Verkennend onderzoek

Misbruik van persoonsgegevens door gemeenteambtenaren

Adviezen voor het voorkomen en opsporen van datalekken

AP | bescherming in een digitale wereld

Januari 2026

Inhoud

Samenvatting verkenning

- De Autoriteit Persoonsgegevens (AP) heeft voor de verkenning 3 gemeenten bezocht en 29 functionarissen gegevensbescherming (FG's) van gemeenten bevraagd over misbruik van gegevens door ambtenaren. Ook sprak de AP met de Rijksrecherche en de Vereniging van Nederlandse Gemeenten (VNG).

- Uit de verkenning blijkt dat het lastig is voor gemeenten om misbruik van persoonsgegevens door eigen ambtenaren te signaleren. Gemeenten ontdekten misbruik regelmatig pas nadat zij hier door de Rijksrecherche of een inwoner op waren gewezen. De AP is bezorgd dat misbruik hierdoor nog vaak onontdekt blijft.

- Gemeenten die misbruik wel ontdekten, beschouwden het misbruik niet altijd als datalek en meldden het niet aan de AP. Slachtoffers kregen geen waarschuwingsbericht over het datalek. Hierdoor weten slachtoffers niet wat er met hun gegevens is gebeurd en wat zij kunnen doen tegen de gevolgen.

- Naar aanleiding van deze verkenning geeft de AP gemeenten adviezen voor het voorkomen, opsporen en aanpakken van datalekken en weerlegt de AP misvattingen over datalekken.

- De AP roept gemeenten op om onderling ervaringen en kennis uit te wisselen. Ook als dat reputatieschade kan opleveren. Door ervaringen te delen, krijgen gemeenten beter zicht op de omvang van het misbruik en kunnen zij (toekomstige) datalekken beter opsporen en voorkomen. De burgemeester van de gemeente Brunssum vertelt in deze rapportage over de impact van een datalek en hoe haar gemeente daarmee is omgegaan.

De AP is in de praktijk verschillende situaties tegengekomen waarin misbruik van persoonsgegevens door gemeenteambtenaren een datalek veroorzaakte. Enkele voorbeelden:

- Een onder druk gezette ambtenaar deelt gegevens met een criminele organisatie.
- Vanwege een familieconflict zoekt een ambtenaar informatie over familie op in gemeentesystemen.
- Uit nieuwsgierigheid bekijkt een ambtenaar de gegevens van een BN'er.

Zulke incidenten hebben vervelende gevolgen. Gemeenten verwerken veel en gevoelige informatie. Mensen moeten erop kunnen vertrouwen dat de informatie vertrouwelijk blijft. Als gegevens met criminelen worden gedeeld, kunnen zelfs ernstige veiligheidsrisico's voor mensen ontstaan.

Datalekken blijven onontdekt

Jaarlijks ontvangt de AP van ongeveer 10 gemeenten een datalekmelding waarbij een ambtenaar onrechtmatig persoonsgegevens bekeek. Meerdere gemeenten ontdekten deze datalekken pas nadat zij hier door de Rijksrecherche op werden gewezen. Of nadat een burger een klacht indiende vanwege vermoedens van misbruik. Hierdoor is bij de AP het beeld ontstaan dat gemeenten deze datalekken niet zelf ontdekken.

De AP bezocht 3 gemeenten die dit soort datalekken meldden aan de AP, om erover in gesprek te gaan. Deze bezoeken gaven de AP de indruk dat gemeenten de basisbeveiligingsmaatregelen uit de Baseline Informatiebeveiliging Overheid (BIO) kennen en toepassen. Maar gemeenten vinden het moeilijk om te zorgen dat die maatregelen ook het

gewenste effect hebben. Gemeenten doen bijvoorbeeld wel aan logging, maar vinden het ingewikkeld om vervolgens vast te stellen of raadplegingen van persoonsgegevens rechtmatig zijn of niet. De beveiligingsmaatregelen leiden er ook niet altijd toe dat gemeenten vergelijkbaar misbruik voortaan wel zelf denken te kunnen signaleren.

