

Wet politiegegevens

Rapportage: Hercontrole van opzet en bestaan op basis van artikel 4 Regeling periodieke audit politiegegevens (artikel 33 5e lid Wet politiegegevens en artikel 6:5, 4e lid Besluit Politiegegevens)

Afdeling Interne Audit en Beleidsonderzoek| Audit 2026.03a | 9 juli 2026

Colofon

Voor u ligt het assurance-rapport van de hercontrole inzake de externe privacy audit (181.600.24-R) op de politiegegevens die de buitengewoon opsporingsambtenaren (boa's) van gemeente Amsterdam verwerken en die in een bestand zijn opgenomen, of die bestemd zijn daarin te worden opgenomen.

De hercontrole heeft alleen betrekking op het onderdeel of de onderdelen van de wet ten aanzien waarvan tijdens de externe privacy audit tekortkomingen zijn geconstateerd 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.

Deze verwerkingen vallen onder de reikwijdte van de Wet politiegegevens (Wpg) en het Besluit politiegegevens voor buitengewoon opsporingsambtenaren (Bpg boa).

Dit rapport is mede gebaseerd op NOREA Handreiking Privacy audit Wpg voor boa's 2024, versie 1.0 d.d. 3 september 2024 en is opgesteld door de afdeling Interne Audit en Beleidsonderzoeken van gemeente Amsterdam. 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 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.

Inhoudsopgave

1	Inleiding	2
2	Managementsamenvatting	4
3	Oordeel	6
4	Beschrijving privacy-doelstellingen	10

1. Inleiding

Aanleiding

In de Wet Politiegegevens (WPG) en de bijbehorende ministeriële regeling is vastgelegd dat jaarlijks een interne audit moet worden uitgevoerd om de naleving van de WPG te controleren. De interne audit kan betrekking hebben op één of meerdere onderdelen van de wet. Daarnaast moet eens in de vier jaar een externe audit worden uitgevoerd.

Als uit de externe audit bevindingen naar voren komen, is de organisatie verplicht om voor de geconstateerde punten een verbeterplan op te stellen en binnen een jaar een hercontrole te laten uitvoeren. Wanneer de hercontrole binnen zes maanden na dagtekening van het externe auditrapport plaatsvindt, volstaat een toetsing van de opzet en het bestaan van de verbetermaatregelen. De hercontrole is op advies van ACAM door ons (afdeling Interne Audit en Beleidsonderzoek) uitgevoerd.

Doelstelling

Het doel van de audit is vaststellen in hoeverre de onderdelen van de WPG waarop ACAM in de externe audit bevindingen heeft geconstateerd, in opzet en bestaan beheerst worden.

Hoofdvraag

De audit kent de hoofdvraag: *In hoeverre is de interne beheersing effectief geborgd voor de onderdelen van de WPG waarop ACAM bevindingen heeft geconstateerd in de externe audit?*

Scope van de audit

In de hercontrole hebben we de opzet en het bestaan van de onderwerpen waarvoor in de externe audit een andere conclusie is getrokken dan voldoet én een aanbeveling is geformuleerd, getoetst. In de toetsing hebben we vastgesteld of in voldoende mate in opzet en bestaan invulling is gegeven aan de verbetermaatregelen die zijn geformuleerd ter verbetering van de interne beheersing van tikverbalen (THOR), delen gegevens met derden (allen), logging (allen) en overig (allen). Als onvoldoende invulling is gegeven aan de verbetermaatregelen zijn wij nagegaan of de gemeente andere maatregelen heeft getroffen waarmee alsnog wordt voldaan aan de vereisten van de WPG. In de bijlage is een overzicht opgenomen van de verbetermaatregelen per directie in scope.

Niet in scope

In onze audit voeren we geen onderzoek uit naar de normen opgenomen in de WPG welke in de externe audit niet tot aanbevelingen hebben geleid. Ook onderzoeken we niet de werking van de normen wel in scope voor onze audit. Verder voeren we geen integrale toetsing uit van de naleving van de AVG of naleving van de komende cyberbeveiligingswet met de daarbij horende ministeriële regeling (de BIO2).

Omdat de hercontrole binnen zes maanden na dagtekening van het externe auditrapport is afgerond is volstaan met toetsen van opzet en bestaan. Dit in overeenstemming met hetgeen de Autoriteit Persoonsgegevens heeft aangegeven.

