Gemeente Amsterdam

Assurance-rapport
NOREA Richtlijn 3000D

Privacy-audit Wet politiegegevens
1 juli 2021 tot en met 31 december 2024

Gemeente Amsterdam

Uitgebracht door:	Auditdienst ACAM
Uitgebracht aan:	Gemeente Amsterdam
Contactpersoon:	dr. M. van Hattem (coördinator Wet politiegegevens)
Datum:	12-01-2026
Rapportnummer:	181.600.24-R
Versie:	1.0
Status:	Definitief

Inhoud

1 Assurance-rapport van de onafhankelijke auditor 4
1.1 Ons afkeurend oordeel 4
1.3 Criteria 9
1.4 Aangelegenheden met betrekking tot de reikwijdte van ons onderzoek 9
1.4.1 Object van onderzoek 9
1.4.2 Specificatie van de controleperiode 9
1.4.3 Beperkingen 10
1.5 Beoogde gebruikers en doel 10
1.6 Verantwoordelijkheden gemeente Amsterdam 10
1.7 Verantwoordelijkheden van de IT-auditor 10
1.8 Aanbeveling met betrekking tot de hercontrole 11

2 Beschrijving privacy-doelstellingen 13

3 Managementreactie 18

Colofon

Voor u ligt het assurance-rapport inzake de politiegegevens die de buitengewoon opsporingsambtenaren (boa's) van de gemeente Amsterdam 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 (Bpg boa). 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 Auditdienst ACAM.

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 de gemeente Amsterdam zoals een overzicht van de getoetste interne beheersingsmaatregelen 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: gemeente Amsterdam

1.1 Ons afkeurend oordeel

Naar ons oordeel voldoen de door de gemeente Amsterdam 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) 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 beheersingsdoelstellingen, beheersingsmaatregelen en testresultaten (Wpg) en Bijlage 2 - Beschrijving van de beheersingsdoelstellingen, 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 er bij 10 of meer beheersingsmaatregelen[1] in opzet, bestaan en/of werking (over het jaar 2024) niet werd 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 de gemeente Amsterdam 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 N.O. - Niet onderzocht.

[1] Hieronder worden zowel de algemene als de technische en organisatorische (IT) onderwerpen verstaan.

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 de gemeente Amsterdam.
***) Niet onderzocht omdat we geen of onvoldoende controle informatie hebben ontvangen om de norm te kunnen vaststellen.

TZM = toezichtsmaatregelen (dit betreft de normen 29 en 31)

Directie Toezicht Handhaving Openbare Ruimte en Sport en Bos - Toezicht en handhaving van milieudelicten en openbare ruimte & aanpak van ernstige overlast in openbaar vervoer

Verwerking Toezicht en handhaving van milieudelicten en openbare ruimte & aanpak van ernstige overlast in openbaar vervoer Onderwerpen	Oordelen				
	Opzet Juni 2024	Bestaan Juni 2024	Opzet december 2024	Bestaan december 2024	Werking jan – dec 2024
1. Reikwijdte					
2. Doelbinding					
3. Noodzakelijkheid en rechtmatigheid, vermelding herkomst					
4. Juistheid en volledigheid politiegegevens					
5. Onderscheid feiten en oordeel					
6. Gegevensbescherming door beveiliging en ontwerp					
7. Gegevensbescherming door standaardinstellingen					
8. Gegevensbeschermingseffectbeoordeling/Data protection impact assessment (DPIA)					
9. Bijzondere categorieën van politiegegevens					
10. Autorisaties en toegang tot politiegegevens					
11. Autorisaties: aanwijzen functionarissen	**	**	**	**	**
12. Onderscheid tussen verschillende categorieën van betrokkenen					
13. Verwerker en Verwerkersovereenkomst					
14. Geheimhoudingsplicht					
15. Geautomatiseerde individuele besluitvorming	**	**	**	**	**
16. Uitvoering van de dagelijkse politietaak					
17. Ter beschikking stellen van politiegegevens binnen het Wpg-domein					
18. Geautomatiseerd vergelijken en in combinatie zoeken	**	**	**	**	**
19. Ondersteunende taken	**	**	**	**	**
20. Bewaartermijnen, verwijderen en vernietigen					
21. Verstrekking van politiegegevens aan anderen dan politie en Koninklijke marechaussee					
22. Doorgiften aan derde landen	**	**	**	**	**
23. Verstrekking aan derden structureel voor samenwerkingsverbanden	***	***			***
24. Rechtstreekse verstrekking	**	**	**	**	**
25. Informatie aan de betrokkene, recht op inzage, rectificatie en verwijdering		*			
26. Register					

