De Rekenkamer neemt een onafhankelijke positie in binnen de gemeente Nijmegen.

Nijmegen

Postadres
Gemeente Nijmegen
BM60
Postbus 9105
6500 HG Nijmegen

Bezoekadres
Korte Nieuwstraat 6
6511 PP Nijmegen

T 14 024
nijmegen.nl

Contactpersoon
Jelly Smink
j.smink@nijmegen.nl
T 024 – 329 23 38

Ons kenmerk
BM60/10/E21.001523

Gemeenteraden en colleges gemeenten regio Rijk van Nijmegen

Verstuurd via e-mail

Datum 23 juni 2021
Betreft Regionaal rekenkameronderzoek

Geachte leden van de gemeenteraden en colleges van de gemeenten in de regio Rijk van Nijmegen,

Via deze brief informeren wij u over een onderzoek dat de rekenkamer(commissie)s van de gemeenten Berg en Dal, Beuningen, Nijmegen, en Wijchen gaan uitvoeren naar de informatiebeveiliging en privacybescherming en de rol van de raden daarbij.

In het Plan van Aanpak dat als bijlage bij deze brief is gevoegd, gaan wij in op de aanleiding, de onderzoeksvragen, de aanpak en de planning voor het onderzoek.

Wanneer u vragen heeft naar aanleiding van deze brief kunt u contact opnemen met de voorzitter of secretaris van uw eigen rekenkamer(commissie), of met Jelly Smink (j.smink@nijmegen.nl of 024 329 2338), secretaris van de Rekenkamer Nijmegen.

Met vriendelijke groet,
Mede namens de voorzitters van de rekenkamer(commissie)s Berg en Dal, Beuningen en Wijchen

G. Backus
Voorzitter Rekenkamer Nijmegen

J. Smink
Secretaris Rekenkamer Nijmegen

In verband met de corona-maatregelen is deze brief via e-mail verzonden en niet ondertekend.



Plan van aanpak
Regionaal rekenkameronderzoek informatiebeveiliging en privacybescherming Berg en Dal, Beuningen, Nijmegen en Wijchen

Juni 2021

Inhoudsopgave

Inhoudsopgave **2**

1. Aanleiding **3**

2. Doelstelling en vraagstelling **3**

3. Plan van aanpak **7**

4. Planning van het onderzoek **9**

5. Normenkader **10**

DMC GROUP
SECURITY MANAGEMENT

1. Aanleiding

Gemeenten doen op forse schaal aan gegevensverwerking en zij verzamelen, beheren en verwerken daarbij niet zelden gevoelige persoonsgegevens. Die verwerking vindt vervolgens plaats in steeds complexere structuren van (keten-)samenwerking en uitbesteding. Zij moeten daarbij in toenemende mate letten op de informatiebeveiliging en privacybescherming. Met name de introductie van de AVG in 2018 dwingt hen om hun informatiebeveiliging zeer serieus te nemen.

Doordat de (persoons)gegevens en informatieprocessen steeds meer gedigitaliseerd zijn, worden gemeenten ook kwetsbaarder voor cybercriminaliteit, of die nu bedoeld is om bepaalde gegevens te verkrijgen of als afpersingsmiddel. Gemeenten dienen zich daartegen te wapenen, maar slagen daar niet altijd goed in, getuige de recente datalekken en veiligheidsincidenten in bijvoorbeeld de gemeente Hof van Twente.

De uitdagingen waarmee gemeenten worden geconfronteerd vormen de aanleiding voor de gezamenlijke rekenkamer(commissie)s in de regio Rijk van Nijmegen om de stand van zaken van de informatiebeveiliging en privacybescherming in hun gemeentelijke organisatie(s) te onderzoeken. Dit openbare document bevat het plan van aanpak voor het onderzoek.

2. Doelstelling en vraagstelling

Informatiebeveiliging en privacybescherming zijn twee verschillende dingen. Informatiebeveiliging kan worden omschreven als het treffen en onderhouden van een samenhangend pakket maatregelen om de beschikbaarheid, integriteit (juistheid) en vertrouwelijkheid van de (digitale) gegevens in de organisatie te waarborgen. Bij privacybescherming gaat het om de toepassing van normen die bepalen hoe persoonsgegevens mogen worden gebruikt.

