centrum informatiebeveiliging en privacybescherming

Handreiking gegevensverwerking in complexe ketens

Naar rechtmatige en betrouwbare informatie-uitwisseling tussen organisaties

November 2026

Het CIP betracht zorgvuldigheid bij het samenstellen van zijn publicaties. Het kan voorkomen dat er toch sprake is van omissies, onjuistheden en/of gedateerdheid. Het is altijd de verantwoordelijkheid van de lezer zelf dit te beoordelen en desgewenst te corrigeren indien hij zich baseert op of gebruik maakt van een CIP-publicatie. Het CIP ontvangt graag correctieverzoeken en suggesties.



©Centrum Informatiebeveiliging en Privacybescherming. Het CIP heeft voor deze publicatie licentie Creative Commons Naamsvermelding-NietCommercieel-GelijkDelen (CC BY-NC-SA 4.0) verleend. Voor meer informatie zie: https://creativecommons.org/licenses/by-nc-sa/4.0/deed.nl.

Handreiking gegevensverwerking in complexe ketens

Titel	Handreiking gegevensverwerking in complexe ketens
Datum	November 2026
Versie en status	Definitief
Opdrachtgever	Centrum Informatiebeveiliging en Privacybescherming (CIP)
Regime	Becommentarieerde praktijk
Auteurs	Marie-José Bonthuis en Peter Seignette
Reviewers	Leden van de Adviesgroep Privacy

Considerans

CIP-producten steunen op kennis van professionals uit verschillende organisaties actief in het CIP-netwerk, zowel uit de overheid als de markt. Opmerkingen en aanvullingen kun je melden op cip-overheid.nl/contact.

Kern van de handreiking

Het vertrekpunt voor organisatie-overstijgende gegevensverwerking is niet de AVG-rol (verwerkingsverantwoordelijke (al dan niet gezamenlijk), verwerker), een overeenkomst of een technische voorziening, maar de maatschappelijke opgave. Eerst dient te worden bepaald welk probleem op ketenniveau moet worden beheerst en welke informatie daarvoor noodzakelijk is. Pas daarna volgen beoordeling van de rechtmatigheid, inrichting, afspraken en waarborgen.

Doelgroep

Deze handreiking is primair bedoeld voor beleidsmakers, programmamanagers, informatiearchitecten, juristen, privacy professionals, Functionarissen Gegevensbescherming, informatiebeveiligers en uitvoeringsorganisaties die samenwerking tussen zelfstandige organisaties ontwerpen, beoordelen of besturen.

Hoe deze handreiking te gebruiken

Hoofdstuk 1 helpt bepalen om welk type samenwerking het gaat. Hoofdstuk 2 behandelt de betekenis van gegevens in een organisatie-overstijgende context. Hoofdstuk 3 onderzoekt het gerechtvaardigde doel en de informatiebehoefte. Hoofdstuk 4 behandelt de beoordeling van de rechtmatigheid en instrumenten. Hoofdstuk 5 werkt de AVG-rollen en verantwoordelijkheden uit. Hoofdstuk 6 onderzoekt de impact van gegevensverwerking in complexe ketens. Hoofdstuk 7 bevat een stappenplan voor de ketenanalyse. Hoofdstukken 8 en 9 bevatten conclusies en aanbevelingen.

Inleiding

De CIP-handreiking Privacyafspraken bij ketensamenwerking biedt een waardevol kader voor het maken van afspraken tussen samenwerkende organisaties met aandacht voor AVG-rollen, verantwoordelijkheden en overige onderlinge afspraken.

Deze handreiking richt zich op complexe, organisatie-overstijgende samenwerking waarin geen enkele deelnemer de maatschappelijke opgave zelfstandig kan realiseren. De centrale vraag is niet welke gegevens organisaties kunnen uitwisselen, maar welke informatie nodig is om het gezamenlijke probleem aan te pakken. Door gegevens samen te brengen, te combineren en te interpreteren kan een nieuwe informatiepositie ontstaan, met gevolgen die bij afzonderlijke organisaties niet volledig zichtbaar zijn. Daarom onderscheiden we het organisatieniveau en het ketenniveau: rechtmatigheid bij de bron betekent niet automatisch dat de gezamenlijke verwerking en het gebruik van de informatie rechtmatig zijn. De betekenis, betrouwbaarheid, herkomst en onzekerheid van gegevens verdienen daarbij evenveel aandacht als hun beschikbaarheid. De noodzakelijke informatieverwerking en de beoordeling van de rechtmatigheid vormen vervolgens het vertrekpunt voor de keuze van AVG-rollen, organisatorische afspraken, passende waarborgen en blijvende herbeoordeling. Het stappenplan in hoofdstuk 7 brengt deze onderdelen bijeen.

Inhoudsopgave

Inleiding 3

1 Soorten ketens 6

1.1 Wat verstaan we onder een keten? 6

1.2 Eenvoudige en complexe samenwerkingsketens 6

1.3 Herkennen van complexe ketensamenwerking 7

1.4 Praktijkvoorbeeld: de epidemiebestrijdingsketen 7

2 Van organisatiegegevens naar keteninformatie 11

2.1 Twee niveaus van gegevensverwerking 11

2.2 Gegevens krijgen betekenis binnen een bepaalde context 12

2.3 Door gegevens te verbinden ontstaat nieuwe informatie 13

2.4 Een andere informatiepositie vraagt om een beoordeling van de rechtmatigheid op ketenniveau 14

2.5 De gevolgen voor de inrichting van de informatievoorziening 14

2.6 Wanneer maken we (nog meer) een niveauvergissing? 16

3 Het gerechtvaardigde doel van de keten 18

3.1 Van probleem naar minimale informatiebehoefte 18

3.2 Beroepsgeheim, professionele context en beperkte informatie-uitwisseling 19

3.3 Toestemming als juridisch instrument bij ketensamenwerking 20

3.4 Generieke toestemmingsvoorzieningen: functie en grenzen 20

4 Juridische en organisatorische instrumenten voor ketensamenwerking 21

4.1 Wettelijke kaders voor gegevensverwerking op ketenniveau 21

4.2 De functie en grenzen van verschillende instrumenten 22

5 AVG-rollen en verantwoordelijkheden in de keten 24

5.1 Verwerkingsverantwoordelijke: beslissend is de feitelijke zeggenschap 24

5.2 Gezamenlijke verwerkingsverantwoordelijkheid 24

5.3 De verwerker: handelen namens een verantwoordelijke 25

5.4 Rolbepaling bij gedeelde voorzieningen 25

5.5 Van rolbepaling naar werkbare afspraken 25

6 De impact van gegevensverwerking in complexe ketens 27

7 Stappenplan voor gegevensverwerking in complexe ketens 29

7.1	Fase 1: De maatschappelijke opgave en de keten	29
7.2	Fase 2: De noodzakelijke informatieverwerking en de beoordeling van de rechtmatigheid	31
7.3	Fase 3: De rechten, risico's en waarborgen	32
7.4	Fase 4: De inrichting en blijvende verantwoording	34
7.5	Het stappenplan als samenhangende beoordeling	36
8	Conclusies	37
9	Aanbevelingen	38
10	Tot slot	39
11	Bronnen	40

1 Soorten ketens

1.1 Wat verstaan we onder een keten?

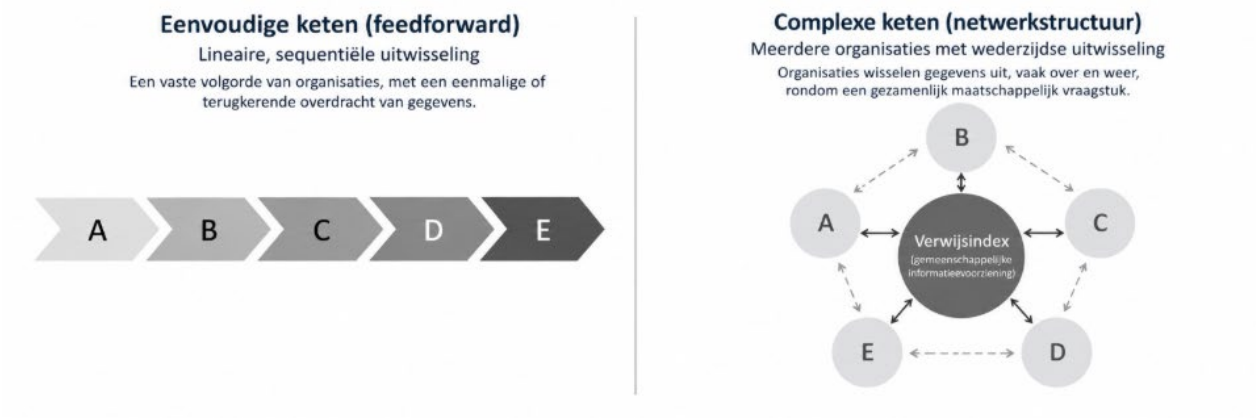
Niet ieder samenwerkingsverband, netwerk of gegevensuitwisselingsproject is in de betekenis van deze handreiking een keten. Van een relevante maatschappelijke keten is sprake wanneer meerdere zelfstandige organisaties voor een terugkerende maatschappelijke opgave van elkaar afhankelijk zijn, terwijl geen van hen over voldoende gezag, informatie of uitvoeringsvermogen beschikt om het probleem zelfstandig op te lossen. De 'grens' volgt daarom niet primair uit een sector, contract, platform of organisatieschema, maar uit het probleem dat gezamenlijk moet worden beheerst. Een keten is daarnaast een abstract concept dat weliswaar in de praktijk te herkennen is maar niet formeel bij wet is aangewezen of correspondeert met een maatschappelijke sector, departement van de rijksoverheid of juridisch verbonden organisaties.