Verwerking Toezicht en handhaving van milieudelicten en openbare ruimte & aanpak van ernstige overlast in openbaar vervoer Onderwerpen	Oordelen				
	Opzet Juni 2024	Bestaan Juni 2024	Opzet december 2024	Bestaan december 2024	Werking jan – dec 2024
27. Documentatie					
28. Logging					
29. Audits	TZM	TZM	TZM	TZM	TZM
30. Melding datalekken					
31. Functionaris voor gegevensbescherming	TZM	TZM	TZM	TZM	TZM

Technische en organisatorische maatregelen Informatiesysteem CityControl	Oordelen				
	Opzet juni 2024	Bestaan juni 2024	Opzet december 2024	Bestaan december 2024	Werking 2024
1. Wijzigingenbeheer					
2. Logische toegangsbeveiliging					
3. Beheer van kwetsbaarheden (patchmanagement)					
4. Cryptografie					
5. Vulnerability scans en Penetratietesten					

Directie Onderwijs - Onderzoek en proces mogelijk leidend tot proces verbaal naar ongeoorloofd verzuim ten opzichte van de leerplicht

Onderzoek en proces mogelijk leidend tot proces verbaal naar ongeoorloofd verzuim ten opzichte van de leerplicht Onderwerpen	Oordelen				
	Opzet juni 2024	Bestaan juni 2024	Opzet december 2024	Bestaan december 2024	Werking jan – dec 2024
1. Reikwijdte					
2. Doelbinding					
3. Noodzakelijkheid en rechtmatigheid, vermelding herkomst		***			
4. Juistheid en volledigheid politiegegevens		***			
5. Onderscheid feiten en oordeel		***			
6. Gegevensbescherming door beveiliging en ontwerp					
7. Gegevensbescherming door standaardinstellingen		***			
8. Gegevensbeschermingseffectbeoordeling/Data protection impact assessment (DPIA)					
9. Bijzondere categorieën van politiegegevens					
10. Autorisaties en toegang tot politiegegevens					
11. Autorisaties: aanwijzen functionarissen	**	**	**	**	**
12. Onderscheid tussen verschillende categorieën van betrokkenen		***			
13. Verwerker en Verwerkersovereenkomst		***			
14. Geheimhoudingsplicht					
15. Geautomatiseerde individuele besluitvorming	**	**	**	**	**
16. Uitvoering van de dagelijkse politietaak		***			***
17. Ter beschikking stellen van politiegegevens binnen het Wpg-domein	**	**	**	**	**

Onderzoek en proces mogelijk leidend tot proces verbaal naar ongeoorloofd verzuim ten opzichte van de leerplicht **Onderwerpen**	Oordelen				
	Opzet juni 2024	Bestaan juni 2024	Opzet december 2024	Bestaan december 2024	Werking jan – dec 2024
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	TZM	TZM	TZM	TZM	TZM
30. Melding datalekken		*		*	*
31. Functionaris voor gegevensbescherming	TZM	TZM	TZM	TZM	TZM

Technische en organisatorische maatregelen Informatie systemen: Erisa (tot en met 31 juli 2024) en BRS (vanaf 1 augustus 2024)	Oordelen				
	Opzet juni 2024	Bestaan juni 2024	Opzet december 2024	Bestaan december 2024	Werking jan - dec 2024
1. Wijzigingenbeheer	***	***			***
2. Logische toegangsbeveiliging	***	***			***
3. Beheer van kwetsbaarheden (patchmanagement)	***	***			***
4. Cryptografie	***	***			***
5. Vulnerability scans en Penetratietesten	***	***			***

Directie Inkomen: Het uitvoeren van strafrechtelijke (fraude)onderzoeken o.g.v. Participatiewet, IOAW en IOAZ (Inkomen)

Verwerking: Het uitvoeren van strafrechtelijke (fraude)onderzoeken o.g.v. Participatiewet, IOAW en IOAZ (Inkomen) **Onderwerpen**	Oordelen				
	Opzet juni 2024	Bestaan juni 2024	Opzet december 2024	Bestaan december 2024	Werking jan - dec 2024
1. Reikwijdte					
2. Doelbinding					
3. Noodzakelijkheid en rechtmatigheid, vermelding herkomst					
4. Juistheid en volledigheid politiegegevens		***			
5. Onderscheid feiten en oordeel					
6. Gegevensbescherming door beveiliging en ontwerp					
7. Gegevensbescherming door standaardinstellingen					

Verwerking: Het uitvoeren van strafrechtelijke (fraude)onderzoeken o.g.v. Participatiewet, IOAW en IOAZ (Inkomen) **Onderwerpen**	**Oordelen**				
	Opzet juni 2024	**Bestaan juni 2024**	**Opzet december 2024**	**Bestaan december 2024**	**Werking jan - dec 2024**
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	**TZM**	**TZM**	**TZM**	**TZM**	**TZM**
30. Melding datalekken		*		*	*
31. Functionaris voor gegevensbescherming	**TZM**	**TZM**	**TZM**	**TZM**	**TZM**