Gemeenten herkennen integriteitsincidenten niet als datalek en melden daarom niet

De AP onderzocht of gemeenten integriteitsincidenten als datalekken melden aan de AP als dat nodig is. Hierbij gebruikte de AP een nieuwsartikel met een lijst van integriteitsschendingen uit 2020-2022, naast een eigen overzicht vanuit het meldloket datalekken van de AP. Op de lijst met integriteitsschendingen stonden 8 datalekken die onterecht niet waren gemeld aan de AP. Deze gemeenten moesten dat alsnog doen. Bij 12 andere integriteitsschendingen vermoedde de AP ook dat er sprake was van een niet-gemeld datalek. De gemeenten beschikten ten tijde van dit verkennend onderzoek niet meer over voldoende informatie om dit met zekerheid vast te stellen.

Uit het contact met FG's bleek dat bij een aantal gemeenten de afdeling integriteit en de afdeling privacy niet goed met elkaar samenwerkten. Hierdoor was misbruik wel als integriteitsschending opgepakt, maar niet als datalek herkend. Er waren ook misvattingen over wat een datalek is en wanneer het melden aan de AP en aan slachtoffers verplicht is.

Het is belangrijk dat datalekken aan de AP gemeld worden, zodat de AP kan bijsturen als onvoldoende beveiligingsmaatregelen worden getroffen of kan ingrijpen als slachtoffers niet worden geïnformeerd.

Het aantal gevallen van misbruik kan een stuk hoger zijn dan het aantal gemelde datalekken. Bijvoorbeeld omdat niet alle datalekken gemeld zijn aan de AP. Of omdat misbruik onontdekt bleef. Juist ook gemeenten die de afgelopen jaren geen bekende gevallen van misbruik hadden, moeten zich afvragen of zij voldoende maatregelen nemen om misbruik op te sporen en aan te pakken.

Meer transparantie en kennisuitwisseling tussen gemeenten nodig

Gemeenten vinden onderlinge kennisuitwisseling zeer belangrijk. Maar uit de gesprekken met gemeenten blijkt dat zij bij misbruik door eigen ambtenaren terughoudend zijn met informatie delen. Dat ligt aan de gevoelige aard van de gebeurtenissen. De AP begrijpt dit, maar vindt het tegelijkertijd een gemiste kans. Door niet te spreken over misbruik, kan ten onrechte het beeld ontstaan dat dit soort datalekken niet vaak voorkomt. Ook worstelen gemeenten met dezelfde problemen rondom het voorkomen en ontdekken van misbruik. Kennisuitwisseling en samenwerking zijn daarom noodzakelijk.

De burgemeester van Brunssum over datalekken door ondermijning

’Dit incident was een absolute eyeopener’

Wilma van der Rijt
Burgemeester van Brunssum

Datalek door ondermijning

”In onze gemeente hebben we meegemaakt dat een medewerker Dienstverlening de gemeentesystemen misbruikte voor toegang tot en doorspelen van persoonsgegevens aan criminelen. De Rijksrecherche werd ingeschakeld, stelde het misbruik vast en de medewerker is daarvoor vervolgd.

Dit incident was voor ons een echte eyeopener. Wij en andere gemeenten moeten echt rekening houden met ondermijning. Dat betekent ook dat criminelen misbruik willen maken van data uit de gemeentesystemen voor hun criminele doeleinden. Daarnaast moeten we ons beseffen dat de mens, en dus onze eigen medewerkers, bij dit soort incidenten altijd een belangrijke rol heeft.

Soms bestaat het beeld dat het er altijd om gaat dat een persoon bewust de gemeente ’infiltreert’ om misbruik te kunnen maken van de gemeentesystemen. Maar dat is niet altijd zo. Een medewerker kan worden beïnvloed door criminelen, en gaat vervolgens telkens een stapje verder en wordt steeds onvoorzichtiger.”

Collega’s blijven achter met een onveilig gevoel

”Deze kwestie had een enorme impact op de organisatie, specifiek op de directe collega’s van de medewerker. Er ontstond veel onrust en zij bleven achter met een onveilig gevoel, omdat dit speelde bij een directe collega. Tegelijkertijd heeft het incident ook heel veel belangrijke acties bij ons in gang gezet.