De samenwerking wordt niet door één organisatie bestuurd: de deelnemers behouden eigen taken en verantwoordelijkheden. Het terugkerende maatschappelijke probleem verklaart waarom zij elkaar nodig hebben. Dit sluit aan bij het uitgangspunt uit de keteninformatisering dat het gezamenlijke probleem, en niet een centrale bestuurder, de samenwerking bepaalt.

1.2 Eenvoudige en complexe samenwerkingsketens

Bij een relatief eenvoudige keten verloopt de samenwerking grotendeels sequentieel: een herkenbare reeks stappen met vooraf bekende betrokken partijen en informatiebehoeften. Bij een complexe keten is de samenhang dynamischer: verschillende trajecten lopen naast elkaar, nieuwe informatie kan eerdere beslissingen beïnvloeden en pas in een concrete situatie wordt duidelijk welke partijen en gegevens relevant zijn. Complexiteit is gradueel en hangt onder meer af van autonomie, afhankelijkheden, veranderlijkheid, terugkoppeling en het aantal mogelijke routes. Ook een sequentiële keten kan complex zijn.

Een ketensamenwerking kan gegevens uit verschillende bronnen samenbrengen, combineren en interpreteren. Het onderscheid tussen eenvoudige en complexe ketens hangt echter niet af van de gekozen techniek, maar van de aard van de onderlinge afhankelijkheden, de informatiebehoefte en de samenhang van de activiteiten.



Figuur 1. Eenvoudige en complexe ketens: sequentiële uitwisseling versus netwerkstructuur

Links is een eenvoudige keten weergegeven, waarin informatie volgens een vooraf bekende volgorde tussen organisaties wordt overgedragen. Let wel, er kunnen ook tijdens een eenvoudige of sequentiële

keten ook feedbackloops ontstaan. Rechts is een complexe/dynamische keten weergegeven, waarin verschillende zelfstandige organisaties beschikken over informatie die gezamenlijk nodig kan zijn om een organisatie-overstijgend probleem aan te pakken. Daarbij is niet altijd vooraf bekend bij welke organisatie de relevante op welk moment informatie beschikbaar is (of wordt). Informatie die bij de ene organisatie ontstaat, kan bovendien relevant zijn voor beslissingen bij een andere organisatie, ongeacht de volgorde van hun werkzaamheden. Dit vraagt om voorzieningen waarmee relevante informatie kan worden gevonden en, waar nodig en toegestaan, uitgewisseld. Een koppelmechanisme zoals bijvoorbeeld een verwijsindex in de figuur illustreert zo'n mogelijke voorziening. We komen later terug op dat niet alle inhoudelijke gegevens centraal hoeven te worden opgeslagen. Met enkel *communicatie* kan immers al een maatschappelijke ketenopgave worden gerealiseerd.

1.3 Herkennen van complexe ketensamenwerking

De volgende acht vragen helpen om de kenmerken van een keten vast te stellen en te bepalen welke vorm van samenwerking en informatievoorziening passend is:

1. Welke maatschappelijke uitkomst moet worden beschermd of verbeterd?
2. Welke zelfstandige organisaties zijn noodzakelijk om die uitkomst te bereiken?
3. Verloopt de samenwerking overwegend volgens een vaste, sequentiële volgorde, of zijn meerdere, wisselende verbindingen tussen organisaties nodig?
4. Is vooraf bekend waar de benodigde informatie beschikbaar is, of moet deze bij verschillende organisaties worden gevonden en in samenhang worden beoordeeld?
5. Welke gegevens worden samengebracht of gecombineerd, welke nieuwe informatie kan daardoor ontstaan en wie gebruikt die informatie?
6. Welke informatie kan bilateraal of binnen de eigen organisatie blijven?
7. Welke gemeenschappelijke informatie- of communicatiefunctie is daadwerkelijk nodig?
8. Is de voorgestelde infrastructuur een antwoord op een aantoonbaar organisatie-overstijgend probleem, of is zij zelf het vertrekpunt geworden?

1.4 Praktijkvoorbeeld: de epidemiebestrijdingsketen

Hoe werken de acht vragen uit de vorige paragraaf in de praktijk? We illustreren dit aan de hand van de epidemiebestrijdingsketen. Hiervoor gebruiken we een bestaande analyse van de samenwerking bij de bestrijding van infectieziekten (Visser e.a., 2011).

De analyse laat zien hoe organisaties die ieder een eigen taak hebben, afhankelijk zijn van informatie van anderen om een infectieziekte effectief te kunnen bestrijden. De oorspronkelijke analyse is hier vertaald naar de acht vragen uit paragraaf 1.3. De beschrijving is illustratief en geeft niet noodzakelijk de huidige inrichting van de infectieziektebestrijding weer.

1.4.1 *Welke maatschappelijke uitkomst moet worden beschermd of verbeterd?*

Het doel is om de verspreiding van infectieziekten te beheersen en maatschappelijke ontwrichting te voorkomen. Daarbij gaat het niet alleen om het voorkomen van besmettingen, maar ook om het vermijden van onnodig ingrijpende maatregelen. Dat vraagt om een zo goed mogelijk beeld van de

aard, omvang en verspreiding van een infectieziekte. Zonder voldoende informatie bestaat het risico dat te laat, onvoldoende of juist te zwaar wordt ingegrepen.

1.4.2 *Welke zelfstandige organisaties zijn noodzakelijk om die uitkomst te bereiken?*

Bij de bestrijding van infectieziekten zijn verschillende organisaties betrokken, zoals huisartsen, ziekenhuizen, laboratoria, GGD'en, het RIVM en bestuurlijke instanties. Zij vervullen verschillende taken. Zorgverleners herkennen ziekteverschijnselen, laboratoria onderzoeken mogelijke ziekteverwekkers, publieke gezondheidsorganisaties beoordelen de verspreiding en bevoegde instanties beslissen over maatregelen.

Geen van deze organisaties beschikt zelfstandig over alle informatie of mogelijkheden die nodig zijn om een epidemie te bestrijden.

1.4.3 *Verloopt de samenwerking overwegend volgens een vaste, sequentiële volgorde, of zijn meerdere, wisselende verbindingen tussen organisaties nodig?*

De infectieziektebestrijding kent herkenbare activiteiten: signaleren, onderzoeken, beoordelen, maatregelen nemen en evalueren. Deze activiteiten volgen echter niet altijd een vaste volgorde. Terwijl onderzoek nog loopt, kunnen nieuwe besmettingen worden gemeld of maatregelen nodig zijn. Nieuwe onderzoeksresultaten kunnen aanleiding geven om eerdere besluiten te herzien.

Organisaties moeten daarom op verschillende momenten informatie kunnen uitwisselen en hun werkzaamheden op elkaar afstemmen. De samenwerking verloopt niet uitsluitend van de ene organisatie naar de volgende.

1.4.4 *Is vooraf bekend waar de benodigde informatie beschikbaar is, of moet deze bij verschillende organisaties worden gevonden en in samenhang worden beoordeeld?*

Informatie over een mogelijke uitbraak kan op verschillende plaatsen ontstaan. Een huisarts ziet bijvoorbeeld meerdere patiënten met vergelijkbare klachten, een laboratorium ontdekt een bijzondere ziekteverwekker en een GGD constateert een ongebruikelijke toename van besmettingen.

Bij bekende infectieziekten zijn veel meldingen en informatieprocessen vooraf geregeld. Bij een onbekende ziekteverwekker of onverwacht verspreidingspatroon is minder duidelijk waar relevante informatie beschikbaar is. Het is dan niet voldoende om bestaande gegevensstromen te volgen. Organisaties moeten ook kunnen achterhalen waar relevante informatie aanwezig is en wat verschillende signalen gezamenlijk betekenen.

1.4.5 *Hoe worden gegevens samengebracht, gecombineerd en geïnterpreteerd?*

Informatie wordt op verschillende manieren gedeeld. Laboratoria en zorgverleners kunnen meldingen doen, organisaties kunnen onderzoeksresultaten uitwisselen en professionals kunnen gericht informatie bij elkaar opvragen. Sommige gegevens worden volgens vaste afspraken verstrekt. Andere informatie wordt pas opgevraagd wanneer een concrete situatie daarom vraagt. Beide vormen kunnen binnen dezelfde keten voorkomen. De manier waarop gegevens worden uitgewisseld, bepaalt daarom niet op zichzelf of een keten eenvoudig of complex is.

1.4.6 *Welke informatie kan bilateraal of binnen de eigen organisatie blijven?*

Niet alle informatie die organisaties verzamelen, hoeft voor de hele keten beschikbaar te zijn.

Medische dossiers kunnen bijvoorbeeld bij de zorgverlener blijven en gedetailleerde onderzoeksgegevens bij het laboratorium. Voor een gezamenlijke beoordeling kan het voldoende zijn om te weten om welke infectieziekte het gaat, welk gebied mogelijk wordt getroffen en hoe ernstig de situatie is.

In de oorspronkelijke analyse werden daarom drie gegevens voorgesteld die de gezamenlijke beoordeling konden ondersteunen: de infectieziekte, het risicogebied en een aanduiding van de ernst van de dreiging.

Dit illustreert dat samenwerking niet noodzakelijk vraagt om het bijeenbrengen van *alle* beschikbare gegevens.