Voor beide thema's geldt dat de gemeente niet in een vacuüm opereert. Integendeel, zij werkt op bijna alle beleidsterreinen samen met andere organisaties, of het nu andere overheden zijn, maatschappelijke instellingen, bedrijven, etc. Bij de uitvoering van haar taken is de gemeente in veel gevallen genoodzaakt om informatie, en persoonsgegevens in het bijzonder, te delen met allerlei partijen. Dat is een complicerende factor bij de zorg voor de informatiebeveiliging en privacybescherming.

Beide thema's zijn van groot belang voor de inwoners van onze gemeenten. Van de gemeentebesturen mag enerzijds worden verwacht dat zij beleid, organisatie, uitvoering en toezicht voor deze beide onderwerpen op orde hebben; dat geldt vanzelfsprekend ook voor het deel van de taken en verantwoordelijkheden dat aan de iRvN[1] is uitbesteed. Anderzijds weten we uit de incidenten binnen en buiten het openbaar bestuur dat ook grote, professionele organisaties slachtoffer kunnen worden van digitale inbraken en lekken. Er is geen reden om aan te nemen dat onze gemeenten onkwetsbaar zijn. We houden er in onze vraagstelling en aanpak van het onderzoek rekening mee dat we op kwetsbaarheden zullen stuiten. Om die reden nemen we expliciet de onderzoeksvraag mee of onze gemeenten effectief en efficiënt werken aan het analyseren en verminderen van de risico's.

1. ICT Rijk van Nijmegen (iRvN) is de regionale samenwerkingspartner op ICT-gebied voor de gemeenten in Het Rijk van Nijmegen. Alle zeven gemeenten hebben hun ICT ondergebracht bij iRvN.

Behalve op de vraag wat de colleges doen, richt het onderzoek zich ook welbewust op de gemeenteraden. De gemeenteraden, die als lekenbestuur geen informatiespecialisten (kunnen) zijn, moeten in deze context hun kaderstellende en controlerende taak goed (kunnen) vervullen. Daarbij is het van belang dat zij dit op het juiste niveau doen: de hoofdlijnen en vereisten bepalen (kaderstelling) en controleren of het college die goed invult (controle), maar niet teveel meegaan in de (bedrijfsvoerings)details.

De doelstelling van het onderzoek is daarom tweeledig:

1. Voor de gemeenteraden inzichtelijk maken hoe de informatiebeveiliging en privacybescherming door hun eigen gemeente ervoor staat, en hoe daaraan wordt gewerkt in hun gemeente.
2. De gemeenteraden ondersteunen bij de kaderstelling en controle op dit vlak. Een belangrijke voorwaarde daarvoor is de manier waarop het college de raad informeert.

De dubbele vraagstelling van dit onderzoek is dan ook:

> **Is de informatiebeveiliging en privacybescherming van de gemeenten Berg en Dal, Beuningen, Nijmegen en Wijchen voldoende op orde, is er voldoende zicht op de risico's en werken de gemeenten op effectieve en efficiënte wijze aan verbetering van de onderdelen die niet voldoende op orde zijn?**
>
> **Hoe kunnen de gemeenteraden de komende jaren hun kaderstellende en controlerende taak op deze thema's goed vervullen?**

Om deze vraag te beantwoorden zijn deelvragen geformuleerd. We onderscheiden onderzoeksdeel A voor de informatiebeveiliging, onderzoeksdeel B voor privacybescherming, en onderzoeksdeel C voor de rol van de raad.

A. Informatiebeveiliging

A1. Hoe zijn de taken en verantwoordelijkheden op het terrein van ICT- en informatiesystemen en met name de informatiebeveiliging tussen de gemeenten en iRvN verdeeld?

A2. Wat zijn de beleidskaders van de gemeenten en de iRvN t.a.v. hun informatiebeveiliging, met name van persoonsgegevens?