Technische en organisatorische maatregelen **Informatie systemen: Sherlock (tot en met 30 juni 2024) en BRS (vanaf 1 juli 2024)**	**Oordelen**				
	Opzet juni 2024	**Bestaan juni 2024**	**Opzet december 2024**	**Bestaan december 2024**	**Werking jan – dec 2024**
1. Wijzigingenbeheer	***	***			***
2. Logische toegangsbeveiliging	***	***			***
3. Beheer van kwetsbaarheden (patchmanagement)	***	***			***
4. Cryptografie	***	***			***
5. Vulnerability scans en Penetratietesten	***	***			***

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 beheersingsmaatregelendaadwerkelijk geïmplementeerd en toegepast.
Werking	De organisatie heeft de beheersingsmaatregelen gedurende de controleperiode 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 de gemeente Amsterdam bestond uit de hierna genoemde verwerkingen van politiegegevens:

#	Organisatie-onderdeel	Domein	Processen/verwerkingen	Applicaties
1	Toezicht Handhaving in de Openbare Ruimte en Sport en Bos	I/II/IV	Verwerking Toezicht en handhaving van milieudelicten (II) en openbare ruimte (I) & aanpak van ernstige overlast in openbaar vervoer (IV)	**1-1-2024 tot en met 31-12-2024:** City Control
2	Onderwijs, Jeugd en Zorg — afdeling Onderwijs	III	Onderzoek en proces mogelijk leidend tot proces verbaal naar ongeoorloofd verzuim ten opzichte van de leerplicht	**1-1-2024 tot en met 31-7-2024:** Erisa **1-8-2024 tot en met 31-12-2024:** Boa Registratie Systeem (BRS)
3	Inkomen afdeling Handhaving, Werk en inkomen.	V	Het uitvoeren van strafrechtelijke (fraude)onderzoeken o.g.v. Participatiewet, IOAW en IOAZ	**1-1-2024 tot en met 30-6-2024:** Sherlock III **1-7-2024 tot en met 31-12-2024:** Boa Registratie Systeem (BRS)

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

1.4.2 Specificatie van de controleperiode

Ons onderzoek ten aanzien van de opzet en het bestaan van beheersingsmaatregelen strekte zich uit tot de periode 1 juli 2021 tot en met 31 december 2024. Voor ons onderzoek ten aanzien van de opzet en het bestaan van de beheersingsmaatregelen hebben wij, op verzoek van de gemeente Amsterdam, twee peildata gehanteerd. Gekozen is voor peildata 1 juni 2024 en 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' (TZM) strekte zich uit tot de volledige controleperiode (1 juli 2021 tot en met 31 december 2024).

Hierbij merken wij op dat de controleperiode 1 januari 2021 tot en met 30 juni 2021 bij een eerdere externe privacy audit (onder verwijzing naar kenmerk 714.600.21-R en de rapportdatum 16 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 juli 2021 tot en met 31 december 2024.

1.4.3 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

De gemeente Amsterdam 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 de gemeente Amsterdam 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.

1.6 Verantwoordelijkheden gemeente Amsterdam

De gemeente Amsterdam 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[2].

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 Aanbeveling met betrekking tot de hercontrole

Wij hebben vastgesteld dat gemeente Amsterdam niet (geheel) voldoet aan het bij of krachtens de wet bepaalde. Inzake de uitvoering van de hercontrole, bevelen wij de gemeente Amsterdam aan om deze door de interne auditor te laten uitvoeren. Wij baseren deze aanbeveling op het volgende:

- De gemeente Amsterdam heeft een interne auditafdeling met kennis en ervaring op het gebied van de Wpg. De afgelopen jaren zijn ook jaarlijks interne audits uitgevoerd op de Wpg. Ook voor 2026 is er een interne audit op het Auditjaarplan opgenomen. Verder hebben wij bij deze externe audit vastgesteld dat norm 29 (Audits) voor wat betreft opzet, bestaan en werking voldoet.

- De significantie van de bevindingen heeft geleid tot een afkeurend oordeel in deze externe audit, maar dat er wel sterke verbetering zichtbaar is het voldoen aan beheersmaatregelen in opzet en bestaan met peildatum december 2024 ten opzichte van de peildatum juni 2024 (zie par. 1.2).

