Handreiking rekenkameronderzoek naar privacy in het sociaal domein

Nederlandse Vereniging voor Rekenkamers en Rekenkamercommissies (NVRR)

Datum: november 2020

NVRR
Nederlandse Vereniging van
Rekenkamers & Rekenkamercommissies

Chris Nijhuis MSc

Emilie Stumphius Msc LLM

Stef Tomesen MSc

In opdracht van de NVRR

Inhoud

Inleiding

Aanleiding

Privacy, daar heeft iedereen recht op. Van organisaties, en zeker ook van gemeenten, wordt verwacht dat zij de privacy van personen beschermen met soms verregaande maatregelen. Veel rekenkamers doen dan ook onderzoek naar de manier waarop gegevens verwerkt worden, in het bijzonder in het sociaal domein. De NVRR biedt rekenkamers met deze handreiking een overzicht van wat onderzoek naar dit onderwerp oplevert, en concrete suggesties voor rekenkamers die onderzoek willen doen naar dit onderwerp.

Met ingang van 1 januari 2015 zijn de gemeenten belast met de uitvoering van de Jeugdwet, de Wet maatschappelijke ondersteuning 2015 (Wmo 2015) en de Participatiewet en gaan daarom meer dan voorheen taken uitvoeren op het gebied van jeugd, zorg en werk.[1] Deze decentralisaties hebben plaatsgevonden vanuit de gedachte dat de gemeente de bestuurslaag is die het dichtst bij de burger staat en derhalve het meest geschikt is deze taken uit te voeren. De decentralisaties hadden tot gevolg dat gemeenten genoodzaakt zijn veel gegevens te verwerken, zowel intern als extern. Ook nemen de mogelijkheden om dienstverlening te verbeteren op basis van gegevens hand over hand toe. Dit is in potentie goed voor inwoners met een hulpvraag. Het roept echter ook vragen en dilemma's op omtrent de privacy van deze inwoners.

Het is belangrijk om zich te realiseren dat iedere gemeente het sociaal domein op eigen wijze organiseert en dat de keuzes in de organisatie hiervan implicaties hebben voor de privacy van inwoners. In de praktijk staat het borgen van privacy bij gegevensverwerking soms in contrast met het bieden van integrale hulp over de drie domeinen heen, of een snelle en effectieve onderlinge afstemming. De kwaliteit van dienstverlening van de gemeente komt hiermee onder druk te staan. Dat spanningsveld staat in de maatschappelijke belangstelling, tegelijkertijd hebben niet alle gemeenteraden er even veel aandacht voor. Dit hangt samen met een gebrek aan kennis over en inzicht in de rol van de raad op dit thema.

Doel van de handreiking

Het doel van deze handreiking is tweeledig. Enerzijds is het doel om lessen uit eerder rekenkameronderzoek in beeld te brengen, zodat rekenkamers snel inzicht hebben in wat er speelt op het gebied van privacy in het sociaal domein. Daarnaast moet de handreiking handvatten bieden voor rekenkamers die zelf onderzoek willen doen naar dit thema. De handreiking is daarom als volgt opgebouwd.

Hoofdstuk 2 biedt een introductie op privacy en informatieveiligheid in het sociaal domein: waar hebben we het nu eigenlijk over en wat zijn de belangrijkste dilemma's? Hoofdstuk 3 is met name interessant voor rekenkamers die zelf onderzoek willen doen naar dit thema.

Dit hoofdstuk bevat tips en aandachtspunten voor een eigen rekenkameronderzoek, zoals suggesties voor inhoudelijke invalshoeken, methoden en twee mogelijke onderzoeksopzetten.

Bij deze handreiking vindt u tevens een leeslijst van andere (rekenkamer)onderzoeken (bijlage 1) om u verder te kunnen verdiepen in het onderwerp.

De handreiking is opgesteld op basis van een analyse van twaalf recente rekenkameronderzoeken over privacy en informatieveiligheid in het sociaal domein en gesprekken met leden van rekenkamer(commissie)s, ambtenaren en privacy-experts. In bijlage 2 vindt u de lijst met gesprekspartners.

[1] Daarnaast wordt de Wet gemeentelijke schuldhulpverlening (Wgz) ook tot het sociaal domein gerekend. Aangezien deze echter een aanzienlijk kleiner deel van de gemeentelijke taken beslaat, benoemen wij deze niet apart in deze handreiking.

Inzicht in privacy in het sociaal domein

Wettelijk kader

De AVG

Dat een overheid voorzichtig omgaat met de gegevens van inwoners, vinden we vanzelfsprekend. Maar wat 'voorzichtig' betekent, dat verandert nogal eens. Van 2001 tot 2018 was in Nederland de Wet bescherming persoonsgegevens (Wbp) van kracht. Deze wet was erop gericht om op een behoorlijke, noodzakelijke, proportionele en zorgvuldige wijze gegevens te beheren en verstrekken.

In 2016 is de Algemene Verordening Gegevensbescherming (AVG) in werking getreden. In 2018 werd de wet effectief van kracht. De AVG is een Europese standaard die geldt voor alle landen in de Europese Unie. In Nederland verving deze de Wbp. De AVG stelt meer eisen aan de verwerking van persoonsgegevens dan de Wbp. Uitgangspunt van de AVG is dat wij een informatiemaatschappij zijn en dat verwerken van persoonsgegevens ten dienste van de mens moet staan. Medewerkers die informatie verwerken moeten daarom aan zorgvuldigheidseisen voldoen. Zo moet er voor gemeenten een wettelijke basis zijn om gegevens te verwerken, werd het verplicht een functionaris gegevensbescherming aan te stellen en zijn hoge boetes verbonden aan onzorgvuldig handelen. De Autoriteit persoonsgegevens (AP) houdt toezicht op de verwerking van persoonsgegevens. Deze kan waar nodig bedrijven en overheden dwingen zich aan de wettelijke privacy-eisen te houden.

De AVG heeft dus gezorgd voor een versterking en uitbreiding van privacyrechten, en legt de verantwoordelijkheid voor een zorgvuldig gegevensbeheer bij organisaties. Uit de AVG vloeiden onder meer een AVG-gedragscode, richtlijnen voor databescherming en handvatten om privacy-risico's in kaart te brengen voort. Ook is in de AVG geregeld dat datalekken in organisaties bij de AP gemeld moeten worden. De Data Protection Impact Assesment (DPIA) is onderdeel van de AVG en biedt een handvat om voorafgaand aan gegevensverwerking de privacy-risico's in kaart te brengen. Bij een hoog privacy-risico kan het uitvoeren van DPIA verplicht worden gesteld.

