Gemeente Amsterdam

Auditrapport – *short form*

Privacy-audit Wet politiegegevens – Directie OJZD – Onderwijs – afdeling Leerplicht

Referentie: VIC2022/audit#22

Opdrachtgever: Concerncontroller

Auteur: Interne audit en Beleidsonderzoek

Proceseigenaar: Directie Onderwijs, Jeugd, Zorg en Diversiteit

28 juli 2023 (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). Eén keer in de vier jaar vindt een externe privacy audit plaats (artikel 6:5 lid 1 besluit politiegegevens). In de tussenliggende jaren zal de interne audit zich richten op de verschillende afdelingen binnen de gemeente die politiegegevens verwerken of die daar een belangrijke rol in hebben. Zoals de toezichthoudende rol van de Functionaris Gegevensbescherming (FG) op de Wpg en de beleid- en kaderstellende rol van de afdeling Beleid en Kaderstelling binnen de directie Digitale Strategie en Informatie (DS&I).

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 eerste interne audit op de Wpg zal zich richtten op Domein III (Onderwijs).

Doelstelling en centrale vraag

Het doel van de audit is om op systematische wijze te toetsen of aan de bepalingen van de wet op adequate wijze uitvoering is gegeven. Daarnaast biedt de audit aanbevelingen met betrekking tot een effectieve en efficiënte implementatie 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 binnen de gemeente voor domein III en in hoeverre zijn deze maatregelen effectief en efficiënt?'

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 bij deze hercontrole 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 van de verwerking van politiegegevens.
Bestaan	De organisatie heeft de beheersingsmaatregelen overeenkomstig 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 en conclusies

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 binnen de gemeente voor domein III en in hoeverre deze maatregelen effectief en efficiënt zijn. De focus van deze audit ligt op de directie OJZD – Afdeling Onderwijs – team Leerplicht.

Conclusie

De naleving van de Wpg binnen de directie OJZD – afdeling Onderwijs – team Leerplicht (hierna: Leerplicht) is momenteel onvoldoende. Hoewel er belangrijke stappen gezet worden die naleving van de Wpg zullen gaan afdwingen, is de situatie momenteel nog grotendeels ongewijzigd ten opzichte van de externe ACAM-audit in 2021. Belangrijke aandachtspunten zijn de naleving van bewaartermijnen, de documentatieplicht bij de doorgifte of verstrekking van politiegegevens en de autorisatie en toegang tot gegevens. Een klein deel van de normen voldoet wel aan de Wpg. Deze beheersmaatregelen achten we effectief. Dit zijn in opzet de reikwijdte van (politie)gegevens, de verwerkersovereenkomst en de geheimhoudingsplicht. Een efficiëntieslag zal nog gemaakt moeten worden in het moderniseringstraject ERISA.

Er zijn verschillende redenen aan te wijzen voor de onvoldoende naleving van de Wpg:

- Wij hebben geen gemeentebreed beleid aangetroffen waarvan de afdeling Onderwijs - team Leerplicht gebruik kan maken. Aangezien er meerder directies binnen de gemeente Amsterdam te maken hebben met de Wpg, zouden we hiervoor overkoepelend beleid verwachten. Bekend is dat ten tijde van de uitvoering van de externe privacy audit vanuit ACAM dit beleid er niet was. Het ontbreken van gemeenteebreed beleid maakt dat directies hun eigen koers gaan varen. Dit draagt niet bij aan de borging van de wettelijke eisen van de Wpg. Ook is het afzonderlijk opstellen van beleid niet efficiënt. Hier ligt een taak voor de afdeling Beleid en Kaderstelling binnen de directie Digitale Strategie en Informatie (DS&I).
- De afdeling Leerplicht wil de implementatie van beheersingsmaatregelen voor de Wpg combineren met het nog lopende implementatietraject van de Baseline Informatiebeveiliging Overheid (BIO). De Wpg kent een set technische beheersingsmaatregelen die overlappen met de BIO. De afdeling Leerplicht ziet een afhankelijkheid van dit implementatietraject. Ook zien zij het als niet zinvol om deze normen vanuit verschillende hoeken aan te vliegen.
- De applicatie ERISA die binnen de afdeling Leerplicht gebruikt wordt voor het vastleggen van politiegegevens is niet voor dit specifieke doel ontworpen. Dit maakt dat de naleving van de Wpg niet door de applicatie afgedwongen wordt (privacy by design). Vanuit het moderniseringstraject ERISA wordt binnen Leerplicht gewerkt aan het technisch geschikt maken van de applicatie. Dit moet privacy by design in de toekomst mogelijk maken.
- Binnen Leerplicht is externe kennis binnengehaald met betrekking tot de Wpg. Dit is positief. Het blijft desondanks moeilijk om de kennis omtrent de Wpg daadwerkelijk te borgen binnen de gemeente Amsterdam. Hier loopt Leerplicht ook tegenaan.