De Regeling periodieke audit politiegegevens schrijft voor dat, indien bij het uitvoeren van de externe privacy audit tekortkomingen zijn geconstateerd, de verwerkingsverantwoordelijke binnen drie maanden na oplevering van het externe auditrapport een verbeterplan opstelt waarin de maatregelen worden beschreven die getroffen zijn (of zullen worden) ter verbetering van de geconstateerde tekortkomingen.

Op basis van het verbeterplan vindt binnen een jaar na oplevering van het externe auditrapport, de hercontrole plaats. De hercontrole heeft betrekking op het onderdeel of de onderdelen van de wet ten aanzien waarvan tekortkomingen zijn geconstateerd (dus alleen op die beheersingsmaatregelen waar het oordeel "niet voldaan" of "deels voldaan" is bij de externe privacy audit). Op suggestie van de AP en ter bevordering van een efficiënt systeemtoezicht dient in het rapport van de hercontrole een volledige tabel van resultaten te worden opgeleverd en niet alleen een tabel met de in de hercontrole betrokken beheersingsmaatregelen.

[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 politiegegegevens).

Door NOREA is, op suggestie van de AP, aangegeven dat als de hercontrole plaatsvindt binnen een half jaar na uitvoering van de externe audit (gerekend vanaf de datum van deze rapportage), een beoordeling van de opzet en het bestaan van de beheersmaatregelen volstaat. Wordt de hercontrole uitgevoerd tussen een half jaar en een jaar, dan vindt deze plaats op opzet, bestaan en werking van de beheersmaatregelen.

Amsterdam, 12 januari 2026

ARJAN PASCAL SUIJKER Digitally signed by ARJAN PASCAL SUIJKER
Date: 2026-01-12 16:54:36+01:00

A.P. Suijker MSc CISA RA RE
Auditdienst ACAM

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 de gemeente Amsterdam 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.
9. Bijzondere categorieën van politiegegevens

Onderwerpen en beheersingsmaatregelen
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.
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

Onderwerpen en beheersingsmaatregelen
• 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.
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: o Ten behoeve van welk zwaarwegend algemeen belang de verstrekking noodzakelijk is, o Ten behoeve van welk samenwerkingsverband de politiegegevens worden verstrekt, o Het doel waartoe dit is opgericht, o Welke gegevens worden verstrekt, o De voorwaarden onder welke de gegevens worden verstrekt en o Aan welke personen of instanties de gegevens worden verstrekt. o De daadwerkelijke verstrekking van gegevens wordt vastgelegd.
24. Rechtstreekse verstrekking

Onderwerpen en beheersingsmaatregelen

- 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
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.

Onderwerpen en beheersingsmaatregelen
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:
  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.
• 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.

3 Managementreactie

Betreft: Managementreactie gemeente Amsterdam op het Assurance-Rapport Privacy Audit Wpg van Auditdienst ACAM (ontvangen 6 januari 2026).

Het management van de directie Digitale Strategie en Informatie heeft kennisgenomen van de uitkomsten van de audit over de uitvoering van de Wet politiegegevens (Wpg) in 2024. Het voldoen aan de Wpg is van groot belang voor de organisatie. De uitvoering van deze wet is een continu proces, dat in 2024 in een stroomversnelling is geraakt. Daarom hebben wij de auditor ACAM gevraagd om naast 30 juni 2024 ook 31 december 2024 als peildatum op te nemen, en wij zijn blij dat ACAM hieraan gehoor heeft gegeven. De resultaten tonen aan dat beleid en procedures op 31 december 2024 grotendeels op orde zijn gebracht. Dit blijkt uit de normering bij ‘opzet’ en ‘bestaan’ op de peildatum 31 december 2024. Ten opzichte van de peildatum juni 2024 is een significante verbetering zichtbaar, waarbij twee van de drie directies op die datum qua opzet en bestaan (nagenoeg) volledig voldoen. In 2025 is de implementatie voortgezet, waarbij in het eerste kwartaal van 2025 nog een aantal belangrijke verbetermaatregelen zijn doorgevoerd.

De auditor constateert dat de gemeente, terugkijkend op het gehele kalenderjaar 2024, nog niet volledig voldeed aan de Wet politiegegevens. We maken werk van de aanbevelingen die de ACAM doet. Van de 14 aanbevelingen zijn er 8 in 2025 uitgevoerd. De overige maatregelen zijn in uitvoering en wachten op afronding. Dit is mogelijk dankzij de voortdurende inzet van de drie directies. In 2026 zal een hercontrole plaatsvinden volgens de auditregeling (over het jaar 2025). Wij verwelkomen deze hercontrole en blijven ons inzetten om de Wpg op een goede manier uit te voeren en zo de privacy van de Amsterdammers optimaal te beschermen.

De bijlagen van dit rapport zijn vertrouwelijk en uitsluitend bestemd voor gemeente Amsterdam.