Aandachtspunten gegevensverwerking in het sociaal domein

Gemeenten zijn in het sociaal domein verantwoordelijk voor een groot aantal gegevensverwerkingen, op basis van de Wmo 2015, de Participatiewet en de Jeugdwet. Die gegevensverwerking vindt plaats binnen een complexe context: er is snel hulp nodig, en het gaat om gevoelige informatie. De dilemma's die dat met zich meebrengt, zijn in de volgende thema's samen te vatten:

- Spanningsveld kwaliteit dienstverlening en privacy
- Spanningsveld integraal werken en privacy
- Grondslag voor gegevensverwerking
- Samenwerking met ketenpartners
- Belang van een goede organisatie
- Afhankelijkheid van informatieveiligheid

Spanningsveld kwaliteit dienstverlening en privacy

Er bestaat een spanningsveld tussen kwaliteit van dienstverlening en het beschermen van privacy. Dit komt doordat in de AVG is opgenomen dat gegevensverzameling alleen mag als er toestemming wordt gegeven of als het noodzakelijk is in het kader van een specifiek doel. In de AVG is dit concreet gemaakt door zes grondslagen te onderscheiden op basis waarvan persoonsgegevens mogen worden verwerkt voor een organisatie. Deze grondslagen zijn:

- toestemming van de persoon over wie het gaat;
- als het noodzakelijk is bij het uitvoeren van een overeenkomst;
- bij wettelijke plichten;
- als het noodzakelijk is om een taak van algemeen belang of openbaar gezag uit te voeren;
- als het noodzakelijk is om een gerechtvaardigd belang te behartigen;
- als het noodzakelijk is om vitale belangen te beschermen.

Voor het sociaal domein kunnen alle grondslagen van belang zijn. Meestal volstaan de grondslag toestemming of de grondslag noodzaak in het kader van een overeenkomst. Het merendeel van de gemeentelijke dienstverlening wordt momenteel gebaseerd op de grondslagen wettelijke plicht en taak van algemeen belang.

Maar wanneer deze afwezig zijn en in het belang van de cliënt toch gegevens moeten worden gedeeld, kan ook op basis van bescherming van vitale belangen worden gehandeld. Dit is een zeer specifieke en nauwelijks gebruikte grondslag. In overweging 46 van de AVG staat toegelicht dat dit een laatste mogelijkheid is: *"De verwerking van persoonsgegevens dient ook als rechtmatig te worden beschouwd indien zij noodzakelijk is voor de bescherming van een belang dat voor het leven van de betrokkene of dat van een andere natuurlijke persoon essentieel is. Verwerking van persoonsgegevens op grond van het vitale belang voor een andere natuurlijke persoon is in beginsel alleen toegestaan indien de verwerking kennelijk niet op een andere rechtsgrond kan worden gebaseerd."* Vanuit het perspectief van bescherming van vitale belangen zou kunnen worden gesteld dat bescherming van de persoonlijke levenssfeer soms alleen kan áls er informatie wordt gedeeld. Een voorbeeld is een situatie waarin een persoon (bijvoorbeeld als gevolg van een ongeluk of medische oorzaak) niet meer aanspreekbaar is.

Dit spanningsveld leidt tot situaties waarin medewerkers in het sociaal domein belangrijke informatie niet delen uit angst de regels te overtreden. Voor inwoners kan dat frustrerend zijn: zij voelen zich niet gehoord omdat ze bij meerdere medewerkers van de gemeente hun verhaal opnieuw moeten vertellen.

Spanningsveld integraal werken en privacy

Ten tijde van de decentralisaties werden er als het ware schotten geplaatst tussen de drie domeinen. Voor elk domein gelden andere grondslagen en regels voor wat betreft gegevensverwerking. Hoewel het de bedoeling was om integraal te werken, zorgde het hanteren van verschillende grondslagen ervoor dat men voor elk onderwerp apart informatie op ging vragen. Informatie die in het kader van een Wmo-aanvraag is verzameld over een inwoner, mag bijvoorbeeld niet gebruikt worden door een re-integratieconsulent. In overweging 50 van de AVG is dit toegelicht. In de AVG en de wetten binnen het sociaal domein is echter niet geregeld dat de wetten in samenhang mogen worden uitgevoerd voor een gezamenlijk doel.

Vanuit het oogpunt om snel en effectief goede zorg te leveren, kan gegevensdeling juist van belang zijn. Het komt bijvoorbeeld voor dat medewerkers van het sociaal wijkteam (vanuit de Wmo 2015) niet op de hoogte zijn van schuldenproblematiek die bij consulenten van het werkbedrijf (vanuit de Participatiewet) wel bekend zijn. Het spanningsveld werkt ook de andere kant op. Om multi-problematiek in kaart te brengen, wordt door gemeenten vaak een brede check gedaan waarbij vragen worden gesteld over meerdere leefgebieden. Dit kan logischerwijs als een inbreuk op de privacy beleefd worden. Een goede afweging tussen kwaliteit van dienstverlening en het borgen van privacy vereist veel inschattingsvermogen van medewerkers van de gemeente. Zij kunnen daarbij geholpen worden door de juiste training en goede werkafspraken.

In maart 2020 heeft het Ministerie van Binnenlandse Zaken en Koninkrijksrelaties een concept wetsvoorstel gepubliceerd dat meer wettelijke basis moet gaan bieden voor integraal werken. Dit is het wetsvoorstel Aanpak meervoudige problematiek sociaal domein (Wams). Het wetsvoorstel biedt een grondslag voor gemeenten om indien noodzakelijk gezien de hulpvraag van de inwoner of op verzoek van een betrokken professional, te komen tot een integrale aanpak en hiervoor persoonsgegevens uit meerdere domeinen bij elkaar te brengen. Op deze manier kunnen mensen met meervoudige problematiek beter worden geholpen. De grondslag om dit te kunnen doen, ontbreekt in de huidige wetgeving. Dit wetsvoorstel zou een aanpassing in de Wmo 2015 betekenen, met spiegelbepalingen in de Participatiewet en de Jeugdwet en de Wet gemeentelijke schuldhulpverlening.

