

GEMEENTERAAD

REKENKAMER

GEGEVENS- BESCHERMING IN REGIONALE CONTEXT

**REKENKAMERONDERZOEK NAAR
GEGEVENSDELING IN
SAMENWERKINGSVERBANDEN**



ENSCHEDE

INTRODUCTIE

Dit onderzoek gaat over het delen van persoonsgegevens in samenwerkingsverbanden. Dit zijn allebei ingewikkelde onderwerpen. Als die onderwerpen gecombineerd worden, neemt de complexiteit verder toe. Dit rapport begint daarom met een korte introductie van beide onderwerpen.

PERSOONSGEGEVENS

Bescherming van persoonsgegevens is in Nederland een grondrecht: burgers moeten ervan op aan kunnen dat persoonsgegevens¹ alleen wordt gebruikt waarvoor dit mag en dat de omgang van deze gegevens veilig plaatsvindt. Elke gemeente is verplicht zich te verantwoorden voor de verwerking en het beheer van persoonsgegevens.

Onzorgvuldig beheer kan verstrekkende gevolgen hebben. Bij onvoldoende beveiliging kunnen kwaadwillenden toegang krijgen tot gevoelige informatie zoals medische dossiers, financiële gegevens of privécommunicatie. Er kunnen cyberaanvallen of datalekken optreden ('persoonsgegevens liggen op straat'). Er kan misbruik van gegevens worden gemaakt in de vorm profilering en discriminatie bijvoorbeeld bij het toekennen van leningen, verzekeringen of banen of het overnemen van iemands (digitale) identiteit. Onbeveiligde gegevens kunnen worden ingezet voor commerciële exploitatie zonder toestemming van een persoon. Vaak hebben burgers geen toegang tot eigen gegevens, zij weten niet welke gegevens worden verzameld en wat er mee gebeurt, en vinden de regels en voorwaarden moeilijk te begrijpen. Besluiten op basis van onjuiste of verouderde informatie zijn vaak moeilijk aan te vechten.

Deze voorbeelden geven duidelijk aan dat een gemeente de bescherming van persoonsgegevens op orde moet hebben, omdat het anders grote gevolgen voor zijn burgers kan hebben. Dat geldt ook voor persoonsgegevens die in opdracht van gemeenten worden verzameld, verwerkt en gedeeld in regionale samenwerkingsverbanden. Het gaat dan bijvoorbeeld om Naam, Adres en Woonplaatsgegevens (NAW-gegevens), paspoortnummers, e-mailadressen en telefoonnummers, geslacht, huwelijks staat, familiesamenstelling en beroep. Of gemeenteraden voldoende zicht hebben op dit onderwerp is een open vraag.

SAMENWERKINGSVERBANDEN

Uit onderzoek blijkt dat veel raadsleden in Nederland onvoldoende grip ervaren op regionale samenwerkingen. De structuur van regionale samenwerkingsverbanden zijn ingewikkeld en heel verschillend. Rollen en verantwoordelijkheden van partijen die deelnemen in een samenwerkingsverband zijn vaak onduidelijk. Een goed overzicht van het functioneren van samenwerkingsverbanden ontbreekt met regelmaat. Ook de gemeente Enschede neemt deel aan veel verschillende regionale samenwerkingsverbanden. De Wet Gemeenschappelijke Regelingen (Wgr) staat deze publiekrechtelijke samenwerkingsvormen in verschillende vormen toe: openbaar lichaam, gemeenschappelijk orgaan, centrumgemeente, regeling zonder meer en bedrijfsvoeringsorganisatie. De Veiligheidsregio Twente is een voorbeeld van publiekrechtelijke samenwerkingsvorm (openbaar lichaam). Daarnaast zijn er verschillende privaatrechtelijke samenwerkingsvormen zoals deelnemingen, stichtingen, verenigingen, coöperaties waar de gemeente in meedoet. In het kader van regionale samenwerking wordt ook vaak gesproken van Verbonden Partijen: samenwerking met een privaatrechtelijke of publiekrechtelijke organisatie waarin de gemeente Enschede een bestuurlijk en een financieel belang heeft. En dit is nog maar een deel van het verhaal. Er bestaan daarnaast ook allerlei andere samenwerkingsverbanden waar de gemeente aan deelneemt. Denk bijvoorbeeld aan een samenwerkingsverband als het RIEC Oost-Nederland dat zich bezighoudt met samenwerking op het gebied van criminaliteitsbestrijding in de regio, penvoerderschap rondom Beschermd wonen en de Sociale recherche.

