Gemeente Amsterdam

Auditrapport – *short form*

Privacy audit Wet politiegegevens Domein I, II, IV, V

Referentie: AOJP/2023audit10/2024audit19

Opdrachtgever: Concerncontroller

Auteur: Interne Audit en Beleidsonderzoek

Proceseigenaren: Directie Inkomen, Toezicht en Handhaving Openbare Ruimte en Sport en Bos

31-01-2024 (definitieve versie 1.0)

1 Inleiding

Sinds 1 januari 2019 is de Wet politiegegevens (Wpg) van toepassing op buitengewoon opsporingsambtenaren (boa's) die gegevens verwerken in het kader van hun opsporingstaak. Aangezien er binnen de gemeente Amsterdam binnen verschillende directies boa's werkzaam zijn met een opsporingstaak, moet ook de gemeente Amsterdam aan deze wetgeving voldoen.

In 2021 is een verplichte externe privacy audit uitgevoerd door ACAM (de accountant van Amsterdam) naar de Wpg binnen de gemeente Amsterdam. Uit deze externe audit is gebleken dat de gemeente Amsterdam de beheersingsmaatregelen om te voorzien in de borging van de wettelijke eisen met betrekking tot de verwerking van politiegegevens door boa's niet op afdoende wijze heeft geïmplementeerd. De Wpg verplicht om jaarlijks een interne audit naar de toepassing van de Wpg in de gemeente uit te voeren (artikel 3 lid 1 regeling periodieke audit politiegegevens). Daarnaast schrijft artikel 33 lid 3 van de Wpg voor dat de verwerkingsverantwoordelijke binnen een jaar een hercontrole dient uit te voeren op de onderdelen die niet voldoen aan de gestelde voorwaarden. ACAM heeft geadviseerd om deze hercontrole uit te laten voeren door de interne auditor (overeenkomstig artikel 4 lid 3 regeling periodieke audit politiegegevens). Met deze audit geven we invulling aan de jaarlijkse interne audit en de hercontroleplicht. Deze audit richt zich op de verwerking van politiegegevens in de domeinen V (Inkomen), II (Sport & Bos) en I/II/IV (Toezicht en Handhaving Openbare Ruimte). In een eerdere interne audit is de verwerking van politiegegevens binnen Domein III (Onderwijs) onderzocht. Zie voor een overzicht van de domeinen tabel 1 en 2.

Domein	Boa-werkterrein
I	Openbare ruimte
II	Milieu, welzijn en infrastructuur
III	Onderwijs

Domein	Boa-werkterrein
IV	Openbaar vervoer
V	Werk, inkomen en zorg
VI	Generieke opsporing

Tabel 1: Domeinen waarin politiegegevens verwerkt kunnen worden. Onderwijs is niet in scope van deze audit. Zie hiervoor eerder uitgebrachte rapportage.

#	Organisatieonderdeel	Domein	Processen/verwerkingen	Applicatie
1	Onderwijs, Jeugd en Zorg – afdeling Onderwijs	III	Toezicht en handhaving op leerplicht en aanpak thuiszitters.	Erisa
2	Inkomen	V	Het uitvoeren van strafrechtelijke (fraude)onderzoeken o.g.v. de Participatiewet, IOAW en IOAZ.	Sherlock
3	Sport en Bos	II	Toezicht en handhaving van milieudelicten.	CityControl
4	Toezicht en Handhaving Openbare Ruimte	I / II / IV	Toezicht en handhaving in de openbare ruimte en aanpak van ernstig overlast in het openbaar vervoer.	CityControl

Tabel 2: Organisatieonderdelen binnen de gemeente Amsterdam waar politiegegevens verwerkt worden. Onderwijs is niet in scope van deze audit. Zie hiervoor eerder uitgebrachte rapportage.

Doelstelling en centrale vraag

Het doel van de audit is om op systematische wijze te toetsen of op adequate wijze uitvoering is gegeven aan de bepalingen van de Wpg.

De volgende onderzoeksvraag is geformuleerd:

'In hoeverre zijn de interne maatregelen en procedures die in de borging van de wettelijke eisen van de Wpg moeten voorzien in opzet en bestaan aanwezig voor de normen die in de externe privacy audit niet aangemerkt zijn als afdoende opgezet en geïmplementeerd voor de domeinen I, II, IV en V?'

Gehanteerde criteria

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

Opzet	De organisatie heeft de beheersingsmaatregelen beschreven die, indien deze werken zoals beschreven, een redelijke mate van zekerheid bieden dat voorzien is in de borging van de wettelijke eisen van de verwerking van politiegegevens.
Bestaan	De organisatie heeft de beheersingsmaatregelen, overeenkomstig met de opzet, daadwerkelijk geïmplementeerd en toegepast.