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 door de auditor bij de hercontrole worden getoetst. De 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. *Buiten scope in deze hercontrole*

Beoogde gebruikers en doel

De gemeente Amsterdam dient ingevolge artikel 33 2e lid van de Wet politiegegevens een afschrift van de controleresultaten van de 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 (het volledige interne

auditrapport inclusief bijlagen) zonder opgaaf van redenen bij 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.

Verantwoordelijkheden gemeente Amsterdam

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

Verantwoordelijkheden van de 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 de standaarden van het IIA, het GIAS, 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 hercontrole, zoals bepaald in artikel 6 van de Regeling periodieke audit politiegegevens.

De werkzaamheden zijn afhankelijk van de door de 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.

Dankwoord

Wij bedanken de WPG-coördinator en de directies voor de fijne en constructieve samenwerking tijdens deze audit. Hun waardevolle input heeft geholpen bij het inzichtelijk maken van de beheersing van de resterende risico's voor de naleving van de WPG. Wij waarderen bovendien de positieve en proactieve houding van de betrokkenen, vooral ook gezien het korte tijdsverloop tussen afronding van de externe audit, het opstellen van het verbeterplan en de uitvoering van de hercontrole.

2. Managementsamenvatting

Conclusie

De interne beheersing van de Wet Politiegegevens is voor bijna alle aanbevelingen in opzet en bestaan effectief gebleken met uitzondering van drie aanbevelingen waarop verdere doorontwikkeling noodzakelijk is. Dit betreffen met name de migratie van de oude tikverbalen en de toetsing op rechtmatig gebruik van de databases.

Bij achterwege blijven van doorontwikkeling loopt de gemeente het risico dat niet voldaan wordt aan de wettelijke bewaarplicht voor de tikverbalen. Ook loopt de gemeente het risico dat onrechtmatig gebruik van de databases onopgemerkt blijft. Beide risico's kunnen leiden tot het bemoeilijken van vervolging van de overtreder.

Samenvatting bevindingen

In onze audit hebben we geconstateerd dat na de afronding van de externe audit op 12 januari 2026 een aantal mooie stappen zijn gezet. Er is tijdig een verbeterplan opgesteld en vastgesteld voor de 15 normen waarvoor verbetermaatregelen zijn geformuleerd. Deels parallel aan de opstelling van het verbeterplan is gestart met realisatie van de aanbevelingen. Bij de afronding van de hercontrole resteren drie bevindingen.

Bevindingen	Verbetermaatregel	Prioriteit
1. Migratie oude 'tikverbalen' naar gecentraliseerd archief heeft nog niet geplaats gevonden (overige bevindingen, THOR/Sport&Bos)	20	1
2. Toetsing van de rechtmatigheid van verwerkingen door toetsing van logging is nog niet uitgevoerd (THOR/Sport&Bos + Onderwijs)	28	1
3. Interne kwaliteitstoets toetst niet expliciet op volledigheid van de verwerkte politiegegevens (THOR/Sport&Bos)	04	2

In het bovenstaande schema hebben wij op basis van een risico-inschatting aangegeven welke prioriteit aan de bevindingen moet worden gegeven.

Wij maken daarbij het volgende onderscheid in de bevindingen:

- Prioriteit 1: Zeer belangrijk, grote impact, urgent, opvolging direct vereist
- Prioriteit 2: Belangrijk, gemiddelde impact, minder urgent, opvolging nodig
- Prioriteit 3: Aandacht nodig, beperkte impact, niet urgent, opvolging niet noodzakelijk

Aanbevelingen

Voor het mitigeren van de resterende risico's geven wij de volgende aanbevelingen:

1. Realiseer archivering van de oude tikverbalen op een daarvoor geschikte locatie. Voer de geplande migratie van oude tikverbalen op korte termijn zorgvuldig en gecontroleerd uit, zodat alle tikverbalen centraal, volledig en beheerst worden opgeslagen en gearchiveerd.
2. Voer op korte termijn de rechtmatigheidscontrole op de gegevensverwerking uit door het toetsen van de logging. Leg de resultaten daarvan vast en volg eventuele bevindingen tijdig op.
3. Neem volledigheid op als expliciet criterium in de checklist waarop de chef van dienst bij de interne kwaliteitstoets moet controleren.