AANLEIDING VOOR DIT ONDERZOEK

In Nederland wordt op dit moment veel gewezen op het belang van informatieveiligheid in samenwerkingsverbanden. De Autoriteit Persoonsgegevens ziet gegevensuitwisseling in samenwerkingsverbanden als een van de belangrijkste thema's in 2024. In het Dreigingsbeeld Informatiebeveiliging worden gemeenten genoemd als kwetsbare organisaties als het gaat om veilige informatie. En de Vereniging van Nederlandse Gemeenten (VNG) heeft verschillende handreikingen gepubliceerd over de Algemene Verordening Gegevensbescherming (AVG), privacy en gegevensuitwisseling. De Rekenkamer Enschede ziet dat de ontwikkelingen op dit gebied snel gaan en vaak voorbehouden lijken aan deskundigen. Voor leken is het een moeilijk te doorgronden materie.

Samengevat, *i)* de gemeente Enschede neemt deel in veel regionale samenwerkingsverbanden, die sterk van elkaar verschillen; *ii)* in het algemeen hebben volksvertegenwoordigers weinig grip en zicht op het functioneren van regionale samenwerkingsverbanden; *iii)* in deze regionale samenwerkingsverbanden wordt met persoonsgegevens gewerkt en het is belangrijk dat deze persoonsgegevens goed worden beschermd (een grondrecht); en *iv)* de regelgeving over persoonsgegevens is ingewikkeld en voortdurend in beweging.

Dit alles heeft de Rekenkamer doen besluiten in 2024 een onderzoek te starten naar de gegevensbescherming in regionale context. Wat is de stand van zaken bij de uitwisseling van persoonsgegevens waar de gemeente Enschede bij betrokken is, welke risico's kunnen zich voordoen en hoe gaat de gemeente Enschede met deze risico's om?

WAT HEEFT DE REKENKAMER ONDERZOEKT?

De Rekenkamer wil met dit onderzoek laten zien hoe het in samenwerkingsverbanden gaat met uitwisseling van gegevens, welke risico's er kunnen ontstaan rondom de uitwisseling van gegevens en hoe de gemeente omgaat met die risico's.

De volgende onderzoeksvragen zijn opgesteld:

1. Gaat de gemeente Enschede adequaat om met de risico's van gegevensuitwisseling in samenwerkingsverbanden?
2. Is de raad voldoende in positie gebracht op zijn kaderstellende en controlerende rol uit te voeren?

De daarbij horende deelvragen zijn:

- a. Welke kaders bestaan er voor rechtmatige gegevensuitwisseling in samenwerkingsverbanden?
- b. Wat is het gemeentelijk beleid en het beleid van samenwerkingsverbanden ten aanzien van gegevensuitwisseling?
- c. Hoe vindt de gegevensuitwisseling plaats in samenwerkingsverbanden waarin de gemeente Enschede participeert?
- d. Is de raad voldoende in positie om haar wettelijke taken uit te voeren (kaderstelling en controle)?

UITVOERING EN VERANTWOORDING VAN HET ONDERZOEK

De Rekenkamer heeft Berenschot opdracht gegeven voor dit onderzoek. Het onderzoek is begeleid door leden van de Rekenkamer. De Klankbordgroep, bestaande uit vier leden van de raad, heeft bij de start meegedacht over de onderzoeksopzet zoals geformuleerd door de Rekenkamer en heeft inbreng geleverd op een concept versie van dit eindrapport. De verantwoordelijkheid voor deze rapportage ligt volledig bij de Rekenkamer.

Het onderzoek is uitgevoerd in de eerste helft van 2024. Meestal onderzoekt de Rekenkamer achteraf (ex-post) de resultaten van gemeentelijk beleid. Dit onderzoek heeft een meer verkennend karakter en keek naar de huidige situatie (beleid in uitvoering).

De onderzoekers hebben documenten bestudeerd en interviews gehouden. In het onderzoek zijn twee cases bekeken: Stadsbank Oost Nederland en Zorg- en Veiligheidshuis Twente. Daarbij is niet het functioneren van deze samenwerkingsverbanden beoordeeld; er is gekeken naar de manier waarop gegevens worden beschermd en beheerd.

Voor een uitgebreide verantwoording van het uitgevoerde onderzoek verwijst de Rekenkamer naar de bijlagen van het Berenschot rapport.

WELKE REGELS ZIJN ER EN WAAR IS DE GEMEENTE VOOR VERANTWOORDELIJK?

Er zijn twee soorten wetten van belang bij dit onderwerp:

- Algemene (Europese en nationale) wettelijke kaders waarin verschillende (algemene) beginselen rondom de uitwisseling van gegevens zijn vastgelegd. De belangrijkste algemene kaders zijn de Algemene verordening gegevensbescherming (hierna: de AVG), de Uitvoeringswet AVG (hierna: de UAVG), de Wet politiegegevens en de Algemene wet bestuursrecht (hierna: Awb). Bij alles wat de gemeente doet, moet voldaan worden aan deze wetten.
- Zogenaemde materiële wetten, zoals Wet gemeenschappelijke schuldhelpverlening, de Wet maatschappelijke ondersteuning, de Jeugdwet en de Participatiewet. Deze wetten beschrijven doelen, taken, bevoegdheden en verantwoordelijkheden van de gemeente en andere bestuursorganen.