Leeswijzer

In hoofdstuk 2 hebben wij de samenvatting en conclusies opgenomen. In hoofdstuk 3 zijn de afzonderlijke normen beoordeeld. De bijlagen met specifieke beheersingsmaatregelen zijn geen onderdeel van de short form versie van de rapportage.

2 Samenvatting

In dit onderzoek hebben we onderzocht of de interne maatregelen en procedures die in de borging van de wettelijke eisen van de Wpg moeten voorzien in opzet en bestaan aanwezig zijn voor de normen die in de externe privacy audit niet aangemerkt zijn als afdoende opgezet en geïmplementeerd voor de domeinen I, II, IV en V.

Conclusie

Niet alle beheersingsmaatregelen om te voorzien in de borging van de wettelijke eisen met betrekking tot de verwerking van politiegegevens zijn opgezet en geïmplementeerd. Dit betekent dat de gemeente Amsterdam nu al ruim vijf jaar niet aan de Wpg voldoet. Wel is er sprake van een duidelijke opwaartse lijn ten opzichte van de externe privacy audit over de periode 1 juli 2020 tot en met 30 juni 2021. Zo geldt voor de directies Toezicht en Handhaving Openbare Ruimte (THOR) en Sport en Bos dat er geen normen meer zijn die in het geheel niet voldoen aan de Wpg. Dit komt mede doordat in de applicatie CityControl een onderscheid gemaakt wordt tussen verwerkingen onder de AVG en de Wpg. Dit onderscheid was nog niet gerealiseerd ten tijde van de externe privacy audit.

Met de aanstaande overgang van de applicatie Sherlock naar de applicatie BRS wordt verwacht dat het overgrote deel van de normen voor de directie Inkomen minimaal gedeeltelijk zullen voldoen aan de Wpg. Dit is momenteel nog niet het geval.

Aan de basis van de opwaartse lijn ligt de aanstelling van een Wpg-coördinator die borging van de wettelijke eisen aanjaagt. Dit heeft mede geleid tot een Data Protection Impact Assesment (DPIA) voor de directies Toezicht en Handhaving Openbare Ruimte, Sport en Bos en Inkomen. Hierin zijn de (privacy)risico's inclusief tekortkomingen in de beheersing van de risico's in kaart gebracht. Dit is het uitgangspunt voor de implementatie van noodzakelijke maatregelen. Voorbeelden van concreet getroffen maatregelen zijn: het opnemen van verwerkingen in een verwerkingsregister, opstellen van specifieke privacyverklaringen en het inrichten van het inzageproces voor de Wpg. Daarnaast valt op dat ten tijde van de externe privacy audit veel centraal beleid bijna uitsluitend gericht was op de AVG. Inmiddels zijn veel beleidsstukken Wpg-specifiek of Wpg-inclusief gemaakt. Sommige van deze stukken zijn momenteel nog onderhanden.

Tegelijkertijd blijft er ook ruimte voor verbetering. Hier wordt door de directies aan gewerkt. De belangrijkste aandachtspunten hebben we hier opgenomen inclusief aanbevelingen.

Algemene aandachtspunten

We zien een aantal aandachtspunten die gelden voor alle directies / domeinen.

- Bij het verstrekken van gegevens dient duidelijk te zijn wat de beoogde ontvanger met de gegevens gaat doen (doelbinding), of alle gegevens die verstrekt worden noodzakelijk zijn voor dat doel en of hier een grondslag voor is. Op dit moment is niet altijd bepaald of de verstrekking noodzakelijk is en of voor de verstrekking een grondslag aanwezig is. Zo worden veel gegevens gedeeld naar de applicatie Focus bij Inkomen en worden gegevens grotendeels ongefilterd vanuit CityControl via een API gedeeld naar een data warehouse waartoe OOV en de Stadsdelen toegang hebben.
- Het ontbreekt veelal aan formele procedures en werkinstructies. Zo zijn er directie overstijgend geen formele procedures ten aanzien van de actualisatie van DPIA's en het opstellen en onderhouden van het verwerkingsregister. Directie specifiek ontbreekt het aan werkinstructies voor het uitvoeren van controles en het opstellen van tikverbalen.

Specifieke aandachtspunten directies THOR en Sport en Bos

Tikverbalen worden in de regel opgeslagen op persoonlijke schijven van boa's. Omdat deze niet in CityControl worden verwerkt, is het risico aanwezig dat de politiegegevens op de persoonlijke netwerkschijven niet worden beheerd

volgens de Wpg-vereisten rondom informatiebeveiliging, logging, beschikkingstelling en bewaartermijnen. Daarnaast is er een risico op onjuiste en/of onvolledige registratie van politiegegevens. Dit risico is voor registraties in CityControl beperkt.

