Berenschot



REKENKAMERONDERZOEK

# Gegevens-bescherming in regionale context

## Rekenkamer Enschede

## Uitgevoerd door Berenschot

*19 juli 2024*



REKENKAMERONDERZOEK

# Gegevensbescherming in regionale context

## Rekenkamer Enschede

## Uitgevoerd door Berenschot

Auteurs: Rebecca Spruijt, Lisa de Graaf, Annelore Beukema en Joost Christians

*19 juli 2024*

# Inhoudsopgave


**1. Inleiding ..... 4**

1.1 Inleiding ..... 4
1.2 De risico's van gegevensuitwisseling in samenwerkingsverbanden ..... 4
1.3 Onderzoeksvragen ..... 6
1.4 Onderzoeksverantwoording ..... 6
1.5 Leeswijzer ..... 8

**DEEL 1**
**Conclusie en aanbevelingen ..... 9**

**2. Conclusie en aanbevelingen ..... 10**

2.1 Conclusie ..... 10
2.2 Aanbevelingen ..... 12

**DEEL 2**
**Onderbouwing van de bevindingen ..... 16**

**3. Kaders voor gegevensbescherming ..... 17**

3.1 Nationale wet- en regelgeving ..... 17
3.2 Schaalkracht in regionale gegevensuitwisseling ..... 18

**4. Gegevensuitwisseling in de praktijk ..... 26**

4.1 Legitimiteit ..... 26
4.2 Organisatie ..... 29
4.3 Ambitie ..... 33

**5. Positie van de raad ..... 35**

5.1 Mogelijkheden tot sturing ..... 35
5.2 Positionering van de gemeenteraad ..... 36

**BIJLAGEN ..... 38**

B1 Onderzoeksverantwoording ..... 39
B2 Documenten ..... 41
B3 Wettelijk kader ..... 42

HOOFDSTUK 1

# Inleiding

## 1.1 Inleiding

Uit onderzoek (2022) blijkt dat raadsleden in het algemeen onvoldoende grip ervaren op de regionale samenwerkingen.[1] Het gaat hier bijvoorbeeld om de inrichting, governance en procedures van de samenwerkingsverbanden. Ook binnen de regio Twente wordt er volop gebruikgemaakt van samenwerkingsverbanden, waar de gemeente Enschede bijvoorbeeld deelneemt aan de Veiligheidsregio Twente of aan SamenTwente. Landelijk zien we dat gegevensuitwisseling in samenwerkingen een onderwerp van aandacht is. Zo zijn Nederlandse gemeenten in het Dreigingsbeeld Informatiebeveiliging expliciet benoemd als een van de grootste bedreigingen voor veilige informatie[2], benoemt de Autoriteit Persoonsgegevens gegevensuitwisseling in samenwerkingsverbanden een van de focusthema's van 2024[3] en heeft de VNG verschillende handreikingen gepubliceerd met betrekking tot de AVG, privacy en gegevensuitwisseling.

Er zijn verschillende typen gegevens die in regionale samenwerkingsverbanden van Enschede uitgewisseld worden. Denk bijvoorbeeld aan persoonsgegevens maar ook aan bedrijfsgevoelige gegevens. In dit onderzoek ligt de nadruk op de omgang met persoonsgegevens. Dit is in overleg met de Rekenkamer en de gemeente Enschede bepaald, met daaraan twee voorname redenen ten grondslag. De eerste overweging is dat onzorgvuldige omgang met persoonsgegevens verregaande persoonlijke consequenties heeft voor burgers. In de politiek-bestuurlijke context van de gemeente is het belangrijk om te borgen dat dit zorgvuldig plaatsvindt. De tweede overweging is dat er landelijk veel onduidelijkheid bestaat over de omgang met persoonsgegevens. De AVG wordt veelal als beperkend gezien en in combinatie met sectorale wetgeving is het soms een zoektocht wat wel of niet mogelijk is.

Grip op verantwoordelijkheden met betrekking tot gegevensbescherming is een belangrijk onderwerp voor de gemeente Enschede aangezien zij een (centrum)rol vervult in de regio Twente en zij deelneemt aan tal van verschillende samenwerkingsverbanden. Tegen het licht van de bovenstaande ontwikkelingen wil de Rekenkamer Enschede inzicht in de huidige situatie en de mogelijke risico's die hierbij ontstaan. Om deze reden onderzoekt Berenschot in opdracht van de Rekenkamer Enschede de omgang van de gemeente Enschede met mogelijke risico's van gegevensuitwisseling door en van samenwerkingsverbanden.

## 1.2 De risico's van gegevensuitwisseling in samenwerkingsverbanden

Zoals eerder al benoemd is grip op gegevensuitwisseling van en door samenwerkingsverbanden een onderwerp dat niet enkel bij de gemeente Enschede speelt. Bij veel gemeenten (en ook hun raadsleden) zien we in de praktijk terug dat de grip op gegevensuitwisseling onvoldoende is en dat het lastig blijkt hier wat aan te doen.[4]

1 Decentraal bestuur (2022).
2 Informatiebeveiligingsdienst & VNG (2022).
3 Autoriteit Persoonsgegevens (2023).

4 Dit is gebaseerd op ervaringen van de onderzoekers en trends die we zien door het land. Daarnaast hebben de onderzoekers voor de concretisering met de Autoriteit Persoonsgegevens en met een aantal FG's van verschillende gemeenten gesproken. Hierbij is gelet op variatie qua regio en grootte van de gemeenten.

Een gespreksronde met functionarissen gegevensbescherming (FG) van verschillende gemeenten levert het volgende beeld op:

- Uitvoering op afstand. Door de vaak gecompliceerde governancestructuur tussen een gemeente, andere deelnemende gemeenten en regionale andere partijen in een samenwerkingsverband, ontstaat een situatie waarin colleges op papier wel betrokken zijn bij een samenwerkingsverband maar in de praktijk niet altijd de ruimte hebben om daadwerkelijk te sturen. Het is afhankelijk van de gekozen bestuurlijke governance op welke manier een individuele gemeente sturingsmogelijkheden heeft. Daarnaast staat een samenwerkingsverband op afstand van het toezicht in een gemeente (in dit geval de FG), maar het is niet in alle gevallen verplicht om zelf toezicht in te stellen. Dit resulteert in een situatie waarin er wel gemeentelijke taken worden uitgevoerd en hiervoor gegevens worden verwerkt, maar dat hier beperkte sturing en toezicht op (mogelijk) is.

- Onduidelijkheid met betrekking tot rollen en verantwoordelijkheden. Ondanks dat verantwoordelijkheden in beleid wel toegewezen zijn, is in de gemeentelijke uitvoering vaak weinig kennis van verantwoordelijkheden met betrekking tot gegevensuitwisseling. Bestuur en directie hebben zelf vaak ook onvoldoende begrip van de rollen en verantwoordelijkheden die bestaan in relatie tot gegevensbescherming bij samenwerkingsverbanden. Mede hierdoor wordt er beperkt gestuurd op naleving in de uitvoering door het management en de directie. Er wordt vaak naar privacy officers (PO), de Chief Information Security Officer (CISO) en de FG gekeken.[5] Deze rollen staan echter op afstand van de uitvoering. Hierdoor ontstaat het gevaar op een papieren werkelijkheid, waardoor de organisatie zich niet bewust is van risico's in de praktijk.

- Gebrek aan overzicht. Gemeenten blijken veelal geen compleet en centraal overzicht te hebben van de samenwerkingsverbanden waar zij aan deelnemen. Ook is er vaak geen inzicht in gegevensstromen van en naar samenwerkingsverbanden. Hierdoor is het voor FG's lastig om toezicht te houden op de veilige omgang met persoonsgegevens.

**Wat zijn persoonsgegevens?**
Elk gegeven dat betrekking heeft op een natuurlijke persoon (betrokkene) is een persoonsgegeven. Om van een persoonsgegeven te spreken is het voldoende dat de betrokkene identificeerbaar is met de binnen de organisatie vastgelegde gegevens. Gegevens waarmee dit rechtstreeks kan, zijn bijvoorbeeld de NAW-gegevens, maar het kan ook via indirecte gegevens zoals een paspoortnummer of een IP-adres. Andere voorbeelden van persoonsgegevens zijn: e-mailadressen, telefoonnummers, geslacht, huwelijkse staat, familie en beroep.

**Bijzondere en strafrechtelijke gegevens**
Een speciale categorie van persoonsgegevens zijn bijzondere persoonsgegevens. Deze zijn extra beschermd. Dit zijn bijvoorbeeld medische of gezondheidsgegevens. Er geldt een verbod op het verwerken van bijzondere persoonsgegevens tenzij daarvoor een zwaarwegend belang of wettelijke grondslag aanwezig is. Een andere speciale categorie zijn strafrechtelijke gegevens. Deze worden alleen verwerkt onder toezicht van de overheid of als dat uitdrukkelijk in een wet is toegestaan. In Nederland is dit vastgelegd in de Uitvoeringswet AVG. Het verwerken van strafrechtelijke gegevens is toegestaan door en ten behoeve van publiekrechtelijke samenwerkingsverbanden als dat noodzakelijk is voor de uitvoering van hun taak. Voorwaarde daarbij is dat er zodanige waarborgen zijn dat de persoonlijke levenssfeer van de betrokkene niet onevenredig wordt geschaad.

Voor deze beide categorieën van persoonsgegevens gelden zwaardere eisen voor de beveiliging van de gegevens. Denk bijvoorbeeld aan het direct verwijderen van deze gegevens na uitvoering van de taak waarvoor ze verzameld zijn.

**Persoonsgegevens van gevoelige aard**
Verwerkingen van gegevens die kunnen leiden tot discriminatie, identiteitsdiefstal of –fraude, financiële verliezen, reputatieschade of enig ander aanzienlijk economisch of maatschappelijk nadeel, en verwerkingen van persoonsgegevens van kwetsbare natuurlijke personen, met name van kinderen, behoren tot persoonsgegevens van gevoelige aard. Ook deze krijgen specifieke bescherming.

5 Privacy officers en functionarissen gegevensbescherming hebben beide de verantwoordelijkheid voor de veilige omgang met (persoons)gegevens. Een privacy officer is verantwoordelijk voor het actualiseren en uitvoeren van het beleid rondom privacy en ondersteunt ook in de uitvoering. Een functionaris gegevensbescherming is een interne toezichthouder en ziet toe dat het beleid ook daadwerkelijk wordt uitgevoerd. Een functionaris gegevensbescherming focust op signaleren en rapporteren. De CISO is met name verantwoordelijk voor het informatiebeveiligsbeleid. De CISO is verantwoordelijk voor zowel de implementatie van dit beleid als het toezicht erop.

## 1.3 Onderzoeksvragen

In het onderzoek staan de volgende twee onderzoeksvragen centraal:

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

Om tot beantwoording van de hoofdvragen te komen, zijn de volgende deelvragen opgesteld voor het onderzoek:

1. Welke kaders (wetten, regels en besluiten) bestaan er voor rechtmatige gegevensuitwisseling in samenwerkingsverbanden?
2. Welk beleid bestaat er momenteel binnen de gemeente Enschede en in de regionale samenwerkingsverbanden waaraan de gemeente deelneemt met betrekking tot gegevensuitwisseling?
3. Hoe vindt gegevensuitwisseling momenteel plaats in samenwerkingsverbanden waarin de gemeente Enschede participeert?
4. Is de raad voldoende in positie gebracht om zijn kaderstellende rol uit te voeren?
5. Is de raad voldoende in positie gebracht om zijn controlerende rol uit te voeren?

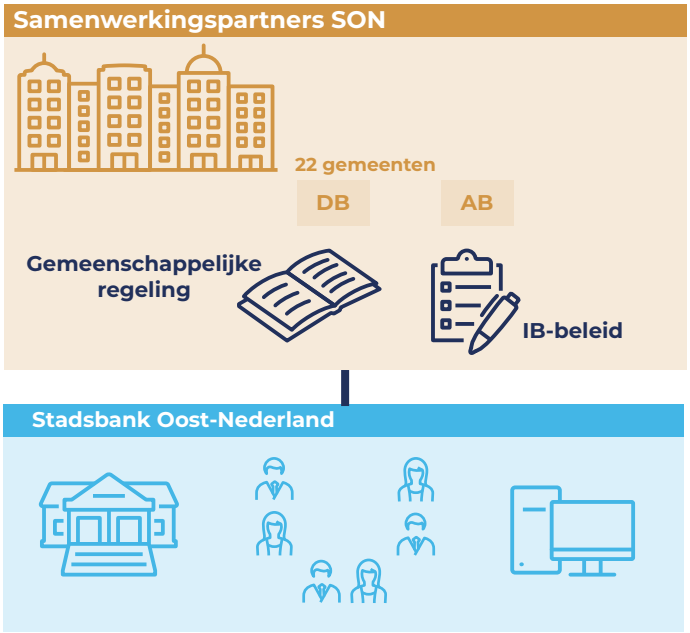
## 1.4 Onderzoeksverantwoording

Het onderzoek betreft een ex-durante-evaluatie van beleid en de invulling hiervan van de gemeente Enschede. Voor het onderzoek is gebruik gemaakt van een combinatie van een documentenstudie en interviews. Het onderzoek zet daarmee specifiek in op kwalitatieve onderzoeksmethoden en is vooral verkennend van aard. Om te beoordelen in hoeverre de gemeente Enschede stuurt op rechtmatige gegevensuitwisseling in samenwerkingsverbanden, vergelijken we bij wijze van steekproef het beleid en de uitvoeringspraktijk met betrekking tot twee regionale samenwerkingsverbanden: Stadsbank Oost Nederland en het Zorg- en Veiligheidshuis Twente. De selectie van onze twee casussen is in nauw overleg met de Rekenkamer tot stand gekomen. De casussen zijn op basis van een aantal criteria geselecteerd uit het totaaloverzicht van samenwerkingsverbanden (in totaal 26) waaraan de gemeente Enschede deelneemt[6]. In bijlage 1 vindt u meer informatie over de onderzoeksverantwoording.

### Stadsbank Oost Nederland

De Stadsbank Oost Nederland (hierna: SON) is een gemeenschappelijke regeling waarin 21 gemeenten in Twente en de Achterhoek hebben besloten om de uitvoering van taken op het gebied van schuldhulpverlening deels of volledig uit te besteden. In feite neemt de Stadsbank Oost Nederland wettelijke taken over van de gemeenten op het gebied van schuldhulpverlening. De Stadsbank Oost Nederland is een gemeentelijke regeling (GR) en kent een rechtspersoonlijkheid bezittend lichaam dat is gevestigd in Enschede. De Stadsbank presenteert zich aan cliënten als financiële dienstverlener zonder winstoogmerk, gericht op het creëren van duurzame financiële stabiliteit en financiële gezondheid. Cliënten kunnen zich rechtstreeks bij de Stadsbank melden of worden aangedragen door de gemeente: na een intakegesprek, of na een gemeentelijke indicatie waarvan de SON alleen de uitvoering verzorgt.

Figuur 1. **Verhouding SON en de samenwerkingspartners.**




De bestuurlijke verantwoordelijkheid ligt in handen van het algemeen bestuur (AB) en het dagelijks bestuur (DB). Het AB bestaat uit één collegelid uit elk van de deelnemende gemeenten. Het DB bestaat uit acht leden die door en uit het AB worden aangewezen. In ieder geval hebben AB-leden uit de gemeenten Enschede, Almelo en Hengelo zitting in het DB. De voorzitter (die het AB in het DB voorzit) is een wethouder uit de gemeente Enschede.

6 RegioAtlas (2024).

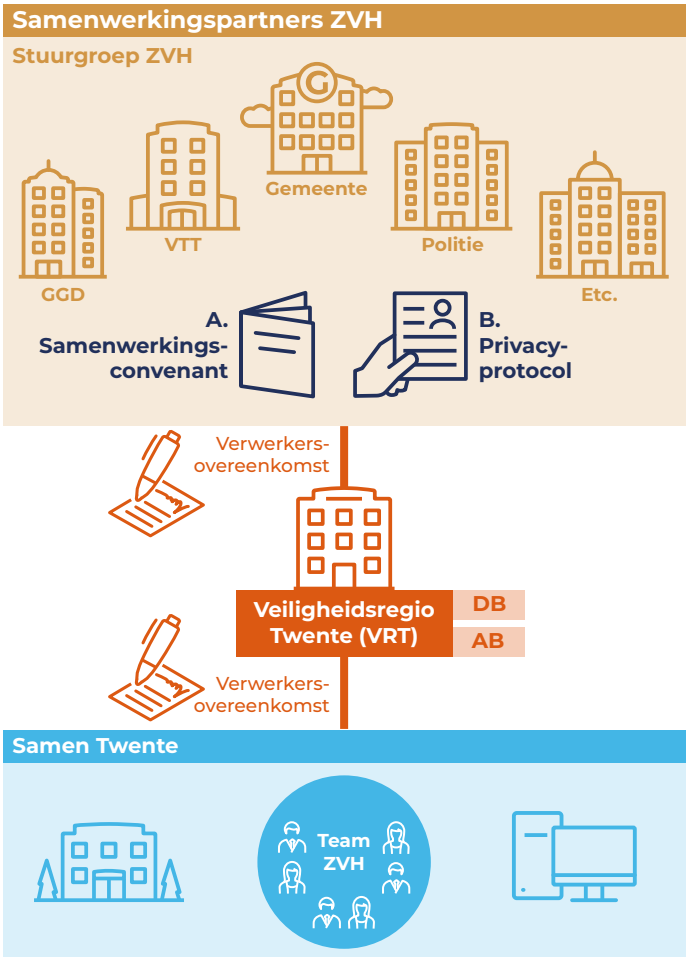
## Zorg- en Veiligheidshuis Twente

Het Zorg- en Veiligheidshuis Twente (hierna: ZVH) is een netwerksamenwerking tussen strafpartners, zorgpartners en de dertien gemeentelijke partners in de regio Twente.[7] Het ZVH komt tot een ketenoverstijgende aanpak van complexe problematiek om ernstige overlast en criminaliteit te bestrijden. Partners wisselen hierin informatie uit over 'complexe casuïstiek' op het snijvlak van het sociaal domein en het veiligheidsdomein. Het doel daarvan is het terugdringen van overlast, huiselijk geweld en criminaliteit. Partners signaleren gezamenlijk problemen, stemmen werkprocessen en oplossingen af en zorgen dat het handelingsrepertoire van de strafrecht- en zorgketen elkaar aanvullen. Het ZVH is geen zelfstandige organisatie, maar voert zijn taken uit ten behoeve van alle samenwerkende organisaties. De oprichting geschiedde in een samenwerkingsovereenkomst tussen alle partijen. Het ZVH heeft geen rechtspersoonlijkheid en wordt daarom door middel van dienstverleningsovereenkomsten gefaciliteerd door de Veiligheidsregio Twente (GR) en SamenTwente (GR)[8].

De (bestuurlijke) verantwoordelijkheden met betrekking tot informatiebeveiliging zijn verdeeld over de Stuurgroep Zorg, Veiligheid en Straf (geen rechtspersoonlijkheid en niet bevoegd tot zelfstandig handelen), de VRT en SamenTwente (beide wel een rechtspersoonlijkheid en bevoegd tot zelfstandig handelen). Zie de nevenstaande figuur voor de onderlinge verhoudingen.

De Veiligheidsregio Twente (hierna: VRT) is een wettelijk verplichte GR en heeft rechtspersoonlijkheid. Daarom zijn medewerkers van het ZVH in dienst bij de VRT en verzorgt de VRT hr-administratie. De VRT draagt zorg voor informatie-beveiliging in het ZVH (samenwerkingsconvenant, 2022). Alle dienstverlening aan het ZVH is vastgelegd in een dienst-verleningsovereenkomst.[9] De VRT heeft op zijn beurt een dienstverleningsovereenkomst afgesloten met SamenTwente (opnieuw een GR met rechtspersoonlijkheid) voor de huisvesting en de ICT van het ZVH. Dit omdat de VRT zelf niet met persoonsgegevens werkt, en SamenTwente dat wel doet. De beveiliging van gegevens is daarom in handen van SamenTwente (Privacy protocol (2023)). Dat maakt SamenTwente verantwoordelijk voor het in stand houden van procedures om inbreuk op beveiligingsmaatregelen te voorkomen.