Samenwerkingsverbanden en de onderwerpen waarvoor zij zijn opgericht zijn heel verschillend. Per samenwerkingsverband kunnen andere wetten en dus andere regels gelden, afhankelijk van de gekozen vorm van samenwerking en het beleidsonderwerp. In het ene samenwerkingsverband kan de verantwoordelijkheid van de gemeente anders zijn dan in het andere. De Rekenkamer komt hier later in dit rapport op terug.

CASESTUDIES: STADSBANK OOST NEDERLAND EN ZORG- EN VEILIGHEIDSHUIS TWENTE

In dit onderzoek zijn twee cases bekeken om te zien hoe de verschillende wetten op lokaal/regionaal niveau worden vertaald in beleid voor gegevensbescherming. Berenschot heeft in overleg met de Rekenkamer twee duidelijk verschillende cases te onderzocht. Er is gekozen voor de Stadsbank Oost Nederland (SON) en Zorg- en Veiligheidshuis Twente (ZVH). De Stadsbank helpt mensen met financiële problemen en het Zorg- en Veiligheidshuis brengt bij complexe (gezins)situaties informatie van partners uit het strafrecht, de zorg en gemeenten samen.

Bij de casestudies is gekeken naar:

- het vastgestelde beleid om gegevensuitwisseling rechtmatig te laten plaatsvinden (legitimiteit).
- de inrichting van de organisatie om op legitimiteit rondom gegevensuitwisseling te sturen.
- de ambities van de organisaties met betrekking tot gegevensbescherming.

De Rekenkamer verwijst naar hoofdstuk 3 en 4 van het rapport van Berenschot, waar elk van de bovengenoemde aspecten is beschreven. De Rekenkamer noemt hier een paar uitkomsten.

LEGITIMITEIT: BELEID VOOR RECHTMATIGE GEGEVENSUITWISSELING

De gemeente Enschede blijft eindverantwoordelijk voor zorgvuldige gegevensverwerking binnen het ZVH. Het ZVH is een netwerkorganisatie zonder rechtspersoonlijkheid. Daardoor kan het ZVH zelf geen verantwoordelijkheid voor de verwerking van gegevens hebben. Dat betekent dat elke partij die deelneemt in dit samenwerkingsverband er zelf voor moet zorgen dat de geldende wetten en regelgeving worden toegepast. Omdat de uitvoering van de taken op diverse plekken ligt (versnippering) is er geen organisatie die de volledige verantwoordelijkheid voelt of neemt. De gemeente zou dit, gezien haar verantwoordelijkheid voor gegevensbescherming, wel moeten organiseren.

De gemeente Enschede is samen met de SON verantwoordelijk voor de verwerking van gegevens. De gemeente heeft haar taken omtrent wettelijke schuldhelpverlening overgedragen aan de SON. De SON verwerkt dus gegevens waar de gemeente verantwoordelijk voor is en blijft.

Dit betekent dat de gemeente geen (volledige) grip kan uitoefenen op de kwaliteit van gegevensuitwisseling terwijl zij daar wel juridisch verantwoordelijk voor is: de gemeente staat relatief ver af van de uitvoering van de taken en kan daar niet continu zicht op houden.

AMBITIES: AMBITIES VAN DE ORGANISATIE VOOR GEGEVENSUITWISSELING

De gemeente Enschede heeft weinig mogelijkheden om de eigen ambities voor veilige gegevensuitwisseling te realiseren binnen het ZVH. De gemeente Enschede neemt geen zitting in de Stuurgroep Zorg, Veiligheid en Straf, waarin informatiebeveiligingsbeleid bestuurlijk wordt besproken. Het is dus niet zomaar mogelijk voor de gemeente om in de gaten te houden of de wet- en regelgeving wordt nageleefd. De enige mogelijkheid om dit te doen is in het Dagelijks Bestuur of Algemeen Bestuur van de Veiligheidsregio. De Veiligheidsregio wordt namelijk in 2024 verantwoordelijk voor het systeem. Op het moment dat het onderzoek werd uitgevoerd, was het onbekend of dienstverleningsovereenkomsten aan derden hoog op de agenda van de Veiligheidsregio komen te staan.

De gemeente Enschede heeft mogelijkheden om (de uitvoering van) het informatieveiligheidsbeleid van de SON te monitoren en te verbeteren. De gemeente Enschede kan de SON vragen om verantwoording te afleggen over de kwaliteit of de risico's van gegevensuitwisseling. De gemeente Enschede is vast lid van het Dagelijks Bestuur van de SON, dat bestuurlijk verantwoordelijk is voor de (kwaliteit van de) informatieveiligheid en dit onderwerp minstens jaarlijks agendeert. Dat geeft de gemeente de mogelijkheid om kritisch – en waar nodig vanuit de eigen gemeentelijke ambities – de uitvoering van het beleid op het gebied van informatieveiligheid te beoordelen. Omdat het Dagelijks Bestuur van de SON ook het informatieveiligheidsbeleid vaststelt, kán de gemeente Enschede zelfstandig wijzigingen voorstellen.