1.4.7 *Welke gemeenschappelijke informatie- of communicatiefunctie is daadwerkelijk nodig?*

Voor effectieve bestrijding moeten onderzoeksresultaten tijdig beschikbaar kunnen komen voor degenen die over maatregelen beslissen. De oorspronkelijke analyse constateerde dat de aansluiting tussen onderzoek en besluitvorming onvoldoende was. Daardoor konden beslissingen worden genomen zonder dat alle relevante inzichten beschikbaar waren.

De vraag is dan welke gezamenlijke ondersteuning nodig is. Moeten organisaties elkaar sneller kunnen informeren? Moet duidelijk zijn waar bepaalde informatie beschikbaar is? Of is vooral een gemeenschappelijk beeld van de ernst en verspreiding van een infectieziekte nodig?

Afhankelijk van het probleem kunnen bestaande informatiekanalen, gerichte meldingen, een verwijzingsfunctie of een aanvullende gezamenlijke voorziening passend zijn.

1.4.8 *Is de voorgestelde infrastructuur een antwoord op een aantoonbaar organisatie-overstijgend probleem, of is zij zelf het vertrekpunt geworden?*

(Integrale) informatie is nodig om een bepaalde ketenopgave te realiseren. De infrastructuur is slechts het middel waarmee communicatie wordt ondersteund. Dat onderscheid is cruciaal: een landelijk schakelpunt (LSP), verwijsindex, generieke functie, portal of gegevensknooppunt is geen keten op zichzelf. Andersom kan één maatschappelijke keten gebruikmaken van meerdere infrastructuren.

Aan de hand van dit onderscheid kan worden beoordeeld of het initiatief is begonnen bij het probleem en de noodzakelijke communicatie, of bij een beschikbare voorziening die vervolgens een use case zoekt? Het AcICT-advies over Implementatie Generieke Functies illustreert het risico van het tweede. Het adviescollege constateert dat onvoldoende concreet is voor welke problemen de generieke functies een oplossing zijn en dat het opleveren van functies te veel een doel op zichzelf is geworden.

In deze casus begint de analyse bij het risico dat bestrijdingsmaatregelen niet goed aansluiten op de werkelijke dreiging. Vervolgens wordt onderzocht welke informatie organisaties nodig hebben om gezamenlijk beter te kunnen handelen.

De oorspronkelijke onderzoekers concludeerden in 2011 dat aanvullende gezamenlijke informatievoorziening noodzakelijk en op termijn haalbaar was. Zij adviseerden deze stapsgewijs te ontwikkelen.

1.4.9 *Wat leert deze casus?*

De epidemiebestrijdingsketen laat zien dat een complexe keten niet simpelweg een lange reeks organisaties is. De organisaties hebben verschillende taken, informatie ontstaat op uiteenlopende plaatsen en nieuwe ontwikkelingen kunnen steeds aanleiding geven om eerdere beoordelingen en beslissingen te herzien.

De gezamenlijke opgave vraagt daarom om informatie die uit verschillende bronnen afkomstig is en in samenhang moet worden beoordeeld.

Tegelijkertijd hoeft niet alle informatie voor alle betrokken organisaties beschikbaar te zijn. Een belangrijk resultaat van de analyse is juist dat duidelijk wordt welke informatie binnen een organisatie kan blijven, welke informatie rechtstreeks kan worden uitgewisseld en waarvoor een gezamenlijke voorziening nodig kan zijn.

De ketenanalyse helpt zo om de noodzakelijke samenwerking en informatievoorziening vast te stellen, voordat wordt besloten over technische oplossingen en de juridische inrichting daarvan.

2 Van organisatiegegevens naar keteninformatie

Bij ketensamenwerking worden persoonsgegevens verwerkt in een context waarin meerdere organisaties betrokken zijn bij het realiseren van een gezamenlijk of samenhangend doel. Hoewel de betrokken organisaties ieder eigen taken, bevoegdheden en verantwoordelijkheden hebben, staan de gegevensverwerkingen binnen een keten niet altijd op zichzelf. Gegevens kunnen tussen organisaties worden uitgewisseld, gecombineerd of voor opeenvolgende doeleinden worden gebruikt. Hierdoor kunnen privacyvraagstukken ontstaan die niet uitsluitend vanuit de afzonderlijke gegevensverwerkingen kunnen worden beoordeeld, maar ook aandacht vragen voor de samenhang binnen de keten. Niet iedere ketensamenwerking kent zulke afhankelijkheden. Juist het verschil tussen een eenvoudige, sequentiële gegevensuitwisseling en een complexere netwerkstructuur maakt duidelijk wanneer beoordeling op ketenniveau meerwaarde heeft.

Privacyafspraken bij ketensamenwerking hebben betrekking op meer dan de afzonderlijke gegevensuitwisselingen tussen organisaties. Ook de inrichting van de samenwerking als geheel is relevant. Daarbij gaat het onder meer om de gezamenlijke doelstelling, de samenhang tussen gegevensverwerkingen, de verdeling van verantwoordelijkheden en de wijze waarop betrokken organisaties gezamenlijk invulling geven aan de bescherming van persoonsgegevens.

Om deze verschillende aspecten te kunnen beoordelen, maakt deze handreiking onderscheid tussen twee niveaus van ketensamenwerking.

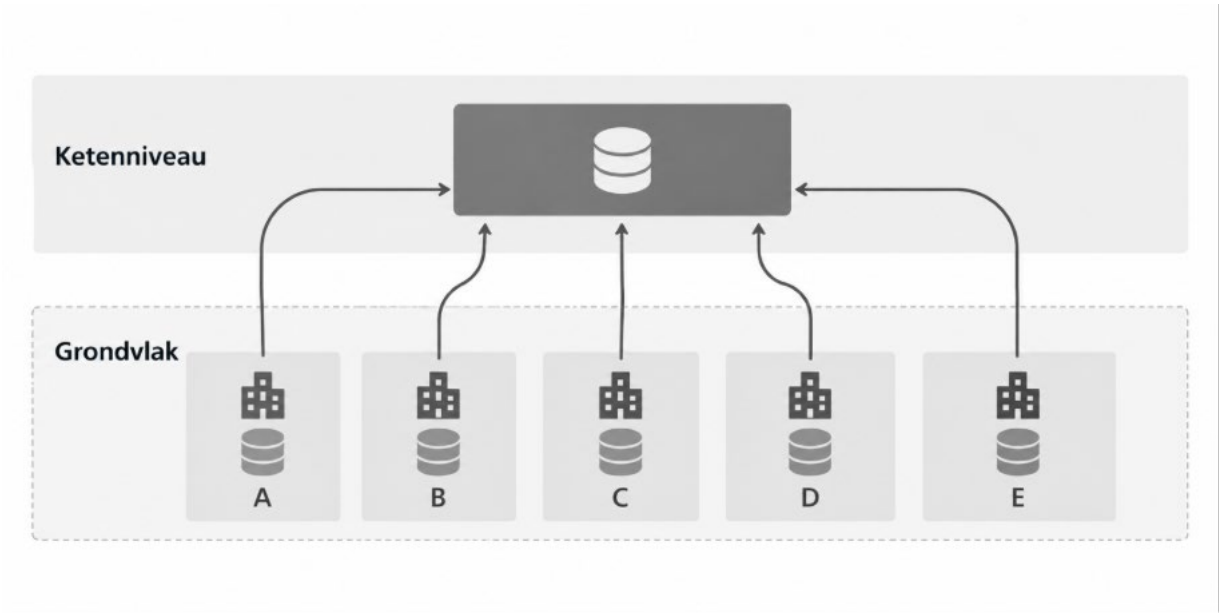
2.1 Twee niveaus van gegevensverwerking

Bij complexe/dynamische ketens is het van belang onderscheid te maken tussen twee niveaus waarop gegevens worden verwerkt.

Op het *organisatieniveau*, in de theorie van keteninformatisering ook wel het ‘grondvlak’ genoemd, verwerken afzonderlijke organisaties gegevens voor hun eigen taken en verantwoordelijkheden. Bij de infectieziektebestrijding gaat het bijvoorbeeld om gegevensverwerkingen door zorgverleners, laboratoria en GGD'en, ieder vanuit hun eigen rol.

Op het *ketenniveau* gaat het om de informatie die nodig is om een maatschappelijke opgave aan te pakken die geen van deze organisaties zelfstandig kan realiseren. Daarvoor kan het noodzakelijk zijn gegevens uit verschillende organisaties met elkaar in verband te brengen. De gegevens hoeven daarvoor niet zondermeer op één plaats te worden opgeslagen.

Dit onderscheid gaat niet in de eerste plaats over de technische inrichting van de gegevensuitwisseling, maar over het niveau waarop de informatiebehoefte ontstaat en de gegevensverwerking moet worden beoordeeld.



Figuur 2. Onderscheid organisatieniveau en ketenniveau

In het vorige hoofdstuk is beschreven hoe zelfstandige organisaties voor een maatschappelijke opgave van elkaar afhankelijk kunnen zijn. Daarbij is niet alleen sprake van samenwerking tussen organisaties, maar ook van het gebruik van informatie buiten de omgeving waarin deze oorspronkelijk is verzameld.