A3. Voldoen deze beleidskaders aan de gangbare standaarden en wetgeving op het vlak van privacy en informatiebeveiliging?

A4. Wat is het beschikbare budget van de deelnemende gemeenten en iRvN voor informatiebeveiliging, en is het mogelijk om een oordeel te geven (bijvoorbeeld door benchmarking) over de toereikendheid hiervan?

A5. In hoeverre worden de beleidskaders in de praktijk in de gemeenten en de iRvN nageleefd?

A6. Op welke manier worden gemeentelijke medewerkers bewust gemaakt van hun verantwoordelijkheden ten aanzien van het bewaken van de informatiebeveiliging? Daarbij kan worden gedacht aan onder meer trainingen en ondersteuning, maar ook via functieomschrijvingen, aandacht in functioneringsgesprekken etc.

A7. Heeft de gemeente een proces van continue verbeteren in werking voor haar informatiebeveiliging en opslag en beheer van persoonsgegevens in het bijzonder?

A8. Hebben de gemeenten en de iRvN voldoende zicht op de risico's (zowel veiligheidsrisico's als financiële risico's ingeval van lekken of incidenten) op het gebied van informatiebeveiliging, en zijn er maatregelen getroffen om de grootste risico's te kunnen ondervangen?

A9. Hebben de gemeenten en de iRvN een concreet plan voor het effectief en efficiënt verkleinen van de risico's, en voldoet dat plan aan de gebruikelijke standaarden?

B. Privacybescherming

Onderzoeksdeel B richt zich op de omgang met persoonlijke gegevens van burgers door de gemeenten, en zo nodig ook de iRvN. Om het onderzoek uitvoerbaar te houden, beperken we dit deel van het onderzoek. Dat betekent dat met name voor de deelvragen B3, B4, B5, B6 en eventueel B10 wordt ingezoomd op een kleiner subdomein (zie paragraaf 3 Plan van aanpak).

B1. Wat zijn de gemeentelijke beleidskaders t.a.v. privacybescherming in het sociaal domein? Hoe wordt er geanticipeerd op de AVG?

B2. Voldoen deze beleidskaders aan de gangbare standaarden en wetgeving?

B3. Hoe is het beleid uitgewerkt en geborgd in processen? Hierbij moet ook aandacht zijn voor de samenwerking met eventuele (keten)partners.

B4. Hoe is de toegang tot dossiers (autorisaties) geregeld? Hierbij moet ook aandacht zijn voor de samenwerking met eventuele (keten)partners.

B5. In hoeverre worden de beleidskaders en vastgestelde processen en regels nageleefd in de praktijk in de gemeenten (en binnen de iRvN)? Hierbij moet ook aandacht zijn voor de samenwerking met eventuele (keten)partners.

B6. Wanneer en op welke manier geven burgers toestemming voor het gebruik en verwerken van gegevens?

B7. Op welke manier worden burgers geïnformeerd over het gebruik en de verwerking van hun persoonsgegevens?

B8. Hoe ziet het toezicht op de omgang met de persoonsgegevens eruit, op papier en in de praktijk? Hierbij moet ook aandacht zijn voor de samenwerking met eventuele (keten)partners.

B9. Op welke manier worden gemeentelijke medewerkers bewust gemaakt van hun verantwoordelijkheden ten aanzien van het bewaken van de privacy van persoonsgegevens? Daarbij kan worden gedacht aan onder meer trainingen en ondersteuning, maar ook via functie-omschrijvingen, aandacht in functioneringsgesprekken etc.

B10. In hoeverre heeft de gemeente een balans gevonden tussen regels en procedures rondom de bescherming van privacy enerzijds en een goede dienstverlening aan de burger anderzijds?

C. Kaderstelling en controle door de gemeenteraden

C1. Op welke wijze verloopt het proces van kaderstelling en controle door de gemeenteraden tot op heden t.a.v. de informatiebeveiliging en privacybescherming in hun gemeente, en hoe moet dit proces en het resultaat ervan worden beoordeeld?

