitkomst op het totaal.
Desondanks waarderen wij dat de groei en inhoudelijke vooruitgang ook worden herkend. Met name binnen het domein openbare ruimte, waar de meeste politiegegevens worden verwerkt, zijn de resultaten overwegend positief en is groei te zien t.o.v. voorgaande jaren.'

'Sinds 2022 zijn belangrijke stappen gezet, waaronder het aanstellen van een interne auditor en het versterken van beheersmaatregelen.'

'De uitkomsten en aanbevelingen van deze externe audit zijn door de intern auditor herkend en hebben ertoe geleid dat er concrete acties zijn uitgezet in onze organisatie.
Verder zijn er sinds de komst van de intern auditor acties ter verbetering van aandachtspunten ondernomen. Deze hebben inmiddels tot verbetering geleid in opzet en bestaan bij een aantal onderwerpen. In werking worden deze nog verder geoptimaliseerd.'

'Zo wordt er bijvoorbeeld gewerkt aan verbetering van logging; dit traject loopt nog en heeft onze voortdurende aandacht.'

'Tot slot danken wij de auditorganisatie ‘2-Control’ voor het onderzoek en de constructieve aanbevelingen.'

'De FG herkent zich in de uitkomsten van dit onderzoek en de reactie van de organisatie.
Vanuit de FG-rol zal worden toegezien op de verbeteringen die de organisatie heeft door te voeren

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

Deze bijlage is geen onderdeel van de Short form versie van het rapport.

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

Deze bijlage is geen onderdeel van de Short form versie van het rapport.

Legenda toegepaste uitzonderingsgrondslagen

In dit document zijn gegevens definitief geanonimiseerd op grond van:

Wet	Artikel	Omschrijving	Pagina's
Wet open overheid	Art. 5.1 lid 2 sub h	De beveiliging van personen en bedrijven en het voorkomen van sabotage	6, 7, 8, 9