Figuur 2. **Verhouding tussen de betrokken organisaties van het ZVH.**




De stuurgroep Zorg, Veiligheid en Straf (hierna: de stuurgroep) draagt - namens alle gemeenten die deelnemen aan het ZVH-netwerk, dus ook namens de gemeente Enschede - bestuurlijke verantwoordelijkheid voor het algehele functioneren van het ZVH (samenwerkingsconvenant 2022), waaronder voor een rechtmatige omgang met persoonsgegevens. Deelnemers zijn bestuurlijke vertegenwoordigers van een aantal van de deelnemende gemeenten en vertegenwoordigers van de directie van de deelnemende partijen. In de huidige praktijk gaat het om een wethouder van de gemeente Almelo en de burgemeester van Rijssen-Holten (2023). De stuurgroep is verantwoordelijk voor het opstellen van langetermijnvisies, inhoudelijke/financiële jaarplannen en het borgen van de kwaliteit van de samenwerking, waaronder ook de informatiebeveiliging en de evaluatie daarvan vallen.

7 Dertien Twentse Gemeenten, Politie, Justitie (OM) en zorgverleners (Veilig Thuis Twente, GGD).
8 Uitvoeringsorganisatie GGD Twente, Veilig Thuis Twente en de Organisatie voor Zorg en Jeugdhulp.
9 Uiteraard geldt bij samenwerkingsverbanden dat het vereiste veiligheidsniveau voor de gegevens verschilt per organisatie en het/(de) type(n) domein(en) waar-binnen de gegevens worden uitgewisseld. Daarbij dient er rekening te worden gehouden met bepaalde waardeafwegingen, zoals de balans tussen veiligheid en vertrouwelijkheid bij bijvoorbeeld kritieke infrastructuren. Dit kan zeker binnen het domein van veiligheid leiden tot andere veiligheidsvereisten vergeleken met bijvoorbeeld het domein leefbaarheid.

### Theoretisch kader

De gemeente is verantwoordelijk voor het verantwoord en legitiem omgaan met persoonsgegevens. Hierbij moet 'wat we willen' (ambitie) altijd in balans zijn met 'wat we kunnen' (organisatie) en met 'wat we mogen en waar we toe bereid zijn' (legitimiteit). Op het moment dat er sprake is van regionale samenwerking, is de gemeente echter afhankelijk van andere organisaties. In regionale samenwerking interacteren de drie aspecten daarom met elkaar op gemeentelijke en regionale schaal. Risicobeheersing heeft daarom te maken met schaalkracht en wordt vormgegeven door dit samenspel. In dit onderzoek kijken we daarom door de lens van drie aspecten; ambitie, organisatie en legitimiteit. In bijlage 1 vindt u ook een uitgebreidere beschrijving van het theoretisch kader.

## 1.5 Leeswijzer

Deze rapportage is ingedeeld in drie delen.

### Deel 1: conclusies en aanbevelingen

- In hoofdstuk 2 beantwoorden we de onderzoeksvragen en schetsen we de algemene conclusies. Daarnaast doen we een aantal aanbevelingen voor de ambtelijke organisatie en de gemeenteraad.

### Deel 2: onderbouwing van de bevindingen

- In hoofdstuk 3 beschrijven we de kaders voor gegevensuitwisseling. We gaan in op de nationale wet- en regelgeving die relevant is voor het onderwerp. Nationale wet- en regelgeving moet vertaald worden naar regionaal en lokaal beleid om hier invulling aan te geven. De beschrijving hiervan doen we aan de hand van de thema's legitimiteit, organisatie en ambitie.
- In hoofdstuk 4 analyseren we de toepassing van de geschetste kaders in de praktijk. Dit doen we aan de hand van de thema's legitimiteit, organisatie en ambitie.
- Hoofdstuk 5 focust op de positionering van de raad ten opzichte van gegevensuitwisseling in samenwerkingsverbanden. We analyseren de wijze waarop de raad zijn rollen invult.

### Deel 3: bijlagen

- In bijlage 1 vindt u de onderzoeksverantwoording en het theoretisch kader dat we hebben gebruikt voor onze analyse. In bijlage 2 vindt u een weergave van de gebruikte documenten en bijlage 3 bevat een toelichting op het wettelijk kader dat van toepassing is op de onderzochte casussen.



DEEL 1

# Conclusie en aanbevelingen

In dit deel beantwoorden we de onderzoeksvragen en schetsen we de algemene conclusies. Daarnaast doen we een aantal aanbevelingen voor de ambtelijke organisatie en de gemeenteraad.

HOOFDSTUK 2

# Conclusie en aanbevelingen

In dit hoofdstuk beantwoorden we de onderzoeksvragen en formuleren we een aantal aanbevelingen voor de ambtelijke organisatie en de raad van de gemeente Enschede.

## 2.1 Conclusie

### 1. Gaat de gemeente Enschede adequaat om met de risico's van gegevensuitwisseling in samenwerkingsverbanden?

Bescherming van persoonsgegevens is een grondrecht in Nederland. De verschillende vereisten vanuit het landelijke wet- en regelgevingskader dienen als waarborg hiervoor. Burgers moeten ervan op aan kunnen dat persoonsgegevens enkel gebruikt worden waarvoor dit mag en dat de omgang hiermee veilig plaatsvindt. Een adequate omgang met gegevensuitwisseling is dus vooral een rechtmatige omgang met gegevensuitwisseling tussen overheidspartijen (en niet-overheidspartijen), en is daarmee essentieel voor de invulling van goed bestuur.

Gegevensuitwisseling staat altijd ten dienste van het vervullen van publieke taken. Het inzetten van gegevensuitwisseling als instrument draagt daarom bij aan het realiseren van publieke waarde als gemeente. Op het moment dat een dergelijk instrument niet rechtmatig wordt ingezet, ontstaan er risico's voor het realiseren van publieke waarde op de opgaven en (wettelijke) taken waarvoor de gemeente verantwoordelijk is.

In de gemeente Enschede is het besef van de verstrekkende gevolgen van onrechtmatige gegevensuitwisseling groeiende en wordt er flink ingezet om de waarborgen hiervoor te versterken. Dit zien we op de lokale schaal enerzijds terug in het sterk geprofessionaliseerde beleidskader omtrent informatiebeveiliging en privacy, en anderzijds in het groeiende bewustzijn bij medewerkers. We zien echter ook dat de gemeente nog volop bezig is met de ontwikkeling en uitvoering van het beleid en er nog niet is. Waar er op strategisch niveau een solide beleidskader ligt, blijft de tactische vertaling en operationele invulling achter. Dit is logisch en maakt deel uit van de professionaliseringsslag, maar de gemeente is erbij gebaat om zich hiervan bewust te zijn en extra op in te zetten.

Een belangrijk aandachtspunt hierbij is dat voor de verdere professionalisering en adequate omgang met de risico's, het van belang is dat de directie en het bestuur zich van de risico's bewust zijn. Veilige omgang met persoonsgegevens zal niet uit zichzelf goed gaan, hier moet actief op worden gestuurd en toegezien. We hebben geen volledige risicoanalyse uitgevoerd op het niveau van de gemeente, maar zien wel dat er onder beleidsmedewerkers nog onvoldoende bewustzijn is over wat rechtmatige gegevensuitwisseling wel en niet is, en wat er van hen verwacht wordt om verbeteringen aan te brengen. Als de verantwoordelijkheid voor rechtmatige gegevensuitwisseling alleen op privacy officers wordt afgewend, maakt de gemeente Enschede haar ambities voor rechtmatige gegevensuitwisseling niet waar.

Op de regionale schaal verschilt het in formele zin én in de praktijk in hoeverre de gemeente Enschede sturingsmogelijkheden heeft en uitoefent. In de casusonderzoeken naar twee regionale samenwerkingsverbanden zagen we formele verschillen in:

- de mate waarin de gemeente Enschede gehele verwerkingsverantwoordelijkheid heeft (bij een netwerksamenwerking) of dit deelt met de regio (bij mandatering van taken).
- de mogelijkheden die de governancestructuur van het samenwerkingsverband aan de gemeente Enschede biedt om te sturen op rechtmatige gegevensuitwisseling. De gemeente Enschede komt bijvoorbeeld op afstand te staan van regionaal beleid ten aanzien van gegevensuitwisseling als de gemeente Enschede niet deelneemt aan een bestuurlijke stuurgroep waar jaarverslagen en de voortgang van de implementatie van privacy protocollen worden besproken. Het risico is dan dat de gemeente Enschede op afstand komt te staan van het regionale beleid voor gegevensuitwisseling.
- de mate waarin de beschikbare (organisatie-)capaciteit was afgestemd op het ambitieniveau voor veilige gegevensuitwisseling op het niveau van de regio. In sommige samenwerkingsverbanden ligt er duidelijk strategisch beleid voor rechtmatige gegevensuitwisseling en wordt er voldoende capaciteit vrijgemaakt voor de uitvoering daarvoor: bijvoorbeeld door uitwisseling tussen privacy officers vanuit deelnemende gemeenten of omdat er een privacy officer in dienst is van het openbaar lichaam. Maar soms is er slechts beleid op hoofdlijnen, en lukt het niet om specialistische capaciteit vrij te maken voor de uitvoering.

In de praktijk zagen we dat de gemeente Enschede niet optimaal gebruik maakt van de mogelijkheden die er zijn om te sturen op rechtmatige gegevensuitwisseling. Daarbij geldt ook dat de twee samenwerkingsverbanden die zijn bestudeerd, onderling erg verschillen in de beschikbare sturingsmogelijkheden. Bestuurlijk en binnen de gemeentelijke organisatie heerst bovendien de perceptie dat de verantwoordelijkheid hiervoor bij de samenwerkingsverbanden ligt. Toch is dit niet altijd het geval. Ondanks dat de uitvoeringsverantwoordelijkheid inderdaad (deels) bij het samenwerkingsverband ligt, blijft de juridische verwerkingsverantwoordelijkheid bij de gemeente. Dit is bijvoorbeeld het geval bij het mandateren van taken naar GR's (ondanks dat deze rechtspersoonlijkheid bezitten), maar ook bij samenwerkingsverbanden die geen rechtspersoonlijkheid bezitten.

Hierdoor ben je als organisatie juridisch aansprakelijk voor de juiste invulling van taken, terwijl je maar beperkte controle kunt uitoefenen in de regionale governancestructuur op de uitvoering van die taken.

Daarnaast merken we dat er in de praktijk, en door uitwisseling tussen lokale en regionale functionarissen gegevensbescherming of privacy officers, ook vertrouwen ontstaat in de sturing die het samenwerkingsverband voert op rechtmatige gegevensuitwisseling en het mitigeren of beperken van risico's. Maar: ook als de gemeentelijke organisatie de mening is toegedaan dat het regionale beleid voor gegevens-uitwisseling 'op orde is' en goed wordt uitgevoerd door de goede mensen, ontslaat dat de gemeente Enschede niet van haar formeel-juridische verwerkingsverantwoordelijkheid en dus de plicht om dit te controleren.

Bij sommige samenwerkingsverbanden bestaat er om bovenstaande redenen een grotere afstand tussen de regionale uitvoeringsverantwoordelijkheid en de lokale verwerkings-verantwoordelijkheid. Ons beeld, gebaseerd op onze casestudies, is dat de gemeente Enschede beperkt inzicht heeft op welke manier dit voor verschillende samenwerkingsverbanden is georganiseerd, en daarmee zorgvuldiger invulling kan geven aan verwerkingsverantwoordelijkheden waar de gemeente lokaal voor aansprakelijk blijft.

## 2. Is de raad voldoende in positie gebracht om zijn kaderstellende en controlerende rol uit te voeren?

De raad heeft een zeer minimale positie op dit onderwerp ingenomen. Dit geldt zowel voor de kaderstellende als voor de controlerende rol. Hiervoor moeten we echter zowel naar het college als naar de raad zelf kijken. Enerzijds is het aan het college om meer informatie over de mechanismen in de gemeente te delen met de raad, zodat de raad invulling aan de rollen kan geven.

Anderzijds is het ook aan de gemeenteraad zelf om positie in te nemen in de rollen. Ook als het gaat om de rechtmatigheid van gegevensuitwisseling op regionale schaal. Hoewel het lijkt alsof 'de regio' zich op afstand bevindt van de inwoners van de gemeente Enschede, zijn het wél Enschedeërs wiens gegevens worden gedeeld met regionale partners om bijvoorbeeld diensten te verlenen op het gebied van schuldhulpverlening of om de juiste zorg- en veiligheidsexpertise in te winnen.

Inwoners van Enschede hebben daarom – vanuit het voorgenoemde beginsel van goed bestuur – het recht om te weten wie er kan worden aangesproken op de verwerking van hun persoonsgegevens, met welk doel, en om daarover geïnformeerd te worden.

De gemeenteraad heeft de mogelijkheid om te sturen op de rechtmatigheid van gegevensuitwisseling. De landelijke AVG verplicht gemeentebesturen om hun beleid inzake de verwerking van persoonsgegevens te delen met de gemeenteraad, en daar ligt dan ook een taak om die te beoordelen. Het is echter niet realistisch om te verwachten dat raadsleden zich specialiseren op het thema gegevensuitwisseling om zo een stevige expertmatige controlerende rol uit te oefenen. Ten eerste is er weinig tot geen kennis van digitalisering aanwezig binnen de raad en ten tweede is het onderwerp ook niet politiek gemaakt. Dit resulteert in weinig aandacht voor het thema. Het is realistischer om dit op een hoger abstractieniveau te verwachten. Raadsleden kunnen de rechtmatigheid van gegevensuitwisseling – lokaal en in regionale samenwerkingsverbanden – relatief eenvoudig beoordelen door consequent te vragen naar 'wie', 'waarom' en naar 'transparantie' (zijn inwoners geïnformeerd?). Ze wijzen zo bestuur en organisatie op een adequate omgang met de complexiteit van verdeelde verwerkingsverantwoordelijkheid, doelbinding en het goed informeren van de inwoners in kwestie (zie paragraaf 2.2 voor concrete aanbevelingen hiertoe).

## 2.2 Aanbevelingen

### Aanbevelingen voor het college

- **Inrichting.** De mate van grip en beheersbaarheid op gegevensuitwisseling staat of valt vaak bij aan de voorkant tijdens de inrichting van een samenwerkingsverband al goed na te denken over rollen en verantwoordelijkheden. In de context van samenwerkingsverbanden is een belangrijk aspect de juridische vorm van de samenwerking, aangezien dit bepaalt welke grondslag voor gegevensuitwisseling er bestaat. Door vanaf het begin duidelijke afspraken te maken over rollen en verantwoordelijkheden, weten alle betrokken partijen waar zij voor aan de lat staan. Op deze manier kun je het vanaf het begin al goed inrichten en hoef je niet achteraf pleisters te plakken. Bij samenwerkingsverbanden die al bestaan, is het relevant om de inrichting kritisch tegen het licht te houden. Wat moet er wellicht anders of duidelijker? Het helpt hierbij als er binnen het samenwerkingsverband ook rollen zijn aangewezen om toe te zien op naleving van wet- en regelgeving.
- **Verantwoordelijkheid beleggen.** Maak ook in samenwerkingsverbanden expliciet afspraken over rollen en verantwoordelijkheden met betrekking tot de uitvoering van beleid. Denk bijvoorbeeld aan het uitvoeren van DPIA's.[10] Maak expliciet wie dit coördineert en leg vast op welk niveau de DPIA vastgesteld moet worden (bijvoorbeeld bestuurlijk). Door dit formeel vast te leggen, zullen mechanismen om hierop te sturen effectiever zijn.
- **Digitaal leiderschap.** Het belang van rechtmatige gegevensuitwisseling wordt meer doorleeft als de directie en het bestuur actief sturen op naleving van beleid, zowel lokaal als regionaal. Maak als directie en bestuur gebruik van de kennis van bijvoorbeeld de Functionaris Gegevensbescherming om hier invulling aan te geven.
- **Controle.** Regel eerstelijns controle in op het niveau van de uitvoering. Gebruik dit vervolgens niet om te 'straffen' als het niet goed gaat, maar gebruik dit om inzicht te verkrijgen in mogelijkheden tot verbetering. Op deze manier voorkom je een papieren werkelijkheid met aanzienlijke risico's ten gevolg. Denk er bijvoorbeeld aan om afdelingen zelf datalekken te laten melden (en hier ook wel op te controleren) of door lijnmanagers over betreffende onderwerpen te laten rapporteren via managementverantwoording. Op deze manier borg je dat er controle plaatsvindt op de uitvoering en kan je op naleving sturen.
- **Bundel de toezichtkracht.** Bundel de krachten vanuit de interne toezichtfuncties (denk aan de FG, gemeentearchivaris en controllers maar wellicht ook aan adviserende functies zoals de CISO). Een mogelijkheid is om één jaarverslag in te dienen, met verschillende hoofdstukken per onderwerp. Op deze manier benadruk je de verbondenheid van alle digitaliseringsonderwerpen en kom je in gezamenlijkheid hoger op de bestuurlijke agenda.

10 DPIA staat voor Data Protection Impact Assessment. Een DPIA is verplicht op het moment dat het gebruik van persoonsgegevens in een organisatie mogelijk een hoog risico kan opleveren. Het uitvoeren van een DPIA is een verplichting die is opgenomen in de Algemene verordening gegevensbescherming (AVG), de Wet politiegegevens (Wpg) en de Wet justitiële en strafvorderlijke gegevens (Wjsg).

- **Positioneer rechtmatige gegevensuitwisseling binnen het bredere thema 'goed digitaal bestuur'.** Het college kan verschillende raadsinformatiebrieven of besluiten binnen dit thema bundelen en op deze manier de raad meenemen in de omgang van de gemeente met digitalisering voor het vervullen van de publieke taken. Hierdoor kan de raad het kennisniveau verhogen en de werking van het bestaande beleid, de governance en de processen beter leren kennen. Op deze manier wordt de raad gepositioneerd om te controleren of het gemeentelijke systeem werkt zoals beoogd, en – nog belangrijker - of die werking daadwerkelijk bijdraagt aan het realiseren van de gewenste 'publieke waarde' voor inwoners, op de opgaven die direct raken aan hun belevingswereld.

## Een praktisch instrument voor grip op gegevens-uitwisseling in samenwerkingsverbanden: checklist gemeentelijke verwerkingsverantwoordelijkheid

Om actief aan de slag te gaan met de bovenstaande aanbevelingen, is het nodig dat de gemeente Enschede inzicht krijgt in de verwerkingsverantwoordelijkheden per samenwerkingsverband[11]. Zoals ons casusonderzoek duidelijk maakt, verschillen de regionale samenwerkingsverbanden immers veel in de mate waarin de gemeente Enschede (gedeeltelijk) verantwoordelijkheid heeft voor veilige en rechtmatige gegevensuitwisseling. De lopende actie om het totaal aan samenwerkingsverbanden waaraan Enschede deelneemt in kaart te brengen is een goede eerste stap. We adviseren om vervolgens voor elk samenwerkingsverband (denk aan netwerksamenwerkingen, stichtingen, bedrijven en andere mogelijke verbanden) een 'checklist gemeentelijke verwerkingsverantwoordelijkheid' te doorlopen. Het doel van zo'n exercitie is om – vanuit het lokale perspectief – te specificeren in welke mate de gemeente Enschede verantwoordelijkheden voor rechtmatige gegevensuitwisseling behoudt, deelt of overdraagt én welke sturingsmogelijkheden de gemeente houdt om toe te zien op het veilig delen van persoonsgegevens in het samenwerkingsverband.

De checklist per samenwerkingsverband zou in onze optiek in ieder geval de volgende elementen moeten bevatten:

1. **Verwerkingsverantwoordelijkheid: waar bevindt zich dit na het overdragen van taken?** Het is afhankelijk van de wijze van overdragen van taken of de gemeente haar verwerkingsverantwoordelijkheid overdraagt naar een samenwerkingsverband. In geval van mandatering blijft de gemeente altijd verantwoordelijk, maar kan dit wel in gezamenlijkheid gedragen worden als de GR feitelijk invloed uitoefent. Bij delegatie van bevoegdheden wordt een GR zelfstandig bevoegd gemaakt en is de GR bestuurlijk verantwoordelijk. Toch is de gemeente niet altijd ontheven van verwerkingsverantwoordelijk, bijvoorbeeld als de gemeente door middel van beleid het doel van de verwerking vaststelt. In dat geval kan er op zijn hoogst sprake zijn van gezamenlijke verwerkingsverantwoordelijkheid. Overigens is de rechtsvorm van de samenwerking hiervoor ook relevant, een netwerksamenwerking (geen rechtspersoonlijkheid) kan sowieso niet zelfstandig rechtshandelingen verrichten en kan daarmee nooit verwerkingsverantwoordelijkheid hebben.