Dat heeft gevolgen voor de betekenis van gegevens, de inzichten die daaruit kunnen ontstaan en de wijze waarop de verwerking moet worden beoordeeld. Informatie die binnen één organisatie voor een bepaald doel is vastgelegd, kan in een andere context een andere betekenis krijgen. Door informatie uit verschillende bronnen met elkaar in verband te brengen, kunnen bovendien nieuwe inzichten ontstaan waarover geen van de afzonderlijke organisaties zelf beschikte. Daarom kan organisatie-overstijgende gegevensverwerking niet uitsluitend worden beoordeeld als een optelsom van afzonderlijke gegevensverstrekkingen. Er moet ook worden onderzocht wat de samenwerking als geheel mogelijk maakt, welke nieuwe informatie daarbij ontstaat en hoe dit gebruik wordt gerechtvaardigd.

2.2 Gegevens krijgen betekenis binnen een bepaalde context

Organisaties verwerken (persoons)gegevens voor de uitvoering van hun eigen taken. De betekenis van die gegevens hangt samen met het doel waarvoor zij zijn vastgelegd, de omstandigheden waaronder dat is gebeurd en de manier waarop zij worden geïnterpreteerd. Een registratie van een betalingsachterstand kan bijvoorbeeld binnen een organisatie een administratief gegeven zijn. Bij een andere organisatie kan dezelfde registratie worden opgevat als een aanwijzing voor financiële kwetsbaarheid.

Wanneer gegevens buiten hun oorspronkelijke context worden gebruikt, bestaat het risico dat belangrijke informatie verloren gaat of dat er een nieuwe betekenis aan wordt gegeven. Denk aan de herkomst van het gegeven, het moment van vastlegging, de betrouwbaarheid, de gebruikte definities en de beperkingen waaronder het gegeven mag worden geïnterpreteerd. Dit wordt decontextualisatie genoemd: gegevens raken geheel of gedeeltelijk los van de context waarin zij oorspronkelijk betekenis hadden.

Voorbeeld: een adreswijziging in de Basisregistratie Personen zegt waar iemand staat ingeschreven, maar verklaart niet waarom iemand is verhuisd. Een gemeente die de wijziging gebruikt als signaal voor

mogelijke woonfraude moet die oorspronkelijke betekenis en de onzekerheid van de gevolgtrekking blijven onderscheiden.

Dat betekent niet dat gegevens buiten hun oorspronkelijke context onbruikbaar zijn. Wel moet opnieuw worden beoordeeld of zij geschikt zijn voor het beoogde gebruik. Een gegeven kan juist zijn binnen het oorspronkelijke proces, maar onvolledig, verouderd of misleidend zijn wanneer het voor een andere beslissing wordt gebruikt.

"Meer beschikbare gegevens leiden daarom niet vanzelf tot betere informatie of betere beslissingen."

2.3 Door gegevens te verbinden ontstaat nieuwe informatie

Bij organisatie-overstijgende samenwerking gebeurt meer dan het overdragen van bestaande gegevens. Door informatie uit verschillende bronnen in samenhang te beoordelen, kunnen nieuwe inzichten, verbanden en kwalificaties ontstaan. Een betalingsachterstand, een verandering in woonsituatie en een onderbreking van zorgverlening kunnen afzonderlijk iets zeggen over iemands persoonlijke omstandigheden. Wanneer deze gegevens worden gecombineerd, kan daaruit een vermoeden van kwetsbaarheid of een risico op maatschappelijke problemen ontstaan. Dat vermoeden is nieuwe informatie. Het is niet als zodanig vastgelegd in een van de oorspronkelijke registraties en kan bovendien onzeker of onjuist zijn.

Een gemeente kan signalen over schulden, schoolverzuim en een verhuizing combineren om te bepalen of contact (bemoeizorg) met een gezin wenselijk is. Het samengestelde signaal is een nieuwe beoordeling, geen feit dat al in een van de afzonderlijke registraties stond. Of deze combinatie juridisch is toegestaan, moet afzonderlijk worden getoetst.

Daarbij kunnen drie vormen van informatie worden onderscheiden:

- Vastgelegde informatie: gegevens die een organisatie expliciet heeft geregistreerd.
- Vindbare informatie (ook wel: discoverability): informatie waarvan het bestaan en de vindplaats kunnen worden achterhaald, zonder dat de inhoud zelf al beschikbaar hoeft te zijn. Het vinden van informatie kan bovendien op zichzelf iets nieuws onthullen, bijvoorbeeld wanneer blijkt dat een persoon bij een gespecialiseerde hulpverlener bekend is.
- Afleidbare informatie (ook wel: inferability): nieuwe inzichten of conclusies die ontstaan door gegevens te combineren, te analyseren of met behulp van een model te interpreteren.

Vooral de derde vorm laat zien dat op het niveau van de samenwerking iets nieuws kan ontstaan. De gezamenlijke informatiepositie kan meer omvatten dan de informatie waarover de afzonderlijke organisaties beschikken. Het gaat daarbij niet alleen om de hoeveelheid gegevens, maar om de nieuwe betekenis die door hun onderlinge samenhang ontstaat.

Deze nieuwe informatie kan vervolgens worden gebruikt voor beoordelingen, signaleringen of besluiten die gevolgen hebben voor personen of groepen. Dat roept vragen op over de betrouwbaarheid van de afleiding, de verantwoordelijkheid voor de nieuwe informatie en de mogelijkheden om onjuiste conclusies te herkennen en te corrigeren.

Wanneer door combinatie of interpretatie nieuwe informatie over identificeerbare personen ontstaat, kan ook die afgeleide informatie onder de AVG vallen (artikel 4, onder 1 en 2, AVG). Of sprake is van

verdere verwerking voor een ander doel, vergt een afzonderlijke juridische beoordeling (artikel 5, eerste lid, onder b, en artikel 6, vierde lid, AVG). Voor de ketenanalyse staat daarnaast centraal welke nieuwe informatiepositie op ketenniveau ontstaat en hoe deze kan worden gerechtvaardigd.

2.4 Een andere informatiepositie vraagt om een beoordeling van de rechtmatigheid op ketenniveau

De oorspronkelijke gegevensverwerkingen vinden plaats binnen de taken, bevoegdheden en verantwoordelijkheden van afzonderlijke organisaties. Voor deze verwerkingen bestaan juridische en organisatorische kaders. Wanneer gegevens vervolgens in een organisatie-overstijgende samenwerking worden gebruikt, kan een andere informatiepositie ontstaan. De samenwerking maakt verbanden zichtbaar die afzonderlijke organisaties niet konden leggen en kan nieuwe beoordelingen of interventies mogelijk maken.

Daarmee ontstaat een eigen beoordelingsvraag: is het rechtmatig om deze informatie op het niveau van de samenwerking bijeen te brengen, te verbinden of daaruit nieuwe conclusies af te leiden? Dat een organisatie gegevens rechtmatig heeft verzameld, betekent niet automatisch dat ieder volgend gebruik binnen een samenwerkingsverband eveneens rechtmatig is. Ook het feit dat afzonderlijke organisaties een wettelijke taak hebben of gegevens mogen verstrekken, vormt op zichzelf nog geen voldoende juridische basis voor de gezamenlijke informatieverwerking. De maatschappelijke noodzaak en de gevolgen voor betrokkenen moeten daarbij eveneens worden onderbouwd en beoordeeld.

De beoordeling moet daarom ook betrekking hebben op:

- Het maatschappelijke probleem waarvoor de samenwerking noodzakelijk is.
- De informatie die daarvoor daadwerkelijk nodig is.
- De nieuwe inzichten of kwalificaties die door het combineren van gegevens kunnen ontstaan.
- De gevolgen van deze informatie voor betrokkenen.
- De verdeling van verantwoordelijkheden voor het gebruik, de betrouwbaarheid en de correctie van informatie.

Deze beoordeling betreft de rechtmatigheid van de gegevensverwerking op ketenniveau. Zij vervangt niet de beoordeling van wettelijke grondslagen, bevoegdheden, geheimhoudingsplichten en overige verplichtingen van de betrokken organisaties. Evenmin betekent dit dat de keten automatisch één verwerkingsverantwoordelijke heeft of dat altijd een afzonderlijke wettelijke grondslag moet worden gecreëerd. Het gaat om de beoordeling van de noodzaak, juridische toelaatbaarheid en gevolgen van de organisatie-overstijgende verwerking als geheel. De juridische uitwerking daarvan komt in hoofdstuk 4 aan de orde.

2.5 De gevolgen voor de inrichting van de informatievoorziening

Het onderscheid tussen organisatie- en ketenniveau heeft ook gevolgen voor de inrichting van de informatievoorziening. Binnen een organisatie kunnen processen, systemen, gegevensdefinities en verantwoordelijkheden veelal vanuit één bestuurlijke structuur worden ingericht. In een keten blijven de deelnemende organisaties zelfstandig en beschikken zij over eigen taken, systemen en verantwoordingslijnen.

Het is daarom niet vanzelfsprekend dat de inrichting van een organisatie zonder meer kan worden uitgebreid naar de gehele keten. Een gezamenlijke informatievoorziening hoeft bijvoorbeeld niet alle gegevens uit de deelnemende organisaties te bevatten. Afhankelijk van het maatschappelijke probleem kan het voldoende zijn om vast te stellen waar relevante informatie beschikbaar is, wie kan worden benaderd of welke gebeurtenis voor andere organisaties van belang is.

Een communicatiesysteem voor de keten omvat de afspraken en voorzieningen waarmee organisaties relevante informatie kunnen vinden, uitwisselen en gebruiken. Een koppelmechanisme, zoals een verwijsindex of identificatievoorziening, kan daar onderdeel van zijn, maar is niet in iedere keten noodzakelijk.