Grondslag voor gegevensverwerking

In de AVG wordt 'toestemming' benoemd als één van de grondslagen voor gegevensverwerking. In de beginjaren werd deze grondslag veel gebruikt door gemeenten, maar naar aanleiding van een uitspraak van de AP zijn gemeenten hiervan terug gekomen. In het sociaal domein is er geen gelijkwaardige relatie tussen cliënt en gemeente en kan er dus geen sprake zijn van vrije toestemmingsverlening. Nu wordt de grondslag wettelijke plicht veelvuldig gebruikt. Gegevensverwerking is vaak noodzakelijk om aan een concrete zorgvraag te voldoen. Dit zag men ook in het onderzoek van de rekenkamercommissie van Tynaarlo (2017): de Wmo 2015 is erop gericht om noodzakelijke hulp te verlenen aan mensen die vanwege beperkingen niet zelfredzaam zijn of problemen hebben met maatschappelijke participatie. Het op voorhand uitsluiten van burgers wat betreft het recht op ondersteuning/jeugdhulp - wegens een weigerachtige houding omtrent het verstrekken van gegevens - getuigt dus niet van een doelmatig privacybeleid.

Samenwerking met ketenpartners

Voor het leveren van passende ondersteuning in het sociaal domein, werken gemeenten met veel verschillende partners samen. Hierbij zijn twee veel voorkomende vormen te onderscheiden, met eigen knelpunten.

1) Het eerste vorm betreft de uitbesteding van een deel van de taken door de gemeente. In die gevallen moet er een duidelijke verwerkersovereenkomst zijn, en blijft de gemeente verantwoordelijk. Hier speelt het zogenaamde 'pettenprobleem' een rol. Dit houdt in dat organisaties zowel als hulpverlener als ook als beslisser voor zorgtoekenning bij cliënten betrokken zijn. Het is daarom zaak dat medewerkers hun taken zorgvuldig scheiden. Daarnaast conflicteert het beroepsgeheim dat bij hulpverleners hoort soms met de informatieverzameling en registratie die hoort bij het beslissen over toekenning van zorg (dit speelt met name in de Jeugdzorg).
2) Gemeenten werken samen met gelijkwaardige partners die eigen taken uitvoeren. Het is in dit geval niet altijd duidelijk of gegevens met deze partijen gedeeld mogen worden, en er kan sprake zijn van andere opvattingen over privacy. In dat geval is het belangrijk om duidelijke werkafspraken te maken over de uitwisseling van persoonsgegevens. Dit kan in de vorm van convenanten, privacy protocollen en in de vorm van een overeenkomst tussen twee partijen als mede-verwerkingsverantwoordelijken (op grond van artikel 26 van de AVG). In de praktijk blijkt dit niet altijd goed te verlopen. Uit de rekenkameronderzoeken in Rijssen-Holten (Rekenkamer West-Twente) en de gemeenten Blaricum, Eemnes en Laren blijkt dat het hanteren van een vaste werkwijze voor gegevensverwerking in het sociaal domein lastig is, wanneer met ketenpartners wordt samengewerkt.

Momenteel beperkt rekenkameronderzoek zich tot de gemeentelijke verantwoordelijkheid; eerder rekenkameronderzoek bekijkt de samenwerking met partners daarom vanuit die invalshoek. De aanstaande Wet versterking decentrale rekenkamers maakt onderzoek naar de verantwoordelijkheden van partners in het sociaal domein ook mogelijk. Deze handreiking loopt op deze wijziging vooruit.

Belang van een goede organisatie

Het organiseren van privacy kan niet worden gezien als een project, maar als een dynamisch en doorlopend proces. Veel gemeenten besteden steeds meer aandacht aan het onderwerp en komen tot smeer vaste werkafspraken. Daarnaast wordt het onderwerp privacy steeds eerder in projecten betrokken. Bijvoorbeeld wanneer er een nieuwe digitale applicatie voor inwoners wordt geïntroduceerd. Een uitdaging voor gemeenten is het borgen van privacy in een steeds meer data-gedreven manier van werken. Bewustwording over het juiste gebruik van gegevens blijft daarom essentieel.

Om privacy goed te kunnen borgen, is het belangrijk om dit goed te organiseren. Dit heeft een organisatorisch, een technisch en een sociaal aspect.

- Organisatorisch: dit gaat over de wijze waarop verantwoordelijkheden binnen de organisatie zijn belegd en hoe visie en werkwijze zijn vastgelegd in beleid. Ook de organisatie van uitbesteding danwel samenwerking met externe partijen is hierbij van belang.
- Technisch: dit gaat met name om informatiebeveiliging en het gebruik van beveiligingsmethoden voor bijvoorbeeld werklaptops en -telefoons.
- Sociaal: in de keten om privacy en informatieveiligheid te borgen, is het menselijk handelen het meest kwetsbaar. Bewustwording van risico's en training op bepaalde werkwijzen is essentieel.

Duidelijkheid vanuit het bestuur en management over de afspraken en de handelingsvrijheid van medewerkers is cruciaal voor de borging van privacy in het sociaal domein. Een goede organisatie met heldere afspraken, waarin medewerkers een heldere verantwoording voor gegevensverwerking afleggen, draagt bij aan het gevoel van zekerheid bij medewerkers. Dit geeft hen het vertrouwen dat ze op de juiste wijze gegevens verwerken en tegelijkertijd zo goed mogelijk in het belang van de cliënt kunnen handelen.

Wanneer hierover twijfel bestaat, ontstaat handelingsverlegenheid bij medewerkers, wat vaak leidt tot vertraging. De privacy officer kan hierbij hulp bieden.

Afhankelijkheid van informatieveiligheid

Randvoorwaardelijk voor het waarborgen van privacy, is goed werkende informatiebeveiliging. Ook hiervoor zijn een aantal wettelijke kaders. De basis is hiervoor geregeld in de AVG, dit is nader uitgewerkt in de Baseline Informatiebeveiliging Overheid (BIO). Vanaf 2013 hanteerden alle gemeenten, anders dan andere overheidslagen, de Baseline Informatiebeveiliging Gemeenten (BIG) als normenkader. Vanaf 1 januari 2020 hanteren alle overheidsorganen één gezamenlijk normenkader, genaamd de BIO.[2] De BIO heeft als doel de informatie(-systemen) bij alle bestuurslagen en bestuursorganen van de overheid te beschermen. Alle bestuursorganen van de overheid dienen erop toe te zien dat onderling uitgewisselde gegevens beveiligd zijn, in overeenkomst met wet- en regelgeving. Aan de raad wordt gerapporteerd middels de Eenduidige Normatiek Single Information Audit (ENSIA)[3], zodat rapportage over informatieveiligheid, aansluit bij de planning- en control cyclus van de gemeente.