Managementreactie

De resultaten van de hercontrole laten zien dat de organisatie de openstaande aanbevelingen uit de externe audit van de ACAM snel en goed heeft opgepakt. Intussen is aantoonbaar een goed fundament gelegd om blijvend te voldoen aan de Wet politiegegevens.

De directie Onderwijs heeft in maart 2026 een nieuw systeem voor leerplicht in gebruik genomen (Jeugd Volg Systeem, JVS). De applicatie wordt verder vervolmaakt met medenemen van de aanbevelingen uit de audits.

Alle directies hebben te maken met verouderde convenanten als gevolg van nieuwe wetgeving (bijvoorbeeld de Wet gegevensverwerking door samenwerkingsverbanden). Deze liggen aan de basis van gegevensuitwisselingen met maatschappelijke partners. Het actualiseren van deze convenanten is onderhanden. De hoeveelheid ketenpartners maakt dit tot tijdrovend proces; het belang ervan wordt echter volledig onderkend.

Voor de toekomst zullen de inspanningen onverminderd blijven. In de lopende processen moet bij de eerstkomende audits de werking van de maatregelen worden aangetoond. Ook bij wijzigingen in processen of systemen moet worden geborgd dat deze aan de Wpg blijven voldoen.

Als auditee danken we DMC voor de goede samenwerking en de snelheid waarmee de audit is uitgevoerd. De ruimte voor de tussentijdse afstemming is als prettig ervaren. We zien uit naar een vervolg in de samenwerking voor de interne Wpg audits in de komende jaren.

Datum status opvolging van aanbevelingen

Het auditteam en de auditee hebben de afspraak gemaakt om zes maanden na oplevering van het definitieve auditrapport een gesprek te voeren over de opvolging van de aanbevelingen. Dit zal plaatsvinden op 14 januari 2027.

Actiehouder

De actiehouder voor de aanbevelingen zijn:

- THOR: proceseigenaar en -beheerder tikverbalen
- Inkomen: de expert uitvoering
- Onderwijs: adviseur Kennis en Informatie Leerplicht

3. Oordeel

Onderstaande tabellen nemen we op in onze auditrapportage en in de short form t.b.v. de Autoriteit Persoonsgegevens (AP). Dit is overeenkomstig de vermelding van ACAM in paragraaf 1.8. Onderdeel van onze audit waren alle normen waarop ACAM aanbevelingen heeft gegeven. Dit kunnen ook normen betreffen die in opzet en bestaan al als voldoen (groen) waren aangemerkt en voor werking een andere conclusie kenden. Ook voor deze onderwerpen is opzet en bestaan voor de invulling van de aanbeveling van de ACAM getoetst. De kolom Werking in de tabel Hercontrole is leeg gelaten om daarmee zichtbaar te maken dat de hercontrole alleen betrekking heeft op toetsing van opzet en bestaan en niet op onderzoek van de werking, dit in overeenstemming met de aanwijzing van de AP.

Toelichting gebruikte kleuren:

Groen - De beheersingsmaatregelen voldoen;
Oranje - De beheersingsmaatregelen voldoen deels. Om geheel aan de beheersingsmaatregelen te voldoen dien(t)(en) de resterende geconstateerde afwijking(en) te worden opgelost;
Rood - De beheersingsmaatregelen voldoen niet. Om aan de beheersingsmaatregelen te voldoen dien(t)(en) de resterende geconstateerde afwijking(en) te worden opgelost;
Grijs – Met goede reden niet toetsbaar. Bij de controls in scope van de hercontrole is in de kolommen voor hercontrole de reden vermeld. NO = non occurence, niet toetsbaar wegens geen data. Bij niet getoetst wegens geen aanbeveling externe audit en daarmee buiten scope is BS (= buiten scope) vermeld.
TZM = toezichtsmaatregelen (dit betreft de normen 29 en 31)

De redenen waarom normen niet zijn onderzocht in de externe audit zijn door de extern accountant 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.