Een keteninformatiesysteem kan dus in hoofdzaak een communicatiesysteem zijn, waarbij de brongegevens bij de afzonderlijke organisaties blijven en uitsluitend kritische signalen, verwijzingen of verificaties worden uitgewisseld. Een centrale database is daarvoor niet noodzakelijk.

De keuze voor een voorziening moet volgen uit de informatiebehoefte en het probleem dat de samenwerking moet oplossen. Daarbij moet niet alleen worden gekeken naar technische werking en beveiliging, maar ook naar de betrouwbaarheid van informatie, de geschiktheid voor het beoogde gebruik en de gevolgen van eventuele fouten.

Ook gemeenschappelijke of generieke voorzieningen moeten vanuit deze vragen worden beoordeeld. Hergebruik van voorzieningen kan doelmatig zijn, maar de wens om een generieke oplossing te ontwikkelen is op zichzelf geen rechtvaardiging voor het verbinden of centraal beschikbaar stellen van gegevens.

De inrichting van de informatievoorziening bij ketensamenwerking veronderstelt niet noodzakelijk dat de betrokken organisaties hun informatiesystemen, gegevensstructuren en begrippen volledig standaardiseren. Organisaties kunnen vanuit verschillende taken en verantwoordelijkheden met eigen informatieprofielen werken, terwijl onderlinge communicatie en gegevensuitwisseling mogelijk blijven.

Interoperabiliteit betreft in dat verband niet uitsluitend de technische mogelijkheid om gegevens uit te wisselen, maar ook de wijze waarop informatie tussen verschillende systemen kan worden geïnterpreteerd en betekenis kan behouden. Dit onderscheid is relevant voor ketensamenwerking, omdat een gezamenlijke informatievoorziening niet zonder meer een uniform informatiemodel of een gedeelde interpretatie van alle gegevens vereist.

Standaardisering en interoperabiliteit vervullen verschillende functies binnen de informatievoorziening. Standaardisering kan de uitwisseling van gegevens vergemakkelijken, maar is geen noodzakelijke voorwaarde voor (keten)communicatie. Betekenisvolle communicatie vereist daarom niet dat organisaties dezelfde gegevens op dezelfde wijze structureren of interpreteren, maar dat de uitgewisselde informatie binnen het informatieprofiel van de ontvangende organisatie kan worden begrepen en gebruikt.

Gegevensbescherming door ontwerp en door standaardinstellingen (privacy by design en by default; artikel 25 AVG) vraagt dat de noodzakelijke informatieverwerking vanaf het ontwerp zo beperkt en beschermend mogelijk wordt ingericht. Daarbij kan worden onderzocht of codes, gerichte signaleringen, pseudonimisering of Privacy Enhancing Technologies (PETs), zoals secure multiparty computation en federatieve analyse, de blootstelling van brongegevens kunnen beperken. Deze technieken lossen verschillen in betrouwbaarheid, betekenis of juridische bevoegdheden niet vanzelf op.

Standaardisering op ketenniveau vereist geen uniform gegevensmodel voor alle deelnemers. Wel zijn expliciete afspraken nodig over begrippen, herkomst, status, kwaliteit en interpretatie van de beperkte

set kritische keteninformatie. Verschillen tussen bronregistraties en werkprocessen worden waar nodig in de ketenanalyse zichtbaar gemaakt.

Dit onderscheid is van belang voor de inrichting van ketensamenwerking. De mogelijkheid om gegevens tussen organisaties uit te wisselen, betekent niet dat zij dezelfde betekenis aan die gegevens toekennen of vanuit dezelfde doelstellingen handelen. Wanneer technische uitwisselbaarheid wordt gelijkgesteld aan inhoudelijke of organisatorische samenhang, worden eigenschappen van verschillende niveaus met elkaar verward. Dit duiden we aan als een niveauvergissing.

2.6 Wanneer maken we (nog meer) een niveauvergissing?

De voorgaande paragrafen laten zien dat organisatie-overstijgende gegevensverwerking niet uitsluitend een uitbreiding is van bestaande gegevensstromen. Gegevens worden buiten hun oorspronkelijke context gebruikt, kunnen gezamenlijk nieuwe informatie opleveren en maken andere vormen van beoordeling en besluitvorming mogelijk. Wanneer deze verschillen niet worden onderkend, ontstaat het risico van een niveauvergissing. Van een niveauvergissing is sprake wanneer uitgangspunten, beoordelingsinstrumenten of sturingsmechanismen die voor één organisatie of verwerking zijn ontwikkeld, zonder voldoende herbeoordeling worden toegepast op het niveau van de samenwerking.

Dat kan op verschillende manieren gebeuren. Een bestuurlijke niveauvergissing ontstaat bijvoorbeeld wanneer wordt verondersteld dat een netwerk van zelfstandige organisaties op dezelfde manier kan worden aangestuurd als één organisatie. Een technische niveauvergissing ontstaat wanneer wordt aangenomen dat het samenbrengen van alle beschikbare gegevens vanzelf leidt tot een betere gezamenlijke informatievoorziening. Een juridische niveauvergissing ontstaat wanneer uitsluitend wordt gekeken naar de rechtmatigheid van afzonderlijke gegevensverstrekkingen, zonder te onderzoeken of de organisatie-overstijgende verwerking en de daaruit voortkomende nieuwe informatie voldoende zijn gerechtvaardigd.

De niveauvergissing ontstaat wanneer het gereedschap dat is ontwikkeld voor het organisatieniveau, het niveau van afzonderlijke organisaties en hun gegevensverwerkingen, zonder meer wordt toegepast op het ketenniveau. Door gegevens uit verschillende organisaties met elkaar te verbinden en in samenhang te gebruiken, kan op ketenniveau een nieuwe informatiepositie ontstaan. Gegevens kunnen daarbij hun oorspronkelijke context verliezen of een andere betekenis krijgen. Bovendien kunnen nieuwe inzichten, verbanden en kwalificaties ontstaan die niet in de afzonderlijke bronnen aanwezig waren.

Wat op ketenniveau ontstaat, is niet noodzakelijk de optelsom van wat op het niveau van de afzonderlijke organisaties bestaat. Daarom kan ook de rechtmatigheid van de gezamenlijke verwerking niet zonder meer worden afgeleid uit de rechtmatigheid van de afzonderlijke verwerkingen.

Voorbeeld: afzonderlijke instanties kunnen rechtmatig gegevens verwerken voor hun eigen wettelijke taken. Als een samenwerkingsverband die gegevens combineert tot een gezamenlijk risicoprofiel, is niet alleen de oorspronkelijke verstrekking relevant, maar ook het nieuwe profiel, het gebruik ervan en de gevolgen voor de betrokkene.

De bestaande juridische normen, methoden en instrumenten blijven van toepassing, maar moeten ook worden ingezet om deze nieuwe informatiepositie en de daaruit voortvloeiende verwerkingen te beoordelen. De rechtmatigheid van de verwerking op ketenniveau kan niet zonder meer worden afgeleid uit de afzonderlijke beoordelingen op organisatieniveau.

De niveauvergissing bestaat erin dat we de beoordeling van de afzonderlijke verwerkingen als voldoende beschouwen voor de beoordeling van het geheel, terwijl op ketenniveau iets nieuws is ontstaan dat een eigen beoordeling van de rechtmatigheid vraagt.

De kern is dat een keten niet alleen bestaande informatie uitwisselt, maar ook een nieuwe informatiepositie kan creëren. Die informatiepositie vraagt om een eigen beoordeling van noodzakelijkheid, rechtmatigheid, betrouwbaarheid, gevolgen en verantwoordelijkheid.

De volgende hoofdstukken werken uit hoe deze beoordeling kan plaatsvinden, te beginnen bij het maatschappelijke probleem dat de (keten)samenwerking moet oplossen.

Ook bij de bescherming van persoonsgegevens ligt een niveauvergissing op de loer. Veel van de uitgangspunten, methodieken en normen zijn gebaseerd op een individuele verwerking onder verantwoordelijkheid van één verwerkingsverantwoordelijk die doel en middelen bepaald. De methodieken die helpen om deze situatie te toetsen en in kaart te brengen, zijn niet per se overdraagbaar op ketenniveau.

Op het organisatieniveau beschikken partners over eigen wettelijke taken, processen, bronregistraties, architecturen, budgetten en verantwoordingslijnen. Het ketenniveau bevat alleen die gemeenschappelijke informatie- of coördinatiefuncties die nodig zijn voor het organisatie-overstijgende probleem. Wie interne standaarden, volledigheidseisen of governance één-op-één naar het ketenniveau kopieert, vergroot afhankelijkheden en maakt de keten kwetsbaar.

3 Het gerechtvaardigde doel van de keten

Veel samenwerkingsinitiatieven beginnen met een brede gezamenlijke ambitie: betere zorg, integrale dienstverlening, veiligheid, fraudebestrijding of efficiëntere gegevensuitwisseling. Zulke formuleringen zijn veelal te ruim om te bepalen welke informatieverwerking op ketenniveau noodzakelijk en proportioneel is. Het centrale maatschappelijke probleem dwingt tot precisie: welk terugkerend maatschappelijk probleem is zó ernstig en organisatie-overstijgend dat partijen elkaar nodig hebben?