HOE STAAT DE GEMEENTE ENSCHEDE ER IN DE PRAKTIJK VOOR?

Uit het onderzoek komt een aantal algemene bevindingen naar voren:

- De gemeente heeft in de periode 2022-2023 een flinke beleidsmatige inhaalslag in de bescherming van persoonsgegevens gemaakt, vooral op strategisch niveau, maar er is nog geen duidelijke tactische/operationele vertaling naar de verschillende domeinen. Er is een gat tussen het strategisch beleid aan de ene kant en de operationele invulling aan de andere kant.
- De naleving van het beleid wordt beperkt gecontroleerd door het management, waardoor er onvoldoende zicht is op mogelijke risico's.
- Hoewel steeds meer mensen in de gemeente zich bewust zijn van het belang van gegevensbescherming, kennen niet alle medewerkers het beleidskader en weten zij niet allemaal wat rechtmatige gegevensverwerking precies inhoudt. De gemeentelijke organisatie weet dit en zet actief in op bewustwording bij en ondersteuning van medewerkers.
- De mogelijkheden van de gemeente Enschede om te sturen op veilige gegevensuitwisseling nemen toe naarmate de governance van een samenwerkingsverband formeel beter op orde is. De gemeente Enschede maakt echter nauwelijks tot geen gebruik van deze sturingsmogelijkheden. De onderzoekers schatten in dat gegevensuitwisseling en de risico's hiervan geen bestuurlijk gespreksonderwerp zijn. Niet bij alle raadsleden leeft het onderwerp gegevensuitwisseling. Om de controlerende rol van de raad te versterken is met name een versterking van de kennispositie gewenst.
- De gemeentelijke ambities over informatieveiligheid worden in een aantal gevallen op de regionale schaal tot uitvoering gebracht. Het is van belang (en vaak wettelijk verplicht) dat de gemeente Enschede in

samenwerkingsverbanden actief stuurt op het realiseren van haar eigen ambities. Dit gebeurt echter beperkt.

- In de praktijk blijkt vooral menselijk handelen de zwakke schakel te zijn voor de realisatie van de gemeentelijke ambities.
- De gemeente wisselt gegevens uit voor veel van haar taken (opgaven). Als de uitwisseling van die gegevens niet rechtmatig en veilig plaatsvindt, kan dat invloed hebben op de uitvoering van die taken.

MOGELIJKE RISICO'S VOOR DE GEMEENTE

De onderzoekers van Berenschot geven een overzicht van de mogelijke risico's die een gemeente kan lopen en de impact die deze kunnen hebben. De Rekenkamer verwijst naar de tabellen op pagina 28, 32 en 34 in het onderzoeksrapport van Berenschot. Het gaat hier om mogelijke risico's, die op dit moment nog niet optreden. Maar als de gemeente niet handelt, wordt de kans reëel dat één of meer van deze risico's optreedt. Het gaat bijvoorbeeld om een beperkt inzicht in gegevensstromen in samenwerkingsverbanden, beperkte toegang tot gegevens, onjuiste omgang met gegevens of het ontbreken van duidelijke mechanismen voor veilige en rechtmatige gegevensuitwisseling.

POSITIE VAN DE RAAD

Het Algemeen Bestuur van een Gemeenschappelijke Regeling heeft een informatieplicht voor de betrokken Gemeenteraden. Het Algemeen Bestuur bestaat vaak uit een aantal wethouders van gemeenten die bij een Gemeenschappelijke Regeling zijn aangesloten. Zij moeten alle aangesloten Gemeenteraden informeren. Niet voor alle regionale samenwerkingsverbanden zijn er duidelijke verplichtingen. Voor de meer informele samenwerkingsverbanden en bijvoorbeeld netwerksamenwerkingen zijn er geen duidelijke regels. Daar moet de raad zelf in actie komen als zij informatie willen en hun controlerende taak willen invullen.

Gegevensuitwisseling of gegevensbescherming lijken niet hoog op de raadsagenda te staan. De raad vervult zijn rol met name reactief op het moment dat er een concrete casus politiek wordt gemaakt. De reden voor deze weinig actieve rol van de raad zou gelegen kunnen zijn in de ingewikkeldheid van het onderwerp (er is veel specifieke kennis voor nodig) en mogelijk een onvoldoende besef van het belang van dit onderwerp. Ook het grote aantal, sterk van elkaar verschillende samenwerkingsverbanden zorgt er voor dat het lastig is om grip op de materie te krijgen en dat een fikse inspanning moet worden geleverd.

