Gemeente Amsterdam

Annotatie - Rapport vervolgonderzoek: Misbruik van (persoons)gegevens

Datum: 6 januari 2026
Opgesteld door: 5.1, 2, e 5.1, 2, e
Onderwerp: Audit beheersing risico's misbruik persoonsgegevens BRP
Afdeling: WPI B&K, team D&I – Compliance / Privacy

Q&A – Voorbereiding gesprek 16 januari 2026 audit BRP-gegevens

1. Wie nemen deel aan het gesprek en wat is hun rol?

1. **Directie WPI**
   Verantwoordelijk voor de uitvoering van processen, het dagelijks gebruik van BRP-gegevens en het realiseren van verbeteringen in de praktijk.
2. **Interne Audit en Beleidsonderzoek (IA&BO)**
   Toelichting op onderzoeksopzet, bevindingen, conclusies en duiding van risico's.
3. **Compliance Officer**
   Adviserend over privacywetgeving, informatiebeveiliging en haalbaarheid van maatregelen.

2.Waarom is dit onderzoek uitgevoerd?

Het onderzoek is uitgevoerd:

a) ter opvolging van aanbevelingen uit het beleidsonderzoek naar corruptie (2024);
b) naar aanleiding van twee incidenten waarbij BRP-gegevens zijn gelekt naar het criminele circuit;
c) om vast te stellen of de beheersing van het gebruik van BRP-gegevens voldoende is ingericht om misbruik te voorkomen en tijdig te signaleren.

Het onderzoek richt zich op structurele oorzaken en leerpunten, niet op individuele schuldvraag.

3. Wat is de kernconclusie?

De kernconclusie is dat het risico op misbruik van persoonsgegevens vanuit de BRP **onvoldoende wordt beheerst**. Hoewel er randvoorwaarden aanwezig zijn (zoals vastgelegde afspraken, reviews vooraf en opvolging bij incidenten), ontbreken structurele waarborgen in zowel hard controls als soft controls. Hierdoor is het risico op onrechtmatig gebruik reëel en onvoldoende beheerst.

4. Wat komt er in hoofdlijnen uit het onderzoek?

In hoofdlijnen laat het onderzoek zien dat:

a) medewerkers toegang hebben tot meer BRP-gegevens dan noodzakelijk;
b) technische beperkingen op zoekgedrag en dossiervorming ontbreken;
c) logging en actieve monitoring beperkt zijn;
d) leidinggevenden en collega's door gebrek aan informatie weinig zicht hebben op het raadpleeggedrag van medewerkers;
e) structureel toezicht op BRP-gebruik ontbreekt;

f) aanspreken en bekrachtigen vooral plaatsvinden bij ernstige incidenten, terwijl positieve bekrachtiging vrijwel ontbreekt.

Zonder structureel toezicht is het niet mogelijk om afwijkend gedrag tijdig te signaleren, waardoor onrechtmatig gebruik onopgemerkt kan blijven.

5. Hoe komt WPI uit het onderzoek?

WPI komt **niet uitzonderlijk negatief** of positief naar voren ten opzichte van andere directies. Het onderzoeksrapport richt zich op alle directies en niet uitsluitend op WPI. In het rapport worden de directies Werk en Participatie en Inkomen benoemd als best practice bij het gebruik van Suwinet. De directies Werk en Participatie en Inkomen gebruiken Suwinet voor het controleren van uitkeringsaanvragen, met strikte autorisatie, whitelisting en maandelijkse steekproeven op rechtmatig gebruik. Deze aanpak bevordert bewust en zorgvuldig omgaan met persoonsgegevens en wordt daarom in het rapport benoemd als **best practice**.

De bevindingen uit het rapport zijn grotendeels organisatiebreed en hangen samen met gemeentebrede systemen, processen en afhankelijkheden van landelijke ontwikkelingen en softwareleveranciers. Wel geldt dat WPI vanwege het intensieve gebruik van BRP-gegevens extra kwetsbaar is voor de gevolgen van tekortkomingen in beheersing. Dit vraagt om actieve betrokkenheid bij verbetermaatregelen en aandacht voor gedrag en toezicht in de dagelijkse praktijk.

6. Waarom kunnen leidinggevenden nu onvoldoende sturen en aanspreken?

Leidinggevenden worden onvoldoende gefaciliteerd doordat:

a) zij beperkt inzicht hebben in het feitelijke raadpleeggedrag van medewerkers;
b) informatie over gebruik en afwijkingen ontbreekt of niet structureel beschikbaar is;
c) toezicht en monitoring niet structureel zijn ingericht;
d) bekrachtiging vooral reactief plaatsvindt bij ernstige incidenten.