De noodzaak van samenwerking wordt waar mogelijk onderbouwd met waarneembare maatschappelijke verschijnselen, zoals cijfers, trends, terugkerende incidenten of afwijkende patronen. Die onderbouwing helpt het dominante ketenprobleem af te bakenen en het beoogde resultaat toetsbaar te maken. Bij nieuwe of onvoorspelbare ontwikkelingen, zoals een epidemie, kan de analyse aanvankelijk op signalen, scenario's en expliciete aannames steunen. De ernst van het maatschappelijke probleem rechtvaardigt op zichzelf nog niet iedere gegevensverwerking: de noodzakelijkheid van de kritische informatie en minder ingrijpende alternatieven moeten afzonderlijk worden onderzocht.

Naast een rechtsgrond zijn een aantoonbare maatschappelijke noodzaak, professionele bruikbaarheid, begrijpelijkheid voor betrokkenen, bestuurlijke verantwoording en democratische controle relevant. Deze aspecten vervangen de juridische toets niet; zij maken zichtbaar waarom een technisch mogelijke gegevensstroom niet vanzelf maatschappelijk gerechtvaardigd is.

3.1 Van probleem naar minimale informatiebehoefte

Wanneer duidelijk is welk maatschappelijk probleem de (keten)samenwerking moet aanpakken, is de volgende vraag welke informatie daarvoor daadwerkelijk nodig is. Niet alle gegevens die bij de betrokken organisaties beschikbaar zijn, hoeven immers ook op ketenniveau te worden gebruikt. De informatiebehoefte wordt daarom afgeleid uit het probleem dat de organisaties gezamenlijk moeten oplossen, en niet uit de gegevens die technisch beschikbaar kunnen worden gemaakt.

Bij infectieziektebestrijding kan bijvoorbeeld de noodzaak bestaan om een besmettingsbron te achterhalen, contacten te identificeren of de verspreiding van een infectieziekte te volgen. Voor elk van deze doelen kan andere informatie nodig zijn. Soms volstaat een signaal dat een relevante gebeurtenis heeft plaatsgevonden, terwijl in andere gevallen aanvullende gegevens nodig zijn om een verband te onderzoeken of een passende maatregel te treffen.

De analyse van de informatiebehoefte maakt duidelijk welke gegevens op welk moment, voor welke beslissing en door welke betrokken organisatie nodig zijn. Daarbij wordt ook onderzocht of het noodzakelijk is gegevens tussen organisaties uit te wisselen, of dat een verwijzing, bevestiging of gerichte raadpleging voldoende is. Zo wordt voorkomen dat de samenwerking uitgaat van een bredere gegevensverzameling dan de maatschappelijke opgave rechtvaardigt.

Deze afbakening vormt vervolgens het vertrekpunt voor de juridische beoordeling. Daarbij wordt vastgesteld voor welke doeleinden de gegevens mogen worden verwerkt, welke wettelijke taken en bevoegdheden relevant zijn, op welke rechtsgrondslagen de verwerkingen kunnen berusten en welke waarborgen noodzakelijk zijn. De vastgestelde informatiebehoefte is daarmee niet automatisch juridisch toegestaan, maar maakt wel concreet welke gegevensverwerkingen juridisch moeten worden beoordeeld.

3.2 Beroepsgeheim, professionele context en beperkte informatie-uitwisseling

In complexe ketens kunnen deelnemers verschillende taken, professionele verplichtingen en informatieposities hebben. Voor hulpverleners kan het beroepsgeheim een grens stellen aan het delen van vertrouwelijke gegevens; voor politieorganisaties speelt onder meer dat signalen en vermoedens nog niet zijn geverifieerd. De informatiebehoefte van de keten moet daarom steeds worden verbonden met de herkomst, betekenis, betrouwbaarheid en gebruiksbeperkingen van gegevens.

Het beroepsgeheim beschermt de vertrouwensrelatie tussen de professional en de patiënt of cliënt. Die bescherming dient niet alleen een individueel belang, maar ook een maatschappelijk belang: mensen moeten zich tot een hulpverlener kunnen wenden zonder te vrezen dat vertrouwelijke informatie buiten de hulpverleningsrelatie wordt gebruikt. De terughoudendheid van beroepsgroepen bij het delen van gevoelige gegevens is daarom niet slechts een juridische belemmering voor samenwerking, maar berust op een wezenlijk belang dat ook op ketenniveau bescherming verdient.

Tegelijkertijd kan een maatschappelijke opgave ontstaan die niet vanuit één hulpverleningsrelatie of organisatie kan worden beoordeeld. Wanneer verschillende organisaties ieder over een deel van de relevante informatie beschikken, kan het ontbreken van onderlinge afstemming ertoe leiden dat samenhangende problemen niet worden herkend of noodzakelijke hulp uitblijft. Het individuele belang bij vertrouwelijkheid en het maatschappelijke belang bij effectieve samenwerking kunnen daardoor met elkaar op gespannen voet komen te staan.

Ook hier kan een niveauvergissing ontstaan. Dat is het geval wanneer de beoordeling van de afzonderlijke hulpverleningsrelatie zonder meer bepalend wordt geacht voor wat op ketenniveau noodzakelijk of gerechtvaardigd kan zijn. Omgekeerd ontstaat eveneens een niveauvergissing wanneer de maatschappelijke opgave op ketenniveau wordt aangevoerd als voldoende rechtvaardiging om vertrouwelijke gegevens uit afzonderlijke hulpverleningsrelaties beschikbaar te stellen. De rechtmatigheidsbeoordeling van de samenwerking heft het beroepsgeheim niet op, evenmin als het beroepsgeheim de noodzaak van een afzonderlijke beoordeling op ketenniveau wegneemt.

Deze spanning is anno 2026 ook zichtbaar in de discussies over de Wet aanpak meervoudige problematiek sociaal domein (Wams) en de Wet gegevensverwerking door samenwerkingsverbanden (WGS). Beroepsorganisaties hebben daarbij gewezen op de risico's voor de vertrouwensrelatie, de toegankelijkheid van zorg en de professionele verantwoordelijkheid van hulpverleners. Tegelijkertijd bestaat de zorg dat noodzakelijke samenwerking wordt belemmerd wanneer organisaties onvoldoende informatie kunnen uitwisselen. De discussie laat zien dat een wettelijke regeling voor gegevensverwerking op ketenniveau niet zonder meer een oplossing biedt voor de afweging die de individuele professional moet maken.

Het beroepsgeheim kent onder bepaalde voorwaarden uitzonderingen, waaronder toestemming, specifieke wettelijke bepalingen en het conflict van plichten. In bepaalde wettelijke regelingen speelt ook het criterium van goed hulpverlenerschap een rol. Deze mogelijkheden bieden echter geen algemene grondslag voor structurele gegevensdeling binnen een samenwerkingsverband. Vooral het conflict van plichten veronderstelt een concrete, zorgvuldig gemotiveerde afweging in een uitzonderlijke situatie. Het kan niet zonder meer dienen als vervanging van een ontbrekende structurele juridische regeling voor gegevensverwerking op ketenniveau.

Een minder ingrijpende mogelijkheid is om informatie op een hoger abstractieniveau te delen. Een hulpverlener kan bijvoorbeeld, voor zover het beroepsgeheim en het overige toepasselijke recht dat toelaten, aangeven of een voorgestelde interventie professioneel passend of uitvoerbaar is, zonder de

onderliggende medische of sociale informatie prijs te geven. Ook een dergelijke terugkoppeling kan een persoonsgegeven of vertrouwelijke informatie zijn; abstractie vervangt de juridische toets niet.

Deelnemers hoeven dus niet dezelfde informatie te ontvangen om zinvol bij te dragen. De keten moet bepalen welke beslissing of interventie nodig is, welke partij daaraan kan bijdragen en welke minimale terugkoppeling daarvoor volstaat. Zo kan vertrouwelijkheid worden behouden zonder de gezamenlijke opgave uit het oog te verliezen.

Bij deze afweging zijn de gevolgen van delen én niet-delen relevant. Dat levert geen algemene uitzondering op het beroepsgeheim op: toestemming, een specifieke wettelijke plicht of bevoegdheid en een eventueel conflict van plichten moeten steeds aan hun eigen voorwaarden worden getoetst.

De infectieziektebestrijding vormt hiervan een treffend voorbeeld. De Wet publieke gezondheid voorziet bij bepaalde infectieziekten in een wettelijke meldplicht voor artsen en laboratoria, die onder de daarvoor geldende voorwaarden doorbreking van het medisch beroepsgeheim mogelijk maakt. Daarmee heeft de wetgever uitdrukkelijk onderkend dat de bescherming van de volksgezondheid onder bepaalde omstandigheden gegevensverstrekking buiten de individuele hulpverleningsrelatie noodzakelijk maakt. De vertrouwensrelatie wordt daarmee niet terzijde geschoven, maar afgewogen tegen de bescherming van anderen en voorzien van specifieke wettelijke voorwaarden en waarborgen.

3.3 Toestemming als juridisch instrument bij ketensamenwerking

Toestemming kan in een concrete relatie relevant zijn, maar is niet vanzelfsprekend een geschikte basis voor de gezamenlijke informatieverwerking. Zij moet voldoen aan de toepasselijke voorwaarden en kan een ontbrekende wettelijke bevoegdheid of uitzondering op het beroepsgeheim niet vervangen.

3.4 Generieke toestemmingsvoorzieningen: functie en grenzen

Een generieke voorziening kan keuzes of wettelijk vereiste toestemmingen vastleggen. Zij bepaalt echter niet zelfstandig of een latere verwerking rechtmatig is, of een ontvanger bevoegd is, of gegevens geschikt zijn voor het nieuwe doel. Die vragen blijven per verwerking en in hun ketencontext te beoordelen.