De Raad heeft een aantal instrumenten tot zijn beschikking om grip op een regionale samenwerking te krijgen en op de gegevensuitwisseling die in deze samenwerkingen plaatsvindt. Raadsleden kunnen het college om informatie vragen, het college of een lid van het Algemeen Bestuur om verantwoording vragen of sturen door bijvoorbeeld een motie of een zienswijze in te dienen.

De Rekenkamer wijst er op dat hoofdstukken 3 en 4 van het Berenschotrapport diverse interessante passages bevatten over de positie van de raad inzake gegevensuitwisseling en -bescherming bij regionale samenwerkingsverbanden. In deze hoofdstukken staan suggesties waarmee raadsleden invulling aan hun rol geven.

CONCLUSIES

1. Er kunnen voor de gemeente serieuze risico's verbonden zijn aan het niet op orde hebben van gegevensuitwisseling en -bescherming.

Het is erg belangrijk om gegevensbeheer en -bescherming te professionaliseren, gezien de mogelijke risico's die kunnen optreden als de gemeente fouten maakt. Veilige uitwisseling van persoonsgegevens in samenwerkingsverbanden is uiterst ingewikkeld, ook al omdat er door de verschillende wet- en regelgeving allerlei verschillende regels gelden. Iedereen moet zich hiervoor inspannen: de ambtelijke organisatie, maar ook het college en de raad. De verantwoordelijkheid voor rechtmatige gegevensuitwisseling en -bescherming kan niet alleen worden toevertrouwd aan privacy officers. Dan loopt de gemeente Enschede risico's en kunnen ambities voor rechtmatige gegevensuitwisseling niet gehaald worden.

2. De gemeente Enschede zet zich in voor de bescherming van gegevens (professionaliseringsslag), maar vooral nog op strategisch niveau.

De gemeente is zich bewust van het belang van bescherming van persoonsgegevens en heeft een professionaliseringsslag gemaakt op het gebied van gegevensuitwisseling, -beheer en -bescherming. Het college heeft in 2022 een sterk geprofessionaliseerd beleidskader omtrent informatiebeveiliging en privacy ontwikkeld en de raad hierover geïnformeerd. Dit beleidskader is vooral intern gericht. Medewerkers zijn zich steeds meer bewust van het belang van gegevensbescherming. Dit is vooral op strategisch niveau. De tactische vertaling en operationele invulling blijven achter: beleidsmedewerkers weten niet altijd goed wat rechtmatige gegevensuitwisseling precies betekent en wat er van hen verwacht wordt om verbeteringen aan te brengen. De gemeente is hier mee bezig, maar het is van belang hier alert op te blijven en op in te zetten.

3. Ook als de uitvoering van bepaalde taken in regionale samenwerkingsverbanden zijn belegd, blijft de gemeente juridisch verantwoordelijk voor de gegevensuitwisseling en -bescherming.

Verantwoordelijkheid voor rechtmatige gegevensuitwisseling ligt niet per definitie bij samenwerkingsverbanden. De verantwoordelijkheid voor de uitvoering ligt daar wel, maar de juridische verwerkingsverantwoordelijkheid ligt vaak bij de gemeente. Dit plaatst de gemeente in een spagaat: de gemeente is juridisch aansprakelijk voor de juiste invulling van taken, terwijl zij maar beperkte controle kan uitoefenen op de uitvoering van die taken en daar ook niet altijd zicht op heeft, omdat die door een ander worden uitgevoerd.

Uit dit onderzoek ontstaat het beeld dat de gemeente Enschede beperkt zicht heeft op de manier waarop de uitwisseling van gegevens in samenwerkingsverbanden is georganiseerd en dat de verantwoordelijkheid van de gemeente voor de verwerking van gegevens beter ingevuld kan worden.

4. De rol van de raad kan worden geïntensiveerd.

Regionale samenwerkingsverbanden, en zeker de gegevensuitwisseling en -bescherming lijken vooralsnog niet hoog op de raadsagenda te staan. Dit is niet alleen in de gemeente Enschede het geval. Uit onderzoek van Berenschot naar Bestuurlijke Regionale Ecosystemen blijkt dat Nederlandse raadsleden zich beperkt betrokken voelen bij regionale samenwerkingsverbanden.

Het college is verantwoordelijk voor het beleid om te voldoen aan de verplichtingen uit de AVG. Het college heeft dit beleid inderdaad vastgesteld en de raad daar per brief van 27 september 2022 over geïnformeerd. De raadscommissie Bestuur en Middelen heeft op 15 januari 2024 beeldvormend de Nota “Waardengedreven digitalisering, ethische visie op het gebruik van data en technologie”, besproken. In de nota worden college en gemeenteraad beide gevraagd om deze visie voortaan te gebruiken bij het nemen van besluiten over de inzet van data en technologie. De ‘digitale overheid’ krijgt dus steeds meer aandacht maar een explicietere rol van de raad op het gebied van gegevensveiligheid in regionale context is mogelijk. Het rapport van Berenschot geeft een aantal handvatten en onderstaand doet de Rekenkamer hierover een aantal aanbevelingen.