2. **Juridische grondslag voor gegevensuitwisseling: hoe zijn verantwoordelijkheden verdeeld?** Een gemeenschappelijke regeling, samenwerkingsconvenant of andere oprichtingsgrondslag van een samenwerkingsverband kan ook taken, verantwoordelijkheden en bevoegdheden bevatten die betrekking hebben op de verdeling van verantwoordelijkheden rondom de uitwisseling van gegevens tussen deelnemende partijen. Dit betekent echter niet in alle gevallen dat hiermee ook de formele verantwoordelijkheid voor het voldoen aan wet- en regelgeving kan worden overgedragen. De gemeente Enschede heeft er baat bij om deze (formele) verantwoordelijkheidsverdeling als partij in elk van de samenwerkingsverbanden te kennen, en er vragen over te stellen als er geen melding is gemaakt van (aanvullend beleid om) rollen en verantwoordelijkheden met betrekking tot gegevensuitwisseling.

11 Hiermee bedoelen we zowel samenwerkingsverbanden met rechtspersoonlijkheid als samenwerkingsverbanden zonder rechtspersoonlijkheid (bijvoorbeeld netwerksamenwerkingen).

3. **Ambitieniveau: welke uitwisseling van persoonsgegevens dient het belang van Enschede?** De gemeente doet er goed aan om per samenwerkingsverband te beoordelen hoe hoog de lat moet liggen als het gaat om de invulling van de eigen, lokale verwerkingsverantwoordelijkheid en de manier waarop het samenwerkingsverband omgaat met de verwerkingsverantwoordelijkheid. De gemeente zet een standaard voor haar eigen verwerkingsverantwoordelijkheid binnen de samenwerking, maar ook voor die van 'de regio'. De gemeente kan het ambitieniveau bijvoorbeeld uitwerken aan de hand van:
   - Het type persoonsgegevens dat wordt gedeeld in het samenwerkingsverband: gaat het om algemene of bijzondere (strafrechtelijke) gegevens en dus casuïstiek die wordt behandeld?
   - Wat is het doel van de gegevensverwerking, en is er sprake van (voldoende) doelbinding?
   - De aanwezigheid (of afwezigheid) van informatiebeveiliging- of privacybeleid van het samenwerkingsverband waarin de verdeling van verantwoordelijkheden en regionale ambities zijn uitgewerkt.
   - Zorgen over de praktische invulling van verwerkingsverantwoordelijkheden door het samenwerkingsverband of de regio-organisatie, bijvoorbeeld beschikbare ambtelijke capaciteit.

4. **Sturingsmogelijkheden: waar stuurt Enschede bij?** De gemeente Enschede kan vervolgens duiden hoe er kan worden gestuurd op de rolverdeling: welke mogelijkheden biedt de governance van elk samenwerkingsverband om informatiebeveiliging- of privacybeleid te agenderen? Hoe verloopt de ambtelijke samenwerking? Is er op beleidsniveau een gremium dat zich buigt over vraagstukken omtrent gegevensuitwisseling, of moeten vragen daarover elders worden ingebracht? Welke bestuurlijke escalatiemogelijkheden biedt dit samenwerkingsverband? Worden thema's omtrent veilige gegevensuitwisseling periodiek bestuurlijk geagendeerd (bijvoorbeeld als onderdeel van de jaarcyclus)? Als deze mechanismen duidelijk in kaart zijn, kunnen ze effectiever worden ingezet.

5. **Toedeling aan (beleids)medewerkers en de privacy officer: wie kijkt mee in Enschede?** Ons advies is om per samenwerkingsverband duo's te vormen van een beleidsmedewerker en een privacy officer die toezien op de praktische invulling van de uitkomst van deze checklist. Zo wordt er ook op tactisch en operationeel niveau (in het three lines of defence-model van de gemeente ) verantwoordelijkheid ervaren voor het vervullen van verwerkingsverantwoordelijkheden in samenwerkingsverbanden, en is er bewustzijn van de risico's die zich voordoen of zich voor (kunnen) doen als de verdeling van verantwoordelijkheden onduidelijk is of niet wordt nageleefd in de praktijk.

## Aanbevelingen voor de raad

- **Versimpel tot sturing op de rechtmatigheid van gegevensuitwisseling: lokaal en regionaal.** Zoals in paragraaf 2.1 is aangegeven, hebben raadsleden vanuit hun controlerende rol en onder de AVG een verantwoordelijkheid om de rechtmatigheid van het gebruik en de verwerking van persoonsgegevens door de gemeente Enschede te beoordelen. Invulling van de (wettelijke) verantwoordelijkheid om te sturen op rechtmatigheid van gegevensuitwisseling behoeft geen expertkennis. Hoofdvragen over wie verantwoordelijkheid draagt voor gegevensuitwisseling, hoe rechtmatige omgang wordt geborgd en of/hoe inwoners geïnformeerd zijn, vormen voldoende beoordelingskader van beleid over het delen van persoonsgegevens. Of dat beleid nu lokaal of regionaal tot stand komt. Raadsleden bevragen op deze manier actief de omgang met de grootste risico's van onrechtmatige gegevensuitwisseling voor de inwoners wiens persoonsgegevens worden gedeeld: een gebrek aan verantwoordelijkheidsbesef, onjuiste invulling van gegevensuitwisseling en gebrek aan transparantie richting de inwoners wiens gegevens worden gedeeld.

- **Vraag om informatie als dat niet automatisch wordt gedeeld.** Dit kan bijvoorbeeld door de FG een informerende presentatie te laten geven aan de raad: waar gaat gegevensuitwisseling over, hoe gaat de gemeente ermee om en waarom is dit belangrijk? Daarnaast wordt beleid over gegevensuitwisseling (en risicobeheersing) niet automatisch door ieder samenwerkingsverband gedeeld met de gemeenteraad.

Overheidslichamen onder een GR volgen de jaarcyclus en leggen als onderdeel daarvan verantwoording af over hun beleid ten aanzien van gegevensuitwisseling aan deelnemende gemeenten en hun raden, maar zogenaamde netwerksamenwerkingen hebben vaak geen staande praktijk. Raadsleden kunnen proactief om regionaal beleid ten aanzien van gegevensuitwisseling verzoeken om de rechtmatigheid te beoordelen. Dat is nodig, want de verantwoordelijkheid voor rechtmatige gegevensverwerking blijft in vele gevallen (deels) bij de gemeente Enschede. Niet alleen voor deze onderzochte casussen, maar bij samenwerkingsverbanden in het algeheel.

- **Ken en gebruik (reguliere) sturingsmogelijkheden voor grip op regionale samenwerking.** Als raadsleden twijfelen aan de beantwoording van de drie hoofdvragen over rechtmatige gegevensuitwisseling in samenwerkingsverbanden, zullen zij gebruik moeten maken van de controlerende processen en procedures die gangbaar zijn voor het samenwerkingsverband in kwestie. Het instrumentarium daarvoor verschilt per samenwerkingsverband: bij gemeenschappelijke regelingen kan er via een zienswijzeprocedure worden gestuurd op wijzigingen van het regiobeleid omtrent gegevensuitwisseling (volgens artikel 35 van de WGR), maar bij andere vormen van samenwerking zal de raad een portefeuillehouder of DB-lid uit het college van Enschede moeten aansturen op dit type wijzigingen. Het helpt als raadsleden zich verdiepen in de governance van elk samenwerkingsverband: reguliere sturingsmogelijkheden kunnen ook worden ingezet voor verbetering van beleid ten aanzien van gegevensuitwisseling.

- **Stel kaders voor lokale verwerkings-verantwoordelijkheden in regionale samenwerkingsverbanden.** De raad van de gemeente Enschede vervult zijn controlerende rol met de voorgaande aanbevelingen op de regionale schaal. We adviseren daarnaast om op de lokale schaal ook kaderstellend te werk te gaan. De raad van de gemeente Enschede kan bijvoorbeeld aansturen op het formuleren van de praktische checklist ‘gemeentelijke verwerkingsverantwoordelijkheid’, die hierboven is gesuggereerd. Bij eventuele toetreding tot een nieuw samenwerkingsverband, of een wijziging in de governancestructuur van een samenwerkingsverband, kan de raad aansturen op het (opnieuw) doorlopen van de checklist.

  Raadsinformatiebrieven over voortgang of koerswijzigingen binnen regionale samenwerkingsverbanden kunnen bovendien worden voorzien van een korte paragraaf over wijzigingen in de ‘checklist gemeentelijke verwerkingsverantwoordelijkheid’. Zo stuurt de raad op bewustzijn van verwerkingsverantwoordelijkheden van de gemeente Enschede en een duidelijker, explicieter antwoord op de hoofdvraag ‘wie is verantwoordelijk voor rechtmatige gegevensverwerking?’

### Praktische instrumenten voor de rolinvulling van de raad rondom digitalisering

Er zijn veel instrumenten, handvaten en kaders beschikbaar die kunnen helpen bij de rolinvulling van raadsleden op het gebied van digitalisering. Deze documenten kunnen raadsleden helpen om grip te krijgen op het thema. Zie hieronder een korte lijst:

- ***Raad weten met digitalisering:*** het Rathenau Instituut heeft een denkraam ontwikkeld dat raadsleden kan helpen bij het stellen van vragen over digitaliseringsprojecten. Leer over de verschillende knoppen waar een raadslid aan kan draaien.[12]
- ***De rol van de gemeenteraad op het gebied van digitalisering:*** ook vanuit de VNG wordt er aandacht gegeven aan de rol van de gemeenteraad op het gebied van digitalisering. In dit artikel wordt helder uiteengezet waarom digitalisering op meerdere domeinen van belang is, en niet pas onderwerp van gesprek moet zijn op het moment dat er iets misgaat.[13]
- ***De DataWijzer:*** De DataWijzer is een instrument dat speciaal voor raadsleden is ontwikkeld. Het helpt raadsleden om tot een goed afgewogen en onderbouwd besluit te komen bij raadsvoorstellen waarin digitale technologie is ingezet.[14]
- ***De Digitale Raadgever:*** De Digitale Raadgever is een interactieve tool die gemeenteraadsleden helpt om vragen te stellen over de doelgroep, het beleidsdoel en de impact van een datagerelateerd voorstel. Deze tool kan raadsleden helpen om tot een geïnformeerd besluit te komen over het voorstel.[15]
- ***Commissie digitale zaken voor de raad en meer:*** uit onderzoek blijkt dat er veelal informatieasymmetrie bestaat tussen het college en de raad. De raad voelt zich meestal onzeker door het gebrek aan duidelijke informatie en weinig grip op de materie. Het onderzoek biedt handzame aanbevelingen om hier mee aan de slag te gaan.[16]

12 Rathenau Instituut (2020).
13 VNG (2021).
14 Data School, Universiteit Utrecht (2021).
15 Datawerkplaats, Universiteit Utrecht (2022).
16 Universiteit Utrecht (2022).



DEEL 2

# Onderbouwing van de bevindingen

Dit deel bevat de uitgebreide beschrijvingen van onze bevindingen. We beginnen met een uitleg van de relevante wet- en regelgeving en de bestuurlijke schalen die van toepassing zijn op de casussen. Vervolgens leggen we onze bevindingen en analyse van de gemeente voor. We sluiten af met een analyse van de positionering van de raad.

HOOFDSTUK 3

# Kaders voor gegevens-bescherming

In dit hoofdstuk beschrijven we de kaders voor gegevensbescherming. Op welke manier wordt door de gemeente Enschede geborgd dat gegevensuitwisseling op een veilige manier plaatsvindt? Dit dient als vertrekpunt om vervolgens in hoofdstuk 4 inzichtelijk te maken op welke manier er in de praktijk mogelijk risico's ontstaan.

Eerst schetsen we de juridische kaders voor gegevensuitwisseling in de context van regionale samenwerking. Vervolgens beschrijven we hoe op de regionale en lokale schaal invulling wordt gegeven aan gegevensbescherming. Dit doen we aan de hand van legitimiteit (de vertaling van wet- en regelgeving naar beleid), organisatie (de wijze waarop de organisatie invulling geeft aan beleid) en ambities (regionale/lokale accenten).

## 3.1 Nationale wet- en regelgeving

In deze paragraaf beschrijven we hoe het juridisch kader met betrekking tot gegevensuitwisseling in samenwerkings-verbanden eruitziet. De relevante wettelijke kaders kunnen in algemene zin opgesplitst worden in twee typen. Ten eerste zijn er 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).

In beginsel dient al het handelen van de gemeente hieraan te voldoen.[17]

Daarnaast zijn er per domein materiële wetten (algemeen bindende voorschriften) die invloed hebben, zoals de Wet gemeenschappelijke schuldhulpverlening, de Wet maatschappelijke ondersteuning, de Jeugdwet en de Participatiewet. In bijlage 3 staat een uitgebreidere beschrijving van de verschillende wetten. In de materiële wetten worden de doelen, taken, bevoegdheden en verantwoordelijkheden van bestuursorganen nader uitgewerkt. Zij zijn in dit opzicht bepalend voor de wijze waarop de algemene kaders toegepast dienen te worden. Materiewetten vormen hiermee de verdere uitwerking van de formele nationale kaders (zie figuur 3).

17 In juni 2024 is de Wet gegevensuitwisseling samenwerkingsverbanden (Wgs) aangenomen. Deze wet is relevant voor bijvoorbeeld het Zorg- en Veiligheidshuis Twente en biedt de juridische basis voor verwerking van persoonsgegevens binnen het samenwerkingsverband. In de wet en de nog nader uit te werken maatregelen van bestuur worden nadere regels bepaald over de wijze waarop gegevensuitwisseling kan plaatsvinden. Dit zal impact hebben op de wijze waarop de gemeente Enschede deze taken uitvoert. Alhoewel deze wet ten tijde van dit rapport nog niet van kracht is, en daarom niet meegenomen kan worden in de juridische analyse, zal deze na inwerkingtreding wel van invloed zijn.

Figuur 3. **Verhouding tussen formele en materiële wetgeving.**




Bij de uitwisseling van (persoons-)gegevens tussen de gemeente Enschede en andere deelnemers binnen een samenwerkingsverband zal de impact, afhankelijk van het beleidsonderwerp en de gekozen samenwerkingsvorm, verschillen. Dit ontstaat onder meer doordat de wet- en regelgeving per beleidsterrein verschilt. Het samenspel van de algemene juridische kaders met sectorale juridische kaders heeft als gevolg dat er per sector een ander juridisch kader bestaat.[18] De wettelijke grondslagen voor het uitwisselen van gegevens staan dus beschreven in verschillende wetten waar diverse organisaties en professionals in de samenwerkingsverbanden mee te maken hebben bij de juiste uitvoering van hun taken en bevoegdheden.

## 3.2 Schaalkracht in regionale gegevensuitwisseling

Nationale wet- en regelgeving wordt op regionale en lokale schaal vertaald in beleid. In dit beleid geven organisaties invulling aan gegevensbescherming. In deze paragraaf beschrijven we hoe er op regionale en lokale schaal invulling wordt gegeven aan gegevensbescherming. We gaan voor beide cases en voor de lokale situatie van de gemeente Enschede achtereenvolgens in op de volgende onderwerpen:

- *Legitimiteit.* Welk beleid is vastgesteld om gegevensuitwisseling rechtmatig te laten plaatsvinden?
- *Organisatie.* Hoe is de organisatie ingericht om op legitimiteit rondom gegevensuitwisseling te sturen?
- *Ambitie.* Welke ambities hebben de organisaties gesteld met betrekking tot gegevensbescherming?

**Wat betekent dat voor de gemeenteraad van Enschede?**
Bescherming van persoonsgegevens is een grondrecht voor alle inwoners van Nederland. Dat grondrecht vraagt bescherming. Op grond van de AVG zijn gemeenten verplicht om verantwoording af te leggen over de verwerking van persoonsgegevens. Over maatregelen die een gemeente neemt om gegevens van inwoners te beschermen zal het college van B en W dus proactief moeten rapporteren aan de gemeenteraad.

De koers die de gemeente kiest – of de principes die worden gehanteerd bij de keuze van de hiervoor bedoelde maatregelen – legt het college vaak vast in een beleidsplan. In dit geval is dat het 'Strategisch informatiebeveiligings- en privacybeleid".

Het beleidsplan wordt ter goedkeuring voorgelegd aan de gemeenteraad, zodat raadsleden vanuit hun controlerende rol kunnen toezien op het naleven van de bescherming van persoonsgegevens – en dus de bescherming van een belangrijk grondrecht. Volgens de *Autoriteit Persoonsgegevens* kunnen raadsleden aan de hand van drie eenvoudige vragen een beleidsplan beoordelen:

- **Wie is verantwoordelijk?** Volgens de AVG moet een gemeente vastleggen wie 'verwerkingsverantwoordelijkheid' draagt als er gebruik wordt gemaakt van persoonsgegevens. Is dat de gemeente, of een uitvoerende organisatie? Het moet voor inwoners glashelder zijn waar zij terecht kunnen met vragen over hun persoonsgegevens.
- **Waarom is het noodzakelijk?** De gemeente zal moeten aantonen waarom en met welke aanleiding er persoonsgegevens worden verwerkt. Het college moet in het beleidsplan aantonen op basis van welke 'materiewetten' op specifieke beleidsterreinen er sprake mag zijn van gegevensuitwisseling door en in de gemeente. Inwoners moeten erop kunnen vertrouwen dat hun gegevens worden verwerkt om een doel te behalen dat hen óók dient.
- **Hoe zijn inwoners geïnformeerd?** Transparantie over het gebruik van persoonsgegevens door de gemeente vraagt om proactieve communicatie. Het beleidsplan voor de AVG zal melding moeten maken van maatregelen om inwoners in begrijpelijke taal voor te lichten over de manier waarop hun persoonsgegevens worden gebruikt en beschermd.

18 Daarnaast komt er, met name vanuit de Europese Unie, steeds meer nieuwe wet- en regelgeving bij die mogelijk impact heeft voor de gemeente Enschede.

### 3.2.1 Legitimiteit

*Regionaal: Stadsbank Oost Nederland*

Ook voor de SON geldt dat er meerdere wettelijke kaders van toepassing zijn: naast de AVG heeft de SON te maken met de Wet gemeentelijke schuldhulpverlening, de Wet op het consumentenkrediet (Wck), de Wet financiering decentrale overheden, de Participatiewet en de Faillissementswet (zie bijlage 3 voor een beschrijving van de wetten).

De wet gemeentelijke schuldhulpverlening bepaalt in artikel 3a dat het college door middel van mandatering taken op het gebied van schuldhulpverlening door derden kan laten verrichten. Bij mandatering van taken blijft de verwerkingsverantwoordelijkheid bij het college liggen, dit kan niet worden overgedragen. Er is wel sprake van (deels) gezamenlijke verwerkingsverantwoordelijkheid omdat de SON feitelijk invloed uitoefent en mede bepaalt welke persoonsgegevens worden verwerkt en voor welk doel. De SON heeft bij bestuurlijk besluit bepaald dat voor de feitelijke uitvoering van de taken, de SON de verantwoordelijkheid draagt. Daarmee ligt de uitvoeringsverantwoordelijkheid bij de SON terwijl de juridische verantwoordelijkheid gezamenlijk door de partijen wordt gedragen.

De SON is een openbaar lichaam met een zelfstandige rechtspersoonlijkheid. De SON moet als overheidslichaam daarom voldoen aan de bepalingen in de Baseline Informatiebeveiliging Overheid (BIO) en de AVG. In het informatieveiligheidsbeleid (IB-beleid) is beschreven op welke manier de SON veilige omgang met persoonsgegevens borgt. Er is in het IB-beleid onder andere vastgelegd voor welke doelen en met welke partijen de SON gegevens uitwisselt, en welke afspraken er daarvoor gelden. Bijvoorbeeld: voor de opslag van persoonsgegevens wordt gewerkt met derden, die als gegevensverwerkers worden aangemerkt en waarmee verwerkersovereenkomsten worden gesloten. Of: er is sprake van kleinschalige verwerkingen van persoonsgegevens door deurwaarders en bewindvoerders die gegevens van de SON verstrekt krijgen, waarbij de vertrouwelijkheid in het onderlinge contact en in het contact en de cliënten wordt benadrukt.

*Regionaal: Zorg- en Veiligheidshuis Twente*

Naast het juridische kader, beschreven in paragraaf 3.1, heeft het ZVH te maken met de Wet geneeskundige behandelovereenkomst (WGBO), de Jeugdwet, de Wet politiegegevens (Wpg), de Wet justitiële en strafvorderlijke gegevens (Wjsg) en de Reclasseringsregeling 1995.[19] Het ZVH heeft geen zelfstandige wettelijke taak en heeft daarom geen wettelijke basis om gegevens te verwerken. Hierdoor blijven de verschillende deelnemers allemaal zelfstandig verwerkingsverantwoordelijk. Het ZVH verwerkt geen gegevens uit eigen naam, maar ten behoeve van de partijen in de samenwerking. Dit betekent dat deelnemers aan de samenwerking hun eigen verantwoordelijkheid behouden met betrekking tot het delen van gegevens en dat ze hierdoor soms een gezamenlijke verwerkingsverantwoordelijkheid hebben. Hiervoor moeten de partijen gezamenlijk afspraken hebben gemaakt. Het gaat dan bijvoorbeeld om afspraken rondom het te gebruiken informatieverwerkingssysteem, de werkwijze voor verwerkingen en verstrekkingen van persoonsgegevens (inclusief de bijbehorende geheimhoudingsplichten voor personeel van het ZVH) en protocollen voor bewaren, vernietigen, beveiliging en het tegengaan van datalekken.