Om de kwaliteit van informatiebeveiliging inzichtelijk te maken, is het belangrijk dat rekenkamers toetsen of het aan de wetgeving voldoet, en te toetsen of er beleid is dat voldoet aan de juiste normen en richtlijnen. Dit zijn de Code voor Informatiebeveiliging (NEN ISO 27000-normenserie) en de BIO. De belangrijkste inhoudelijke adviseur over informatieveiligheid bij gemeenten is de Chief Information Security Officer (CISO). Bij grotere gemeenten kunnen onder de CISO meerdere ISO's worden aangesteld.

[2] Voor meer informatie over BIO, zie: https://www.informatiebeveiligingsdienst.nl/project/baseline-informatiebeveiliging-overheid/
[3] Voor meer informatie over ENSIA, zie: https://www.informatiebeveiligingsdienst.nl/project/ensia/

Specifieke privacy uitdagingen van de drie wetten

Het sociaal domein omvat zoals gezegd voornamelijk taken op basis van de Wmo 2015, de Participatiewet en de Jeugdwet. Elke wet heeft zijn eigen doelgroep, bevoegdheden en grondslagen voor gegevensverwerking en daarom ook zijn eigen uitdagingen voor het omgaan met privacy.

Enkelvoudige of meervoudige problematiek

Een meerderheid van de cliënten die aanklopt bij de gemeente heeft enkelvoudige problematiek. In deze gevallen is de gegevensverwerking relatief eenvoudig en duidelijk. Bij inwoners waarbij (mogelijk) sprake is van meervoudige problematiek wordt dit ingewikkelder; hier speelt het eerder beschreven vraagstuk van integraal werken en gegevensuitwisseling.

Een groot vraagstuk voor gemeenten is de wijze waarop wordt vastgesteld of er sprake is van meervoudige problematiek. Het is daarbij zaak om dit in de intake en het bijbehorend onderzoek zorgvuldig te verkennen. Juist deze doelgroep is kwetsbaar. Daarnaast zijn in deze gevallen veel partners betrokken bij de cliënt, wat de situatie complex maakt.

Wmo 2015

Binnen de Wmo 2015 is er sprake van een brede doelgroep, met sterk uiteenlopende vaardigheden van inwoners en hulpvragen, dit maakt het lastiger om vaste handelswijzen te hanteren. Er speelt vaak meervoudige problematiek, zonder dat er een hulpvraag op meerdere terreinen is. Het is voor consulenten zaak om zaken indien noodzakelijk integraal uit te vragen. Een mogelijk risico hierbij is dat er (te)veel gegevens worden vastgelegd in dossiers.

Jeugdwet

Vanuit de Jeugdwet zijn veel mensen betrokken bij de behandeling van een cliënt. Dit zijn niet alleen ouders, maar in veel gevallen ook andere instanties zoals de huisarts of de politie. Dit maakt het omgaan met gegevens complex, temeer omdat veel betrokkenen ook te maken hebben met een beroepsmatige geheimhoudingsplicht. De Jeugdwet kent mede daarom veel specifieke situaties waarin privacyoverwegingen een rol spelen. Een voorbeeld is een kind met ouders die in scheiding liggen, maar die wel beide gezag bevoegd zijn.

Bij de Jeugdwet speelt tevens de uitdaging over wie toegang heeft tot gegevens. Hebben de cliënten zelf toegang tot de gegevens? En welke ouders hebben dit? Bij familieproblematiek kan het wenselijk zijn om informatie voor de ouders af te schermen. Een andere uitdaging manifesteert zich als cliënten 18 jaar worden. Dan volgt er een overstap naar een nieuwe zorgverlener, waarbij ook de gegevens moeten worden overgedragen.

Participatiewet

Bij re-integratieproblematiek speelt vaak meer dan alleen de beoogde terugkeer naar een werksituatie. Als er sprake is van aanvullende problematiek, bemoeilijkt dat de begeleiding vanuit de gemeente. Denk hierbij aan middelenmisbruik en/of schuldenproblematiek. Vanuit privacy overwegingen is het niet noodzakelijk om hierover gegevens te verzamelen en te verwerken, dit is strikt genomen niet relevant bij het al dan niet toekennen van een uitkering. In het geval van een re-integratietraject is het breed uitvragen van situaties die re-integratie mogelijk belemmeren, wel noodzakelijk. Gedacht vanuit een integrale benadering, waarbij goede zorg en dienstverlening centraal staan, kan het juist wel als relevant gezien worden om een brede uitvraag te doen wanneer een inwoner zich meldt voor de aanvraag van een uitkering. Voor de rekenkamer kan het interessant zijn om te onderzoeken welke keuzes de specifieke gemeente maakt in de omgang met deze problematiek.

Aandachtspunten bij afstemming tussen de drie wetten

Elke wet binnen het sociaal domein bevat zijn eigen grondslagen op basis waarvan gegevens verwerkt mogen worden. Bij multi-problematiek (waarbij mensen aanspraak kunnen maken op dienstverlening op basis van meerdere wetten) is het belangrijk dat hiermee rekening wordt gehouden bij het uitwisselen van gegevens tussen de verschillende 'loketten'. Zoals eerder genoemd, is er tot de invoering van de Wams geen grondslag om integraal te kunnen werken, dit maakt het voor gemeenten extra lastig om zich enerzijds aan de wet te houden en anderzijds integraal te werken. Voor rekenkameronderzoek is het interessant om inzicht te krijgen welke keuzes er in de specifieke gemeente worden gemaakt in de uitwisseling van gegevens tussen de loketten. Worden hier van bovenaf duidelijke kaders opgelegd, of hangt dit af van afspraken tussen consulenten? En welke impact heeft dit op de kwaliteit van dienstverlening en hoe wordt het voldoen aan de privacywetgeving geborgd?