Voorbeeld: een patiënt staat gegevensdeling met behandelaar A toe. Dat rechtvaardigt niet vanzelf een voorspellend profiel voor een regionaal samenwerkingsverband. Beoordeel apart het doel van die nieuwe analyse, de rollen, eventuele uitzonderingen voor gezondheidsgegevens, de informatieplicht en de mogelijkheid van bezwaar of correctie. Zie tevens de richtsnoeren van de EDPB over toestemming onder Verordening 2016/679 (Guidelines 05/2020).

4 Juridische en organisatorische instrumenten voor ketensamenwerking

In de voorgaande hoofdstukken is uiteengezet hoe de maatschappelijke opgave, de noodzakelijke informatiebehoefte en de rechtmatigheid van gegevensverwerking op ketenniveau met elkaar samenhangen. Wanneer duidelijk is welke informatieverwerking noodzakelijk en juridisch toegestaan is, ontstaat de vraag hoe de samenwerking juridisch en organisatorisch vorm kan krijgen.

Daarvoor bestaan verschillende instrumenten, variërend van wetgeving en sectorale normen tot samenwerkingsovereenkomsten en technische voorzieningen. Deze instrumenten vervullen verschillende functies. Sommige bieden de noodzakelijke wettelijke basis voor gegevensverwerking, andere concretiseren bestaande verplichtingen of regelen de uitvoering van de samenwerking. Het onderscheid tussen organisatieniveau en ketenniveau blijft daarbij relevant, omdat een instrument dat geschikt is voor de afzonderlijke organisatie niet vanzelfsprekend ook de gezamenlijke informatieverwerking regelt.

4.1 Wettelijke kaders voor gegevensverwerking op ketenniveau

De AVG vormt het algemene juridische kader voor de verwerking van persoonsgegevens. Bij complexe ketensamenwerking kunnen daarnaast nationale en sectorale wettelijke regelingen van belang zijn, bijvoorbeeld wanneer bijzondere persoonsgegevens worden verwerkt, specifieke geheimhoudingsplichten gelden of publieke organisaties gegevens verwerken ter uitvoering van wettelijke taken.

De Wet gegevensverwerking door samenwerkingsverbanden (WGS) illustreert hoe de wetgever voor vier specifiek aangewezen samenwerkingsverbanden een kader voor gezamenlijke gegevensverwerking heeft gecreëerd. De WGS biedt geen algemene grondslag voor andere ketensamenwerkingen. Ook binnen haar toepassingsbereik blijven de wettelijke doeleinden, bevoegdheden, voorwaarden en waarborgen bepalend.

De Regionale Informatie- en Expertisecentra (RIEC's) illustreren deze benadering. Hun gezamenlijke gegevensverwerking kan niet uitsluitend worden beoordeeld aan de hand van de bevoegdheden van iedere deelnemer afzonderlijk. Ook de specifieke wettelijke voorwaarden voor de samenwerking zijn bepalend.

Een ander voorbeeld is het wetsvoorstel Wet aanpak meervoudige problematiek sociaal domein (Wams). Dit voorstel richt zich op de juridische mogelijkheden voor een integrale en gecoördineerde aanpak van meervoudige problematiek. De discussie over het voorstel laat zien hoe ingewikkeld het is om gegevensverwerking voor een gezamenlijke maatschappelijke opgave te regelen wanneer verschillende organisaties eigen wettelijke taken, professionele verantwoordelijkheden en geheimhoudingsplichten hebben.

Deze voorbeelden laten zien dat wetgeving op ketenniveau verschillende vormen kan aannemen. De noodzaak van een specifieke wettelijke regeling hangt onder meer af van de aard van de gegevens, de betrokken organisaties, de bestaande bevoegdheden en de gevolgen van de gezamenlijke verwerking. Een afzonderlijke ketenwet is daarom niet in alle gevallen noodzakelijk, maar bestaande wettelijke bevoegdheden bieden evenmin vanzelfsprekend voldoende ruimte voor iedere vorm van gezamenlijke gegevensverwerking.

4.2 De functie en grenzen van verschillende instrumenten

Wanneer specifieke wetgeving ontbreekt, houdt de juridische analyse niet op. Dan moet je onderzoeken welke ruimte bestaande taken, bevoegdheden, open normen, grondrechten en zwaarwegende belangen bieden. Daarbij worden de tekst, systematiek en het doel van toepasselijke bepalingen in samenhang beoordeeld. Een teleologische interpretatie kan ruimte verduidelijken waar het recht die laat, maar kan geen bevoegdheid scheppen in strijd met een duidelijke wettelijke beperking.

Wetsvoorstellen kunnen inzicht geven in beoogde oplossingen en toekomstige bevoegdheden, maar bieden vóór inwerkingtreding geen zelfstandige basis voor verwerking. De WGS is een voorbeeld van specifieke wetgeving voor aangewezen samenwerkingsverbanden, niet van een algemene bevoegdheid. Blijkt het bestaande recht na zorgvuldige interpretatie en onderzoek naar minder ingrijpende alternatieven ontoereikend, dan kan aanvullende wetgeving noodzakelijk zijn.

Een zwaarwegend algemeen belang en professionele normen, zoals goed hulpverlenerschap, kunnen richting geven aan de beoordeling van noodzaak, proportionaliteit, subsidiariteit en de gevolgen van handelen of nalaten. Zij zijn niet zonder meer een zelfstandige rechtsgrond of een uitzondering op een wettelijke geheimhoudingsplicht. De belangenafweging is richtinggevend binnen de grenzen van het toepasselijke recht; beoordeel zowel de gevolgen van gegevensverwerking als de gevolgen van het achterwege laten daarvan.

Deze instrumenten kunnen elkaar aanvullen, maar zijn niet onderling uitwisselbaar. Een convenant kan bijvoorbeeld afspraken vastleggen over verantwoordelijkheden, besluitvorming en beheer, maar geen ontbrekende wettelijke bevoegdheid creëren. Een technische standaard kan de uitwisseling van gegevens ondersteunen, maar bepaalt niet of die uitwisseling noodzakelijk of rechtmatig is.

De onderstaande tabel laat zien welke functie verschillende instrumenten kunnen vervullen en waar hun grenzen liggen.

Instrument	**Geschikt voor**	**Niet geschikt voor**
Wet- en regelgeving	Wettelijke taken en bevoegdheden, voorwaarden voor verwerking, doelen, deelnemers en waarborgen	Alle operationele details van de samenwerking
Convenant of samenwerkingsovereenkomst	Governance, verantwoordelijkheden, werkafspraken, beheer en escalatie	Het creëren van ontbrekende wettelijke bevoegdheden of AVG-grondslagen
Gedragscode of professioneel normenkader	Concretisering van open normen en professionele verantwoordelijkheden	Het zelfstandig opheffen van wettelijke geheimhoudingsplichten
Technische standaard	Betrouwbare gegevensuitwisseling,	Het vaststellen van het maatschappelijke doel of de juridische rechtvaardiging

	interoperabiliteit en technische beveiliging	
DPIA of gezamenlijke risicoanalyse	Het identificeren en beoordelen van risico's en passende maatregelen	Het achteraf rechtmatig maken van een verwerking waarvoor de juridische voorwaarden ontbreken

Sectorale gedragscodes en Europese regelgeving kunnen algemene verplichtingen nader invullen voor specifieke sectoren of vormen van samenwerking. Hun betekenis hangt af van hun juridische status en toepassingsbereik. Een gedragscode kan bijvoorbeeld richting geven aan de uitvoering van bestaande verplichtingen, terwijl rechtstreeks toepasselijke Europese regelgeving aanvullende rechten, verplichtingen of bevoegdheden kan bevatten.

De juridische en organisatorische inrichting sluit daarmee aan op de eerder vastgestelde informatiebehoefte en beoordeling van de rechtmatigheid. Niet de beschikbaarheid van een bepaald instrument, maar de aard van de noodzakelijke gegevensverwerking bepaalt welke instrumenten nodig zijn en welke functie zij moeten vervullen.

De keuze voor juridische en organisatorische instrumenten maakt duidelijk onder welke voorwaarden de samenwerking kan functioneren. Daarmee is ook de basis gelegd voor het vaststellen van de verantwoordelijkheden van de betrokken organisaties. Pas wanneer de maatschappelijke opgave, de noodzakelijke informatieverwerking en de juridische voorwaarden voldoende zijn uitgewerkt, kan worden beoordeeld welke AVG-rollen de betrokken partijen bij de verschillende verwerkingen vervullen en welke afspraken daarover nodig zijn.

Deze volgorde vormt een belangrijk uitgangspunt van de handreiking. De rolverdeling is niet het vertrekpunt voor het ontwerpen van de samenwerking, maar volgt uit de wijze waarop de gegevensverwerking feitelijk is ingericht.

5 AVG-rollen en verantwoordelijkheden in de keten

De CIP-handreiking *Privacyafspraken bij ketensamenwerking* uit 2020 bood een waardevol kader voor het bepalen en vastleggen van AVG-rollen, verantwoordelijkheden en onderlinge afspraken. Deze handreiking kiest bij complexe ketensamenwerking een andere volgorde. Waar de eerdere handreiking de privacyafspraken als vertrekpunt neemt, worden deze hier geplaatst aan het einde van de analyse van de maatschappelijke opgave, de informatiebehoefte en de beoordeling van de rechtmatigheid.