5. Er zijn veel regionale samenwerkingsverbanden en die verschillen in diverse opzichten sterk van elkaar. Dat maakt een goede controle op gegevensuitwisseling, toedeling van verantwoordelijkheden moeilijke opgave.

De gemeente Enschede werkt in veel verbanden samen. Dat zijn formele samenwerkingsverbanden, zoals Gemeenschappelijke Regelingen, NV's, BV's enzovoort, maar daarnaast zijn er allerlei informele samenwerkingsverbanden, zoals netwerksamenwerkingen en ondernemingen. In de Gemeentebegroting en Gemeenterekening wordt elk jaar een paragraaf opgenomen over Verbonden partijen. Dat is verplicht (BBV: Besluit Begroting en Verantwoording).

Voor 13 verbonden partijen, waaronder de gemeenschappelijke regelingen, is informatie opgenomen over het financieel belang van de gemeente en het vermogen. Verder sturen de Twentse Gemeenschappelijke Regelingen elk voorjaar hun jaarrekening en begroting voor het volgende jaar naar de gemeenteraden. Gemeenteraden kunnen een zienswijze indienen op deze stukken en het college bevragen op wat zij in deze stukken lezen. Zij worden hierbij geholpen door de quick scan die in opdracht van de Samenwerkende Rekenkamers wordt gemaakt. Via deze stukken kan de Gemeenteraad op de hoogte blijven van het reilen en zeilen bij deze verbonden partijen.

De Rekenkamer constateert dat er in de afgelopen twee paragrafen verbonden partijen (Gemeentebegroting 2024-2027 en Gemeenterekening 2023) en in de quick scan op de jaarstukken niet is ingegaan op het thema gegevensuitwisseling of privacy.

Naast de Verbonden partijen zijn er nog allerlei informele samenwerkingsverbanden, zoals Ondernemingen en Netwerksamenwerkingen. Dergelijke partijen hebben niet altijd rechtspersoonlijkheid en worden niet opgenomen in de Paragraaf verbonden partijen. Ook zijn ze niet verplicht om jaarstukken naar college en raad te sturen. Het is voor de Gemeenteraad dus nog moeilijker dan voor de Verbonden partijen om inzicht in deze samenwerkingsverbanden en hun omgang met gegevens te krijgen.

AANBEVELINGEN

Aan de raad

1. Stuur op rechtmatige gegevensuitwisseling door te vragen naar het ‘wie’, ‘waarom’ en ‘hoe’ van gegevensuitwisseling.

Bescherming van gegevens die in samenwerkingsverbanden worden gedeeld is een ingewikkeld onderwerp. Het lijkt dan ook alsof raadsleden expert zouden moeten zijn om te sturen op rechtmatigheid van gegevensuitwisseling. Toch ziet de Rekenkamer mogelijkheden om als raadslid de wettelijke verantwoordelijkheid in te vullen en te vragen naar het ‘wie’, ‘waarom’ en ‘hoe’ van gegevensuitwisseling. De raad kan gaan sturen op rechtmatige gegevensuitwisseling als onderdeel van een breder thema ‘goed digitaal bestuur’. Het college heeft hierin een verantwoordelijkheid: zij moet informatie delen met de raad, laten zien hoe de mechanismen in met samenwerkende

gemeenten en andere betrokkenen in zijn werk gaan, zodat raadsleden hun rol kunnen invullen. De AVG verplicht het gemeentebestuur dan ook om zijn beleid te delen met de raad. Ook zou de Functionaris Gegevensbescherming van de gemeente (regelmatig) een informerende presentatie kunnen geven aan de raad over de stand van zaken. In het rapport van Berenschot staat een aantal bruikbare suggesties. Hiermee kan de raad het college actief vragen hoe zij omgaat met de grootste risico's van onrechtmatige gegevensuitwisseling in samenwerkingsverbanden:

- Wie is er verantwoordelijk voor gegevensuitwisseling (verantwoordelijkheidsbesef)?
- Hoe wordt rechtmatige omgang geborgd (invulling van gegevensuitwisseling)?
- Zijn inwoners geïnformeerd en op welke manier (transparantie)?