Aanbevelingen

Onze aanbevelingen doen we in principe per norm uit ons toetsingskader. Aanvullend hierop hebben we een aantal overkoepelende aanbevelingen die we de afdeling Leerplicht willen meegeven. Dit zijn:

- De directie OJZD – Onderwijs – afdeling Leerplicht is niet de enige directie binnen de gemeente die te maken heeft met de Wpg en is hier ook niet alleen verantwoordelijk voor. Naast de directies die binnen de gemeente politiegegevens verwerken, betreft dit ook de rol van interne toezichthouder (Functionaris Gegevensbescherming), beleid en kaderstelling (afdeling binnen Directies Digitale strategie & Informatie) en de leveranciers (Hydrogenics en KPN). We bevelen Leerplicht aan om nadrukkelijk de afstemming te zoeken met genoemde partijen in het implementatietraject van de Wpg. Vanuit de afdeling Leerplicht hebben we vernomen dat inmiddels op een meer formele manier invulling gegeven wordt aan de afstemming met de directies die ook politiegegevens verwerken (Inkomen, THOR en Sport & Bos).
- De applicatie ERISA wordt gemoderniseerd zodat deze straks geschikter is voor de vastlegging van politiegegevens. Hoewel een positieve ontwikkeling, kent het moderniseringstraject ERISA een lange doorlooptijd. De verwachting is dat niet eerder dan 2024 het gewenste technische fundament gelegd is. De planning is om binnen de applicatie ERISA in Q1 2024 een aantal quick wins te realiseren. Dit betreffen technische beheersmaatregelen. Tot die tijd zullen de politiegegevens die in ERISA vastgelegd worden ook afdoende beheerst dienen te worden. We bevelen dan ook aan om de aanbevelingen zoals benoemd in de bijlage, die niet afhankelijk zijn van het technische fundament van ERISA, spoedig op te volgen en hierbij niet de uitkomsten van het moderniseringstraject af te wachten.

Managementreactie Marije van Mens, hoofd Onderwijs
Directie OJZD – afdeling Onderwijs – team Leerplicht heeft op 27-07-2023 een managementreactie gegeven op dit rapport. Samengevat heeft hoofd Onderwijs als reactie aangegeven:

Binnen Onderwijs onderschrijven wij het belang dat de overheid zorgvuldig om moet gaan met de verwerking van gegevens om incidenten en datalekken te voorkomen. En hierdoor het vertrouwen van de burger niet te schaden. Het toetsen van onze interne maatregelen en procedures is dan ook noodzakelijk. Dit auditrapport draagt bij aan een effectieve en efficiënte implementatie van de Wet Politiegegevens.

De uitkomsten van deze audit komen niet als een verrassing. Deze zijn in lijn met het Assurance rapport privacy audit Wet Politiegegevens uit maart 2022. De timing van deze audit bij team Leerplicht is ongelukkig. Vooraf was bekend dat deze audit niet tot nieuwe inzichten en adviezen zou leiden. En dat het op dit moment voor Leerplicht niet mogelijk is om te voldoen aan alle vereisten die de Wpg aangeeft. Enerzijds omdat wij een modernisering van onze applicatie Erisa moeten doen om dit te kunnen realiseren. Wij werken momenteel richtlijnen uit en nemen daar passende maatregelen om de Wpg te voldoen. De verwachting is dat deze modernisering uiterlijk einde Q2 van 2024 wordt afgerond.

Anderzijds is het op dit moment niet mogelijk om aan alle vereisten van de Wpg te voldoen omdat Leerplicht moet aansluiten op een stedelijk kader. Dit stedelijk kader ontbreekt nog op dit moment en ook de stedelijke expertise is nog niet op orde. Hier wordt aan gewerkt.

Verder wil ik meegeven dat er relatief weinig politiegegevens worden verwerkt binnen team Leerplicht
Binnen team Leerplicht (afdeling Onderwijs) zijn leerplichtambtenaren (LPA) werkzaam. Zij zijn zowel toezichthouder als opsporingsambtenaar. Toezicht houden valt onder de AVG en opsporen valt onder de Wpg. Het werk van de LPA'ers bestaat grotendeels uit toezichthouden (AVG). Pas als er blijkt dat er sprake is van een strafbaar feit, wordt overgegaan tot de Wpg. Dit komt relatief weinig voor. Bij de categorieën van verzuim waarbij een proces-verbaal wordt opgemaakt, zijn dit voor het (school)jaar 2021-2022: 3,4% voor relatief verzuim, 0,1% voor absoluut verzuim en 26,1% voor luxe verzuim.

Tenslotte wil ik opmerken dat wij alle aanbevelingen en adviezen serieus nemen en hard blijven werken aan een efficiënte en effectieve implementatie van de Wpg.

3 Oordeel

Onderstaand de uitkomst van de audit voor Directie OJZD – Onderwijs – afdeling Leerplicht.

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

Toelichting gebruikte kleuren:
Groen - Voldoet aan de beheersingsmaatregel.
Oranje - Voldoet deels aan de beheersingsmaatregel. Om geheel aan de beheersingsmaatregel te voldoen dien(t)(en) de aanbeveling(en) te worden opgevolgd.
Rood - Voldoet niet aan de beheersingsmaatregel.
Donkergrijs - Niet onderzocht (de norm is niet onderzocht vanwege het ontbreken van controle informatie of de norm valt niet binnen de scope van ons onderzoek).
Grijs - Niet van toepassing (de norm is niet van toepassing. De specifieke norm geldt niet voor Leerplicht).

24. Rechtstreekse verstrekking	N.o.	N.o.
25. Informatie aan de betrokkene, recht op inzage, rectificatie en verwijdering	N.o.	N.v.t.
26. Register	N.o.	
27. Documentatie		
28. Logging		
29. Audits	N.o.	N.o.
30. Melding datalekken	N.o.	N.v.t.
31. Functionaris voor gegevensbescherming	N.o.	N.o.

Technische en organisatorische maatregelen Informatiesysteem: ERISA Onderwerpen	Opzet	Bestaan
1. Wijzigingenbeheer		N.o.
2. Logische toegangsbeveiliging		N.o.
3. Beheer van kwetsbaarheden (patchmanagement)	N.v.t.	
4. Cryptografie	N.o.	N.o.
5. Vulnerability scans en penetratietesten	N.o.	N.o.