Handvatten voor onderzoek

Wilt u zelf aan de slag met rekenkameronderzoek naar privacy in het sociaal domein? De tips en aandachtspunten hieronder dienen ter inspiratie en kunnen afhankelijk van de situatie in uw gemeente en de behoeften van uw raad gecombineerd worden toegepast. Er zijn veel opties voor het vormgeven van uw rekenkameronderzoek, zowel op inhoudelijk als methodologisch vlak. Allereerst geven wij voorbeelden van methoden die andere rekenkamers hebben gebruikt en wat deze opleveren (paragraaf 3.1). Hierna beschrijven wij zeven belangrijke inhoudelijke invalshoeken om uw onderzoek richting mee te geven (3.2). Vervolgens presenteren wij een voorzet voor een onderzoeksopzet in de vorm van een quickscan (3.4) en een verdiepend onderzoek (3.5).

Onderzoeksmethoden

In de rekenkameronderzoeken worden diverse onderzoeksmethoden gebruikt. Hieronder geven wij een overzicht van interessante onderzoeksmethoden uit verschillende onderzoeken en bespreken wij een aantal methodologische keuzes die u in het onderzoeksdesign tegenkomt.

Rekenkamers gebruiken diverse onderzoeksmethoden

- Een startbijeenkomst tussen de onderzoekers en de ambtelijke organisatie zorgt voor een warme start van het onderzoek. Eventuele vragen of bezwaren komen direct op tafel, dit versterkt het draagvlak voor het onderzoek. Daarnaast worden in de startbijeenkomst werkafspraken gemaakt die het proces vergemakkelijken.
- Het meest gebruikelijk is om een documentanalyse van de diverse beleidsstukken uit te voeren. Denk hierbij aan privacy- en informatiebeveiligingsbeleid, documenten ten aanzien van de implementatie van dit beleid zoals werkafspraken en protocollen, audits en interne evaluaties.
- Dossieronderzoek (geanonimiseerd): Welke gegevens zijn vastgelegd, en is dit in overeenstemming met de wetgeving en de afspraken binnen de gemeente?
- Middels interviews toetst men de uitkomsten van de documentanalyse vervolgens aan de praktijk. Hiervoor worden meestal interviews gedaan met privacy specialisten en consulenten uit het sociaal domein.
- In een enquête worden inwoners bevraagd over hoe zij aankijken tegen het opslaan en delen van persoonsgegevens door de gemeente (Rekenkamer Amsterdam).
- Betrekken van (zorg)ketenpartners, bijvoorbeeld middels een groepsbijeenkomst en een enquête onder medewerkers van zorgpartners (Rekenkamer Arnhem).
- Praktijkonderzoek met een casestudy, waarin is getoetst of beleid en afspraken worden nageleefd. (Rekenkamer Doetinchem).
- Technische toetsing, bijvoorbeeld door middel van een penetratietest (ethisch hacken). Hiermee wordt getest of toegang te krijgen is tot (bijzondere) persoonsgegevens in systemen en tot andere gevoelige informatie die de gemeente in beheer heeft (Rekenkamer Rotterdam).

Deelvragen per invalshoek

Onderzoek naar privacy in het sociaal domein wordt ingestoken vanuit meerdere inhoudelijke invalshoeken. Wij presenteren zes belangrijke invalshoeken met bijpassende opties voor onderzoeksvragen. Deze lijst is niet uitputtend en niet wederzijds uitsluitend: het is juist nodig om binnen een onderzoek meerdere invalshoeken te combineren. In 3.3 geven we aan welke invalshoeken goed passen binnen een quickscan en welke van toegevoegde waarde zijn binnen een verdiepend onderzoek.

Wetmatigheid

Een belangrijke taak van rekenkamer(commissie)s is het controleren van de rechtmatigheid van gemeentelijk beleid. Deze invalshoek stelt u in staat te controleren in hoeverre de gemeente handelt volgens de wettelijke plichten op het gebied van privacy. Dit zijn onder andere het hebben van een privacybeleid, het bijhouden van een verwerkingsregister, DPIA's worden uitgevoerd en er worden verwerkingsovereenkomsten opgesteld. De Vereniging van Nederlandse Gemeenten (VNG) biedt hiervoor een handige checklist.[4] Dit aspect is goed middels documentanalyse te onderzoeken, mogelijk gecombineerd met interviews met de privacy officer, de CISO en de functionaris gegevensbescherming.

- In hoeverre voldoet het gemeentelijk privacybeleid aan de relevante wet- en regelgeving zoals de BIO en AVG?
- In hoeverre zijn algemene privacykaders vertaald naar en toegespitst op specifieke vraagstukken binnen het sociaal domein?
- In hoeverre voldoet de uitvoeringspraktijk in het sociaal domein aan de relevante wet- en regelgeving rondom privacy die zijn geborgd in de Wmo 2015, Jeugdwet en Participatiewet?
- Hoe zijn de wet- en regelgeving geïmplementeerd en hoe functioneren deze binnen het sociaal domein?
- In hoeverre en op welke wijze wordt de wetmatigheid van het handelen binnen de organisatie gemonitord en gecontroleerd?
- Welke privacyrisico's loopt de gemeente, hoe is dit in kaart gebracht en welke maatregelen worden genomen om hiermee om te gaan?
- Welke privacyrisico's lopen inwoners?
- Worden inwoners actief en duidelijk geïnformeerd over gegevensverwerking?

Informatieveiligheid

Informatieveiligheid is onlosmakelijk verbonden met privacy. Er kunnen immers zeer zorgvuldige afspraken en overwegingen zijn over het opslaan en uitwisselen van persoonsgegevens, maar wanneer dit niet veilig gebeurt liggen privacyrisico's alsnog op de loer. Het strekt daarom tot aanbeveling om binnen een onderzoek naar privacy ook aandacht te besteden aan informatieveiligheid.

Deze invalshoek biedt de raad inzicht over de mate waarin de technische infrastructuur omtrent privacy van de gemeente op orde is. Informatiebeveiliging is niet alleen een technisch geheel, juist en vooral de medewerker is vaak de zwakste schakel. Rekenkameronderzoek biedt daarom naast de technische kant met name inzicht in de sociale aspecten van veiligheid, namelijk in hoeverre medewerkers hun verantwoordelijkheid voor informatieveiligheid hebben geïnternaliseerd en vertaald in verantwoord handelen. Binnen het sociaal domein spelen vragen als: liggen er dossiers op tafel, gebruiken consulenten onbeveiligde email en/of Whatsapp om met partners over cliënten te overleggen?