Tabel 1 Conclusies realisatie aanbevelingen directies THOR en Sport & Bos (Domein I, II en IV)

Toezicht en handhaving van milieudelicten en openbare ruimte & aanpak van ernstige overlast in openbaar vervoer	Externe audit					Hercontrole		
	Opzet juni 2024	Bestaan juni 2024	Opzet december 2024	Bestaan december 2024	Werking jan-dec 2024	Opzet juni 2026	Bestaan juni 2026	Werking
1. Reikwijdte								
2. Doelbinding								
3. Noodzakelijkheid en rechtmatigheid, vermelding herkomst								
4. Juistheid en volledigheid politiegegevens								
5. Onderscheid feiten en oordeel								
6. Gegevensbescherming door beveiliging en ontwerp								
7. Gegevensbescherming door standaardinstellingen								
8. Gegevensbeschermingseffectbeoordeling/ Data protection impact assessment (DPIA)								
9. Bijzondere categorieën van politiegegevens								
10. Autorisaties en toegang tot politiegegevens								
11. Autorisaties: aanwijzen functionarissen	**	**	**	**	**			
12. Onderscheid tussen verschillende categorieën van betrokkenen								
13. Verwerker en Verwerkersovereenkomst								
14. Geheimhoudingsplicht								
15. Geautomatiseerde individuele besluitvorming	**	**	**	**	**			
16. Uitvoering van de dagelijkse politietaak								
17. Ter beschikking stellen van politiegegevens binnen het WPG-domein								
18. Geautomatiseerd vergelijken en in combinatie zoeken	**	**	**	**	**			
19. Ondersteunende taken	**	**	**	**	**			
20. Bewaartermijnen, verwijderen en vernietigen							NO	

Toezicht en handhaving van milieudelicten en openbare ruimte & aanpak van ernstige overlast in openbaar vervoer	Externe audit					Hercontrole		
	Opzet juni 2024	Bestaan juni 2024	Opzet december 2024	Bestaan december 2024	Werking jan-dec 2024	Opzet juni 2026	Bestaan juni 2026	Werking
21. Verstrekking van politiegegevens aan anderen dan politie en Koninklijke marechaussee							NO	
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							NO	
29. Audits (toezichtsmaatregel)	TZM	TZM	TZM	TZM	TZM	TZM	TZM	TZM
30. Melding datalekken								
31. Functionaris voor gegevensbescherming (toezichtsmaatregel)	TZM	TZM	TZM	TZM	TZM	TZM	TZM	TZM

Technische en organisatorische maatregelen informatiesysteem CityControl	Externe audit					Hercontrole		
	Opzet juni 2024	Bestaan juni 2024	Opzet december 2024	Bestaan december 2024	Werking jan-dec 2024	Opzet juni 2026	Bestaan juni 2026	Werking
1. Wijzigingenbeheer								
2. Logische toegangsbeveiliging								
3. Beheer van kwetsbaarheden (patchmanagement)								
4. Cryptografie								
5. Vulnerability scans en Penetratietesten								

Tabel 2 Conclusies realisatie aanbevelingen directie Onderwijs (Domein III)

De directie heeft in maart van dit jaar een nieuwe applicatie geïmplementeerd.

Toezicht en handhaving van milieudelicten en openbare ruimte & aanpak van ernstige overlast in openbaar vervoer	Externe audit					Hercontrole		
	Opzet juni 2024	Bestaan juni 2024	Opzet december 2024	Bestaan december 2024	Werking jan-dec 2024	Opzet juni 2026	Bestaan juni 2026	Werking
1. Reikwijdte								
2. Doelbinding								
3. Noodzakelijkheid en rechtmatigheid, vermelding herkomst		***						
4. Juistheid en volledigheid politiegegevens		***						
5. Onderscheid feiten en oordeel		***						
6. Gegevensbescherming door beveiliging en ontwerp								
7. Gegevensbescherming door standaardinstellingen		***						
8. Gegevensbeschermingseffectbeoordeling/ Data protection impact assessment (DPIA)								
9. Bijzondere categorieën van politiegegevens								
10. Autorisaties en toegang tot politiegegevens								
11. Autorisaties: aanwijzen functionarissen	**	**	**	**	**			
12. Onderscheid tussen verschillende categorieën van betrokkenen		***						
13. Verwerker en Verwerkersovereenkomst		***						