SamenTwente kwalificeert zichzelf als ‘verwerker’ van gegevens van de partijen uit het convenant. Het privacy protocol geeft aan dat bij het uitbesteden van verwerkingshandelingen buiten de partijen van het convenant, schriftelijke goedkeuring van de stuurgroep nodig is voor verwerkingsovereenkomsten.

De (juridische) verankering van de omgang met wettelijke vereisten in beleid vindt plaats in een samenwerkingsconvenant en een privacy protocol. De inwerkingtreding van deze documenten is echter op het moment van dit onderzoek nog onduidelijk. Beide zijn in 2023 geüpdatet – met een governancewijziging (zie de volgende paragraaf) en door een externe jurist - en zouden in 2024 bestuurlijk worden bekrachtigd, aldus het jaarverslag ZVH 2023. We hebben in dit onderzoek echter geen getekende versies aangetroffen van het herziene convenant en het privacy protocol. Dat verklaart mogelijk ook dat er nog geen verwerkingsovereenkomst is gesloten met het ZVH die door de stuurgroep is goedgekeurd, zoals zou passen bij de rol van het ZVH als verwerker.

19 Zie bijlage 3 voor een uitgebreide beschrijving van het wettelijk kader.

*Lokale schaal: gemeente Enschede*

De gemeente Enschede is verwerkingsverantwoordelijk voor de (wettelijke) taken die aan de gemeente zijn toebedeeld. Voor de uitvoering van die taken werkt de gemeente vaak niet alleen, maar met partners. Voor elke verwerking waarbij partners betrokken zijn – die opereren binnen de gemeentegrenzen maar ook daarbuiten – schrijft de landelijke wet- en regelgeving voor dat er afspraken gemaakt worden over bijvoorbeeld het al dan niet in stand blijven van de verwerkingsverantwoordelijkheid. Zo behoudt, zoals hierboven beschreven, bij mandatering van taken het college de verwerkingsverantwoordelijkheid.

De nationale wet- en regelgeving is in de gemeente Enschede verankerd in het strategisch informatiebeveiliging- en privacybeleid. Uitwerkingen van specifieke onderwerpen, zoals risicoanalyses (DPIA's)[20] en het verwerkingsregister, zijn vastgelegd in onderliggend beleid.

**Samenvattend**

- ***De gemeente Enschede blijft eindverantwoordelijk voor zorgvuldige gegevensverwerking binnen het ZVH.***
  De verwerkingsverantwoordelijkheid blijft bij het college liggen daar waar het de gemeente Enschede aangaat, mede omdat het ZVH als netwerkorganisatie geen verwerkingsverantwoordelijkheid kan hebben. Elke partij zal er daarom op moeten toezien dat de geldende wetten en regelgeving (uit het privacy protocol, en verder) worden toegepast in het ZVH. De uitvoeringsverantwoordelijkheid voor gegevensverwerking in het ZVH is echter versnipperd in de huidige organisatiestructuur, waardoor er geen organisatie is die de volledige verantwoordelijkheid voelt of neemt.
- ***De gemeente Enschede heeft een gezamenlijke verwerkingsverantwoordelijkheid met de SON.***
  Ondanks dat de gemeente vanwege mandatering de verwerkingsverantwoordelijkheid behoud, is de gemeente afhankelijk van de SON voor rechtmatige invulling hiervan omdat de gemeente Enschede alle gemeentelijke taken omtrent wettelijke schuldhulpverlening heeft overgedragen. Het IB-beleid van de SON legt helder vast dat er vooral sprake is van een verdeling van verwerkingsverantwoordelijkheden tussen de SON en enkele derde partijen waarmee de SON samenwerkt voor de uitvoering van taken. Omdat de SON ook verantwoordelijkheid neemt voor het verkrijgen van persoonsgegevens – de overdracht van casuïstiek vanuit de 21 deelnemende gemeenten – ontstaat er een duidelijke knip met de verantwoordelijkheden en het beleid van deelnemende gemeenten om te voldoen aan landelijke wet- en regelgeving rondom gegevensuitwisseling. Zo ook voor de gemeente Enschede. Dat brengt een zekere afhankelijkheid van (de kwaliteit van de uitvoering van) het IB-beleid van de SON met zich mee voor de gemeente Enschede: er kan door middel van het eigen gemeentelijk beleid geen grip meer worden uitgeoefend op de kwaliteit van gegevensuitwisseling terwijl het daar wel juridisch verantwoordelijk voor is.

20 DPIA staat voor Data Protection Impact Assessment. Een DPIA is verplicht op het moment dat het gebruik van persoonsgegevens in een organisatie mogelijk een hoog risico kan opleveren. Het uitvoeren van een DPIA is een verplichting die is opgenomen in de Algemene verordening gegevensbescherming (AVG), de Wet politiegegevens (Wpg) en de Wet justitiële en strafvorderlijke gegevens (Wjsg).

**Wat betekent dat voor de gemeenteraad van Enschede?**
Zoals in paragraaf 2.1 al vermeld, kunnen gemeenteraadsleden op grond van de AVG hun controlerende rol gebruiken om het beleidsplan van de gemeente Enschede te beoordelen op rechtmatigheid van de verwerking van persoonsgegevens. Aangezien de verwerkingsverantwoordelijkheid bij het college blijft bij mandatering van taken, is de controlevraag 'wie is verantwoordelijk' van belang. Heeft het college dit wel scherp en hoe wordt hier invulling aan gegeven?

De plicht onder de AVG om verantwoording af te leggen over de gekozen maatregelen om persoonsgegevens te beschermen geldt voor alle Nederlandse organisaties. Elke organisatie die werkt met persoonsgegevens moet dus een beleidsplan kunnen overleggen waarin maatregelen zijn vastgelegd om die persoonsgegevens te beschermen. Voor regionale samenwerkingsverbanden kan dat complex zijn. Niet elk samenwerkingsverband is immers een overheidslichaam met een regio-organisatie, waardoor het niet evident is dat de verantwoordingsplicht onder de AVG geldt of dat beleid automatisch wordt gedeeld met de samenwerkende gemeenten.

In het geval van de SON (wél een regio-organisatie) zien we dat het staande praktijk is dat er in het jaarverslag dat naar de raden van deelnemende gemeenten wordt gestuurd wordt gerapporteerd over de implementatie van het informatiebeveiligingsbeleid (IB-beleid), en dus maatregelen ter bescherming van persoonsgegevens. Maar bij het ZVH – een netwerkorganisatie en geen overheidslichaam – is er geen automatische rapportagelijn over de invulling van het privacy protocol naar de gemeenteraad van de gemeente Enschede, omdat de gemeente geen zitting heeft in de stuurgroep waaraan het jaarverslag wordt overlegd (zie ook paragraaf 3.2.2 voor een nadere uitwerking).

Dat betekent dat de gemeenteraad van de gemeente Enschede niet voor elk samenwerkingsverband waaraan de gemeente deelneemt beschikt over de benodigde informatie om de rechtmatigheid van gegevensuitwisseling te kunnen beoordelen, langs de lijnen van de drie hoofdvragen die onder paragraaf 2.1 genoemd staan. De raad kan op eigen initiatief wel verzoeken om informatie (over de verdeling van verantwoordelijkheden in het verwerken van persoonsgegevens) in specifieke samenwerkingsverbanden. Zeker in samenwerkingsverbanden waaraan geen GR ten grondslag ligt, en die dus geen overheidslichaam zijn, kan de raad zich scherp controlerend opstellen om de rechtmatigheid van gegevensuitwisseling te beoordelen.

### 3.2.2 Organisatie

*Regionaal: Stadsbank Oost Nederland*

Het DB is volgens het hiervoor beschreven IB-beleid integraal verantwoordelijk voor de beveiliging van informatie binnen de werkprocessen van de SON. Daartoe stelt het DB de kaders voor informatiebeveiliging en gegevensbescherming bestuurlijk vast op basis van landelijke en Europese wet- en regelgeving en normenkaders op het gebied van informatieveiligheid. Deze verantwoordelijkheid voor informatieveiligheid is overigens niet benoemd in de GR-tekst. Omdat het DB een rechtmatigheidsverantwoording moet afleggen over de jaarrekening, waaronder over informatiebeveiliging en privacy, komt informatiebeveiligingsbeleid wel regelmatig als onderwerp op de agenda van het DB.

Zoals gebruikelijk hebben het AB, het DB en de voorzitter een informatieplicht aan de gemeenteraad van elke deelnemende gemeente: alle door de raden verlangde inlichtingen moeten worden verstrekt, en gemeenteraden kunnen mondeling of schriftelijk verzoeken tot inlichtingen indienen. Het AB moet die inlichtingen op korte termijn – binnen een maand – verstrekken.

**Waarom is dit relevant voor de gemeenteraad van Enschede?**
De Enschedese raad ontvangt jaarlijks de jaarrekeningen en de rechtmatigheidsverantwoording over onderwerpen als informatiebeveiliging en privacy van de SON. Deze informatievoorziening stelt de gemeenteraad van Enschede in staat om zijn controlerende taken ten aanzien van de rechtmatigheid en zorgvuldigheid van gegevensuitwisseling binnen de SON te vervullen. Zoals gebruikelijk binnen GR's kan de gemeenteraad van Enschede via een zienswijzeprocedure sturen op verbetering van (de uitvoering van) het IB-beleid.

*Regionaal: Zorg- en Veiligheidshuis Twente*

In paragraaf 1.4 schetsten we de gelaagdheid van de organisatie van het ZVH en de verschillende betrokken gremia. Deze gelaagdheid heeft consequenties voor de sturingsmogelijkheden van de gemeente. Het heeft namelijk als resultaat dat de gemeente Enschede geen directe sturingsmogelijkheden heeft op het functioneren van het ZVH, maar dat dit via de bestuurders van andere gemeenten (de stuurgroep) gaat. Daarnaast is in een in 2023 uitgevoerde risicoanalyse privacy en informatieveiligheid[21] geconstateerd dat het van belang is om in de governance duidelijkheid te scheppen over waar de systeemverantwoordelijkheid voor het ZVH ligt; bij SamenTwente of bij de Veiligheidsregio Twente? Op het moment dat het diffuus is wie waarvoor verantwoordelijk is, geven partijen onvoldoende invulling aan de verantwoordelijkheden. Op basis van deze conclusies heeft de stuurgroep besloten om de volledige IT-infrastructuur voor de verwerking van persoonsgegevens over te hevelen naar VRT. De verantwoordelijkheid voor informatiebeveiliging ligt daarmee bij de VRT. Als onderdeel van deze herziene organisatievorm worden er momenteel een nieuw samenwerkingsconvenant en privacy protocol opgesteld. Deze herziene organisatievorm zal de spreiding van verantwoordelijkheden verminderen, maar heeft verder geen effect op de sturingsmogelijkheden van de gemeente.

Omdat het ZVH geen rechtspersoonlijkheid heeft, is het netwerk zelf geen partij in het convenant en het privacy protocol. Om deze reden blijven convenantpartners ieder zelfstandig verantwoordelijk om te voldoen aan alle wettelijke verplichtingen als zij gegevens delen bij de behandeling van casuïstiek.[22] In andere woorden: elke gemeente en elke ketenpartner dient zelf de 'basis op orde te hebben' als het gaat om risicobeheersing voor het delen van gegevens met of via het ZVH. Tot slot dient met de beheerder van de ICT-systemen (SamenTwente of de Veiligheidsregio) een verwerkersovereenkomst afgesloten te worden.

**Waarom is dit relevant voor de gemeenteraad van de gemeente Enschede?**

Vanwege de manier waarop de governance van het ZVH is ingericht, zijn er verschillende mogelijkheden voor de gemeenteraad om zowel kaderstellend als controlerend grip te houden op de kwaliteit van gegevensuitwisseling en de bescherming van persoonsgegevens binnen dit samenwerkingsverband:

1. ***Op de lokale schaal.*** In de eerste plaats geldt: elke partij binnen het ZVH is zelf verantwoordelijk voor rechtmatige en zorgvuldige gegevensverwerking en -deling. Vanuit zijn controlerende rol zal de raad er dus op moeten toezien dat de gemeente Enschede dat ook doet. Via zogenaamde ENSIA-rapportages[23], begeleidende raadsbrieven en een paragraaf in het financiële jaarverslag legt het bestuur van de gemeente Enschede verantwoording af aan de raad over de eigen rolinvulling bij het delen van persoonsgegevens. Zoals in het kader bij paragraaf 2.1 al werd aangegeven, kan de raad van de gemeente Enschede drie hoofdvragen stellen om de rechtmatigheid van de omgang met gegevensuitwisseling door de gemeente te beoordelen.
2. ***Op de schaal van de VRT.*** Omdat de systeemverantwoordelijkheid voor gegevensuitwisseling en informatieverwerking vanaf 2024 bij de VRT zal komen te liggen, kan de raad van de gemeente Enschede ook via de Veiligheidsregio Twente aansturen op rechtmatige en zorgvuldige informatiedeling binnen het ZVH. De VRT legt jaarlijks (financiële) verantwoording af aan alle gemeenten – inclusief de gemeente Enschede, maar in de jaarverslagen over 2022 en 2023 wordt niet expliciet gerapporteerd over privacy of rechtmatige gegevensuitwisseling. Dat is niet vreemd, omdat de VRT niet dagelijks en direct met persoonsgegevens werkt. De gemeenteraad zou via bijvoorbeeld een zienswijzeprocedure over de jaarverslagen, zoals gebruikelijk bij een GR, wel kunnen verzoeken om jaarlijks te rapporteren over privacy of informatieveiligheid. De raad stelt zich zo in staat ook jaarlijks zijn controlerende rol te kunnen pakken en te monitoren of de VRT de systeemverantwoordelijkheid voor gegevensuitwisseling binnen het ZVH ook pakt en risico's beheerst.

De beoordeling van de informatiebeveiliging van het ZVH ligt bij de stuurgroep. Omdat het college van de gemeente Enschede geen zitting heeft in deze stuurgroep, worden beleidsstukken en andere informatie niet direct gedeeld met de gemeenteraad. Dat maakt het voor de raad moeilijker om kaderstellend of controlerend op te treden als het gaat om de beveiliging van informatie die binnen het ZVH wordt gedeeld. Via de (verantwoording van de) VRT zou de gemeenteraad wel kunnen aansturen op informatievoorziening over het informatiebeveiligingsbeleid van het ZVH.

21 Berenschot (2023b).
22 Zie paragraaf 2.1.
23 ENSIA-rapportages, ook wel Eenduidige Normatiek Single Information Audit, helpen gemeenten om in één keer verantwoording af te leggen over informatieveiligheid gebaseerd op de normen die gelden voor de Nederlandse overheid, de BIO. Met ENSIA sluit de verantwoording over informatieveiligheid aan op de PDCA-cyclus van de gemeente. Hierdoor heeft het gemeentebestuur meer overzicht over de informatieveiligheid van hun gemeente en kan het beter sturen en verantwoording afleggen aan de gemeenteraad. (Bron: https://vng.nl/projecten/ensia).

*Lokale schaal: gemeente Enschede*

De gemeente hanteert de Three Lines of Defence-methodiek[24] om verantwoordelijkheden te beleggen in de organisatie. Hierin is het lijnmanagement (proceseigenaren) verantwoordelijk voor verwerkingsactiviteiten in het eigen organisatieonderdeel. In de context van dit onderzoek betekent dit ook dat het lijnmanagement de verantwoordelijkheid heeft om gegevensbescherming in samenwerkingsverbanden te borgen. De Chief Information Officer is verantwoordelijk voor concernbrede borging van privacy en naleving van de AVG; de gemeentesecretaris is ambtelijk eindverantwoordelijk voor de borging van privacy en naleving van de AVG. De portefeuillehouder blijft bestuurlijk eindverantwoordelijk hiervoor en draagt zorg voor verantwoording naar de gemeenteraad.[25] Deze verantwoordelijkheden worden op dezelfde manier toegepast voor het uitvoeren van DPIA's (Data Protection Impact Assessments) en het actueel houden van het verwerkingsregister (inclusief het sluiten van verwerkersovereenkomsten).[26]

De FG is verantwoordelijk voor het toezicht op de organisatie. Door middel van het jaarverslag rapporteert de FG over de stand van zaken en in het toezichtsplan stelt de FG de focusgebieden voor het komende jaar vast. Voor 2024 wordt het weergeven en in kaart brengen van alle samenwerkingsverbanden waarin de gemeenten Enschede deelneemt en de daarbij behorende datastromen expliciet benoemd als een van de focusgebieden.

**Waarom is dit relevant voor de gemeenteraad van de gemeente Enschede?**

Zoals eerder aangegeven legt het college van B en W met de bestuurlijke ENSIA-rapportages, de raadsbrief én met een aparte paragraaf in het jaarverslag verantwoording af aan de interne toezichthouder (de gemeenteraad) en aan de externe toezichthouders (het Rijk). De gemeenteraad komt door deze verantwoordings- en informatieplicht in de positie om te sturen op de rechtmatigheid of veiligheid van gegevensuitwisseling binnen de gemeente en tussen gemeente en partners – veelal partners binnen de gemeente.
Verdere positionering van de raad voor de invulling van zijn controlerende rol is mogelijk door raadsvragen en, op verzoek, informerende presentaties aan de raad.

24 Het Three Lines of Defence-model heeft als doel om de risicobeheersing in een organisatie vorm te geven. Er worden verschillende functies geïdentificeerd: eerstelijns, tweedelijns en derdelijns. De eerstelijnsfunctie gaat over beheersing in de werkprocessen. Afdelingshoofden/-managers zijn hierbij verantwoordelijk voor het halen van gestelde doelen, het aansturen van medewerkers en het managen van risico's. De tweedelijnsfunctie is ondersteunend aan de eerste lijn door beleid, kaders en technologie beschikbaar te stellen. Tweedelijnsrollen omvatten specialistische kennis op relevante gebieden, denk aan privacy officers. De derde lijn is de interne toezichtsfunctie. Hier wordt ook de werking van de eerste en tweede lijn getoetst. In dit geval is dat de FG.

25 Gemeente Enschede (2022). *Strategisch informatiebeveiligings- en privacybeleid Enschede 2022 tot en met 2025*.

26 Gemeente Enschede (2023). *Beleid en procedure DPIA's.*
Gemeente Enschede (2023). *Procedure actueel houden verwerkingsregister.*

### 3.2.3 Ambities

*Regionaal: Stadsbank Oost Nederland*

De SON richt zich in het beleid specifiek op de zwakste schakel in de informatieveiligheidsketen: de mens. Het gedrag van medewerkers bij de uitvoeringsorganisatie met een relatief kleine staf wordt gezien als het grootste risico. Het streven is daarom om medewerkers in het kader van informatieveiligheid daarom bewust bekwaam te maken. Het IB-beleid vormt de basis voor zorgvuldige omgang met gegevensbescherming of informatiebeveiliging in de eigen rol en taak van SON-medewerkers.

*Regionaal: Zorg- en Veiligheidshuis Twente*

Het ZVH stelt geen eigenstandige ambities over de aard van gegevens die worden gedeeld, de doelstelling van gegevensuitwisseling of het type casuïstiek dat wel en niet moet worden behandeld aan regionale casustafels. Het ZVH ziet zijn regionale opdracht vooral als faciliterend, regisserend en signalerend ter ondersteuning van de ketenpartners als die vanuit hun eigen taak, positie en reguliere processen geen oplossing kunnen bieden voor bepaalde casuïstiek.

Het ZVH stelt wel – zij het impliciet - ambities voor (aan de stuurgroep) over de uitvoering van het werkproces om regie te voeren. Het ZVH geeft daarbij aan dat privacy een belangrijk thema is: 'voor een netwerkorganisatie is het essentieel dat diverse partijen gevoelige persoonsgegevens doelmatig en veilig met elkaar kunnen uitwisselen'.[27] De ambities zijn niet nader geconcretiseerd, maar de eerder benoemde organisatiewijziging heeft ten doel om zo zorgvuldig mogelijk met persoonsgegevens om te gaan.