[4] Het Borgen van de Algemene Verordening Gegevensbescherming in de gemeentelijke organisatie. https://www.vngrealisatie.nl/sites/default/files/2018-11/dec2018%20criteria%20borging%20AVG%20VNG%20Realisatie.pdf

Dit aspect is te onderzoeken door middel van documentanalyse, aangevuld met interviews (waaronder met de CISO), een enquête onder medewerkers en/of een inlooptest.

- In hoeverre is de technische infrastructuur op het gebied van privacy in lijn met de landelijke richtlijnen als de BIO?
- Zijn de functionarissen, zoals CISO en Functionaris Gegevensbescherming, (goed) gepositioneerd?
- In welke mate hebben gemeentelijke medewerkers hun verantwoordelijkheid ten aanzien van informatieveiligheid geïnternaliseerd?
- Heeft de gemeente de risico's in beeld? Zijn hiervoor de juiste analyses uitgevoerd, zoals een GAP- en risicoanalyse? Zijn er heldere afspraken gemaakt over de omgang met een datalek/aanval op de systemen?
- Welke kwetsbaarheden ten aanzien van informatieveiligheid laat een inlooptest zien in de praktijk?

Governance

Essentieel voor het omgaan met privacyvraagstukken is de inrichting van de organisatie. Onderzoek biedt de raad inzicht in de wijze waarop de verantwoordelijkheden zijn belegd binnen de organisatie en het bestuur en in hoeverre deze keuzes logisch zijn. Voor dit aspect zijn een documentanalyse en interviews (portefeuillehouder/teamleider sociaal domein/functionaris gegevensbescherming) en/of een enquête onder medewerkers geschikte onderzoeksmethoden.

- Op welke wijze zijn de verantwoordelijkheden voor privacy (en informatieveiligheid) tussen gemeenteraad, college en ambtelijke organisatie verdeeld?
- Op welke wijze zijn de verantwoordelijkheden voor privacy (en informatieveiligheid) binnen de gemeentelijke organisatie en het sociaal domein belegd?
- Hoe functioneert de verdeling van verantwoordelijkheden in de praktijk binnen het sociaal domein? Waar zitten eventuele knelpunten?

Sociaal en cultureel

Formele structuren en beleid bieden handvatten aan de organisatie voor het omgaan met privacy en informatiebeveiliging. De daadwerkelijke uitkomsten worden echter sterk beïnvloed door informele processen, sociale factoren en de organisatiecultuur. Om de raad volledig inzicht te geven in de gemeentelijke praktijk omtrent privacy, is het daarom van belang om deze sociale aspecten in beeld te brengen in uw rekenkameronderzoek. Hierbij is het zaak om te spreken met vertegenwoordigers uit de gehele organisatie. Te denken valt aan (groeps-)interviews met teamleiders sociaal domein, beleidsmedewerkers en consulenten. Ook in gesprekken met privacy officers, de functionaris gegevensbescherming en de chief information security officer komt dit aspect aan bod.

- In hoeverre is er sprake van breed gedeelde opvattingen over privacy?
- Is er voldoende bewustzijn van het belang van privacy in de verschillende lagen van de organisatie?
- Welke werkafspraken gelden er binnen het sociaal domein omtrent privacy?
- Op welke wijze wordt omgegaan met situaties waarin privacy en kwaliteit van dienstverlening (ogenschijnlijk) met elkaar in tegenspraak zijn?
- Is privacy een terugkerend onderwerp in overleggen?
- Is er voldoende geïnvesteerd in kennis en kunde omtrent privacy in de organisatie?
- Welke trainingen/opleidingen zijn er voor medewerkers en wordt hier gebruik van gemaakt?
- Welke invloed heeft de organisatiecultuur op de wijze waarop met privacy wordt omgegaan?

Samenwerkingspartners

Binnen het sociaal domein wordt veel samengewerkt met zorg- en uitvoeringspartners. Daarnaast hebben gemeentelijke organisaties de opdracht om integraal te werken, samen te werken met medewerkers van verschillende teams/domeinen. Integraal werken en samenwerken met partners brengen aanvullende vraagstukken omtrent privacy met zich mee. Onderzoek biedt de raad zicht op de wijze waarop omgegaan wordt met deze inherente spanning en in de afspraken die gemaakt zijn omtrent privacy met partners.

- Wat zijn de verschillen en overeenkomsten in de opvattingen over privacy tussen de gemeente en haar partners in het sociaal domein?
- Is er voldoende bewustzijn van het belang van privacy bij partners?
- Worden de verwerkersovereenkomsten conform beleid gesloten? Worden daarin heldere en sluitende afspraken gemaakt hoe om te gaan met persoonsgegevens?
- Op welke wijze houdt de gemeente toezicht op de verwerking van gemeentelijke gegevens door partners in het sociaal domein?
- Op welke wijze wordt omgegaan met situaties waarin de opvattingen over privacy van de gemeente en haar partners verschillen?
- Welke spanning ervaart de gemeentelijke organisatie tussen integraal werken en privacy?

De rol van de raad

Als onafhankelijk adviseur van de gemeenteraad is het belangrijk dat de rekenkamer(commissie) zich (ook) buigt over de rol van de raad. Onderzoek kan de raad inzicht bieden over zijn eigen verantwoordelijkheden op het gebied van privacy. Daarnaast kan onderzoek inzicht bieden in de wijze waarop de raad zijn controlerende en kaderstellende rol invult en welke verbetermogelijkheden hieromtrent bestaan.

- Op welke manier geeft de gemeenteraad invulling aan zijn controlerende rol op het gebied van privacy in het sociaal domein?
- Hoe heeft de gemeenteraad beleidskaders gesteld ten aanzien van privacy en informatiebeveiliging?
- Op welke wijze wordt de gemeenteraad geïnformeerd over privacy in het sociaal domein en hoe wordt het ENSIA hierbij ingezet?
- En welke instrumenten zet de raad zelf in om informatie te verkrijgen?
- Op welke wijze vult de raad zijn controlerende en kaderstellende rol in?

Implementatie van de AVG

Sommige rekenkamers kiezen ervoor om de implementatie van de AVG als directe aanleiding voor het onderzoek te nemen. Deze optie belichten we als laatste, omdat deze veel van de bovenstaande elementen in zich heeft. De implementatie van de AVG is namelijk aanleiding geweest voor veel gemeenten om visie, beleid en organisatie opnieuw in te richten. Een onderzoek naar de implementatie moet dus al deze elementen in zich hebben.