Het kan door collega’s als heel lastig worden ervaren om vermoedens van misbruik door een medewerker te melden. Je wilt geen onterechte beschuldigingen uiten. Of misschien heb je zelf wel te lang gewacht met je vermoedens uitspreken, waardoor je je medeschuldig voelt aan wat er gebeurt. Gemeenten moeten daar zorgvuldig mee omgaan. En zorgen dat medewerkers hun vermoedens veilig kunnen melden.”

Zet in op kennis, bewustwording, technische maatregelen en leer van elkaar

”Onze gemeente heeft na dit incident met name ingezet op de rol van de mens. Kennis en bewustwording zijn echt belangrijk. En dat vraagt om een lange adem. Waar het vroeger als normaal werd ervaren om een collega te vragen iets voor je op te zoeken als je zelf geen toegang had, is die cultuur nu echt veranderd. Een uitgebreid traject met nieuwe gedragscodes, bewustwording en een cursus morele oordeelsvorming heeft ertoe geleid dat medewerkers nu zelf inzien waarom bepaalde systemen en gegevens zijn afgeschermd. En waarom hun handelingen worden vastgelegd via ’logging’ en volgens afspraken getoetst. Dat beschermt medewerkers ook tegen criminele invloeden.

Handelingen van medewerkers loggen is daarnaast een belangrijke technische maatregel om misbruik op te kunnen sporen. Maar hoe stel je nou vast welke handelingen misschien onrechtmatig waren, zodat misbruik niet onontdekt blijft? Zeker als kleine en middelgrote gemeente kun je daarbij samenwerken en kennis uitwisselen over wat precies als vreemde handeling moet worden aangemerkt.

Alle gemeenten moeten alert zijn en er absoluut niet van uitgaan dat dit in hun gemeente niet gebeurt of kan gebeuren. Juist daarom is een belangrijke rol weggelegd voor samenwerking tussen de gemeenten en ondersteuning vanuit het Rijk. Bijvoorbeeld bij het aanbieden van opleidingen en het creëren van bewustwording.”

De AP op bezoek na een datalekmelding; spannend, maar ook waardevol

”De AP bezocht onze gemeente nadat wij een datalekmelding indienden. Dat was enorm spannend voor alle betrokken collega’s - het was onze kennismaking met de AP. Betrokken collega’s voelden opnieuw alsof zij misschien degenen waren geweest die fouten hadden gemaakt waardoor het misbruik mogelijk was.

Achteraf gezien was het bezoek van de AP eigenlijk een luxe. De AP vertelde wat we goed deden, waar de aandachtspunten lagen en gaf suggesties over hoe het anders kan. Het was fijn om te zien dat ’Autoriteit’ ook betekent: kennis, ervaring en erkenning van wat wel goed gaat.

Wij denken dat gemeenten het erg zouden waarderen als zij de AP kunnen gebruiken als sparringpartner. Bijvoorbeeld wanneer er vermoedens zijn van misbruik, maar dit nog lang niet zeker is.”

Adviezen voor het voorkomen, opsporen en aanpakken van datalekken

In de Algemene verordening gegevensbescherming (AVG) staat dat wanneer organisaties persoonsgegevens verwerken, zij deze gegevens daarbij goed moeten beveiligen. De BIO biedt een basisnormenkader voor informatiebeveiliging waar de overheid zich aan moet houden. Er staan technische en organisatorische maatregelen in die datalekken kunnen helpen voorkomen, opsporen en aanpakken. Daarnaast bieden de Rijksrecherche en de VNG kennisproducten aan. Aan de hand van praktijksituaties die de AP tijdens de verkenning aantrof, geeft de AP hieronder adviezen gebaseerd op relevante BIO-normen[1] en 'good practices' die gemeenten deelden.