Specifieke aandachtspunten directie Inkomen

We hebben geconstateerd dat de applicatie Sherlock afdoende beveiliging van politiegegevens niet waarborgt. De applicatie dwingt geen privacy af door standaardinstellingen (privacy by design en privacy by default). Momenteel wordt de applicatie Sherlock vervangen door de applicatie BRS. Vanuit de directie Inkomen is aangegeven dat de migratie zal plaatsvinden in Q1 2024. De verwachting is dat de inrichting van de applicatie BRS wel privacy zal waarborgen. Het waarborgen van de veiligheid en de integriteit van gegevens in de overgangsperiode van de applicatie Sherlock naar de applicatie BRS, waaronder de migratie van gegevens, is een aandachtspunt.

Aanbevelingen

- Alle directies / domeinen: bepaal per verstrekking het doel en de grondslag van de verstrekking en neem dit op in een verstrekkingen-register. Voer daarnaast periodiek controles uit op of niet teveel gegevens voor het doel van de verstrekking gedeeld worden (noodzakelijkheid/ proportionaliteit).
- Alle directies / domeinen: stel procedures en werkinstructies op voor directie overstijgende en directie specifieke processen en laat deze procedures en werkinstructies vaststellen. Team bewust verbeteren kan gevraagd worden hierbij te ondersteunen.
- Directies THOR en Sport en Bos: tref aanvullende beheersmaatregelen voor de verwerking van politiegegevens die buiten de applicatie CityControl plaatsvinden. Dit betreffen de tikverbalen. Begin met het opstellen van een beheersprocedure waarin het beheer conform de Wpg is geregeld (zie ook benoemde maatregel DPIA).
- Directie Inkomen: tref tijdelijke maatregelen die voorzien in het waarborgen van veiligheid en de integriteit van de politiegegevens in de overgangsfase van de applicatie Sherlock richting de applicatie BRS.

Managementreactie

Het management van de directies waar de audit betrekking op heeft, te weten de directies Toezicht en Handhaving Openbare Ruimte, Sport en Bos en Werk, Participatie en Inkomen, heeft met grote belangstelling kennisgenomen van de resultaten van het auditrapport. De audit dient voornamelijk om inzicht te krijgen in de vraag, of er bij de implementatie van de Wet Politiegegevens, voor zover van toepassing op boa's, voldoende vooruitgang is geboekt om binnen afzienbare tijd in de verwerking van persoonsgegevens aan de wettelijke voorwaarden te voldoen. De audit geeft hierin ruimschoots inzicht en de resultaten stemmen hoopvol. De aanbevelingen die worden gedaan zullen wij overnemen.

Het beoogde doel is een ruim voldoende compliance score bij de volgende externe audit die in 2025 zal worden afgenomen (en het jaar 2024 betreft). De resultaten van de voorliggende audit wijzen erop dat we op de goede weg zijn. Een groot aantal normen waar in 2021 in het geheel niet aan werd voldaan, wordt nu deels aan voldaan, en het aantal normen waaraan volledig wordt voldaan is ook toegenomen.

De auditor merkt terecht op dat er nog ruimte is voor verbetering. Die opvatting delen wij volledig en de aanbevelingen nemen wij voor het vervolg ter harte. Deze vallen eigenlijk in drie soorten uiteen: aanbevelingen tot maatregelen van technische aard (overgang naar andere ICT-systemen), aanbevelingen van procesmatige aard (het formaliseren van beleid en werkinstructies) en aanbevelingen van organisatorische aard (betere grip op gegevensdeling). De maatregelen van technische aard vergen het meeste tijd, tegelijkertijd kunnen wij constateren dat deze veranderingen al in gang zijn gezet. De auditor merkt terecht op dat niet alleen de hoofdapplicaties voor de verwerking van politiegegevens aandacht verdienen, maar ook de gewone systemen waarop tikverbalen worden verwerkt. Procesmatige aanbevelingen zullen binnen de betreffende directies verder worden uitgewerkt en voor de stedelijke en organisatorische maatregelen wordt vanuit de directie Digitale Strategie en Innovatie gewerkt aan beleidsvoorstellen en stedelijke coördinatie. Mede hiervoor is in de zomer van 2023 een coördinator (tevens privacy officer) Wpg aangesteld. Deze adviseert, ondersteunt en coördineert in het vervolg van het implementatieproces.