*Lokale schaal: gemeente Enschede*

De gemeente ziet in dat digitale ontwikkeling risico's met zich meebrengt en dat het noodzakelijk is om deze risico's te beperken. In het strategisch informatiebeveiligings- en privacybeleid staat de missie beschreven: 'Wij zijn transparant over de verwerking van (persoons)gegevens en staan voor een rechtmatige en veilige verwerking daarvan.'. De missie geldt voor de gemeente zelf, maar er wordt ook verwacht dat partijen waarmee de gemeente Enschede gegevens uitwisselt of die gegevens voor de gemeente Enschede verwerken, hieraan voldoen. Er wordt verdere invulling aan de missie gegeven volgens een aantal speerpunten.

27 Jaarverslag Zorg- en Veiligheidshuis Twente 2023.

Met betrekking tot privacy en het beschermen van persoonsgegevens zijn de volgende speerpunten relevant vanuit de gemeente Enschede:

- **Wij zetten de betrokkenen en belanghebbenden centraal**
  Voor de inrichting van onze informatiehuishouding staan de betrokkenen en belanghebbenden centraal. Informatie wordt op de juiste wijze en rechtmatig verwerkt met daarbij passende beveiliging, zodat wij de betrokkenen en belanghebbenden de beschikbaarheid, integriteit en vertrouwelijkheid die zij mogen verwachten, kunnen bieden.

- **Wij beperken risico's voor betrokkenen en belanghebbenden zo veel mogelijk**
  Wij zorgen ervoor dat risico's voor betrokkenen en belanghebbenden zo laag mogelijk zijn en blijven. Hiervoor voeren wij risicoanalyses en audits uit die in wet- en regelgeving staan beschreven. Daarnaast volgen wij actief Europese, Nederlandse, lokale en interne ontwikkelingen. Wij nemen passende organisatorische en technische maatregelen.

- **Wij hebben privacy en informatieveiligheid verankerd in de organisatie**
  Informatieveiligheid en privacy zijn op strategisch, tactisch en operationeel niveau onderdeel van (dagelijkse) besluitvorming en uitvoering. Wij passen de Plan-Do-Check-Act-cyclus toe om te verbeteren door leren en ervaring. Wij zijn ons bewust van de mogelijke impact op en het risico voor betrokkenen en belanghebbenden. Wij zijn in staat een bewuste keuze te maken waarbij de normen en uitgangspunten van de BIO en de AVG zijn geborgd. Wij vinden verantwoord en bewust gedrag van medewerkers van wezenlijk belang voor de borging van de BIO en de AVG.

- **Wij zien informatie als één van de belangrijkste bedrijfsmiddelen**
  Beschikbare, integere en vertrouwelijke informatie is de fundering voor onze dienstverlening. Een betrouwbare informatievoorziening is dan ook noodzakelijk voor het goed functioneren van de gemeentelijke organisatie. Informatiebeveiliging en privacy zijn dan ook essentiële bouwstenen voor de verbetering van onze dienstverlening.

**Samenvattend**

- ***De gemeente Enschede heeft beperkte sturingsmogelijkheden 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 langetermijnvisies en informatiebeveiligingsbeleid bestuurlijk worden bekrachtigd door een afvaardiging van de convenantspartijen. Dat maakt het lastiger voor de gemeente om erop toe te zien dat het ZVH de wet- en regelgeving naleeft die van toepassing is op de gemeente én om het eigen ambitieniveau voor het voetlicht te brengen bij andere convenantspartijen als referentiekader. Dat zou de gemeente Enschede in theorie kunnen doen in het DB/AB van de VRT (waar systeemverantwoordelijkheid in 2024 zal worden belegd), maar het is onbekend of dienstverleningsovereenkomsten aan derden hoog op de agenda staan.
- ***De gemeente Enschede heeft veel sturingsmogelijkheden om (de uitvoering van) het informatieveiligheidsbeleid van de SON te monitoren en te verbeteren.***
  De gemeente Enschede heeft wel mogelijkheden om de SON verantwoording te laten afleggen over de kwaliteit of de risico's van gegevensuitwisseling. De gemeente Enschede is vast lid van het DB van de SON, dat bestuurlijke verantwoordelijkheid draagt voor de (kwaliteit van) 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 IB-beleid op het gebied van informatieveiligheid te beoordelen. Omdat het DB ook bestuurlijk vaststeller is van het IB-beleid, kan Enschede in theorie ook zelfstandig wijzigingen voorstellen als die nodig worden geacht.

**Waarom is dit relevant voor de gemeenteraad van Enschede?**

De ambities die de gemeente Enschede en regionale samenwerkingsverbanden vastleggen vormen de principes waarmee wordt gewerkt om gegevensuitwisseling veilig en rechtmatig te houden. Hoewel ze vaak zijn ingegeven vanuit de geest van landelijke wet- en regelgeving, is er sprake van accentverschillen. De raad van de gemeente Enschede zou – bij de uitoefening van zijn controlerende rol zoals hierboven weergegeven – kunnen aansturen op de aansluiting tussen lokale en regionale ambities. Omdat verantwoordelijkheden voor veilige gegevensuitwisseling zijn verdeeld tussen de gemeente en samenwerkingsverbanden, en er sprake is van wederzijdse afhankelijkheid, is aansluiting belangrijk. Zijn de accenten die de gemeente Enschede legt gelijk aan de principes die de samenwerkingsverbanden naleven als het gaat om gegevensuitwisseling? Zijn regionale samenwerkingsverbanden even ambitieus als de gemeente Enschede als het gaat om gegevensbescherming?
Of doet Enschede er goed aan om principes over te nemen van regionale samenwerkingsverbanden waar gegevensuitwisselingsbeleid 'op orde' lijkt? Aan de hand van dit type vragen kunnen raadsleden sturen op een logische aansluiting tussen de mate van ambitie en de gekozen accenten. De samenwerking in de regio kan zo ten dienste staan van het realiseren van lokale (stevige) ambities op het gebied van informatieveiligheid.

HOOFDSTUK 4

# Gegevensuitwisseling in de praktijk

In het voorgaande hoofdstuk is beschreven hoe de beleidskaders er uitzien. In dit hoofdstuk beschrijven we hoe dit zich uit in de praktijk en waar dit mogelijk resulteert in risico's. Kortom: wat is het gevolg van het samenspel tussen de verschillende bestuurlijke schalen in de praktijk? We gaan achtereenvolgens in op de onderwerpen legitimiteit, organisatie en ambitie.

## 4.1 Legitimiteit

De nationale, regionale en lokale kaders dragen zorg voor het naleven van de geldende wet- en regelgeving en hiermee voor bescherming van persoonsgegevens. In deze paragraaf beschrijven we verschillende aspecten die invloed hebben op het legitieme handelen van de gemeente.

### Bevindingen documentenstudie en gesprekspartners

Zoals beschreven in paragraaf 3.2.1, is er in 2022 en 2023 nieuw beleid geformuleerd rondom het thema gegevensbescherming. Het strategisch informatiebeveiliging- en privacybeleid vormt het overkoepelende beleidskader. De verantwoordelijkheden zoals beschreven in het beleidskader gelden ook voor gegevensverwerkingen met externe partijen.[28] Er wordt echter niet gespecificeerd hoe dit wordt geborgd in de governance of hoe de grip op de uitvoering in die context wordt bewaard. Dit wordt ook niet in andere beleidsdocumenten beschreven. Het strategisch informatiebeveiliging- en privacybeleid is niet doorvertaald naar tactisch of operationeel niveau voor de verschillende domeinen.

Gesprekspartners geven aan dat het per medewerker verschilt in welke mate het beleid leeft in lijnafdelingen en of medewerkers in de uitvoering bekend zijn met vereisten van legitieme gegevensuitwisseling (zie ook paragraaf 4.2). Dit zien we bijvoorbeeld terug in de achterstand op samenwerkingsverbanden die zijn opgenomen in het verwerkingsregister en in het aantal risicoanalyses (DPIA's) voor samenwerkingsverbanden.[29] Daarnaast is het onbekend of er altijd actuele verwerkingsovereenkomsten zijn afgesloten, omdat deze niet centraal opgeslagen worden. Gesprekspartners geven aan dat een mogelijke oorzaak is dat proceseigenaren beperkt zicht hebben op de aanwezigheid en de actualiteit van verwerkersovereenkomsten en risicoanalyses en dat het afsluiten van actuele overeenkomsten hierdoor geen prioriteit heeft. De oorzaak hiervoor kan ook liggen in de afstand tussen proceseigenaren (clustermanagers) en de medewerkers die de daadwerkelijke uitvoering moeten doen. In het jaarverslag van de FG worden de bovenstaande achterstanden expliciet als aandachtspunt benoemd en ook in het toezichtsplan 2024 van de FG wordt hier aandacht aan besteed.[30]

28 Strategisch informatiebeveiliging- en privacybeleid, pagina 5.

29 Jaarverslag Functionaris Gegevensbescherming 2023 (2024).
30 Jaarverslag Functionaris Gegevensbescherming 2023 (2024). Toezichtsplan Functionaris Gegevensbescherming 2024 (2024).

Een ander signaal waaruit blijkt dat beleid nog beperkt leeft op operationeel niveau, is dat lijnmedewerkers beperkt bewust zijn van de verantwoordelijkheden die bij hen zijn belegd in het beleid. Gesprekspartners geven aan dat de verwachting bestaat dat 'randvoorwaardelijke' aspecten, zoals gegevensbescherming, ingeregeld zijn door de organisatie (lees: privacy officers en de FG). Er is beperkt besef dat het borgen van deze randvoorwaarden onder de eigen verantwoordelijkheid valt. Hierbij benoemen privacy officers en de FG wel dat het besef van het belang van gegevensbescherming toe lijkt te nemen en dat medewerkers ook bereid zijn hiertoe in actie te komen. Hierbij geven gesprekspartners aan dat het MT van het sociaal domein zich sterk inzet voor gegevensbescherming, bijvoorbeeld door het programma 'zorgvuldig werken in het sociaal domein' op te zetten. Ook dit kan overigens wijzen op een afstand tussen de proceseigenaren (clustermanagers) en de uitvoerende medewerkers, omdat de operationele invulling achterblijft op het uitgesproken commitment. Een kanttekening is dat de inzet per domein van de gemeente wat betreft gegevensbescherming verschilt. Andere domeinen hebben hier nog geen invulling aan gegeven en maken gebruik van het programma van het sociaal domein. Deze domeinen hebben echter ook minder te maken met individuele persoonsgegevens dan in het sociaal domein.

De directie lijkt zich in enige mate bewust te zijn van het achterblijven van operationele invulling. Zo worden bewustwording en kennisdeling in gesprekken als twee belangrijke succesfactoren voor gegevensbescherming gezien. Er worden actief acties gepleegd om deze beide factoren te vergroten in de organisatie.

Tot slot geven gesprekspartners aan dat de 'check' op naleving nauwelijks plaatsvindt, waardoor er beperkt op wordt toegezien of het beleid ook daadwerkelijk tot uitvoering wordt gebracht. In het strategisch informatiebeveiligings- en privacybeleid staat er een verbeterproces (PDCA-cyclus) beschreven om de vertaling van beleid naar uitvoering te controleren en verbeteren. Het is daarnaast de verantwoordelijkheid van de directie om hierop te sturen zodat er verantwoording kan plaatsvinden over de naleving van het beleid. Uit gesprekken blijkt dat ook dit beperkt gebeurt.

### Analyse Berenschot

Per 2022-2023 heeft een flinke beleidsmatige inhaalslag plaatsgevonden met betrekking tot de omgang met persoonsgegevens door de gemeente. Hierdoor is er een kader gecreëerd voor de omgang met persoonsgegevens en hoe de gemeente hier grip op beoogt te houden. Dit is echter niet bij alle medewerkers in het sociaal domein even goed bekend.[31] Hierdoor ontstaat er een gat tussen het strategisch beleid en de operationele invulling hiervan. Dit zien we enerzijds terug in beperkte kennis van verantwoordelijkheden zoals beschreven in het beleid en anderzijds in onbekendheid met wat er wel en niet mag met betrekking tot gegevensuitwisseling (meer hierover in paragraaf 4.2). De oorzaak voor het achterblijven van operationele invulling lijkt echter eerder in onbekendheid te liggen dan in onwil.

De gemeente Enschede hanteert het Three Lines of Defence-model voor de inrichting van de informatiebeveiligings- en privacyorganisatie. Dit model definieert drie niveaus waarop de organisatie ingericht kan worden: de eerste lijn is verantwoordelijk voor de interne beheersing van privacy en informatiebeveiliging (lijnmanagers), de tweede lijn ondersteunt de eerste lijn door middel van risicosignalering, het ontwikkelen van beleids- en beheersinstrumenten en adviseert over procesvoering en uitvoering van evaluaties. De derde lijn voorziet de directie van zekerheid over de kwaliteit van sturing en beheersing en rapporteert over inconsistenties van de controls. De aanwezigheid van het beleid is een goed begin, maar zonder controle op de uitvoering is het onzeker of gegevensbescherming geborgd is. In de lijnafdelingen leeft het besef onvoldoende dat de toegewezen verantwoordelijkheid voor borging van informatieveiligheid en privacy in het eigen organisatieonderdeel dient plaats te vinden. Het betekent ook dat hier op gecontroleerd moet worden, maar dat dit onvoldoende gebeurt. Dit heeft als resultaat dat er een blinde vlek ontstaat: het is onduidelijk of gegevensbescherming in de praktijk tot uitvoering wordt gebracht, en waar de mogelijke knelpunten zitten. Er wordt veelal naar de FG gekeken voor deze controlefunctie. Dit is zorgelijk, omdat de controlefunctie in het verbeterproces niet behoort bij de taken van de derde lijn (de FG) maar tot de eerstelijnsrol en daarmee de verantwoordelijk lijnmanager.[32] De controle valt dus buiten de scope van de functie van de FG.

31 Vanwege de geselecteerde casussen is enkel het sociaal domein van de gemeente onderzocht. Het is voor de onderzoekers onbekend hoe andere domeinen binnen de gemeente omgaan met persoonsgegevens, aangezien dit buiten de scope van het onderzoek valt.

32 Gemeente Enschede (2022). *Strategisch informatiebeveiligings- en privacybeleid 2022 tot en met 2025.* Pagina 15.

De bovenstaande beelden lijken voornamelijk voort te vloeien uit een mismatch tussen beleid enerzijds en anderzijds de mate waarin dit beleid leeft en bekend is bij de betreffende ambtenaren. De directie lijkt in enige mate bewust van deze mismatch. Zo worden bewustwording en kennisdeling door de directie als twee belangrijke succesfactoren voor gegevensbescherming gezien. Er worden actief acties gepleegd om deze beide factoren te vergroten in de organisatie. Het is echter wel van belang om te benadrukken dat enkel het plegen van acties rondom bewustwording en kennisdeling een beperkte impact heeft op bescherming van gegevens, als er vanuit de directie niet actief wordt gestuurd op naleving van het beleid en het invullen van de rollen en verantwoordelijkheden die daarin zijn vastgelegd. Op dit moment is die actie nodig om als gemeente Enschede meer grip te krijgen op de gegevensuitwisseling in samenwerkingsverbanden.

**Samenvattend**

- Er heeft in 2022-2023 een flinke beleidsmatige inhaalslag plaatsgevonden in bescherming van persoonsgegevens in de gemeente Enschede. Dit is met name op strategisch niveau, er is geen tactische/operationele vertaling naar de verschillende domeinen.
- Het beleidskader, inclusief verantwoordelijkheden, is niet bij alle medewerkers even goed bekend. Dit resulteert in een gat tussen het strategisch beleid enerzijds en de operationele invulling hiervan anderzijds.
- De naleving van het beleid wordt beperkt gecontroleerd door het management. Hierdoor is er geen zicht op mogelijke risico's.

## Risico's

De bovenstaande paragrafen laten een aantal elementen zien waarin de praktijk afwijkt van de vastgestelde kaders. Hierdoor ontstaan risico's voor onveilige gegevensuitwisseling. In de volgende tabel weergeven we een aantal geconstateerde risico's wat betreft legitimiteit.

**Relevantie voor de gemeenteraad van de gemeente Enschede**

Volgens onze analyse zit de gemeente Enschede midden in een professionaliseringsslag als het gaat om de uitvoering van beleid voor gegevensuitwisseling waar de gemeente zelf aan de lat staat. De raad kan op twee manieren de voortgang van deze professionaliseringsslag volgen en de uitkomsten beoordelen:

- Binnen de eigen gemeente kunnen raadsleden een controlerende rol pakken wanneer de raad wordt geïnformeerd over de stand van zaken door middel van ENSIA-rapportages, maar de raad kan ook specifieke informatieverzoeken uitvaardigen om de gevolgen op verschillende beleidsterreinen te duiden.
  - Het Rathenau Instituut heeft een denkkader voorgesteld voor raadsleden om digitaliseringsvraagstukken te ontrafelen, zonder in de details van beleidsuitvoering te hoeven duiken. Dat denkkader en de bijbehorende vragen kunnen ook worden toegepast op de uitvoering van beleid omtrent veilige gegevensuitwisseling (*Rathenau, 2020*).
- Het overzicht van 'verbonden partijen' of samenwerkingsverbanden waar de gemeente Enschede aan deelneemt helpt raadsleden om te beoordelen op welke wijze en in welke reguliere regionale (verantwoordings)procedures zij vragen kunnen stellen of zienswijzen kunnen uiten over veiligheid van gegevensuitwisseling. De rechtsvorm van het samenwerkingsverband is daarbij bepalend: de jaarlijkse verantwoordingsplicht van gemeenschappelijke regelingen nodigt uit om die procedures in werking te laten treden, terwijl de gemeenteraad bij regionale netwerksamenwerking (zoals in het ZVH, want deze staat niet in het overzicht van samenwerkingsverbanden) actiever om informatievoorziening over IB-beleid zal moeten verzoeken. Dit geldt ook voor andere samenwerkingsvormen zoals bedrijven en stichtingen.

| Geconstateerde risico's | Mogelijke impact |
|---|---|
| DPIA's worden niet (tijdig) uitgevoerd voor gegevensstromen naar/in samenwerkingsverbanden | De gemeente heeft geen inzicht in mogelijke risico's en treft geen mitigerende maatregelen.<br>De gemeente voldoet niet aan de wettelijke vereisten van de AVG |
| Niet voor alle verwerkingen met samenwerkingsverbanden is een verwerkingsovereenkomst afgesloten en opgenomen in het verwerkingsregister | Onrechtmatige gegevensverwerking<br>De gemeente voldoet niet aan de wettelijke vereisten van de AVG |
| Er wordt beperkt invulling gegeven aan eerstelijns verantwoordelijkheden in de gemeentelijke organisatie | Geen zicht op naleving van wet- en regelgeving door de gemeente<br>Incidenten worden niet gesignaleerd<br>Incidenten worden niet gemeld |
| Er is beperkt toezicht op operationele invulling van gegevensbescherming in de samenwerkingen met samenwerkingsverbanden | Risico's worden niet gesignaleerd<br>Incidenten worden niet gesignaleerd<br>Geen toezicht op de rechtmatigheid van gegevensverwerking |

## 4.2 Organisatie

In deze paragraaf gaan we in op de invulling van de organisatie aan gegevensbescherming. Zijn de gemeente en haar medewerkers in staat invulling te geven aan het beleid en hoe wordt dit georganiseerd? We gaan enerzijds in op de invulling binnen de gemeente (lokaal) maar anderzijds ook op de organisatie vanuit de gemeente binnen de regionale context.

De bevindingen zijn grofweg op te splitsen in twee aspecten: 1) in wat gegevensbescherming in de regionale context is en 2) hoe in de organisatie wordt gestuurd op gegevensbescherming in de regionale context. De 'wat'-vraag heeft een menselijk aspect: hebben medewerkers de kennis om op een juiste wijze te handelen en hebben ze de middelen om hier invulling aan te geven? De 'hoe'-vraag is vervolgens meer van organisatorische aard: zijn de juiste mechanismen in plaats en wordt er gestuurd op naleving?

### Bevindingen documentenstudie en gesprekken

#### *Verantwoorde gegevensuitwisseling*

Uit gesprekken blijkt dat project- en beleidsmedewerkers van de gemeente niet altijd weten wat verantwoorde gegevensuitwisseling exact inhoudt. Betrokkenen geven aan dat de oorzaak hiervan tweeledig is. Ten eerste zijn er verschillende relevante juridische kaders, waardoor het als onoverzichtelijk wordt ervaren wat de juridische eisen zijn. Daarnaast verschilt het per samenwerkingsverband wat wel/niet mag en wat je daarvoor geregeld moet hebben (dit ligt veelal aan het wel/niet hebben van rechtspersoonlijkheid maar ook aan het beleidsdomein). Hierdoor is het voor betrokkenen onduidelijk wanneer er gegevens gedeeld mogen worden, en wat hiervoor nodig is (denk bijvoorbeeld aan wettelijke grondslag maar ook aan het sluiten van een verwerkersovereenkomst). Een voorbeeld hiervan dat in gesprekken naar voren kwam, is dat er soms vraagtekens worden geplaatst bij het doel van sommige overleggen over casussen binnen het ZVH. De overwegingen om gevoelige en soms zelfs bijzondere of strafrechtelijke gegevens uit te wisselen aan een tafel met diverse ketenpartners zijn niet altijd – voorafgaand aan een overleg - scherp gesteld of niet meer actueel. Omdat het ZVH geen rechtspersoonlijkheid heeft en betrokkenen zelf verwerkingsverantwoordelijke zijn, blijven zij ook zelf verantwoordelijk voor de juiste gegevensuitwisseling (inclusief grondslag).