Praktijkvoorbeeld 1: Samenwerking afdeling integriteit en afdeling privacy

Een medewerker maakte misbruik van persoonsgegevens. De gemeente doorliep de integriteitsprocedure, maar herkende het incident niet als datalek. Hierdoor werden belangrijke stappen niet genomen, zoals het informeren van slachtoffers en de AP, en het betrekken van de FG.

Advies

Zorg voor afstemming tussen de disciplines
Integriteit, informatiebeveiliging en privacy zijn vaak belegd bij verschillende functies of afdelingen. Bij misbruik van persoonsgegevens door een ambtenaar zijn alle 3 de disciplines van toepassing. Zorg dat de medewerkers in deze situaties samenwerken en afstemmen. Opleiding en voorlichting geven medewerkers de kennis om een integriteitsincident, beveiligingsincident en datalek te herkennen. Door een werkwijze vast te leggen, weten verschillende disciplines bovendien dat – en hoe – ze moeten samenwerken.

[1] Zie met name de volgende BIO-beheersmaatregelnummers: 5.18 (Toegangsrechten), 5.27 (Leren van informatiebeveiligingsincidenten) 6.01 (Screening), 6.02 (Arbeidsovereenkomst), 6.03 (Bewustwording van, opleiding, training in informatiebeveiliging), 6.04 (Disciplinaire procedure), 8.03 (Beperking toegang tot informatie), 8.15 (Logging), 8.16 (Monitoren van activiteiten).

Praktijkvoorbeeld 2:
Aangifte beschermt andere gemeenten

Tegen een medewerker bestond een vermoeden van misbruik van persoonsgegevens. Met de medewerker werd afgesproken dat deze zou vertrekken met een vaststellingsovereenkomst. Er werd geen aangifte gedaan. De medewerker werd bij een andere gemeente aangenomen in een vergelijkbare functie, waar opnieuw misbruik kon plaatsvinden.

Adviezen

Bepaal: wie of wat is kwetsbaar?
Beoordeel regelmatig de risico's van de verwerking van persoonsgegevens. Stel vast welke functies, handelingen of processen binnen de organisatie kwetsbaar zijn. Denk in dit verband juist ook aan medewerkers of afdelingen die toegang hebben tot systemen met veel persoonsgegevens, zoals medewerkers klantcontact, burgerzaken en sociale zaken.

Controleer: wie haalt u binnen?
Zorg voor een screeningsbeleid, waarbij de achtergrond van sollicitanten wordt geverifieerd en waarbij een Verklaring Omtrent het Gedrag (VOG) onderdeel is van het proces bij indiensttreding en bij functiewijziging. Pas het beleid consequent toe, ook als een sollicitant van een andere overheidsinstantie komt.

Win bij vermoedens van misbruik advies in van de Rijksrecherche, doe bij misbruik altijd aangifte
Als er vermoedens zijn dat een medewerker bevoegdheden misbruikt, dan kan de Rijksrecherche advies geven. Blijkt uit onderzoek dat een medewerker inderdaad bevoegdheden heeft misbruikt? Doe dan aangifte.[2] Zo voorkomt u als gemeenten gezamenlijk dat de medewerker kan doorgaan met het misbruik.

Zorg voor een transparante disciplinaire procedure
Zorg voor een disciplinaire procedure waarin staat welke acties de gemeente onderneemt als er sprake is van misbruik. Maak deze procedure ook bekend bij medewerkers. Hoewel opleiding en bewustwording van medewerkers belangrijke maatregelen zijn, heeft een disciplinaire procedure ook een afschrikkende werking. Daarnaast kan de gemeente sneller en adequater optreden.

[2] De Rijksrecherche stelt een onderzoek in als de integriteit van de overheid ernstig wordt aangetast.

Praktijkvoorbeeld 3: Maatregelen om misbruik te voorkomen en op te sporen

Gemeenten ontdekten pas dat een medewerker onrechtmatig persoonsgegevens opzocht en deelde met criminelen, nadat zij hier door de Rijksrecherche op werden gewezen. Als dit niet zou zijn gebeurd, hadden de gemeenten het gedrag waarschijnlijk niet zelf opgemerkt.