Hierdoor ontbreekt een basis om tijdig te sturen, te corrigeren en gewenst gedrag te bevestigen.

7. Hoe versterken hard controls en soft controls elkaar negatief?

In de huidige situatie versterken tekortkomingen in hard en soft controls elkaar:

- Door technische beperkingen en beperkte monitoring wordt afwijkend gedrag niet of te laat gesignaleerd.
- Door onvoldoende training, onduidelijke regels en een beperkte aanspreekcultuur worden medewerkers niet voldoende ondersteund, beschermd of gecorrigeerd in zorgvuldig gebruik.

Het gevolg is dat het risico op misbruik van persoonsgegevens vanuit de BRP onvoldoende wordt beheerst.

8. Wat kan WPI beter doen?

Ondanks technische beperkingen die deels buiten de directe invloedsfeer van WPI liggen, zijn er duidelijke aanknopingspunten voor verbetering, waaronder:

- beter inzicht creëren voor leidinggevenden in BRP-gebruik;
- structureel toezicht (periodieke monitoring) organiseren, ook zonder volledig geautomatiseerde monitoring;

- investeren in training, bewustwording en herhaling;
- regels expliciet maken en structureel communiceren;
- gewenst gedrag actief benoemen en bekrachtigen, niet alleen corrigeren bij incidenten.

Ook relatief kleine gedragsveranderingen bij medewerkers en leidinggevenden kunnen al leiden tot een meer integere omgang met BRP-gegevens. Overigens kunnen deze aanbevelingen ook van toepassing zijn voor de andere directies die onderzocht zijn.

De Cyberbeveiligingswet treedt waarschijnlijk in het tweede kwartaal van 2026 in werking. De wet ligt op het moment van dit schrijven nog bij de Eerste Kamer ter consultatie. Met de komst van deze wet worden de BIO maatregelen voor alle applicaties verplicht en gecontroleerd door de ACAM. Nu wordt er alleen in het kader van de ENSIA op getoetst. Voor alle applicaties moeten hard en soft controls daarom worden aangescherpt. De voorbereiding van de hard en soft controls bij WPI is al gestart voor de tien bedrijfskritische applicaties, zoals Socrates. Socrates heeft een Makelaarsuite raadpleegscherm. Er is stedelijk een Cyberbeveiligingswet-programma dat WPI helpt bij het implementeren met extra maatregelen. Sommige onderdelen doen wij als WPI zelf en andere zijn stedelijk.

9. Welke verbeterstappen worden voorzien?

In hoofdlijnen kan door WPI worden ingezet op:

- versterking van toegangsbeheer en toepassing van *least privilege* waar mogelijk;
- verbetering van logging en (risicogerichte) monitoring;
- structurele onboarding- en herhaaltraining over omgang met persoonsgegevens;
- expliciete rol van leidinggevenden in toezicht, bespreekbaarheid en voorbeeldgedrag;
- een balans tussen corrigerende en positieve bekrachtiging.

Er is nog geen besluit genomen over gemeentebrede maatregelen die naar aanleiding van dit rapport genomen worden. De directie WPI kan in het gesprek vragen hoe wordt voorkomen dat directies zelf het wiel opnieuw uitvinden en welke steun WPI kan verwachten bij de implementatie van maatregelen.

10. Wat zijn de vervolgstappen?

Het tijdpad voor de vervolgstappen ziet er als volgt uit:

- Week 2 en 3 van januari is ruimte voor deelsessies per directie. Team Interne Audit en Beleidsonderzoek licht dan de specifieke punten relevant voor de directie toe.
- Week 4 van januari wil team IA&BO de aanbevelingensessie houden.
- Week 5 van januari levert IA&BO het rapport voorzien van aanbevelingen aan, aan de stedelijk directeur en de directeuren.

Directie WPI kan IA&BO verzoeken om de uitkomsten van de audit te vertalen naar **concrete en uitvoerbare vervolgstappen**. Daarbij kan de directie WPI specifiek vragen om:

- **Praktische aanbevelingen voor WPI**, met concrete voorbeelden op het gebied van autorisaties, training, monitoring en de rol van leidinggevenden.
- Hoe wordt WPI betrokken bij de aanbevelingensessie die team IA&BO wil houden?