Als de raad twijfelt over de beantwoording van deze drie vragen, dan kan de raad gebruik maken van de controlerende processen/procedures. Het lastige is dat het per samenwerkingsverband verschilt hoe die processen er uit zien. Bij een Gemeenschappelijke Regeling gaat dit bijvoorbeeld via een zienswijzeprocedure, maar bij andere samenwerkingen moet een wethouder die lid is van het Dagelijks Bestuur van de samenwerkingspartij op pad worden gestuurd. Per samenwerkingsverband verschilt het hoe de governancestructuur er uit ziet en welke mogelijkheden er zijn voor het verbeteren van beleid ten aanzien van gegevensuitwisseling, en de controle daarop. De Rekenkamer wijst in dit kader ook op de vijfde conclusie in dit rapport: niet alleen de governancestructuur verschilt per samenwerkingsverband, ook de mate waarin de raad informatie krijgt verschilt.

2. Vraag voor álle soorten samenwerkingsverbanden om een moment waarop zij beoordeeld kunnen worden op rechtmatigheid van gegevensverwerking

Gemeenschappelijke regelingen volgen een jaarcyclus en leggen via de jaarstukken in april verantwoording af over hun beleid, ook over gegevensuitwisseling. De zogenaamde netwerksamenwerkingen zonder rechtspersoonlijkheid (zoals het Zorg- en Veiligheidshuis Twente) hebben hiervoor geen vaste werkwijze. Raadsleden kunnen proactief vragen om regionaal beleid over gegevensuitwisseling. Dat kunnen ze gebruiken om de rechtmatigheid te beoordelen. Dat is nodig, want de verantwoordelijkheid voor rechtmatige gegevensverwerking ligt in vele gevallen (deels) bij de gemeente Enschede. Niet alleen voor deze onderzochte casussen, maar bij vele samenwerkingsverbanden.

3. Houd samenwerkingsverbanden van de Gemeente Enschede bij oprichting maar ook periodiek tegen het licht

De aanbevelingen hiervoor gaan over de regionale schaal. De Rekenkamer vindt het verstandig dat de raad ook op lokale schaal, dus voor Enschede zelf, zich beraadt op kaders. In het rapport van Berenschot is op pagina 13 een praktische checklist opgenomen, die per samenwerkingsverband doorlopen kan worden. Dit kan op het moment dat de gemeente toetreedt tot een nieuw samenwerkingsverband of als een governancestructuur van een samenwerkingsverband wijzigt. Uiteraard het is ook mogelijk om de samenwerking en de afspraken periodiek tegen het licht te houden, zonder dat daar een specifieke aanleiding voor is. Op basis van zo'n doorlichting kan de raad het college vragen om nieuwe kaders te stellen. Ook kan de raad vragen om in voortgangsbrieven een paragraaf op te nemen over de punten in deze checklist. Hiermee kan de raad een duidelijker antwoord krijgen op de vraag wie er verantwoordelijk is voor rechtmatige gegevensverwerking en wat de stand van zaken is.

Aan het college

4. Pak als college een meer actieve rol en deel informatie met de raad

Het college kan bijdragen aan de controlerende rol van de raad door informatie met de raad te delen over bijvoorbeeld bepaalde werkwijzen van de gemeente rondom gegevensdeling. Het college kan een aantal onderwerpen binnen dit thema bundelen en daarmee de raad meenemen in de inzet van digitalisering voor het vervullen van publieke taken. De raad kan daardoor zijn kennisniveau verhogen en de werking van beleid, governance en processen beter leren kennen. Dit kan helpen om de raad in zijn controlerende rol te brengen. De gemeentelijke Functionaris Gegevensbescherming kan bijvoorbeeld een informerende presentatie geven aan de raad. Ook zou het college de paragraaf Verbonden partijen in de Gemeentebegroting en Gemeenterekening kunnen gebruiken om de raad te informeren over ICT-beheer en gegevensdeling bij de betreffende Verbonden Partij. In de quick scan Verbonden partijen 2024 is opgemerkt: "In de risicoparagraaf (p. 19 begroting) staat wel dat het risico van cyberaanvallen in het benodigd weerstandsvermogen is meegenomen. In meer algemene zin zou het te overwegen zijn om brede maatschappelijke risico's zoals informatieveiligheid of een plotselinge maatschappelijke crisis buiten het weerstandsvermogen te houden. Dat wil niet zeggen dat er geen aandacht voor moet zijn, maar wanneer dit soort zaken zich voordoen is geld niet meer de eerste prioriteit zoals we de afgelopen jaren hebben moeten ervaren. Voor maatschappelijke veranderingen die de opgaven van de organisatie raken zoals veranderingen in de bevolking of belastinggrondslagen zou in risicoparagrafen aandacht kunnen zijn voor de wijze waarop de organisatie daarop kan anticiperen en bijsturen."

Het college zou hier ook een rol kunnen pakken richting de Verbonden partijen en daarbij ook de raad kunnen informeren.