Adviezen

Bepaal: wat mogen medewerkers wel of niet zien?
Bepaal welke gegevens voor welke medewerkers noodzakelijk zijn om hun werkzaamheden uit te voeren. Beperk vervolgens (technisch) waar medewerkers toegang toe krijgen. Bij een verandering van werkzaamheden of bij uitdiensttreding moeten de toegangsrechten worden aangepast of beëindigd.

Leg handelingen vast en controleer ze
Om achteraf vast te stellen of handelingen in de systemen geoorloofd zijn, is het noodzakelijk om de handelingen te registreren (logging) en deze regelmatig te beoordelen (monitoren van logging). Aanwijzingen van misbruik kunnen zijn:

- Raadplegingen of mutaties buiten kantoortijden;
- Grote toename in het aantal raadplegingen of mutaties;
- Raadpleging van bekende personen, collega's, familieleden of eigen persoonsgegevens;
- Meermaals raadplegen van dezelfde persoon over langere periode.

Zorg voor een open cultuur
Geef aandacht aan integriteit, professionaliteit en een open cultuur. Laat deze onderwerpen ook na de indiensttreding nog regelmatig terugkomen. Dit draagt eraan bij dat een medewerker die bijvoorbeeld onder druk wordt gezet door een crimineel om gegevens te delen, om hulp vraagt. En dat als medewerkers zich zorgen maken over een collega, zij dit aangeven.

Praktijkvoorbeeld 4: Regelmatige aandacht voor integriteit en privacy

Een gemeente maakte bij indiensttreding via de eed en belofte duidelijk dat medewerkers persoonsgegevens alleen mogen raadplegen voor uitvoering van hun taak. Toch raadpleegden medewerkers persoonsgegevens, bijvoorbeeld uit nieuwsgierigheid, vanwege een persoonlijk conflict met de persoon, of om informatie door te spelen aan een derde.

Advies

Leg regels vast en zorg voor training
Wijs medewerkers bij de aanstelling of een functiewijziging op de regels en de verantwoordelijkheden die medewerkers hebben bij het omgaan met persoonsgegevens. Bijvoorbeeld als onderdeel van de 'onboarding' van nieuwe medewerkers. De regelingen en instructies moeten toegankelijk en begrijpelijk zijn. Bijvoorbeeld als rubriek op het intranet of flyers die verspreid worden op werklocaties. Medewerkers laten weten dat handelingen worden gelogd, heeft ook een preventieve werking. Daarnaast moet duidelijk zijn wat er gebeurt als een medewerker de regels overtreedt.

Medewerkers en andere mensen die namens de gemeente met persoonsgegevens omgaan, zoals zelfstandigen of opdrachtnemers, moeten training en regelmatige bijscholing krijgen.

Praktijkvoorbeeld 5:
Zoek elkaar op voor kennisuitwisseling

Een gemeente kreeg te maken met een incident dat ook andere gemeenten zou kunnen overkomen. Maar uit vrees voor reputatieschade, besloot de gemeente geen kennis uit te wisselen met andere gemeenten over het incident en hoe het was afgehandeld.

Adviezen

Analyseer incidenten
Zorg ervoor dat incidenten worden geanalyseerd, zodat gemeenten er lessen uit kunnen trekken en maatregelen kunnen nemen om het risico op toekomstige incidenten te verkleinen.

Leg ieder datalek vast in een register
Documenteer datalekken altijd goed. Leg in ieder geval de feiten, gevolgen en genomen maatregelen vast. Daarnaast raadt de AP aan om belangrijke keuzes en daarbij ondersteunende documenten vast te leggen. Bijvoorbeeld over het melden aan de AP of betrokkenen, en de maatregelen om nieuwe, soortgelijke datalekken te voorkomen. Gebruik het 'datalekregister' om alle datalekken centraal te documenteren en informatie goed te bewaren, en om te leren van eerdere incidenten. Op basis van het datalekregister kan de AP ook controleren of de meldplicht datalekken goed wordt nageleefd. Op de website van de AP vindt u een voorbeeld van een datalekregister.