Als er veel partners uit verschillende domeinen betrokken zijn, en er daarmee een breder palet is aan mogelijke doelen voor het uitwisselen van gegevens, staat de doelbinding[33] onder druk. Het is mogelijk dat er gegevens worden verwerkt terwijl deze verwerkingen niet overeenkomen met de grondslag waarvoor ze verzameld zijn. Daarnaast kan hiermee niet gegarandeerd worden of de doelbinding van de bewaarde gegevens op de juiste manier wordt gehandhaafd. Deze onzekerheid geldt ook voor de deelnemers van overleggen. Het is niet altijd duidelijk of alle deelnemers daadwerkelijk de juiste grondslag hebben om toegang te hebben tot de gedeelde gegevens. Doordat de gegevensuitwisseling op afstand van de gemeentelijke organisatie plaatsvindt, is er beperkt zicht op een juiste naleving van de vereisten. Een van de gevolgen van de afstand die wordt genoemd is dat betrokken beleidsmedewerkers zich in mindere mate verantwoordelijk voelen voor de praktijk van gegevensuitwisseling binnen een samenwerkingsverband.

Gesprekspartners geven aan dat betrokkenen, door de afstand of door beperkte kennis van wat exact wel of niet mag, dergelijke signaleringen maar beperkt doorgeven in de gemeentelijke organisatie. Doordat dergelijke signaleringen echter niet worden doorgegeven, worden ze niet opgepakt en staan ze ook niet op de agenda van de directie of het bestuur. Hierdoor doet zich volgens gesprekspartners geen urgente casuïstiek voor die de gemeente 'wakker zou schudden' om meer of concreter te sturen op verbeteringen in het IB-beleid van de samenwerkingsverbanden.

#### *Ondersteuning voor het naleven van verantwoordelijkheden*

Naast dat betrokkenen niet altijd weten wat verantwoorde gegevensuitwisseling exact inhoudt, is het ook van belang dat zij ondersteund worden om er de juiste invulling aan te kunnen geven. Dit raakt aan de 'hoe'-vraag: hoe vindt de ondersteuning en borging vanuit de organisatie plaats? Dit kan zowel door technologische ondersteuning (denk aan software en autorisaties) als door inhoudelijke ondersteuning (denk aan privacy officers).

33 Wanneer er sprake is van doelbinding bedoelen we daarmee dat een organisatie (persoons)gegevens alleen verzameld en verwerkt met een gerechtvaardigd doel. Gegevens mogen dus bijvoorbeeld onder de AVG niet zomaar verzameld worden.

Het eerste voorbeeld gaat over het borgen van vertrouwelijkheid van gegevens. Medewerkers van de gemeente kunnen twee petten op hebben; die van hulpverlener en die van ambtenaar. Beide rollen zouden toegang tot andere gegevens moeten hebben. Dit komt doordat ambtenaren een andere grondslag hebben voor gegevensverwerking dan hulpverleners in de samenwerkingsverbanden, vanwege de verschillende rollen en bijbehorende geheimhoudingsplicht.[34] In gesprekken werd het voorbeeld genoemd van zorgverleners die ook de toegeleiding doen.[35] Toeleiden is een taak van de gemeente, waardoor de zorgverlener een 'ambtenarenpet' op heeft. Dit resulteert in een situatie waar zij al naar gelang de 'pet' die zij op dat moment op hebben, toegang tot andere gegevens mogen hebben. Systemen moeten voldoende technische mogelijkheden hebben om verschillende autorisaties toe te staan, al naar gelang de rol. In het systeem voor de uitvoering van de Wmo en jeugdzorg bleek hier bijvoorbeeld onvoldoende mogelijkheid toe te zijn. De afbakening van de gegevens op basis van de rollen is niet scherp genoeg. Wel blijkt uit de gesprekken dat, nadat er een DPIA was uitgevoerd, deze mogelijkheid als eis is opgenomen in de aanbesteding voor een nieuw systeem. Gesprekspartners geven echter ook aan dat het de vraag is of desbetreffende medewerkers zich geheel bewust zijn van de verschillende grondslagen tot gegevensverwerking, en wat dit betekent. Om de betreffende medewerkers hierin te ondersteunen, maar ook om veilige gegevensverwerking te waarborgen, is een systeem met de juiste autorisaties noodzakelijk. Mede vanwege dit voorbeeld hebben de privacy officers van Werk en inkomen en Wijkteams het programma 'zorgvuldig werken in het sociaal domein' opgezet, met ondersteuning en handvaten voor de betreffende lijnafdelingen. In andere domeinen van de gemeente bestaan dergelijke programma's niet, maar wordt, zoals eerder benoemd, wel gebruik gemaakt van dit programma. Gesprekspartners geven ook aan dat het bewustzijn van de verschillende vereisten wel groeiende is bij medewerkers.

Daarnaast is het van belang dat medewerkers inhoudelijk ondersteund worden. In het beleid staat beschreven dat privacy officers hier een belangrijke taak in hebben.[36] Uit gesprekken blijkt echter dat medewerkers de privacy officers nog onvoldoende weten te vinden om gebruik te maken van hun ondersteuning en expertise. Vanuit privacy officers wordt hierover gecommuniceerd, bijvoorbeeld met de 'infographic privacyvragen'. Maar ook de privacy officers geven aan dat het uiteindelijk aan de medewerker zelf is om ondersteuning aan te vragen. Een van de oorzaken die wordt genoemd voor de achterblijvende ondersteuning met betrekking tot samenwerkingsverbanden is de huidige organisatie-inrichting. Privacy officers zijn gebonden aan een beleidsdomein, zoals Werk en inkomen of Wijkteams. Samenwerkingsverbanden bevinden zich echter veelal op het snijvlak van meerdere domeinen, denk aan het veiligheidsdomein en het sociaal domein in het Zorg- en Veiligheidshuis. Hierdoor hebben privacy officers minder zicht op de activiteiten van samenwerkingsverbanden en kunnen ze beperkt proactieve ondersteuning bieden. Eventuele ondersteuning vanuit de privacy officers blijft hierdoor vraaggericht waardoor er niet altijd een privacy officer wordt betrokken.

### *Sturing op regionale gegevensuitwisseling*

De bovenstaande bevindingen gingen in op de kennis van medewerkers van de gemeente Enschede met verantwoorde gegevensuitwisseling. In de praktijk heeft de medewerker echter geen controle over alles, en is het ook van belang dat de organisatie van het samenwerkingsverband zelf is gericht op verantwoorde gegevensuitwisseling. Zoals eerder beschreven, verschilt het per vorm van samenwerking welke mogelijkheden tot sturing de gemeente hierop heeft. Een GR (de zwaarste juridische vorm van samenwerking in een regio) biedt de mogelijkheid voor gemeenten om via het DB en het AB toe te zien op de juiste uitvoering van overgedragen taken. Deze samenwerkingsverbanden hebben een gezamenlijke verwerkingsverantwoordelijkheid en zijn daarom verantwoordelijk voor de omgang met persoonsgegevens. De GR heeft hierbij ook een verantwoordingsplicht aan het bestuur, waarbij vanuit de organisatie gekozen kan worden om dit ook actief op het thema organisatieveiligheid in te vullen.[37] Een dergelijke organisatievorm van een samenwerkingsverband geeft de gemeente Enschede ruim baan om bestuurlijk aan te sturen op verbetering van (de uitvoering van) het IB-beleid indien dat nodig of wenselijk is. Uit gesprekken blijkt echter, in de context van de SON, dat het bestuur van de gemeente Enschede hier (onder andere wat betreft gegevensbescherming) geen gebruik van maakt.

34 Een ambtenaar mag gegevens van de burger verzamelen, maar enkel in relatie tot de uit te voeren wettelijke taak (doelbinding). Zorgverleners mogen daarentegen veel breder gegevens verzamelen om de zorgvraag compleet te krijgen. Zorgverleners hebben om deze reden ook een verregaandere zwijgplicht. Een ambtenaar heeft wel geheimhouding, maar bijvoorbeeld ook de zogenaamde 'klikplicht' (de verplichting om direct een melding te doen als zij/hij een misdrijf of fraude constateert).

35 Gemeenten en zorgverleners kunnen burgers of patiënten toeleiden naar zorg of begeleiding die past bij de aard van hun problematiek. Toeleiden gebeurt meestal wanneer een zorgverlener of ambtenaar in bijvoorbeeld het sociaal domein signaleert dat iemand hulp nodig heeft en hier zelf (nog) niet de noodzakelijke hulp voor heeft gevraagd.

36 Strategisch beleidskader Informatiebeveiliging en privacy, pagina 15 (2022).

37 De herziene Wgr schrijft voor dat het DB en het AB een rechtmatigheidsverklaring moeten afleggen over de jaarrekening (en niet, zoals in het verleden, de accountant). Dit dwingt het bestuur om stil te staan bij onderwerpen als informatiebeveiliging.

Op het moment dat een samenwerkingsverband geen eigen rechtspersoon is (zoals bij het ZVH), blijft de gemeente Enschede verwerkingsverantwoordelijke als convenantpartij. Deze situatie vraagt om een stevigere aansluiting tussen het beleid van de gemeente Enschede en dat van het samenwerkingsverband, om te borgen dat het beleid van de gemeente wordt nageleefd in de uitvoering in het samenwerkingsverband. Uit gesprekken blijkt dat hier beperkt bewustzijn van is bij de gemeente Enschede – zowel ambtelijk als bestuurlijk.

Naast bestuurlijke sturing, kan het samenspel tussen gemeente en 'regio' plaatsvinden aan een ambtelijke tafel of overleg. Binnen de SON vindt dit bijvoorbeeld plaats aan een laagdrempelige beleidstafel, waar vooral de FG's van de drie grootste gemeenten – waaronder Enschede – regelmatig kennis en ervaringen met elkaar uitwisselen. De opbrengsten van die uitwisseling en de signaleringsfunctie van deze tafel zijn een belangrijke bron voor het beleid en de tactische/operationele vertaling hiervan. Het ZVH kent een dergelijke tafel niet voor overkoepelende beleidsthema's (waar gegevensbescherming onder zou kunnen vallen), waardoor de gemeente Enschede de signaleringsfunctie mist voor eventuele risico's.

## Analyse Berenschot

De juiste omgang van medewerkers met gegevens is essentieel. Als hier onvoldoende afspraken over zijn gemaakt en/of de betreffende personen zich onvoldoende bewust zijn van de situatie waarin zij zich bevinden, vormt dit een groot risico voor de organisatie. De extra inzet van privacy officers specifiek op het sociaal domein laat zien dat de organisatie zich wel bewust is van dit risico. Daarnaast worden operationele knelpunten (zoals software) al opgepakt door de organisatie. Zoals eerder al kort benoemd, zien we dat, op het moment, de situatie minder overzichtelijk wordt (bijvoorbeeld door meer betrokkenen of meerdere typen gegevens), de doelbinding voor het verwerken van gegevens snel onder druk komt te staan (bijvoorbeeld in overleggen binnen het ZVH). De context van samenwerkingsverbanden is echter vaak complex door de vele betrokkenen en verschillende domeinen. Zeker op het moment dat het samenwerkingsverband enkel een netwerk is en geen organisatie die hier zelf verantwoordelijk voor is, resulteert dit soms in onoverzichtelijke situaties. Mogelijke risico's worden vervolgens echter niet gesignaleerd richting de gemeentelijke organisatie. Hierdoor leeft het besef niet in de gemeente dat hier meer op gestuurd kan of moet worden, enerzijds vanuit de ambtelijke organisatie in de vorm van afspraken en anderzijds vanuit het bestuur richting een stuurgroep of AB/DB.

Daarnaast heerst de perceptie binnen de gemeentelijke organisatie dat het samenwerkingsverband de verantwoordelijkheid heeft om afspraken over gegevens-uitwisseling te beoordelen en verantwoorden. Dit verschilt per juridische vorm van het samenwerkingsverband, maar de eigen verantwoordelijkheden van de gemeente Enschede - bijvoorbeeld als convenantspartij - staan hierbij niet scherp voor de geest. Dit zien we terug in het gebrek aan verwerkersovereenkomsten tussen het ZVH en de gemeente en de onduidelijkheid over de partij die de verwerkersovereenkomsten zou moeten initiëren, maar ook in het beperkte besef dat de gemeente verwerkingsverantwoordelijke blijft als er taken gemandateerd zijn. De inschatting is dat de risico's voor gegevensuitwisseling geen bestuurlijk gespreksonderwerp zijn, omdat er geen concrete problemen en knelpunten worden ervaren, maar ook dat het onduidelijk is op welke bestuurlijke tafel deze typen problemen zouden moeten landen.

Voor een rechtmatige omgang met persoonsgegevens zijn de gemeente Enschede en het samenwerkingsverband wederzijds afhankelijk van (de kwaliteit en output van) het samenspel tussen betrokken beleidsmedewerkers op het niveau van de regio en het niveau van de gemeente. De regio zal niet worden aangestuurd op betere uitvoering van het IB-beleid als de gemeentelijke organisatie van de gemeente Enschede niet actief risico's signaleert, bespreekbaar maakt en eventueel aanstuurt op bestuurlijke besluitvorming. Andersom zal de gemeentelijke organisatie eerder handelen of verbeteren als de regio daarop aandringt – bijvoorbeeld door urgente casuïstiek van dataleks of hacks als die zich voordoen.

Een tafel of overleg hiervoor faciliteert de uitwisseling en het samenspel van betrokken beleidsmedewerkers op beide schalen. Dit versterkt de kennispositie en signaleringsfunctie. Op het moment dat dit niet aanwezig is, kunnen betrokkenen geen gebruik maken van uitwisseling met alle (keten) partners over bijvoorbeeld risico's of de invulling van verwerkingsverantwoordelijkheden. Hierdoor is het voor de gemeentelijke organisatie van de gemeente Enschede ook lastiger om bestuurlijke aandacht te vragen voor concrete onderdelen in de praktijk van gegevensuitwisseling.

### *Risico's*

De bovenstaande paragrafen laten een aantal elementen zien waarin de praktijk afwijkt van de vastgestelde kaders. Hierdoor ontstaan risico's voor onveilige gegevensuitwisseling. In de volgende tabel geven we een aantal geconstateerde risico's wat betreft de organisatie weer.

| Geconstateerd risico | Geschatte impact |
|---|---|
| Beperkt inzicht in gegevensstromen van en naar samenwerkingsverbanden | Onrechtmatige gegevensverwerking (bijvoorbeeld een gebrek aan grondslag door een onjuiste verwerkersrol, het overtreden van doelbinding, onjuiste toegang of onjuiste opslag) |
| Als er veel betrokken partijen zijn, ontstaat er een diffuus beeld van doelbinding | Onrechtmatige gegevensverwerking<br>De gemeente voldoet niet aan de wettelijke vereisten van de AVG |
| Onjuiste toegang tot gegevens | Onrechtmatige gegevensverwerking |
| Onduidelijk waar informatiebeveiliging van samenwerkingsverbanden is belegd, met name op de koppelpunten | Onveilige omgang met gegevens |
| Afspraken zijn niet altijd actueel of vastgelegd | Onjuiste grondslag gegevensuitwisseling |
| Uitvoerend medewerkers zijn zich onvoldoende bewust van de vereisten voor legitieme gegevensuitwisseling in de regionale context (denk bijvoorbeeld aan grondslag en doelbinding) en hoe ze hiermee moeten omgaan | Risico's worden niet gesignaleerd<br>Onjuiste omgang met incidenten |

**Samenvattend**

- Ondanks dat bewustzijn van verplichtingen steeds meer toeneemt, is het niet bij alle medewerkers bekend wat rechtmatige gegevensverwerking exact inhoudt. Ook worden de privacy officers niet altijd gevonden voor ondersteuning hierin. De organisatie is zich hier wel van bewust en zet actief in op bewustwording en ondersteuning.
- Risico's bij gegevensuitwisseling zullen eerder ontstaan op het moment dat de situatie minder overzichtelijk wordt, denk bijvoorbeeld aan veel betrokkenen of verschillende typen gegevens. Een manier om risico's te mitigeren, is om de uitwisseling tussen betrokken beleidsmedewerkers op de verschillende schalen te faciliteren. Dit versterkt de kennispositie en de signaleringsfunctie, waardoor het samenspel van de schalen versterkt wordt.
- Mechanismen om te sturen op de juiste omgang met persoonsgegevens verschillen in effectiviteit al naar gelang de verschijningsvorm van het samenwerkings-verband. Hoe formeler het samenwerkingsverband, hoe effectiever mechanismen werken. Op het moment dat dit minder formeel of diffuus is vastgelegd, verliezen mechanismen aan kracht. In de praktijk worden ze dan minder tot uitvoer gebracht.
- Hoe 'zwaarder' de (juridische) governance van een samenwerkingsverband, hoe meer mogelijkheden de gemeente Enschede heeft om te sturen op veilige gegevensuitwisseling. De gemeente Enschede maakt echter nauwelijks tot geen gebruik van deze mogelijkheden. De inschatting is dat gegevensuitwisseling en de risico's hiervan geen bestuurlijk gespreksonderwerp zijn. Ook bij de raad leeft het onderwerp gegevensuitwisseling niet (net als digitalisering in brede zin). Om de controlerende rol van de raad te versterken, is met name een versterking van de kennispositie gewenst.

**Waarom is dit van belang voor de gemeenteraad van de gemeente Enschede?**

De gemeentelijke organisatie heeft niet altijd grip op de eigen, lokale verwerkingsverantwoordelijkheid bij gegevensuitwisseling in regionale samenwerkingsverbanden. Als het onduidelijk is wie voor welke verwerkingsverantwoordelijkheden aan de lat staat – de regio of de gemeente – levert dat een rechtmatigheidsvraagstuk op. Het is dan immers niet meer aan de inwoner uit te leggen welke instantie zij kunnen aanspreken over de verwerking van hun persoonsgegevens. Als de gemeenteraad van de gemeente Enschede stuurt op de rechtmatigheid van gegevensuitwisseling in samenwerkingsverbanden (zoals gesuggereerd in paragraaf 3.1, vanuit de wettelijke verantwoordelijkheid onder de AVG), is het dus ook zaak om aan te sturen op de verheldering van verwerkingsverantwoordelijkheden tussen de gemeentelijke organisatie van Enschede en 'de regio'. Dat kan door meer informatie te vragen (kan de wethouder de verdeling van verwerkingsverantwoordelijkheid in samenwerkingsverband X verhelderen?) of door kaders te stellen in moties (verzoek het college per samenwerkingsverband aan te geven welke verwerkingsverantwoordelijkheden de gemeente Enschede heeft en hoe die worden ingevuld).

## 4.3 Ambitie

De gemeente Enschede heeft de ambitie gesteld om verantwoord en veilig om te gaan met (persoons)gegevens. In deze paragraaf analyseren we of deze ambitie (wat de gemeente wil) aansluit op de ambities van de regio. De gemeente kan immers beïnvloed worden door regionale sturing. We zetten dit af tegen de capaciteit van de organisatie en de legitieme kaders waarbinnen zij kan handelen.

### Bevindingen uit documenten en gesprekken

Uit documenten blijkt dat de gemeente Enschede de ambitie heeft gesteld om zich in te zetten voor rechtmatige en veilige verwerking van (persoons)gegevens.[38] Hierbij stelt de gemeente de betrokkenen en belanghebbenden centraal en stelt zij dat de risico's zo laag mogelijk moeten zijn. Er zijn verschillende beleidsmatige mechanismen om deze ambitie te borgen. In de gemeentelijke organisatie is dit bijvoorbeeld de PDCA-cyclus[39], die bewerkstelligt dat medewerkers bijsturen op de informatieveiligheid en privacy door ervaringen en leerprocessen. Op regionale schaal wordt de ambitie geborgd door bijvoorbeeld de stuurgroepoverleggen en de overleggen die plaatsvinden tussen de beleidsmedewerkers vanuit de gemeente en het samenwerkingsverband. Op die momenten is er een mogelijkheid om te sturen op veiligheid en verantwoording. Het is echter onbekend tot in hoeverre dit plaatsvindt.