5. Bundel voor de raad meerdere onderwerpen in een breed thema 'goed digitaal bestuur'

Niet alleen op het gebied van gegevensuitwisseling moet de raad in positie gebracht worden. Dat geldt ook voor het bredere thema 'goed digitaal bestuur'. Het college zou verschillende onderwerpen kunnen bundelen in zo'n thema 'goed digitaal bestuur' en de raad daarover per brief kunnen informeren. Op deze manier kan het college de raad meenemen in het gemeentelijk digitaliseringsbeleid. Met zo'n gebundelde aanpak is het voor de raad makkelijker om het kennisniveau te verhogen en de werking van bestaand beleid, de governance en de processen beter te leren kennen. De raad is dan beter in positie om te controleren of het gemeentelijk systeem werkt zoals beoogd.

6. Overweeg een aantal praktische werkwijzen door te voeren in de organisatie.

Berenschot doet in hun eindrapportage een aantal voorstellen voor de gemeentelijke organisatie. Overweeg deze door te voeren in de organisatie:

- Maak vooraf duidelijke afspraken over rollen en verantwoordelijkheden van en in samenwerkingsverbanden.
- Maak in samenwerkingsverbanden expliciete afspraken over rollen en verantwoordelijkheid m.b.t. uitvoering van beleid. Maak duidelijk wie coördineert en leg werkwijzen formeel vast.
- Zorg dat het onderwerp leeft bij directie en bestuur en dat zij actief sturen op naleving van het beleid. Zet als Functionaris Gegevensbescherming, Functionaris Informatievoorziening (CIO) en Functionaris Informatiebeveiligingsbeleid (CISO) in op goed contact en denk mee.
- Regel eerstelijns controle op het niveau van de uitvoering. Zo voorkom je een papieren werkelijkheid die ver van de werkvloer af staat. Denk er bijvoorbeeld aan om afdelingen zelf datalekken te laten melden, of door managers zelf te laten rapporteren. Op deze manier wordt geborgd dat er controle is op uitvoering en kun je op naleving sturen.
- Bundel de krachten van interne toezichtfuncties en laat hen samen één jaarverslag indienen. Op deze manier benadruk je de verbondenheid van alle onderwerpen binnen het thema 'goed digitaal bestuur' en kom je in gezamenlijkheid hoger op de bestuurlijke agenda. Zie ook aanbeveling 5, waarin wordt

voorgesteld om ook voor de raad meerdere onderwerpen te bundelen in een breed thema 'goed digitaal bestuur'.

Daarnaast leest de Rekenkamer in de paragraaf Verbonden Partijen (Gemeentebegroting 2024-2027) dat er jaarlijks een risicoscan van de verbonden partijen wordt uitgevoerd. De risico's voor de verbonden partijen worden geïnventariseerd met behulp van een vragenlijst. De Rekenkamer constateert dat thema's als privacy, gegevensbescherming of AVG hier niet in zijn opgenomen. Overweeg om in de risicoscan een (of meer) vragen op te nemen over gegevensdeling tussen en binnen samenwerkingsverbanden en mogelijke risico's daarvan.

7. Loop voor elk samenwerkingsverband een checklist 'gemeentelijke verwerkingsverantwoordelijkheid' door en ga na welke risico's zich voordoen

Berenschot doet op pagina 13 van hun eindrapport een voorzet voor een checklist, waarmee kan worden gespecificeerd in welke mate de gemeente verantwoordelijkheid voor rechtmatige gegevensuitwisseling behoudt, deelt of overdraagt en welke sturingsmogelijkheden de gemeente houdt om toe te zien op veilige deling van persoonsgegevens in het samenwerkingsverband.

Berenschot geeft op pagina 28 en verder een overzicht van mogelijke risico's die zich kunnen voordoen als de gemeente niet zou handelen. Het is verstandig om voor de samenwerkingsverbanden expliciet na te lopen of dergelijke risico's zich voordoen en welke acties ondernomen kunnen worden.

8. Blijf aandacht schenken aan regionale samenwerking

In het eerder genoemde onderzoek van Berenschot naar Bestuurlijke Regionale Ecosystemen staat een in de ogen van de Rekenkamer zinnige algemene aanbeveling over regionale samenwerking: blijf het onder de aandacht brengen bij volksvertegenwoordigers, organiseer onderlinge ontmoetingen, richt het gesprek op de voorliggende opgaven en oplossingsrichtingen, deel resultaten, zoek steeds de koppeling tussen het regionale en het lokale en wees vooral eerlijk over de beïnvloedingsruimte die zij hebben. In hetzelfde rapport is het advies aan volksvertegenwoordigers: het regionale schaalniveau is een blijvende realiteit, dus verdiep je erin, stel vragen en daag jezelf uit om zowel vanuit het lokale als het regionale perspectief te denken, want het geheel is meer dan de som der delen.

Teksten Rekenkamer Enschede

Datum 20 september 2024

Aan dit document kunnen geen rechten worden ontleend.