Gemeente Amsterdam

- **Inzicht per directie** in welke onderdelen van hard en soft controls al verder zijn ontwikkeld en welke maatregelen in de praktijk effectief blijken, zodat deze als best practices kunnen worden benut.
- **Duiding van gemeentebrede versus directiespecifieke maatregelen**, inclusief advies over welke verbeteringen logisch zijn om te standaardiseren en waar maatwerk nodig blijft.
- **Advies over prioritering en fasering**, rekening houdend met de omvang van WPI en de uitvoeringsimpact van proceswijzigingen.
- **Voorstel voor opvolging**, waaronder de rol van IA&BO bij monitoring van voortgang en het eventueel uitvoeren van een vervolgtoets.

Samenvatting - Rapport vervolgonderzoek: Misbruik van (persoons)gegevens

Datum: 6 januari 2026
Opgesteld door: 5.1, 2, e 5.1, 2, e

Gemeente Amsterdam

Onderwerp: Audit beheersing risico's misbruik persoonsgegevens BRP
Afdeling: WPI B&K, team D&I – Compliance / Privacy

1. **Aanleiding en context**

Het Gemeentelijk Managementteam (GMT) heeft opdracht gegeven tot een vervolgonderzoek naar de risico's van misbruik van vertrouwelijke persoonsgegevens binnen de gemeentelijke organisatie. Deze opdracht vloeit voort uit twee concrete aanleidingen. Enerzijds betreft dit de opvolging van aanbevelingen uit het beleidsonderzoek naar corruptie (2024). Anderzijds hebben zich in het najaar van 2024 en het voorjaar van 2025 twee ernstige incidenten voorgedaan waarbij gegevens uit de Basisregistratie Personen (BRP) zijn gelekt naar het criminele circuit. Deze incidenten benadrukken de noodzaak om de beheersing van het gebruik van BRP-gegevens opnieuw en verdiepend te onderzoeken.

2. **Doel en aanpak**

Het doel van de audit is inzicht te bieden in de mate waarin het risico op misbruik van persoonsgegevens vanuit de BRP wordt beheerst en of de bestaande beheersmaatregelen dit risico voldoende afdekken.

De afdeling Interne Audit en Beleidsonderzoek (IA&BO) heeft dit onderzoek uitgevoerd in de vorm van een audit met twee fasen:

- Fase 1: een QuickScan gericht op gedrags- en cultuurfactoren (soft controls).
- Fase 2: verdieping op hard controls (zoals toegangsrechten en monitoring) en een nadere analyse van soft controls.

Voor de audit zijn ongeveer zestig interviews gehouden en is relevante documentatie bestudeerd.

3. **Scope**

De audit richt zich op de beheersmaatregelen rondom het gebruik van BRP-gegevens via iBurgerzaken en Makelaarssuite (MKS) binnen de directies Belastingen, Dienstverlening, Werk en Participatie, Inkomen en Toezicht Handhaving Openbare Ruimte (THOR).

4. **Hoofdvraag en deelvragen**

De centrale vraag van de audit luidt: *Wordt het risico op misbruik van persoonsgegevens vanuit de BRP in voldoende mate beheerst en welke lessen kunnen worden getrokken om de bescherming van persoonsgegevens verder te verbeteren?*

Deze vraag is uitgewerkt in deelvragen over:

1. de inrichting en werking van hard controls;
2. de beheersing van gedrags- en cultuurfactoren (soft controls);
3. mogelijke verbeteringen op het gebied van gedrag, toegang, gebruik en monitoring.

5. **Hard controls en soft controls**

De beheersing van risico's rond het gebruik van BRP-gegevens berust op een samenhangend stelsel van hard en soft controls.

a. Hard controls betreffen formele, vastgelegde maatregelen zoals autorisaties, procedures, systemen en toezichtmechanismen.
b. Soft controls hebben betrekking op gedrag, houding en cultuur binnen de organisatie en beïnvloeden hoe medewerkers en leidinggevenden in de praktijk met regels en persoonsgegevens omgaan.

Een goede balans tussen beide is essentieel: soft controls versterken hard controls door gewenst gedrag te stimuleren, ongewenst gedrag te ontmoedigen en risico's tijdig te signaleren.