- Hoe is de implementatie van de AVG gerealiseerd in de praktijk?
- Welke gevolgen heeft de implementatie van de AVG gehad op de visie en het beleid ten aanzien van privacy in het sociaal domein?
- Welke gevolgen heeft de implementatie van de AVG gehad op de verdeling van rollen en verantwoordelijkheden binnen de gemeentelijke organisatie?
- Welke gevolgen heeft de implementatie van de AVG gehad op de processen en werkafspraken binnen de gemeentelijke organisatie?
- Welke gevolgen heeft de implementatie van de AVG gehad op de samenwerking met partners in het sociaal domein?
- Op welke wijze was de raad betrokken bij de implementatie van de AVG?

Quickscan of verdiepend onderzoek?

Rekenkamers kunnen afhankelijk van beschikbare tijd en budget kiezen voor een quickscan of een diepteonderzoek. Met een quickscan verkrijgt u op eenvoudige manier inzicht in de stand van zaken in de betreffende gemeente. Een quickscan richt zich met name op het vaststellen of het onderwerp als urgent wordt ervaren, welk beleid er is en of alle posities zijn ingevuld. Wilt u meer inzicht verkrijgen in de wijze waarop privacy wordt geborgd in de (dagelijkse) processen, dan kan een verdiepend onderzoek dit inzicht bieden. In de volgende paragrafen werken we twee onderzoeksopzetten uit. Of er verdiepend onderzoek wordt uitgevoerd, kan natuurlijk ook besloten worden na een quickscan.

Onderzoeksopzet 1 – Quickscan

Een quickscan op het gebied van privacy in het sociaal domein kan de raad snel inzicht bieden in de stand van zaken op dit onderwerp. De vraag die hierin centraal staat, is in hoeverre de gemeente de basis op orde heeft. Inhoudelijk omvat de quickscan de elementen wetmatigheid, informatieveiligheid (op beleidsniveau) en governance.

De onderzoekswerkzaamheden beperken zich voornamelijk tot documentanalyse. Denk hierbij tenminste aan de volgende documenten:

- Privacy- en informatieveiligheidsbeleid;
- Notities en uitgangspunten van de gemeente als controle-organisatie op dit vlak;
- Privacyprotocollen;
- Procedures bij datalekken/incidenten;
- Samenwerkingsovereenkomsten/convenanten;
- Verwerkersovereenkomsten;
- Zelfevaluaties op het gebied van privacy en informatieveiligheid;
- Implementatieplan AVG;
- Passieve en actieve informatievoorziening aan de raad/ENSIA.

De inzichten uit de documentanalyse vult u eventueel aan met interviews. Daarbij kan gedacht worden aan het voeren van twee groepsinterviews: Het eerste interview wordt gevoerd met de portefeuillehouder, teamleider sociaal domein en een beleidsmedewerker en is gericht op het beleid en de verdeling van verantwoordelijkheden. Het tweede interview wordt gevoerd met de functionaris gegevensbescherming, de chief information security officer en een privacy officer en is gericht op juridische en technische aspecten en op kwetsbaarheden en dilemma's.

Deze optie is geschikt voor rekenkamer(commissie)s die een eerste verkennend onderzoek willen doen naar dit thema en/of een bescheiden budget hebben. In deze quickscan kan een normenkader een houvast bieden om het gemeentelijk beleid aan te staven.

Fase 1 – Startgesprek
Fase 2 – Documentanalyse
Fase 3 – Groepsinterviews (optioneel)
Fase 4 – Rapportage

Onderzoeksopzet 2 – Verdiepend onderzoek

Een verdiepend onderzoek geeft de raad inzicht in de praktijk en de dilemma's die spelen op het gebied van privacy in het sociaal domein. Het biedt de rekenkamer(commissie) de gelegenheid om aan te sluiten bij de lokale vraagstukken op basis van de signalen die zij ontvangt. De onderzoeksopzet die hier gepresenteerd wordt kan daarbij ter inspiratie worden gebruikt, en aangepast worden aan de situatie in uw gemeente.

Een verdiepend onderzoek, met een groter budget, kan meerdere inhoudelijke invalshoeken omvatten. Gezien de eerder beschreven impact van menselijk handelen op privacy én de vaak ingewikkelde constellatie van het gemeentelijk sociaal domein, is het aan te raden om voor de verdieping de aspecten 'sociaal' en 'samenwerkingspartners' te overwegen. Dit vereist een uitbreiding van de documentanalyse, met bijvoorbeeld de volgende typen documenten:

- Organisatiestructuur;
- Werkprocessen en -afspraken binnen het sociaal domein;
- Werk- en prestatieafspraken met partners in het sociaal domein.

Wanneer een sociale en culturele invalshoek wordt gekozen in het onderzoek, is het belangrijk om medewerkers met een verscheidenheid aan functies in het onderzoek te betrekken. Dit stelt de onderzoekers in staat om de organisatiecultuur in kaart te brengen en te analyseren of er sprake is van een eenduidige visie en uitvoering.

Het betrekken van samenwerkingspartners vereist extra aandacht in het voorbereiden van het onderzoek. Via het startgesprek kan met de ambtelijk contactpersoon worden besproken wie geschikte respondenten kunnen zijn bij de samenwerkingspartners. De ambtelijk contactpersoon kan ook voor een warme introductie zorgen. De ervaring leert dat zorg- en uitvoeringspartners over het algemeen graag meewerken aan rekenkameronderzoeken.

Daarnaast kan vanuit het aspect van informatieveiligheid gekozen worden voor het uitvoeren van een test. Hierbij is het belangrijk om vooraf heldere afspraken te maken met de organisatie over de voorwaarden waaronder deze test gedaan kan worden. De simpele variant is een inlooptest, waarbij onderzoekers het gemeentehuis binnenlopen en observeren hoe het gesteld is met de informatieveiligheid. Andere opties zijn het gebruik van een phishingmail (om te zien of medewerkers inloggegevens prijsgeven) of de inzet van ethische hackers (om kwetsbaarheden in het systeem te testen).