C2. Op welke wijze faciliteren de colleges de kaderstelling en controle door de gemeenteraden, met name ten aanzien van de informatievoorziening aan de raden?

C3. Welke voorwaarden en vereisten kunnen worden geïdentificeerd om de kaderstelling en controle beter te laten verlopen? In het bijzonder moet daarbij aandacht zijn voor de inrichting van de informatievoorziening.

C4. Zijn er elders in het land relevante best practices ten aanzien van een goed verlopend proces van kaderstelling en controle door de gemeenteraad op dit gebied, en wat zijn de belangrijkste lessen die daaruit kunnen worden geleerd?

3. Plan van aanpak

Het onderzoek richt zich op drie aspecten, te weten:
A. Informatiebeveiliging;
B. Privacybescherming in het sociaal domein;
C. Kaderstelling en controle door de gemeenteraden.

In scope van het onderzoek zijn de gemeenten Berg en Dal, Beuningen, Nijmegen en Wijchen plus ICT Rijk van Nijmegen (iRvN) voor zover het de dienstverlening aan eerdergenoemde gemeenten betreft.

De voorzitters van de rekenkamers vormen de stuurgroep die de uitvoering van het onderzoek aanstuurt.

Onderdeel A & B - Plan van Aanpak informatiebeveiliging en privacybescherming in het sociaal domein

Om goed antwoord te kunnen geven op de geformuleerde hoofd- en deelvragen wordt op hoofdlijnen onderstaande werkwijze gehanteerd.



Stap 1. Voorbereiding

In deze fase zal bepaald worden welke functionarissen geïnterviewd worden en zullen passende vragenlijsten voor hen opgesteld worden afhankelijk van hun functie en/of rol met betrekking tot informatiebeveiliging of privacybescherming. Verder zal een lijst opgesteld worden met schriftelijke informatie die de onderzoekers graag ontvangen ten behoeve van het onderzoek.

Aanvullend daarop zal door middel van open bronnen onderzoek, ook wel Open Source INTelligence (OSINT) genoemd, gezocht worden naar relevante informatie over de vier gemeenten en iRvN. De bevindingen kunnen mogelijk inzicht verschaffen in risico's, kwetsbaarheden of incidenten die hebben plaatsgevonden en daarmee bijdragen aan het algehele beeld over, van, voor informatiebeveiliging en privacybescherming.

Ter afbakening van de scope van het onderzoek over privacybescherming binnen het sociaal domein, is ervoor gekozen het onderzoek in het bijzonder te richten op de verwerkingen door de gemeenten in het kader van de Jeugdwet. Daarnaast richt het onderzoek zich ook op de verstrekkingen van persoonsgegevens door de gemeenten aan samenwerkingsverbanden zoals veiligheidshuizen, RIECS en medewerkers van Openbare Orde en Veiligheid.

In deze fase wordt ook het normenkader vastgesteld.

Stap 2. Documentatie review

Op basis van de aangeleverde informatie kan een eerste analyse plaatsvinden zodat de onderzoekers een beter beeld kunnen vormen van de wijze waarop informatiebeveiliging geïntegreerd is binnen de vier gemeenten en iRvN. Daarnaast zullen de vragenlijsten voor gesprekspartners verfijnd worden op basis van de aangeleverde informatie. Hierdoor kan er beter getoetst worden of bepaalde zaken ook echt geregeld zijn en werken zoals bedoeld (opzet, bestaan en effectieve werking van beheersmaatregelen).

Stap 3. Interviews en observaties

De verschillende functionarissen zullen geïnterviewd worden om vanuit verschillende disciplines vast te kunnen stellen of en in welke mate informatiebeveiliging geïntegreerd is in de dagelijkse gang van zaken. Van elk gesprek wordt een verslag op hoofdlijnen gemaakt dat ter verificatie aan de geïnterviewde(n) wordt voorgelegd.
Daarnaast zullen – afhankelijk van de bevindingen uit de bestudeerde stukken en gevoerde interviews - observaties plaatsvinden in de vier gemeentehuizen en het pand van iRvN om de fysieke (toegangs)beveiliging en de personele veiligheid te kunnen beoordelen.