In gesprekken wordt ook aangegeven dat de ambitie met name is dat er aan de voorkant wordt voorkomen dat er incidenten plaatsvinden, in plaats van een reactieve houding aan te nemen en te handelen als deze incidenten al hebben plaatsgevonden. De nadruk ligt hierbij op het organisatorische vlak: zo goed mogelijk borgen dat er processen ingericht zijn en er een governance is opgetuigd die bijdraagt aan een goede omgang met gegevens. Hierbij wordt benoemd dat de grootste risico's niet in de technische, juridische en organisatorische inregeling zitten, maar voornamelijk voorkomen in het menselijk handelen. De ambitie is dan ook dat bewustwording van de risico's en maatregelen rondom gegevensuitwisseling op peil zijn.

### Analyse Berenschot

Er zijn verschillende (organisatorische) mechanismen ingeregeld om invulling te geven aan de ambities van de gemeente, zowel in de gemeentelijke organisatie zelf als in de regionale samenwerkingen. Zoals eerder beschreven werken deze mechanismen beter in samenwerkingsverbanden waar dergelijke mechanismen formeel zijn vastgelegd, bijvoorbeeld omdat het samenwerkingsverband een rechtspersoonlijkheid heeft en hier zelf invulling geeft. Verantwoordelijkheden zijn bijvoorbeeld expliciet belegd en worden hierdoor ook in de praktijk gebracht. Als er echter veel verschillende partijen aan de lat staan om de ambities in de praktijk te brengen, zoals in een netwerksamenwerking, zien we dat deze aan kracht verliezen en minder goed tot realisatie komen. De gemeente loopt het risico dat gestelde ambities in de praktijk niet worden nageleefd wanneer verantwoordelijkheden niet expliciet zijn belegd. Deze risico's vloeien vooral voort uit menselijk handelen en de beperkte naleving van organisatorische mechanismen.

Daarnaast kan de aansluiting tussen ambities op de gemeentelijke schaal en de regionale schaal beperkt zijn. Als een deelnemende gemeente hier niet actief op stuurt, kan het voorkomen dat de uitvoering op regionale schaal niet overeenkomt met de in de gemeente gestelde ambities. Dat is lastig, want elke gemeente is wel afhankelijk van de regio voor het naleven van haar eigen ambities voor rechtmatige gegevensuitwisseling. Hierbij geldt ook: hoe meer capaciteit op beide schaalniveaus aanwezig is, hoe meer bewustzijn er (bestuurlijk) zal zijn voor de effecten van lokale ambities op de schaal van de regio en andersom. Dit risico heeft consequenties voor de beoogde publieke waarde voor de opgaven waarvoor de gemeente aan de lat staat. Gegevensuitwisseling is immers enkel een instrument om andere taken van de gemeente uit te voeren. Op het moment dat gegevensuitwisseling niet rechtmatig en veilig plaatsvindt, kan de uitvoering van alle taken in het gedrang komen.

#### *Risico's*

De bovenstaande paragrafen laten een aantal elementen zien waarin de praktijk afwijkt van de vastgestelde kaders. Hierdoor ontstaan risico's voor onveilige gegevensuitwisseling. In de volgende tabel geven we een aantal geconstateerde risico's wat betreft ambitie weer.

38 Gemeente Enschede (2023). *Procedure voor het actueel houden van het verwerkingsregister*; Gemeente Enschede (2023). *Toezichtsplan Functionaris Gegevensbescherming 2024*; Gemeente Enschede (2023). *Beleid en procedure voor het uitvoeren van DPIA's*.

39 PDCA-cyclus: Plan-Do-Check-Act cyclus. Deze cyclus beschrijft vier stappen die elkaar cyclisch opvolgen om zo verbetering in een organisatie door te voeren. De stappen zijn als volgt: een plan opstellen (plan), het plan uitvoeren (do), controleren of het plan is uitgevoerd zoals bedacht (check), het plan wijzigen en aanpassen en weer uitvoeren (act). Vervolgens start de cirkel opnieuw door een vervolg te plannen.

**Waarom is dit van belang voor de gemeenteraad van de gemeente Enschede?**

We zien dat het behalen van de ambitie van de gemeente Enschede om het uitwisselen van persoonsgegevens rechtmatig te laten verlopen vooral valt of staat bij het creëren van bewustzijn over de risico's van en passende maatregelen voor gegevensuitwisseling in samenwerkingsverbanden. De raad heeft een (wettelijke, want dit is vastgelegd in de AVG) rol om lokaal beleid ten aanzien van gegevensuitwisseling te toetsen op die rechtmatigheid. De drie vragen 'wie, met welk doel en hoe zijn inwoners geïnformeerd' (zie het kader onder paragraaf 3.1) helpen om te beoordelen of het beleid van de gemeente Enschede voldoende invulling geeft aan de ambitie van rechtmatige gegevensuitwisseling.

**Relevantie voor de raad**

We zien dat het behalen van de ambitie van de gemeente Enschede vooral valt of staat bij het creëren van bewustzijn over de risico's van en passende maatregelen voor gegevensuitwisseling in samenwerkingsverbanden. Bovendien is het behulpzaam om te weten welke afspraken formeel belegd zijn binnen de samenwerkingsverbanden. De raad kan als volgt beoordelen of de ambitie wel of niet gehaald wordt:

- Controleer of er gezamenlijke, concrete opgestelde kaders zijn, zodat de raad weet waarop gecontroleerd dient te worden.
- Bestudeer wat de afwegingen zijn geweest om voor bepaalde gegevensuitwisselingen wel of niet maatregelen in te richten. Zet dat af tegen de visie van de gemeente op dit onderwerp.

**Samenvattend**

- De ambities die door de gemeente zijn gesteld met betrekking tot informatieveiligheid, moeten in de regionale schaal tot uitvoering worden gebracht. Deze afstand resulteert automatisch in een afhankelijkheid van samenwerkingsverbanden en -partners. Door de afhankelijkheid van de regionale schaal, is het van belang dat de gemeente actief stuurt in de regionale schaal op het realiseren van haar ambities. Dit gebeurt echter beperkt.
- In de praktijk blijkt menselijk handelen, namelijk de naleving van mechanismen zoals de PDCA-cyclus, de voornaamste zwakte te zijn voor de realisatie van de ambities.
- Op het moment dat gegevensuitwisseling niet rechtmatig en veilig plaatsvindt, kan dit van invloed zijn op alle taken die de gemeente uitvoert. Gegevensuitwisseling is immers een instrument voor de uitvoering van andere taken.

| Geconstateerd risico | Impact |
|---|---|
| Mechanismen voor veilige en rechtmatige gegevensuitwisseling (onder andere de PDCA-cyclus en signaleringsoverleggen) worden niet ten uitvoer gebracht | De gemeente voldoet niet aan haar eigen ambities |
| De uitvoering op regionale schaal komt niet overeen met de ambities op gemeentelijke schaal | Er wordt geen invulling gegeven aan de ambities van de gemeente, zowel op het gebied van informatieveiligheid en privacy als op andere domeinen |
| Als gegevensuitwisseling onrechtmatig en/of onveilig plaatsvindt, kan dit de uitvoering van andere taken belemmeren | Taken van de gemeente worden onrechtmatig of onveilig uitgevoerd |

HOOFDSTUK 5

# Positie van de raad

De raad heeft twee belangrijke rollen die benut kunnen worden om te sturen op digitalisering binnen en buiten de gemeente: de kaderstellende en de controlerende rol. In dit hoofdstuk reflecteren we op de mate waarin de raad die rollen invult en daarmee hoe de raad zich positioneert op gegevensuitwisseling in samenwerkingsverbanden.

Een onderdeel van het onderzoek was een gesprek met de raadsleden. De focus van dit gesprek lag vooral op de wijze waarop de raad zijn kaderstellende en controlerende rol kan vervullen. We focusten ook op de wensen en behoeften die raadsleden hebben ten aanzien van het krijgen van grip op gegevensuitwisseling. De uitnodiging voor het gesprek met raadsleden is naar de hele raad uitgegaan. Twee van de 39 gemeenteraadsleden zijn op onze uitnodiging in gegaan. Dat leidt tot twee aandachtspunten: 1) de analyses in dit hoofdstuk zijn gebaseerd op een kleine groep, en er kan daarom niet al te veel gewicht aan gegeven worden en 2) het onderwerp leeft inderdaad onvoldoende bij de raad of de uitnodiging beschreef het belang van dit onderwerp niet helder genoeg. Desalniettemin zijn er interessante observaties en analyses naar voren gekomen uit dit gesprek en uit andere gesprekken met de ambtelijke organisatie, die van toepassing zijn op de onderstaande paragrafen.

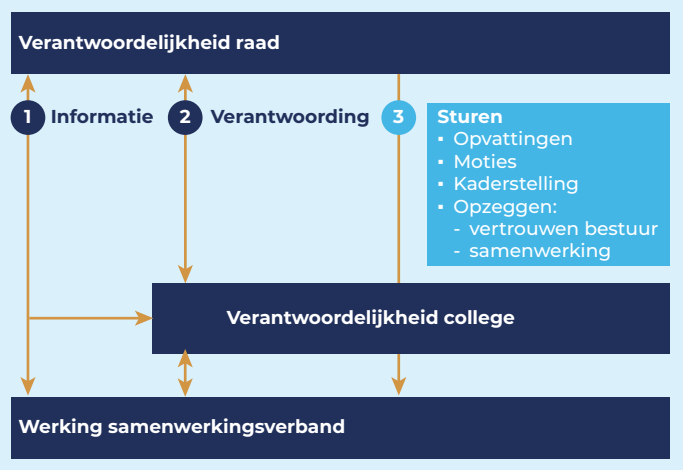
## 5.1 Mogelijkheden tot sturing

Het AB van een GR kent een informatieplicht richting de betrokken raden. Daarnaast heeft een raad een aantal instrumenten tot zijn beschikking om grip op een regionale samenwerking te krijgen, zo ook over het onderwerp gegevensuitwisseling. De praktische instrumenten van de raad zijn onder te verdelen in instrumenten met betrekking tot[40]:

- ***Informatie.*** Naast structurele informatievoorziening, heeft de raad verschillende rechten om incidentele informatie op te vragen. Denk bijvoorbeeld aan informatierecht ten aanzien van het college, informatierecht ten aanzien van het eigen lid van het algemeen bestuur en informatierecht ten aanzien van het algemeen bestuur.
- ***Verantwoording.*** De raad kan verantwoording vragen aan collegeleden en aan een lid van het algemeen bestuur.
- ***Sturing.*** De raad heeft de volgende formele instrumenten om te sturen: zienswijzenprocedure, gemeentelijke begroting (paragraaf verbonden partijen), moties verordenende bevoegdheid, en beleidsregels (of algemene en concrete instructies) van ofwel de raad of het college van B&W.

40 Berenschot (2018).

Figuur 4. **Visuele weergave van de verschillende instrumenten van de gemeenteraad richting het college en samenwerkingsverband.**




In de context van dit onderzoek is met name het stellen van vragen (het opvragen van informatie) relevant. Zoals eerder benoemd in paragraaf 2.1, kan de raad vragen stellen over de rapportages van het college aan de raad. Dit kan dan bijvoorbeeld gaan over de verantwoordelijkheid van de gemeente en hoe dit zich verhoudt tot de samenwerkingsverbanden: is duidelijk wie welke verantwoordelijkheid draagt? Waarom wel of niet? Vragen kunnen ook gaan over de borging van doelmatigheid van gegevensuitwisseling: is het expliciet vastgelegd wat het doel voor de uitwisseling is? Of is daarin ruimte voor interpretatie? Is hierbij vastgelegd hoe inwoners van wie de gegevens worden uitgewisseld, worden geïnformeerd over wie er beschikt over hun gegevens en met welk doel? In feite beoordeelt de raad met dergelijke vragen de rechtmatigheid van de uitwisseling van persoonsgegevens, en met name de borging hiervan door het college. Indien er twijfels ontstaan over de beantwoording van deze informatievragen, kunnen raadsleden méér of gedetailleerdere informatie opvragen over het IB-beleid/privacybeleid van een samenwerkingsverband, of eventueel meer sturend te werk gaan.

## 5.2 Positionering van de gemeenteraad

Uit de gesprekken blijkt dat het onderwerp ‘gegevensuitwisseling’ of ‘gegevensbescherming’ niet leeft bij de raadsleden, zeker niet in de context van regionale samenwerkingen. De gesproken raadsleden geven hierbij ook aan dat digitalisering als onderwerp in het geheel weinig leeft en dat hierdoor ook geen actieve kaderstellende en controlerende rol ingenomen wordt omtrent IT en digitalisering.[41] De raad vervult zijn rol met name reactief op het moment als er een concrete casus politiek wordt gemaakt. Dit blijft echter bij individuele gevallen hangen, bijvoorbeeld bij het probleem rondom onbedoelde wifi-tracking van 2018 tot 2020. Situaties zoals deze komen zelden voor binnen de gemeenteraad. Raadsleden geven aan dat dit komt door een combinatie van gebrek aan kennis enerzijds en gebrek aan gevoelde urgentie anderzijds. Zij geven aan dat er ook geen (gedeeld) beeld is bij de mogelijke risico’s die zich kunnen voordoen rond gegevensuitwisseling of van de toezichthoudende rollen binnen de gemeente waar ze op kunnen voortbouwen voor de invulling van hun controlerende rol.

Daarnaast geven raadsleden aan dat samenwerkingsverbanden in algemene zin ook niet hoog op de agenda staan, omdat ze ervaren dat ze hier relatief weinig invloed op kunnen uitoefenen. Dit komt mede omdat zij het indienen van een zienswijze als enige instrument zien om hun controlerende rol invulling te geven. Uit de documentenstudie blijkt daarnaast ook dat het per samenwerkingsverband verschilt of en op welke manier de raad gevoed wordt met informatie. Dit kan vanuit de GR ingevuld worden vanuit de informatieplicht, maar kan ook door de gemeente zelf moeten plaatsvinden. Hierdoor ervaren raadsleden een afstand tot samenwerkingsverbanden en staat dit niet hoog op de agenda.

De gesproken raadsleden geven aan dat zij weinig ambitie/behoefte zien vanuit de raad om meer positie in te nemen op de kaderstellende rol. Wel zien ze een mogelijkheid om meer positie te kunnen nemen in de controlerende rol, op ontwikkelingen rondom digitalisering als geheel. Raadsleden geven aan dan vooral baat te hebben bij doelgerichte informatie en goede voorbeelden met betrekking tot het invullen van de controlerende rol in deze context. Dit gaat dan niet over gedetailleerde kennis over gegevensuitwisseling, maar over handvaten hoe ze hun controlerende rol eventueel kunnen inzetten.

41 Er is wel een discussienota besproken in de raad: ‘Ethische visie op gebruik van data en technologie’. Er is nog geen besluitvorming over de nota geweest.

## Analyse Berenschot

De raad neemt weinig positie in rondom gegevensuitwisseling, maar lijkt ook op het thema digitalisering als geheel niet veel positie in te nemen. Dit geldt zowel voor de kaderstellende als de controlerende rol. Onderwerpen als ‘gegevensuitwisseling bij samenwerkingsverbanden’ spreken dan ook niet tot de verbeelding bij de gesproken raadsleden.

Hoewel het te begrijpen is dat de raad geen actieve kaderstellende rol op dit specifieke thema inneemt, kan het wel als risico worden bezien als zij ook geen invulling geven aan de controlerende rol op de invulling van het college aan het digitaliseringsthema als geheel. Het is van belang dat de raad als controlerend gremium zicht heeft op de mechanismen voor legitieme omgang met gegevens (of in bredere zin; met data en technologie). Door geïnformeerd en meegenomen te worden in de processen en inrichting in de organisatie, kan de raad zijn controlerende rol op hoofdlijnen invulling geven.



DEEL 3

# Bijlagen

In bijlage 1 vindt u de onderzoeksverantwoording en het theoretisch kader, waarna bijlage 2 de onderzochte documenten beschrijft. Bijlage 3 bevat vervolgens een toelichting op het wettelijk kader dat van toepassing is op de onderzochte casussen.

BIJLAGE 1

# Onderzoeksverantwoording

Het onderzoek poogt met name om het grijze gebied, zowel bestuurlijk als op de uitvoering en toezicht, rondom gegevensuitwisseling in samenwerkingsverbanden door te lichten. Om deze praktijk te onderzoeken, is gebruik gemaakt van twee samenwerkingsverbanden als casussen. Het is belangrijk om te benoemen dat het gebruik van de casussen enkel het doel dient om te illustreren hoe de omgang van de gemeente Enschede met samenwerkingsverbanden vorm krijgt. De casussen zijn daarmee niet het object van de evaluatie.

In de volgende paragraaf lichten we meer toe over de criteria die onderliggend waren aan de casusselectie, evenals een korte beschrijving van de twee casussen.

## Onderzoeksmethoden

De documentenstudie omvat (beleids)documenten van de gemeente Enschede, (beleids)documenten van de geselecteerde samenwerkingsverbanden, relevante wet- en regelgeving, beleidsdocumenten van andere gemeenten binnen dezelfde context en eerdere relevante onderzoeksrapporten. De documentstudie gaf inzicht in het vastgestelde beleid, de gemaakte afspraken, en governance en verantwoordelijkheden binnen de gemeente Enschede. Tevens gaf het inzicht in de historie van de gemeente Enschede op het onderwerp gegevensuitwisseling. In bijlage 2 vindt u een overzicht van de geraadpleegde documentatie.

We hebben voor dit onderzoek dertien (groeps)gesprekken gevoerd. We hebben er zorg voor gedragen om een, voor zover mogelijk, brede afspiegeling van bestuurders, beleidsmedewerkers en raadsleden te spreken vanuit de gemeente Enschede. Ook hebben we een aantal gesprekken gevoerd met experts die niet werkzaam zijn bij de gemeente Enschede. Zodoende hebben de onderzoekers beelden, risico's en best practices extern kunnen valideren. Om de anonimiteit van gesprekspartners te waarborgen, openbaren we de namen van gesprekspartners niet. De gesprekken hadden een tweeledige insteek: 1) inzicht krijgen in de dagelijkse praktijk van de gemeente Enschede binnen en buiten de samenwerkingsverbanden, 2) veelvoorkomende risico's en best practices ophalen bij soortgelijke organisaties die ervaring hebben met gegevensuitwisseling in soortgelijke samenwerkingsverbanden.

## Selectie van regionale samenwerkingsverbanden als casestudy's

Om te beoordelen in hoeverre de gemeente Enschede stuurt op rechtmatige gegevensuitwisseling in samenwerkingsverbanden, vergelijken we bij wijze van steekproef beleid en uitvoeringspraktijk met betrekking tot twee regionale samenwerkingsverbanden. De selectie van onze twee casussen is in nauw overleg met de Rekenkamer tot stand gekomen. De casussen zijn op basis van een aantal criteria geselecteerd uit het totaaloverzicht van samenwerkingsverbanden waaraan de gemeente Enschede (in totaal 26) deelneemt[42].

- het type persoonsgegevens dat wordt uitgewisseld
- de betrokken beleidsdomeinen
- de juridische vorm van het samenwerkingsverband
- de bestuurlijke verantwoordelijkheid van het samenwerkingsverband
- de verwachtingen met betrekking tot knelpunten bij gegevensuitwisseling.

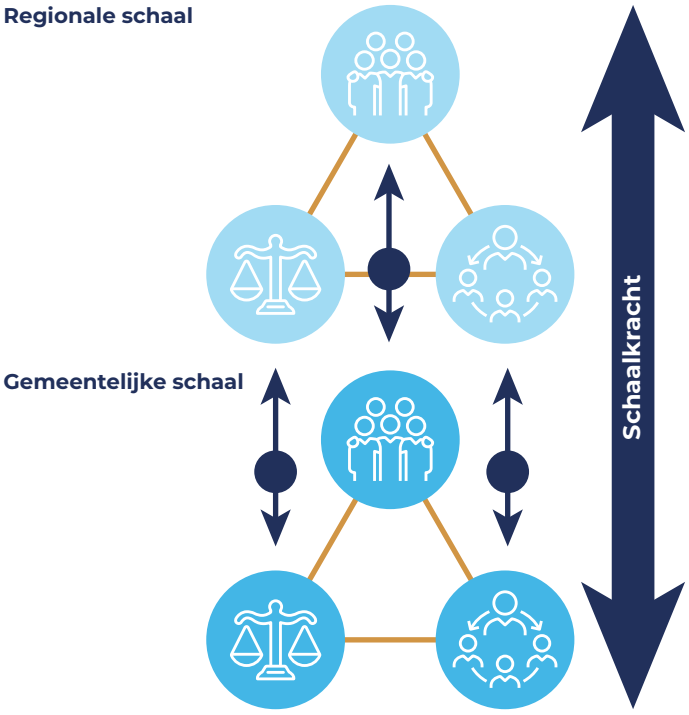
Op het moment dat de casussen op deze criteria voldoende variatie vertonen, zijn ze illustratief voor de omgang van de gemeente met verschillende typen samenwerkingsverbanden. Op basis van de criteria zijn het Zorg- en Veiligheidshuis Twente en de Stadsbank Oost Nederland geselecteerd als casus. Deze casussen behandelen verschillende typen persoonsgegevens (informatie uit zorg- en veiligheidsdossiers en financiële informatie), raken aan verschillende domeinen (zorg-/veiligheidsdomein en werk en inkomen), kennen een andere juridische vorm (gemeenschappelijke regeling en verband zonder rechtspersoonlijkheid), verschillende bestuurlijke verantwoordelijkheid en te verwachten knelpunten.