Tot slot mag de rol van de raad in een verdiepend onderzoek niet ontbreken. Eerder onderzoek wijst uit dat de kennis en het bewustzijn omtrent privacy sterk verschillen tussen gemeenteraden. Rekenkameronderzoek kan er een belangrijke bijdrage aan leveren dat de kennis en het bewustzijn in uw raad versterkt worden. Een interessante optie hierbij is om onder de loep nemen in hoeverre de griffie en raadsleden zelf goed omgaan met privacy.

Fase 1 – Startgesprek
Fase 2 – Beleid in beeld (Documentanalyse plus interviews beleidsmakers en portefeuillehouder)
Fase 3 – Privacy in de praktijk (Interviews organisatie)
Fase 3a – Privacy in samenwerking (interviews partners) - optioneel
Fase 3b – De proef op de som (technische test) - optioneel
Fase 4 – De rol van de raad (Raadsworkshop plus groepsinterview griffie)

Tot slot: enkele overwegingen

Het gebruik van een normenkader

Rekenkamers overwegen om bij onderzoek naar privacy in het sociaal domein een normenkader te hanteren. Een normenkader past niet bij elk onderzoek. Het voordeel van het hanteren van een normenkader is dat u hiermee toetst of de gemeente de basis goed op orde heeft. De harde criteria van privacybeleid en informatieveiligheid worden in kaart gebracht, zoals in hoeverre er wordt voldaan aan wettelijke normen. In een quickscan is dit een logische keuze. Een normenkader werkt echter minder goed wanneer er dieper op de materie wordt ingezoomd. Inzicht bieden in de dilemma's die spelen en de wijze waarop er door de organisatie mee wordt omgaan, vereist nuance en deze aspecten zijn lastiger te vangen in vooraf opgestelde normen.

De rekenkamer valt zelf ook onder de privacywet

De rekenkamer moet zelf ook rekening houden met de privacywet. Dit betekent onder andere dat persoonsgegevens die de rekenkamer verzamelt in het kader van haar onderzoek, niet voor andere doeleinden gebruikt mogen worden. Ook kan het zijn dat de rekenkamer bij samenwerking met externe partijen een verwerkersovereenkomst moet afsluiten. Wij adviseren rekenkamer(commissie)s om vraagstukken omtrent privacy af te stemmen met de FG van hun gemeente. Sommige rekenkamers hebben een eigen FG, of delen deze met een aantal rekenkamers.

Bijlage 1: Leeslijst

Hier vindt u een selectie van relevante rekenkamerrapporten en overige literatuur. U kunt deze bronnen raadplegen om u verder te verdiepen in het onderwerp en als naslagwerk bij de voorbereiding van uw eigen rekenkameronderzoek.

Jaar	Organisatie	Titel
2016	Rekenkamer Amsterdam	Privacy van burgers met een hulpvraag
2016	Rekenkamercommissie Eindhoven	Informatieveiligheid en privacy in het sociaal domein: een open deur
2017	Rekenkamer Arnhem	Privacy made in [Arnhem] Privacy en informatieveiligheid in het sociaal domein
2017	Rekenkamercommissie Doetinchem	Een onderzoek naar het privacybeleid van de gemeente Doetinchem
2017	Rekenkamer West Twente	Privacy en informatieveiligheid in het sociaal domein
2017	Rekenkamercommissies Baarn, Eemnes, Laren	Rekenkameronderzoek Privacy in het sociaal domein
2017	Rekenkamer Rotterdam	In onveilige handen: onderzoek informatiebeveiliging van gevoelige informatie
2017	Rekenkamercommissie Tynaarlo	Privacy in het sociaal domein: nice to know or need to know?
2018	Rekenkamercommissie Smallingerland	Quick Scan Privacy en Informatieveiligheid
2019	Rekenkamercommissies Achtkarspelen en Tytsjerksteradiel	Rekenkameronderzoek 2018 naar informatiebeveiliging en privacy
2019	Rekenkamer Dronten	Privacy en informatieveiligheid in het sociaal domein
2019	Rekenkamercommissie Zaltbommel	Privacy in het sociaal domein

Jaar	Organisatie	Titel
2015	Vereniging van Nederlandse Gemeenten	Privacy – Handreiking voor professionals – verwerken persoonsgegevens
2016	Autoriteit Persoonsgegevens	Gegevensverwerking gemeente Nijmegen bij toeleiding naar hulp. Wordt bij het gebruik van de zelfredzaamheidsmatrix voldaan aan het noodzakelijkheidsvereiste?
2016	Autoriteit Persoonsgegevens	Verwerking van persoonsgegevens in het sociaal domein: De rol van toestemming
2017	Ombudsman Rotterdam	Het hemd van het lijf
n.d.	Informatiebeveiligingsdienst	Diverse factsheets en handreikingen over het onderwerp informatiebeveiliging: https://www.informatiebeveiligingsdienst.nl/kennisproducten-ibd/
n.d.	Vereniging van Nederlandse Gemeenten	Over privacy sociaal domein: https://vng.nl/artikelen/over-privacy-sociaal-domein

Bijlage 2: Gesprekspartners

Voor het schrijven van deze handreiking hebben wij gesproken met een aantal experts, leden van rekenkamer(commissie)s en gemeentelijke medewerkers. In het onderstaande schema benoemen wij onze gesprekspartners.

Gesprekspartners

Achternaam	Initialen (voornaam)	Functie	Organisatie	Onderdeel
Ebbers	Corrie	Privacy jurist	Ebbers Juridisch Advies	
Van Boven	Jolanda	Privacy jurist	Van Boven Juridisch Adviesbureau	
Van der Hulst	Gideon	Onderzoeker	Necker van Naem	
Van Hemmen	Dick	Voorzitter	Rekenkamercommissie Dronten	
Kok	Arjan	Senior onderzoeker	Rekenkamer Metropool Amsterdam	
Lamboo	Terry	Senior adviseur	Ministerie van Binnenlandse Zaken	Traject Uitwisseling persoonsgegevens en Privacy
Bouwer	Astrid	Procescoördinator	Gemeente Zoetermeer	Sociaal Domein
Dohmen	Carlijn	Privacyfunctionaris	Gemeente Zoetermeer	Sociaal Domein
Slooter	Yvonne	Beleidsmedewerker en jurist	Gemeente Zoetermeer	Sociaal Domein
Steenbrink	Erika	Functionaris voor gegevensbescherming	Gemeente Ede Gemeente Wageningen Gemeente Rhenen	
Oosthuizen	Fleur	Privacy officer	Gemeente Eindhoven	Sociaal Domein