Toezicht en handhaving van milieudelicten en openbare ruimte & aanpak van ernstige overlast in openbaar vervoer	Externe audit					Hercontrole		
	Opzet juni 2024	Bestaan juni 2024	Opzet december 2024	Bestaan december 2024	Werking jan-dec 2024	Opzet juni 2026	Bestaan juni 2026	Werking
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	***	***					NO	
29. Audits (toezichtsmaatregel)	TZM	TZM	TZM	TZM	TZM	TZM	TZM	TZM
30. Melding datalekken		*		*	*			
31. Functionaris voor gegevensbescherming (toezichtsmaatregel)	TZM	TZM	TZM	TZM	TZM	TZM	TZM	TZM

Technische en organisatorische maatregelen Informatiesystemen: Erisa (tot en met 31 juli 2024) en BRS (vanaf 1 augustus 2024)	Externe audit					Hercontrole		
	Opzet juni 2024	Bestaan juni 2024	Opzet december 2024	Bestaan december 2024	Werking jan-dec 2024	Opzet juni 2026	Bestaan juni 2026	Werking
1. Wijzigingenbeheer	***	***			***			
2. Logische toegangsbeveiliging	***	***			***			
3. Beheer van kwetsbaarheden (patchmanagement)	***	***			***			
4. Cryptografie	***	***			***			
5. Vulnerability scans en Penetratietesten	***	***			***			

Tabel 3 Conclusies realisatie aanbevelingen directie Inkomen (Domein V)

Toezicht en handhaving van milieudelicten en openbare ruimte & aanpak van ernstige overlast in openbaar vervoer	Externe audit					Hercontrole		
	Opzet juni 2024	Bestaan juni 2024	Opzet december 2024	Bestaan december 2024	Werking jan-dec 2024	Opzet juni 2026	Bestaan juni 2026	Werking
1. Reikwijdte								
2. Doelbinding								
3. Noodzakelijkheid en rechtmatigheid, vermelding herkomst								
4. Juistheid en volledigheid politiegegevens		***						
5. Onderscheid feiten en oordeel								
6. Gegevensbescherming door beveiliging en ontwerp								
7. Gegevensbescherming door standaardinstellingen								

Toezicht en handhaving van milieudelicten en openbare ruimte & aanpak van ernstige overlast in openbaar vervoer	Externe audit					Hercontrole		
	Opzet juni 2024	Bestaan juni 2024	Opzet december 2024	Bestaan december 2024	Werking jan-dec 2024	Opzet juni 2026	Bestaan juni 2026	Werking
8. Gegevensbeschermingseffectbeoordeling/ Data protection impact assessment (DPIA)								
9. Bijzondere categorieën van politiegegevens							NO	
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	***	***		***	***		NO	
29. Audits (toezichtsmaatregel)	TZM	TZM	TZM	TZM	TZM	TZM	TZM	TZM
30. Melding datalekken		*		*	*			
31. Functionaris voor gegevensbescherming (toezichtsmaatregel)	TZM	TZM	TZM	TZM	TZM	TZM	TZM	TZM

Technische en organisatorische maatregelen Informatiesystemen: Sherlock (tot en met 30 juni 2024) en BRS (vanaf 1 juli 2024)	Externe audit					Hercontrole		
	Opzet juni 2024	Bestaan juni 2024	Opzet december 2024	Bestaan december 2024	Werking jan-dec 2024	Opzet juni 2026	Bestaan juni 2026	Werking
1. Wijzigingenbeheer	***	***			***			
2. Logische toegangsbeveiliging	***	***			***			
3. Beheer van kwetsbaarheden (patchmanagement)	***	***			***			
4. Cryptografie	***	***			***			
5. Vulnerability scans en Penetratietesten	***	***			***			

4. 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 NOREA Handreiking Privacy audit Wpg (boa). Die illustratieve beheersingsmaatregelen zijn gebaseerd op de Wet politiegegevens en het Besluit politiegegevens buitengewoon opsporingsambtenaren en omvatten de te verwachten onderwerpen en -beheersingsmaatregelen, gericht op beheersing van privacy in gegevensverwerkende processen en indicatieve controles, in lijn met de geldende wet- en regelgeving.

Onderstaand zijn deze onderwerpen en illustratieve beheersingsmaatregelen weergegeven.