Stap 4. Analyse

Op basis van de documentatie review, interviews en observaties zal een grondige analyse plaatsvinden zodat er conclusies en aanbevelingen kunnen worden geformuleerd. Hierbij worden de bevindingen afgezet tegen de gehanteerde normen (zie onder 5) (inclusief best practices) en worden uitspraken gedaan over het volwassenheidsniveau per organisatie.

Stap 5. Rapportage en presentatie

De bevindingen, conclusies en aanbevelingen worden in rapportage- en presentatievorm verwerkt en voorzien van een samenvatting. Voordat de rapportage aan de raden wordt aangeboden en daarmee openbaar wordt, zijn er twee momenten waarop er mogelijkheid voor reactie is:

- Een toets van de gepresenteerde feiten in het concept-bevindingenrapport (zogenaamd ambtelijk hoor- en wederhoor);
- Een reactie op de conclusies en aanbevelingen door de colleges en het DB van de iRvN (zogenaamd bestuurlijk hoor- en wederhoor).

De rekenkamer(commissie)s zullen, indien nodig, tijdig (dat wil zeggen in ieder geval vóór publicatie) overleggen met de gemeente(n) als er in het onderzoek zwakke plekken worden geconstateerd die urgent moeten worden aangepakt. Zo mogelijk zal daarvoor, in overleg, extra tijd worden gegund.

Onderdeel C – Kaderstelling en controle door de gemeenteraden

Voor onderzoeksdeel C zal in kaart worden gebracht hoe het proces van kaderstelling en controle door de vier gemeenteraden tot op heden verloopt en hoe de colleges dit proces ondersteunen. Daarbij zal ook nadrukkelijk aandacht zijn voor de informatievoorziening aan de raden.

Behalve een beeld van de huidige praktijk zal in het onderzoek worden gezocht naar best practices elders in het land.

Ten behoeve van de formulering van concrete aanbevelingen voor de gemeenteraden zal voor dit onderzoeksdeel mogelijk een raadsgesprek worden georganiseerd.

4. Planning van het onderzoek

De onderstaande planning is voor het onderzoek voorzien:

Wat	Wanneer?
Voorbereiding	Week 22-23
Startoverleg stuurgroep en opdrachtnemer	Week 24
Opstellen definitief plan van aanpak	Week 25
Formele aankondiging onderzoek met definitief onderzoeksplan	Week 25
Startbijeenkomst voor alle betrokken medewerkers en portefeuillehouders en iRvN	Week 26
Opvragen documenten bij gemeenten en iRvN	Week 26
Ontvangst documenten	Week 27/28
Uitvragen namen te interviewen functionarissen bij gemeenten en iRvN	Week 26
Ontvangst namen en plannen interviews	Week 26/27/28
Documentenanalyse en interviews (inclusief tussenmeldingen)	Week 26 t/m 39
Bespreken 1e concept Bevindingenrapport plus aanzet tot conclusies en aanbevelingen (stuurgroep)	Week 39
Bevindingenrapport uitsturen voor ambtelijke wederhoor (gemeenten en iRvN)	Week 42
Opstellen 1e concept bestuurlijk rapport (conclusies en aanbevelingen)	Week 43-45
Ontvangst ambtelijke reactie (4 weken inclusief herfstvakantie)	Week 45
Bespreken (verwerking van) ambtelijke wederhoor en 1e concept Bestuurlijk rapport (stuurgroep)	Week 46
Opstellen definitieve versie Bestuurlijk rapport	Week 47
Vaststellen Bestuurlijk rapport (stuurgroep) en uitsturen voor bestuurlijke wederhoor (4 colleges en DB iRvN)	Week 48
Ontvangst bestuurlijke reactie (4 weken inclusief kerstvakantie)	Week 1 (2022)
Bijvoegen nawoord (stuurgroep) en aanbieden rapport aan gemeenteraden	Week 2
Presenteren in gemeenteraden	(vroege) voorjaar, nader te bepalen in verband met gemeenteraadsverkiezingen

5. Normenkader

Een van de eerste stappen in het onderzoek zal het vaststellen van het normenkader zijn. Hieronder wordt voor onderzoeksdeel A en B alvast een voorzet gegeven.