6. Conclusie

Het risico op misbruik van persoonsgegevens vanuit de BRP wordt op dit moment **onvoldoende beheerst**. Tegelijkertijd laat het onderzoek zien dat enkele randvoorwaarden voor zorgvuldige omgang met BRP-gegevens deels aanwezig zijn. Zo zijn afspraken over gegevensverstrekking vastgelegd in convenanten en transparantiedocumenten, die vooraf worden gereviewd door betrokken directies. Ook is er bij incidenten sprake van opvolging.

Zowel de hard controls als de soft controls vertonen echter duidelijke tekortkomingen. Met name het ontbreken van technische beperkingen in de toegang tot gegevens, onvoldoende toegangsbeheer, beperkte aanvullende maatregelen bij autorisatie en het ontbreken van actieve monitoring zorgen ervoor dat er onvoldoende structurele waarborgen zijn om onrechtmatig gebruik te voorkomen of tijdig te signaleren. Door deze tekortkomingen worden leidinggevenden onvoldoende gefaciliteerd in het toezicht op en de sturing van gewenst gedrag, waardoor ruimte ontstaat voor nieuwsgierig of kwaadwillend gedrag van medewerkers. Daarbij speelt mee dat de beheersing van BRP-gegevens binnen de directies complex is. De gemeente is mede afhankelijk van landelijke ontwikkelingen en de doorontwikkeling van software door leveranciers, waardoor technische beperkingen op toegang, zoekgedrag en monitoring slechts beperkt zijn in te richten. Hierdoor leunt de beheersing in de praktijk in sterke mate op organisatorische en gedragsmatige maatregelen.

Deze afhankelijkheid wordt versterkt doordat ook de soft controls onvoldoende zijn ontwikkeld. Gebrek aan training en bewustwording, onduidelijkheid over regels, beperkt voorbeeldgedrag, een zwakke aanspreekcultuur en het ontbreken van structureel toezicht en handhaving vergroten het risico op misbruik. Uit de gesprekken blijkt bovendien dat onrechtmatige raadplegingen daadwerkelijk voorkomen, wat de noodzaak van een integrale versterking van hard én soft controls onderstreept.

7. Samenvatting van bevindingen

Hard controls

- De hard controls bieden onvoldoende structurele waarborgen voor adequate beheersing van het risico op misbruik van BRP-gegevens.
- Het ontbreken van technische beperkingen leidt ertoe dat medewerkers toegang hebben tot persoonsgegevens van alle inwoners van Nederland en vrij kunnen zoeken in BRP-gegevens zonder koppeling aan een werkvoorraad of dossier. Dit vergroot het risico op misbruik en bemoeilijkt toezicht.

- Het toegangsbeheer is onvoldoende op orde: autorisatiematrixen zijn niet consistent of actueel, toegangsrechten worden niet altijd tijdig ingetrokken en stedelijke processen voor logisch toegangsbeheer worden niet nageleefd.
- Aanvullende maatregelen bij toegang zijn beperkt, waardoor medewerkers onvoldoende worden geïnformeerd over regels en voorwaarden voor zorgvuldig gebruik.
- Door het ontbreken van volledige logging (zoals dossiercodes) en actieve monitoring is effectief toezicht en tijdige signalering van afwijkend gedrag nauwelijks mogelijk.

Soft controls

- Training en bewustwording zijn onvoldoende, met name bij indiensttreding. Verplichte e-learnings worden soms pas laat gevolgd en de focus ligt vooral op inhoudelijke taken.
- Regels over omgang met BRP-gegevens kennen grijze gebieden en zijn niet vastgelegd of structureel gecommuniceerd.
- Er is een discrepantie tussen het voorbeeldgedrag dat leidinggevenden zeggen te tonen en hoe medewerkers dit ervaren.
- Knelpunten worden niet structureel besproken en medewerkers en leidinggevenden spreken elkaar beperkt aan, terwijl uit interviews blijkt dat raadplegingen uit nieuwsgierigheid of privégebruik voorkomen.
- Structureel toezicht en (positieve en negatieve) bekrachtiging ontbreken, waardoor afwijkend gedrag niet tijdig wordt gesignaleerd of gecorrigeerd.

In de huidige situatie versterken de tekortkomingen in hard en soft controls elkaar. Technische beperkingen en beperkte monitoring maken afwijkend gedrag moeilijk zichtbaar, terwijl gebrek aan training, duidelijkheid en aanspreekcultuur ertoe leidt dat medewerkers onvoldoende worden ondersteund in zorgvuldig gebruik van BRP-gegevens.