Zoals de auditor opmerkt, zijn er ook DPIA's (risicoanalyses) uitgevoerd voor de Wpg verwerkingen bij de betreffende directies. Hieruit is een set maatregelen voortgekomen dat samen met de aanbevelingen van de auditor de onderlegger zal vormen voor onze uit te voeren verbeteringen in het komend jaar. Hiervoor wordt momenteel een planning opgesteld door de coördinator in samenspraak met de directies. Op die manier willen wij de opgaande lijn die de auditor constateert, voortzetten op weg naar compliance. Wij danken de auditor voor de bijdrage aan dit proces met de gedetailleerde audit die in zo een korte tijd zo grondig is uitgevoerd.

Mark Crooijmans, CIO
Directie Digitale Strategie en Informatie

3 Oordeel

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

3.1 Directie Inkomen - het uitvoeren van strafrechtelijke (fraude)onderzoeken o.g.v. Participatiewet, IOAW en IOAZ

Onderwerpen	Publicatie rapportage 2022		Publicatie rapportage 2024	
	Opzet ACAM	Bestaan ACAM	Opzet	Bestaan
1. Reikwijdte				
2. Doelbinding				
3. Noodzakelijkheid en rechtmatigheid, vermelding herkomst				
4. Juistheid en volledigheid politiegegevens				
5. Onderscheid feiten en oordeel	N.o.[1]	N.o.[1]		N.o.[1]
6. Gegevensbescherming door beveiliging en ontwerp				
7. Gegevensbescherming door standaardinstellingen				
8. Gegevensbeschermingseffectbeoordeling/ Data protection impact assessment (DPIA)				
9. Bijzondere categorieën van politiegegevens	N.o.[1]	N.o.[1]		
10. Autorisaties en toegang tot politiegegevens			N.i.s.[4]	
11. Autorisaties: aanwijzen functionarissen	N.v.t.[5]	N.v.t.[5]		
12. Onderscheid tussen verschillende categorieën van betrokkenen	N.o.[1]	N.o.[1]		N.o.[1]
13. Verwerker en Verwerkersovereenkomst	N.o.[1]	N.o.[1]	N.v.t.[2]	N.v.t.[2]
14. Geheimhoudingsplicht		N.o.[1]		
15. Geautomatiseerde individuele besluitvorming	N.v.t.[5]	N.v.t.[5]		
16. Uitvoering van de dagelijkse politietaak				
17. Ter beschikking stellen van politiegegevens binnen het Wpg-domein	N.o.[1]	N.o.[1]		
18. Geautomatiseerd vergelijken en in combinatie zoeken	N.o.[1]	N.o.[1]	N.v.t.[2]	N.v.t.[2]
19. Ondersteunende taken	N.o.[1]	N.o.[1]	N.v.t.[2]	N.v.t.[2]
20. Bewaartermijnen, verwijderen en vernietigen				
21. Verstrekking van politiegegevens aan anderen dan politie en Koninklijke marechaussee	N.o.[1]	N.o.[1]		
22. Doorgiften aan derde landen	N.o.[1]	N.o.[1]	N.v.t.[2]	N.v.t.[2]

23. Verstrekking aan derden structureel voor samenwerkingsverbanden	N.o.[1]	N.o.[1]	N.v.t.[2]	N.v.t.[2]
24. Rechtstreekse verstrekking	N.o.[1]	N.o.[1]	N.v.t.[2]	N.v.t.[2]
25. Informatie aan de betrokkene, recht op inzage, rectificatie en verwijdering		N.o.[1]		N.v.t.[3]
26. Register				
27. Documentatie		N.o.[1]		
28. Logging				
29. Audits				
30. Melding datalekken		N.v.t.[5]	N.i.s.[4]	N.v.t.[3]
31. Functionaris voor gegevensbescherming				

	Publicatie rapportage 2022		Publicatie rapportage 2024	
Technische en organisatorische maatregelen Applicatie: Sherlock Onderwerpen	**Opzet ACAM**	**Bestaan ACAM**	**Opzet**	**Bestaan**
1. Wijzigingenbeheer	N.o.[1]	N.o.[1]	N.o.[1]	N.o.[1]
2. Logische toegangsbeveiliging			N.o.[1]	N.o.[1]
3. Beheer van kwetsbaarheden (patchmanagement)	N.o.[1]	N.o.[1]	N.o.[1]	N.o.[1]
4. Cryptografie	N.o.[1]	N.o.[1]	N.o.[1]	N.o.[1]
5. Vulnerability scans en penetratietesten	N.o.[1]	N.o.[1]		