Deel kennis bij netwerkbijeenkomsten of brancheorganisaties
Incidenten komen bij elke organisatie voor en de AP moedigt gemeenten aan om hun ervaringen en kennis te delen met anderen, bijvoorbeeld bij netwerkbijeenkomsten of met brancheorganisaties. Hierdoor kunnen zij andere gemeenten en organisaties waarschuwen of voorlichten over nieuwe ontwikkelingen, bedreigingen of uitdagingen. En oplossingen delen of samen opzetten, bijvoorbeeld voor effectieve monitoring op logging.

Misvattingen weerlegd

Tijdens de verkenning kwam de AP de volgende misvattingen over datalekken tegen:

Misvatting 1: 'Als er een strafrechtelijk onderzoek naar de ambtenaar loopt, dan hoeft de gemeente slachtoffers niet te informeren.'

Alleen in uitzonderingsgevallen kan een gemeente afzien van het informeren van slachtoffers over een datalek met een hoog risico.

Tijdens het onderzoek is de AP meerdere keren tegengekomen dat de gemeente betrokkenen niet informeerde vanwege een strafrechtelijk onderzoek naar de ambtenaar. De gemeente ging ervan uit dat de politie of Rijksrecherche betrokkenen zou informeren. Of de gemeente ging ervan uit de betrokkenen niet te mogen informeren, omdat dit het strafrechtelijk onderzoek zou schaden.

Organisaties mogen afzien van het informeren van betrokkenen zolang dit noodzakelijk is voor de voorkoming, het onderzoek, de opsporing en de vervolging van strafbare feiten (artikel 41 Uitvoeringswet AVG). Zij moeten wel regelmatig evalueren of deze noodzaak er nog steeds is. Dit kan bijvoorbeeld veranderen zodra de ambtenaar weet verdachte te zijn, of zodra het strafrechtelijk onderzoek is afgerond. De gemeente blijft ervoor verantwoordelijk dat betrokkenen worden geïnformeerd over het datalek.

Misvatting 2: 'Als een medewerker geraadpleegde gegevens niet nodig had voor het werk, maar wel geautoriseerd was om de gegevens te raadplegen, dan is er geen datalek.'

Ook wanneer een ambtenaar wel de technische autorisaties had om gegevens te raadplegen, maar dit deed zonder dat dit noodzakelijk was voor het uitvoeren van het werk, is sprake van een datalek. Bijvoorbeeld wanneer de ambtenaar een familielid of buur opzoekt uit nieuwsgierigheid.

Gemeenten die de situatie wél herkenden als datalek, hadden misvattingen over de risico's van het datalek en meldden het datalek daarom niet aan de AP of aan betrokkenen. Dat kwam waarschijnlijk doordat gemeenten bij andere datalekken mogen meewegen dat een ambtenaar vaak een zogenoemde 'betrouwbare ontvanger' is. Maar dat argument gaat niet op als de ambtenaar in strijd met de regels heeft gehandeld. Ook vonden gemeenten het lastig de risico's te duiden. Er zijn vaak wel risico's, bijvoorbeeld reputatieschade, uitsluiting, pestgedrag of het ontstaan van een machtsverschil tussen de betrokkene en de ambtenaar. Dit soort datalekken moet vaak worden gemeld aan de AP.

Misvatting 3: 'Als de ambtenaar gegevens onrechtmatig heeft geraadpleegd, maar niet heeft gedeeld met derden, dan is er geen datalek.'

Gegevens hoeven niet buiten de organisatie terecht te komen om te spreken van een datalek. Het gaat erom of er een inbreuk (op de beveiliging) was in verband met persoonsgegevens. Als een ambtenaar persoonsgegevens onrechtmatig raadpleegt, dan moet de gemeente de kwestie vastleggen in het datalekregister en nagaan of een datalekmelding aan de AP en betrokkenen nodig is.

De Autoriteit Persoonsgegevens is de onafhankelijke toezichthouder op persoonsgegevens die mensen beschermt in een digitale wereld.

Autoriteit Persoonsgegevens
Postbus 93374
2509 AJ Den Haag

autoriteitpersoonsgegevens.nl