Informatiebeveiliging
De baseline informatiebeveiliging overheid (BIO) is het verplichte normenkader voor de overheid en daarmee ook voor gemeenten. De informatiebeveiligingsdienst (IBD) adviseert om naast de BIO ook 'best practices' voor informatiebeveiliging en cyber security te gebruiken. Deze zijn in lijn met dit advies tijdens het onderzoek bruikbaar voor de verdere beeldvorming en een kwalitatief betere duiding van de praktijk bij de gemeenten en iRvN.

Norm / richtlijn	Toelichting
Baseline Informatiebeveiliging Overheid (BIO)	De gemeenten zijn verplicht om sinds 1 januari 2020 aantoonbaar te voldoen aan de eisen van de BIO. De BIO is een afgeleide van de NEN ISO 27002:2013 norm.
ISO 27001:2013	De BIO stelt dat gemeenten voor het inrichten en onderhouden van de continu verbetercyclus[2] de richtlijnen van de ISO 27001:2013 implementeren.
Center for Internet Security (CIS) top 20	De CIS top-20 omvat essentiële beveiligingsmaatregelen die voornamelijk gericht zijn op de technische aspecten van informatieveiligheid. Omdat de techniek in de BIO in onvoldoende mate aan bod komt worden de 'Implementation Group 1 & 2' maatregelen toegepast om de weerbaarheid op ICT-vlak te toetsen.

Privacybescherming
De AVG is de belangrijkste basiswet waar het gaat om de bescherming van persoonsgegevens in het sociaal domein. Daarnaast gelden er materiewetten zoals de Jeugdwet, de WMO, de Participatiewet, de Wet gemeentelijke schuldhulpverlening, etc. De materiewetten brengen op sommige onderdelen specifieke regels die voorgaan op de AVG. Het betreft dan vooral de toepassing van de materiele beginselen uit de AVG (doelbinding, grondslag, verenigbaar gebruik, et cetera). De AVG regelt de algemene beginselen voor de materiele toepassing maar dient bovenal als raamwerk voor het op te stellen privacy risicobeheersingsraamwerk (Privacy Control Risk Framework, PCRF).

De verplichting voor de colleges van burgemeester en wethouders om een PCRF te hebben ingericht vloeit voort uit art. 5 lid 2 in samenhang met art. 24 lid 1 AVG. Verwerkingsverantwoordelijken zoals in onderhavig onderzoek, de colleges van burgemeester en wethouders, dienen bij de toepassing van het PCRF een PLAN-DO-CHECK-ACT cyclus te doorlopen. Kort gezegd betekent dit dat in het onderzoek primair opzet en bestaan van het PCRF wordt beoordeeld. Omdat de centrale onderzoeksvragen ook zijn gericht op de werking in de praktijk, zal na de beoordeling van opzet en bestaan tijdens het bureau onderzoek, ook op hoofdlijnen de werking van de beheersmaatregelen in de praktijk worden getoetst door het uitvoeren van interviews met interne sleutelpersonen.

Als algemeen normatief kader is de Privacy Baseline versie 3.3 van het Centrum Informatiebeveiliging en privacybescherming bruikbaar. Deze privacy baseline bestaat uit 13 thema´s waarin per thema

[2] Plan, Do, Check, Act

een centraal risico is geformuleerd en toetsvragen op deelelementen. Daarnaast kan bij de beoordeling uitdrukkelijk het geambieerde privacy volwassenheidsniveau van de verwerkingsverantwoordelijke worden meegenomen.

Als specifiek normenkader zijn verder bruikbaar in het onderzoek:

- Het handvat gegevensuitwisseling in het zorg- en veiligheidsdomein;
- Handreiking Privacy en Integrale Toeleiding en Dienstverlening in het Sociaal Domein;
- VNG matrix gegevensuitwisseling;
- VNG Privacy afspraken bij ketensamenwerking;
- CIP Overheid Privacy Governance.