Onderwerpen en beheersingsmaatregelen
1. Reikwijdte De verwerkingsverantwoordelijke heeft bestanden met politiegegevens binnen de organisatie geïdentificeerd en gedocumenteerd.
2. Doelbinding Politiegegevens worden alleen verwerkt als dat nodig is voor de in de wet genoemde doeleinden. Geborgd is dat bij het verwerken van politiegegevens altijd sprake is van doelbinding en dat de gegevens niet op een, met die doeleinden onverenigbare wijze, worden verwerkt.
3. Noodzakelijkheid en rechtmatigheid, vermelding herkomst Er wordt geborgd dat de politiegegevens daartoe toereikend, ter zake dienend en beperkt zijn tot wat noodzakelijk is (niet bovenmatig) en dat de herkomst van gegevens voor art 9 verwerkingen wordt vermeld.
4. Juistheid en volledigheid politiegegevens • De verwerkingsverantwoordelijke heeft controles op de kwaliteit ingericht ten behoeve van de borging van de juistheid en nauwkeurigheid van politiegegevens. • Er zijn procedures opgesteld voor het vernietigen en rectificeren van politiegegevens.
5. Onderscheid feiten en oordeel Er zijn maatregelen genomen om politiegegevens die op feiten zijn gebaseerd, voor zover mogelijk, te onderscheiden van politiegegevens die op een persoonlijk oordeel zijn gebaseerd.
6. Gegevensbescherming door beveiliging en ontwerp • Er is (aantoonbaar) een risicoanalyse uitgevoerd waaruit het risiconiveau blijkt en identificeert, evalueert en mitigeert systematisch en periodiek factoren die het beschermen van politiegegevens tegen ongeoorloofde of onrechtmatige verwerking en tegen opzettelijk verlies, vernietiging of beschadiging in gevaar brengen en past de maatregelen hierop aan. • De organisatie heeft gegevensbeschermingsbeleid en procedures ontwikkeld en vastgesteld. De verwerkingsverantwoordelijke heeft de maatregelen die nodig zijn om het risico te beperken (passende technische en organisatorische maatregelen) aantoonbaar geïmplementeerd. • Privacy by design wordt toegepast/geborgd (bijv. bij ontwikkelingen/ wijzigingen). • De verwerkingsverantwoordelijke kan aantonen dat de verwerking van politiegegevens wordt verricht in overeenstemming met wat bepaald is in de wet.
7. Gegevensbescherming door standaardinstellingen De verwerkingsverantwoordelijke treft passende technische en organisatorische maatregelen om te waarborgen dat standaard: • 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. Gegevensbeschermingseffectbeoordeling / 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 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

Onderwerpen en beheersingsmaatregelen
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 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 gebaseerd uitsluitend op geautomatiseerde verwerking dat voor de betrokkene nadelige rechtsgevolgen heeft of hem in aanmerkelijke mate treft, worden niet genomen tenzij voorzien is in de voorwaarden genoemd in de wet. • Het verbod op het gebruik van profilering die leidt tot discriminatie van personen op grond van de bijzondere categorieën van politiegegevens (art 5) is bekend binnen de organisatie. Dit beperkte verbod op profilering is onderwerp van de bewustwordingssessies binnen de organisatie.
16. Uitvoering van de dagelijkse politietaak • 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.
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 ambtenaren van politie die daarvoor geautoriseerd zijn. • Geborgd is dat de ambtenaren die geautomatiseerd vergelijken en ambtenaren die in combinatie zoeken over voldoende kennis en vaardigheden beschikken.
19. Ondersteunende taken Geborgd is dat voor de verwerkingen bedoeld in art 13 lid 1 t/m 3, van tevoren is voldaan aan de schriftelijke vereisten (art 13 lid 4).
20. Bewaartermijnen, verwijderen en vernietigen • 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.

Onderwerpen en beheersingsmaatregelen
• 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.
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 gegevens bevat zoals aangegeven in art 31d lid 1. • De verwerker houdt een register bij dat de gegevens bevat zoals aangegeven in art 31d lid 2.
27. Documentatie • 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 logging van verwerkingen zoals opgenomen in art 32a lid 1. • De organisatie gebruikt de logging uitsluitend ter controle van de rechtmatigheid van de gegevensverwerkingen, interne controles, ter waarborging van de integriteit en de beveiliging van politiegegevens en voor strafrechtelijke procedures.
29. Audits • Er wordt uitvoering gegeven aan de eisen zoals gesteld in de Regeling periodieke audit politiegegevens.
30. Melding datalekken

Onderwerpen en beheersingsmaatregelen
• 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.

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.