42 RegioAtlas Enschede (2024).

## Theoretisch kader

We maken gebruik van het publiekewaardemodel als kader voor het onderzoek. Publieke waarde is het effect dat gecreëerd wordt door een organisatie; de daadwerkelijk positieve effecten op de maatschappij. Het model gaat ervan uit dat 'wat we willen' (publiekewaardepropositie/ambitie) altijd in balans moet zijn met 'wat we kunnen' (capaciteit/organisatie) en 'wat we mogen en waar we toe bereid zijn' (legitimiteit). Bij een goede invulling van en een juiste balans tussen deze drie elementen ontstaat publieke waarde op een effectieve, gelegitimeerde en efficiënte wijze. De juiste balans verschilt hierbij naar gelang de context.

Figuur 5. **Schaalkracht in het publiekewaardemodel.**




In regionale samenwerking interacteren de drie elementen met elkaar op gemeentelijke en regionale schaal (zie figuur 5). Effectieve risicobeheersing bij gegevensuitwisseling met en door samenwerkingsverbanden is een vorm van 'schaalkracht' en wordt bepaald door het samenspel tussen de regionale en gemeentelijke schalen. Bij de implementatie van nationale wet- en regelgeving rondom gegevensuitwisseling ontstaat daarom een samenspel tussen de schalen:

- De gemeente Enschede én de regionale samenwerkingsverbanden stemmen hun ***ambities*** (proposities van publieke waarde) onderling af. Hiermee bedoelen we dat de gemeente Enschede met haar lokale (bestuurlijke) ambities stuurt op het handelen van de regio, maar ook dat de (bestuurlijke) richting die een regio kiest impact kan hebben op het handelen van de gemeente Enschede
- De verschillende ***organisaties*** (operationele capaciteit) interacteren met elkaar én kunnen conflicteren bij een gebrek aan beleid of interactie. Als de gemeente Enschede de kennis, kunde en processen in huis heeft om landelijke wet- en regelgeving te implementeren, kan ze die niet alleen inzetten ten behoeve van legitiem handelen op de lokale schaal, maar ook om de regio daarop aan te sturen. De gemeente Enschede kan haar eigen capaciteit ter beschikking stellen aan de regio, proactief en preventies risico's signaleren voor gegevensuitwisseling én die mitigeren – ook met behulp van lokaal beleid.
- Het is niet vanzelfsprekend dat op alle schalen ***legitiem*** wordt gehandeld en er evenveel draagvlak bestaat voor de manier waarop gegevensuitwisseling plaatsvindt om publieke waarde te realiseren. Er is sprake van wederzijdse afhankelijkheid: de gemeente Enschede is afhankelijk van de invulling van betrokken partijen en van draagvlak hiervoor binnen de regio. Zo kunnen activiteiten van de regio de legitimiteit van het handelen van de gemeente Enschede onder druk zetten, bijvoorbeeld als de regio bepaalde landelijke wet- en regelgeving onvoldoende heeft geïmplementeerd in beleid maar toch als vorm van 'verlengd lokaal bestuur' taken overneemt van de gemeente.

Dit laat zien dat de keuzes die worden gemaakt op regionale en lokale schaal, elkaar wederzijds beïnvloeden en dat een effectieve risicobeheersing hiervan afhankelijk is.

BIJLAGE 2

# Documenten


- Autoriteit Persoonsgegevens (2023). AP Jaarplan 2024.
- Berenschot (2023a). Eindrapportage formatie onderzoek Zorg- en Veiligheidshuis Twente
- Berenschot (2023b). Eindrapportage risicoanalyse Zorg- en Veiligheidshuis Twente
- Berenschot (2018). Grip op samenwerking in de praktijk. Bron geraadpleegd op 28-06-2024: *https://www.griffiers.nl/sites/www.griffiers.nl/files/documenten/grip-op-samenwerking-in-de-praktijk.pdf*
- Data School Universiteit Utrecht (2021). De Data Wijzer. Bron geraadpleegd op 03-07-2024: *https://dataschool.nl/onderzoek/verantwoorde-ai/datawijzer/ - :~:text=De%20DataWijzer%20is%20een%20instrument,een%20tablet%20kan%20worden%20gebruikt*
- Datawerkplaats Universiteit Utrecht (2022). De Digitale Raadgever. Bron geraadpleegd op 03-07-2024: *https://datawerkplaats.org/producten-en-tools/ik-wil-input-verzamelen-voor-de-reflectie-van-en-beraadslaging-over-datapraktijken/de-digitale-raadgever/*
- Decentraal bestuur (2022). Regionale samenwerking en gemeenteraden. Een samenvattend onderzoek naar de legitimiteit, effectiviteit en doelmatigheid van regionale samenwerkingsverbanden. Bron geraadpleegd op 17-05-2024: *https://open.overheid.nl/documenten/ronl-06e1b2b25069b8dbaa7b0294ae5ef18f8f9588dd/pdf*
- Gemeente Enschede (2022). Strategisch informatie-beveiliging- en privacybeleid
- Gemeente Enschede (2023). Beleid en procedure DPIA's
- Gemeente Enschede (2023). Procedure actueel houden verwerkingsregister
- Gemeente Enschede (2023). Programma Zorgvuldig werken in het sociaal domein [intern werkdocument]
- Gemeente Enschede (2023). Toezichtsplan FG 2024
- Gemeente Enschede (2023). Waardengedreven digitaliseren: ethische visie op het gebruik van
- data en technologie door de gemeente Enschede.
- Gemeente Enschede (2024). Borgingsproduct 3.0 Rapportage SD 2023 [vertrouwelijk]
- Gemeente Enschede (2024). Infographic privacyvragen [intern werkdocument]
- Gemeente Enschede (2024). Jaarverslag FG 2023 [vertrouwelijk; niet vastgesteld]
- Gemeente Enschede (2024). Verwerkingsregister Enschede
- Informatiebeveiligingsdienst & VNG (2022). Dreigingsbeeld informatiebeveiliging Nederlandse gemeenten 2023 → 2024. Bron geraadpleegd op 15-05-2024: *https://www.informatiebeveiligingsdienst.nl/wp-content/uploads/2022/10/IBD_dreigingsbeeld_2023-2024_DEF-versie.pdf*
- Rathenau Instituut (2020). Raad weten met digitalisering. Hoe de gemeenteraad kan sturen op de maatschappelijke impact van digitale technologie. Bron geraadpleegd op 03-07-2024: *https://www.rathenau.nl/sites/default/files/2020-09/Raad-weten-met-digitalisering-Rathenau-Instituut.pdf*
- RegioAtlas (2024). Samenwerkingen Enschede. Bron geraadpleegd op 03-07-2024: *https://www.regioatlas.nl/samenwerkingen/samenwerkingen_item/t/enschede*
- Stadsbank Oost Nederland (2022). Informatiebeveiligings-beleid
- Universiteit Utrecht (2022). Hand out Verantwoording over algoritmen in de gemeenteraad. Bron geraadpleegd op 03-07-2024: *https://www.raadsleden.nl/assets/documents/hand-out_bevindingen.pdf*
- VNG (2021). Rol gemeenteraad: digitalisering is een incident. Bron: *https://vng.nl/artikelen/rol-gemeenteraad-digitalisering-is-geen-incident*
- Zorg- en Veiligheidshuis Twente (2022). Privacy Protocol ZVH
- Zorg- en Veiligheidshuis Twente (2022). Samenwerkingsconvenant ZVH
- Zorg- en Veiligheidshuis Twente (2023). Vaststellen Jaarverslag Zorg- en Veiligheidshuis Twente 2024

BIJLAGE 3

# Wettelijk kader

## Algemene kaders

### Grondrechten

Binnen de EU zijn fundamentele rechten van individuen op verschillende plekken goed geregeld. Op Europees niveau is het EU-recht op bescherming ten aanzien van de verwerking van persoonsgegevens en het recht op eerbiediging van het privéleven in verschillende Verdragen vastgelegd.[43] Ook de Nederlandse Grondwet erkent het recht op eerbiediging van de persoonlijke levenssfeer.[44] Wanneer we binnen het kader van dit onderzoek refereren aan privacyrechten, dan refereren we daarbij aan al deze grondrechten. Het recht op privacy is slechts een van deze grondrechten. Ook andere fundamentele rechten, zoals het recht op eigendom, menselijke waardigheid, vrijheid van meningsuiting en diverse andere rechten worden op dit niveau beschermd. Doordat het beschermen van deze grondrechten niet absoluut is, maar deze tegen elkaar moeten worden afgewogen, is verdere uitwerking in nationale en Europese wet- en regelgeving noodzakelijk.

### Algemene verordening gegevensbescherming (AVG)

In de EU vormt de Algemene verordening gegevensbescherming (AVG) de belangrijkste kaders om een hoog (en gelijkwaardig) beschermingsniveau van privacyrechten binnen de EU te waarborgen. In de AVG zijn verschillende algemene kaders vastgesteld die bepalen onder welke voorwaarden gegevens mogen worden verwerkt en aan welke vereisten dan moet worden voldaan. Daarnaast bevat de AVG verschillende maatregelen en instrumenten om naleving te bevorderen en te handhaven.

De AVG kent zes belangrijke beginselen die zijn uitgewerkt in artikel 5 van de AVG. Deze beginselen zijn:

- ***Rechtmatigheid, behoorlijkheid en transparantie:*** dit betekent dat de gemeente Enschede enkel persoonsgegevens mag verwerken indien dit past bij de wettelijke taak die zij vervullen. Het moet helder zijn voor welke doeleinden gegevens worden verzameld en verwerkt en op welke wijze dit gebeurt.
- ***Doelbinding:*** persoonsgegevens moeten voor welbepaalde, uitdrukkelijk omschreven en gerechtvaardigde doeleinden worden verzameld en mogen niet verder worden verwerkt op een wijze die daarmee onverenigbaar is.
- ***Minimale gegevensverwerking:*** er mogen niet meer gegevens worden verzameld en verwerkt dan noodzakelijk is voor het doel waarvoor zij worden verzameld.
- ***Juistheid persoonsgegevens:*** persoonsgegevens moeten juist zijn en zo nodig worden geactualiseerd.
- ***Gegevensbeperking:*** persoonsgegevens worden bewaard in een vorm die het mogelijk maakt de betrokkene niet langer te identificeren dan voor de doeleinden waarvoor de persoonsgegevens worden verwerkt noodzakelijk is.
- ***Integriteit en vertrouwelijkheid:*** persoonsgegevens worden voldoende beschermd zodat de vertrouwelijkheid en integriteit van de persoonsgegevens voldoende gewaarborgd wordt.

Tot slot is er een verplichting voor organisaties om aan te kunnen tonen dat zij voldoen aan deze beginselen. Dit wordt ook wel de verantwoordingsplicht genoemd. Deze verplichting is nader uitgewerkt in concrete maatregelen, zoals de verplichting tot het bijhouden van een verwerkingsregister en het uitvoeren van DPIA's wanneer er sprake is van een hoog risico.

Om ervoor te zorgen dat de AVG aansluit op nationale wet- en regelgeving is de Uitvoeringswet Algemene verordening gegevensbescherming (UAVG) aangenomen.

43 Bijvoorbeeld art. 16 van het Verdrag betreffende de werking van de Europese Unie (VWEU), Art. 7 en 8 van het Handvest van de grondrechten van de Europese Unie (het Handvest), en art. 8 van het Europees Verdrag voor de Rechten van de Mens (EVRM).

44 Art. 10 Grondwet.

### Wet gegevensuitwisseling samenwerkingsverbanden

In juni 2024 is de Wet gegevensuitwisseling samenwerkingsverbanden (Wgs) aangenomen. Deze wet is relevant voor bijvoorbeeld het Zorg- en Veiligheidshuis Twente en biedt de juridische basis voor verwerking van persoonsgegevens binnen het samenwerkingsverband. In de wet en de nog nader uit te werken maatregelen van bestuur worden nadere regels bepaald over de wijze waarop gegevensuitwisseling kan plaatsvinden. Dit zal impact hebben op de wijze waarop de gemeente Enschede deze taken uitvoert. Alhoewel deze wet ten tijde van dit rapport nog niet van kracht is, en daarom niet meegenomen kan worden in de juridische analyse, zal deze na inwerkingtreding wel van invloed zijn.

### Bestuursrechtelijke beginselen

Ook bestuursrechtelijke beginselen hebben impact op gegevensuitwisseling - en de inrichting daarvan – binnen samenwerkingsverbanden. Deze algemene beginselen van behoorlijk bestuur zijn: het zorgvuldigheidsbeginsel, het motiveringsbeginsel, het fair play-beginsel, het rechtszekerheidsbeginsel, het vertrouwensbeginsel en het gelijkheidsbeginsel. De bestuursrechter kan een genomen besluit door een bestuursorgaan of een lagere regeling toetsen aan deze beginselen.[45] Deze algemene beginselen waarborgen dat bestuursrechtelijke beslissingen altijd aan bepaalde minimumvereisten voldoen. Hieronder beschrijven we enkele voorbeelden hiervan. Het zorgvuldigheidsbeginsel houdt in dat bestuursorganen alle relevante feiten en omstandigheden meenemen zodat een zorgvuldige afweging van de belangen van betrokkenen kan worden gemaakt. Hiervoor is het noodzakelijk dat bestuursorganen toegang hebben tot de juiste informatie. Een ander voorbeeld is dat het motiveringsbeginsel. Het motiveringsbeginsel houdt in dat besluiten voldoende onderbouwd zijn zodat de beslissingen navolgbaar zijn voor de betrokkenen.

### Europese ontwikkelingen

- Dataverordening
- AI Act
- NIS2

## Materiewetten

### Openbare veiligheid en opsporing

De AVG is niet geschikt voor alle gebieden. Het verwerken van gegevens op het gebied van openbare veiligheid en opsporing en handhaving van strafrechtelijke feiten is een voorbeeld hiervan. Hiervoor is specifieke wet- en regelgeving aangenomen: de Richtlijn gegevensbescherming opsporing en vervolging (Richtlijn EU.2016/680). Deze richtlijn is in Nederland geïmplementeerd via de Wet politiegegevens (Wpg) voor de politie en de Wet justitiële en strafvorderlijke gegevens (Wjsg) voor het Openbaar Ministerie en de Rechtspraak.

Hoewel er veel overeenkomsten zijn tussen de verplichtingen uit de Wpg en de AVG, zijn er ook belangrijke verschillen tussen beide wetten. Doordat de Wpg en Wjsg zich richten op een specifiek en afgebakend onderwerp, bevatten deze wetten op bepaalde onderdelen meer concrete en strengere eisen dan de AVG. Zo gelden er specifieke verplichtingen rondom het scheiden van feiten en meningen, gelden er concrete bewaartermijnen, en worden er specifieke eisen gesteld op het gebied van logging. Daarnaast is er in de Wpg een auditverplichting vastgelegd.

### Overige materiewetten en uitvoeringsbesluiten

Voor de uitvoering van veel taken worden in zogenaamde materiewetten nadere regels opgesteld rondom het verwerken van gegevens. Het gaat dan bijvoorbeeld om de Wet maatschappelijke ondersteuning, de Jeugdwet, de Participatiewet, de Wet gemeentelijke schuldhulpverlening, de Zorgverzekeringswet, etc. Deze wetten beschrijven vaak de maatschappelijk taak die bij een of meerdere overheidsorganisaties wordt belegd, voor welke doeleinden zij daarvoor gegevens mogen verwerken en verstrekken aan andere organisaties, en aan welke randvoorwaarden daarbij moet worden voldaan.

### (Medisch) beroepsgeheim

Naast bovenstaande wet- en regelgeving vervult het (medisch) beroepsgeheim ook nog een belangrijke rol in de wijze waarop gegevensuitwisseling al dan niet plaatsvindt. Zo geldt voor zorgprofessionals over het algemeen dat zij gehouden zijn aan een (medisch) beroepsgeheim. Dat is een belangrijk recht dat de medische professional en de patiënt hebben, om de vertrouwelijke relatie tussen behandelaar en patiënt te beschermen. Op basis van dit beroepsgeheim mogen zij (patiënt)gegevens alleen onder bepaalde (uitzonderlijke) omstandigheden delen met derden.

45 https://www.kcbr.nl/beleid-en-regelgeving-ontwikkelen/beleidskompas/3-wat-zijn-opties-om-het-doel-te-realiseren/32-rechtmatigheid/323-algemene-rechtsbeginselen#:~:text=Als%20belangrijkste%20algemene%20beginselen%20van,%2C%20het%20vertrouwensbeginsel%2C%20het%20gelijkheidsbeginsel.

### Wet gemeentelijke schuldhulpverlening (Wgs)

De Wgs verplicht gemeenten om inwoners met schulden hulp te bieden. Gemeenten krijgen in de Wgs mogelijkheden voor vroegsignalering van schuldenproblematiek bij haar inwoners, om te voorkomen dat betalingsachterstanden uitgroeien tot problematische schulden. Advies, schuldbemiddeling of saneringskrediet vallen onder de regietaak die aan de gemeente wordt toegekend in de Wgs. De Wgs is in 2018 herzien om het voor gemeenten onder andere mogelijk te maken informatie over inwoners met schuldenproblematiek op te vragen bij derden als onderdeel van vroegsignalering.

De verschillende fasen binnen de schuldhulpverlening (vroegsignalering, toegang tot schuldhulpverlening, opstellen Plan van Aanpak en de uitvoering daarvan) zijn voor de Wgs vastgesteld als doelen voor gegevensverwerking voor gemeenten. De gemeenten die taken met betrekking tot schuldhulpverlening hebben toebedeeld aan de SON kunnen ervoor kiezen om dienstverlening van de SON in te zetten in alle, enkele of slechts één fase(n) van de schuldhulpverlening.

### Wet op het consumentenkrediet (Wck), Wet financiering decentrale overheden en Participatiewet.

De wet op het consumentenkrediet (Wck) en de Wet financiering decentrale overheden reguleren de kredietttransacties die de SON uitvoert voor de deelnemende gemeenten. Ook schuldbemiddeling en het uitvoeren van schuldenregelingen door de SON vallen onder de Wck. Voor de taken van de SON rondom budgetbeheer kunnen gemeenten ervoor kiezen om de SON ook betalingen van bijstandsuitkeringen te laten verrichten die onder de Participatiewet zouden moeten geschieden.

### Faillissementswet (Fw)

Op grond van de Fw kan de SON bewindvoering en curatele uitvoeren, inclusief onderbewindstelling van minderjarigen. Ook kan de SON verklaringen afgeven dat er geen reële mogelijkheden zijn om tot ‘buitengerechtelijke schuldregeling’ te komen als er sprake is van een faillissement.

Berenschot



## ‘WIJ ZIJN BERENSCHOT, GRONDLEGGER VAN VOORUITGANG’

Nederland is continu in ontwikkeling. Maatschappelijk, economisch en organisatorisch verandert er veel. Al ruim 85 jaar volgen wij als adviesbureau deze ontwikkelingen op de voet en werken we aan een vooruitstrevende samenleving. De behoefte om iets fundamenteels te betekenen voor mens en maatschappij zit in onze genen. Met onze adviezen en oplossingen hebben we dan ook actief meegebouwd aan het Nederland van vandaag. Altijd op zoek naar duurzame vooruitgang.

Alles wat we doen is onderzocht, onderbouwd en vanuit meerdere invalshoeken bekeken. Zo komen we tot gefundeerde adviezen en slimme oplossingen. Die zijn op het eerste gezicht misschien niet altijd de meest voor de hand liggende. Juist deze eigenzinnigheid maakt ons uniek. Daarbij zijn we niet van symptoombestrijding. En gaan pas naar huis als het is opgelost.

**Berenschot Groep B.V.**
Van Deventerlaan 31-51, 3528 AG  Utrecht
Postbus 8039, 3503 RA  Utrecht
030 2 916 916
www.berenschot.nl