[1] Niet onderzocht omdat we geen of onvoldoende controle informatie hebben ontvangen om de norm te kunnen vaststellen – N.o. [1]

[2] Niet van toepassing. In de DPIA is aangegeven dat deze norm niet speelt binnen de directie – N.v.t [2]

[3] Niet van toepassing omdat met betrekking tot deze norm geen politiegegevens verwerkt zijn binnen de verslagperiode – N.v.t.[3]

[4] Niet in scope Deze norm is in de externe privacy audit als voldoende beoordeeld. De hercontrole richt zich uitsluitend op de normen die niet als voldoende zijn beoordeeld. De beoordeling vanuit de externe privacy audit is overgenomen – N.i.s.[4]

[5] Niet van toepassing omdat in de externe privacy audit uit een interview bleek dat deze norm niet speelt binnen de directie – N.v.t.[5]

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

Onderwerpen	Publicatie rapportage 2022		Publicatie rapportage 2024	
	Opzet ACAM	Bestaan ACAM	Opzet	Bestaan
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			N.i.s.[4]	N.i.s.[4]
10. Autorisaties en toegang tot politiegegevens				
11. Autorisaties: aanwijzen functionarissen	N.o.[1]	N.o.[1]	N.v.t.[2]	N.v.t.[2]
12. Onderscheid tussen verschillende categorieën van betrokkenen			N.i.s.[4]	N.i.s.[4]
13. Verwerker en Verwerkersovereenkomst		N.o.[1]	N.i.s.[4]	
14. Geheimhoudingsplicht		N.o.[1]	N.i.s.[4]	
15. Geautomatiseerde individuele besluitvorming	N.v.t.[5]	N.v.t.[5]	N.v.t.[2]	N.v.t.[2]
16. Uitvoering van de dagelijkse politietaak				
17. Ter beschikking stellen van politiegegevens binnen het Wpg-domein	N.v.t.[5]	N.v.t.[5]		
18. Geautomatiseerd vergelijken en in combinatie zoeken	N.v.t.[5]	N.v.t.[5]	N.v.t.[2]	N.v.t.[2]
19. Ondersteunende taken	N.v.t.[5]	N.v.t.[5]	N.v.t.[2]	N.v.t.[2]
20. Bewaartermijnen, verwijderen en vernietigen		N.o.[1]		
21. Verstrekking van politiegegevens aan anderen dan politie en Koninklijke marechaussee				
22. Doorgiften aan derde landen	N.v.t.[5]	N.v.t.[5]	N.v.t.[2]	N.v.t.[2]
23. Verstrekking aan derden structureel voor samenwerkingsverbanden	N.o.[1]	N.o.[1]		N.o.[1]
24. Rechtstreekse verstrekking	N.v.t.[5]	N.v.t.[5]	N.o.[1]	N.o.[1]
25. Informatie aan de betrokkene, recht op inzage, rectificatie en verwijdering		N.v.t.[3]		N.v.t.[3]
26. Register				

27. Documentatie				
28. Logging				
29. Audits				
30. Melding datalekken		N.v.t.[3]	N.i.s.[4]	N.v.t.[3]
31. Functionaris voor gegevensbescherming				

Technische en organisatorische maatregelen Applicatie: CityControl Onderwerpen	Publicatie rapportage 2022		Publicatie rapportage 2024	
	Opzet ACAM	Bestaan ACAM	Opzet	Bestaan
1. Wijzigingenbeheer		N.o.[1]		
2. Logische toegangsbeveiliging	N.o.[1]	N.o.[1]		
3. Beheer van kwetsbaarheden (patchmanagement)	N.o.[1]	N.o.[1]		
4. Cryptografie	N.o.[1]	N.o.[1]		
5. Vulnerability scans en penetratietesten				

[1] Niet onderzocht omdat we geen of onvoldoende controle informatie hebben ontvangen om de norm te kunnen vaststellen – N.o. [1]
[2] Niet van toepassing. In de DPIA is aangegeven dat deze norm niet speelt binnen de directie – N.v.t.[2]
[3] Niet van toepassing omdat met betrekking tot deze norm geen politiegegevens verwerkt zijn binnen de verslagperiode – N.v.t.[3]
[4] Niet in scope. Deze norm is in de externe privacy audit als voldoende beoordeeld. De hercontrole richt zich uitsluitend op de normen die niet als voldoende zijn beoordeeld. De beoordeling vanuit de externe privacy audit is overgenomen – N.i.s.[4]
[5] Niet van toepassing omdat in de externe privacy audit uit een interview bleek dat deze norm niet speelt binnen de directie – N.v.t.[5]