Wanneer de samenwerking begint met de vraag wie verwerkingsverantwoordelijke of verwerker is, bestaat het risico dat de bestaande organisatiestructuur bepalend wordt voor de inrichting van de gegevensverwerking. Daarmee kan de informatiebehoefte op ketenniveau buiten beeld blijven of worden teruggebracht tot afzonderlijke gegevensuitwisselingen tussen organisaties.

Bij complexe ketensamenwerking staat daarom eerst de vraag centraal welke informatie nodig is om de maatschappelijke opgave te realiseren, welke gegevensverwerkingen daarvoor noodzakelijk zijn en onder welke voorwaarden deze rechtmatig kunnen plaatsvinden. Vervolgens wordt vastgesteld welke partijen feitelijk de doeleinden en essentiële middelen van die verwerkingen bepalen en welke verantwoordelijkheden daaruit voortvloeien.

De AVG-rollen worden daarbij niet vrij gekozen of door afspraken gecreëerd. Zij volgen uit de feitelijke en juridische positie van de betrokken partijen. De afspraken vormen het sluitstuk waarin deze verantwoordelijkheden worden verduidelijkt en vastgelegd, zodat de samenwerking ook in de uitvoering aan de toepasselijke verplichtingen voldoet.

5.1 Verwerkingsverantwoordelijke: beslissend is de feitelijke zeggenschap

Een verwerkingsverantwoordelijke bepaalt, alleen of samen met anderen, het doel van en de essentiële middelen voor een verwerking van persoonsgegevens (artikel 4, onderdeel 7, AVG). Een wettelijke taak of bevoegdheid kan daarbij bepalend zijn. Het enkele feit dat een organisatie gegevens aanlevert, ontvangt of technisch beheert, is onvoldoende om haar rol voor alle betrokken verwerkingen vast te stellen. Eén organisatie kan voor verschillende verwerkingen verschillende rollen hebben.

Bij samenwerking tussen autonome organisaties blijven partijen vaak ieder zelfstandig verwerkingsverantwoordelijke voor hun eigen taken en verwerkingen. Dat zij een gezamenlijk maatschappelijk belang nastreven, maakt hen niet automatisch gezamenlijk verwerkingsverantwoordelijk. Beoordeel daarom per verwerking wie de doelen en essentiële middelen vaststelt, waaronder de beslissing welke gegevens voor welk gebruik beschikbaar komen.

5.2 Gezamenlijke verwerkingsverantwoordelijkheid

Van gezamenlijke verwerkingsverantwoordelijkheid is sprake wanneer twee of meer partijen gezamenlijk de doeleinden en middelen van dezelfde verwerking bepalen (artikel 26 AVG). Dat kan voortvloeien uit gezamenlijke besluiten of uit nauw samenhangende, elkaar aanvullende beslissingen die de verwerking feitelijk bepalen. Een formeel samenwerkingsverband of overeenkomst is op zichzelf niet doorslaggevend; omgekeerd sluit het ontbreken daarvan gezamenlijke verantwoordelijkheid niet uit.

Als artikel 26 AVG van toepassing is, leggen de betrokken partijen op transparante wijze vast wie welke verplichtingen vervult, in het bijzonder rond informatieverstrekking en de uitoefening van rechten van betrokkenen. De wezenlijke inhoud van deze regeling moet voor betrokkenen beschikbaar zijn. De

regeling laat de rechten van betrokkenen jegens iedere gezamenlijk verwerkingsverantwoordelijke onverlet.

5.3 De verwerker: handelen namens een verantwoordelijke

Een verwerker verwerkt persoonsgegevens ten behoeve van en namens een verwerkingsverantwoordelijke (artikel 4, onderdeel 8, AVG). Een verwerker mag binnen de overeengekomen kaders operationele en niet-essentiële technische keuzes maken, maar bepaalt niet zelfstandig de doeleinden of essentiële middelen van de verwerking. Wanneer een dienstverlener persoonsgegevens voor eigen doeleinden gebruikt, moet die eigen verwerking afzonderlijk worden beoordeeld.

Voor een verwerkersrelatie is een overeenkomst of andere rechtshandeling vereist die voldoet aan artikel 28 AVG. Daarin worden onder meer onderwerp, duur, aard en doel van de verwerking, soorten persoonsgegevens, categorieën betrokkenen, instructies, beveiliging, subverwerkers, ondersteuning en beëindiging geregeld. Een verwerkersovereenkomst is geen vervanging voor de rechtmatige grondslag of bevoegdheid van de verantwoordelijke.

5.4 Rolbepaling bij gedeelde voorzieningen

Een gemeenschappelijke voorziening, verwijsfunctie of technische infrastructuur brengt niet automatisch één AVG-rol voor alle gegevensverwerkingen met zich mee. Bij de beoordeling van de verantwoordelijkheden is onderscheid nodig tussen de oorspronkelijke gegevensverwerking bij de bron, het beschikbaar stellen of opvragen van gegevens, eventuele centrale registratie of routering en het gebruik van de ontvangen informatie. Bij deze verschillende verwerkingen kunnen andere partijen betrokken zijn en kunnen hun AVG-rollen verschillen.

Ook wanneer meerdere organisaties een voorziening financieren of besturen, volgt daaruit niet zonder meer dat zij gezamenlijk verantwoordelijk zijn voor iedere verwerking via die voorziening. Evenmin is de beheerder automatisch verwerker: doorslaggevend is welke beslissingen deze daadwerkelijk neemt en op wiens instructie hij handelt.

5.5 Van rolbepaling naar werkbare afspraken

Waar de eerdere handreiking de nadruk legde op het vastleggen van privacyafspraken tussen samenwerkende organisaties, begint deze handreiking bij de maatschappelijke opgave en de informatie die nodig is om deze gezamenlijk aan te pakken. Vervolgens worden de rechtmatigheid van de gegevensverwerking, de inrichting daarvan en de verantwoordelijkheden van de betrokken partijen beoordeeld.

De vaststelling en vastlegging van AVG-rollen en privacyafspraken vormen daarmee het sluitstuk van een bredere analyse. Zo wordt voorkomen dat bestaande organisatiegrenzen en rolverdelingen op voorhand bepalend worden voor de informatieverwerking die op ketenniveau noodzakelijk is.

Bij complexe samenwerking worden de functionarissen voor gegevensbescherming (FG's) en andere privacyfunctionarissen tijdig betrokken bij de beoordeling van de gevolgen voor betrokkenen. Waar meerdere FG's betrokken zijn, kan een coördinerend FG de afstemming en samenhang in de advisering ondersteunen. Dit is geen zelfstandige AVG-rol en laat de onafhankelijke positie en wettelijke taken van iedere FG onverlet (artikelen 38 en 39 AVG). De betrokken verwerkingsverantwoordelijken blijven verantwoordelijk voor de verwerking.

De vaststelling van AVG-rollen en het vastleggen van verantwoordelijkheden en onderlinge afspraken geven duidelijkheid over de juridische en organisatorische inrichting van de samenwerking. Daarmee zijn echter nog niet alle gevolgen van de gezamenlijke gegevensverwerking in beeld.

Een ketenanalyse biedt inzicht in de gevolgen die door de gezamenlijke werking van de keten ontstaan en die bij afzonderlijke beoordelingen buiten beeld kunnen blijven. Die inzichten kunnen de wettelijke beoordeling van risico's voor rechten en vrijheden, waaronder een DPIA wanneer artikel 35 AVG daartoe verplicht, ondersteunen.

6 De impact van gegevensverwerking in complexe ketens

De impact van gegevensverwerking in een complexe keten wordt niet uitsluitend bepaald door de afzonderlijke verwerkingen, maar ook door de wijze waarop informatie wordt gevonden, gecombineerd, geïnterpreteerd en gebruikt. De ketenanalyse maakt zichtbaar hoe de informatievoorziening bijdraagt aan de oplossing van het dominante ketenprobleem en welke gevolgen de gekozen inrichting voor betrokkenen kan hebben.

In een epidemieketen kunnen gegevens uit laboratoria, zorgverlening en publieke gezondheidszorg worden gebruikt om besmettingspatronen te signaleren en gericht in te grijpen. Het beoogde en toegestane gebruik kan bijdragen aan volksgezondheid, maar ook gevolgen hebben voor de persoonlijke levenssfeer of bewegingsvrijheid. Bij onbedoelde fouten, bijvoorbeeld een onjuiste persoonskoppeling, kunnen onjuiste signalen en besluiten tussen ketenpartners doorwerken. Daarnaast kan informatie oneigenlijk of ongeoorloofd voor andere doeleinden worden gebruikt.

Bij de beoordeling worden daarom de gevolgen van beoogd gebruik, onbedoelde effecten en ongeoorloofd gebruik onderscheiden. Van belang is welke personen worden geraakt, hoe informatie en besluiten doorwerken en wie ongewenste gevolgen kan signaleren, voorkomen, beperken of herstellen.

Wanneer gegevens uit meerdere bronnen worden gecombineerd, ontstaat niet noodzakelijk een volledig of betrouwbaar beeld. Relevante feiten kunnen ontbreken en de betekenis of actualiteit van gegevens kan onzeker blijven. Een groter informatieaanbod mag niet worden verward met grotere zekerheid. Onzekerheden over het informatiebeeld en onvoldoende onderzochte gevolgen moeten worden onderscheiden van resterende risico’s die na beoordeling en maatregelen bewust worden aanvaard.

Wanneer het informatiebeeld onvoldoende betrouwbaar is, kan dat aanleiding zijn om aanvullende informatie te verzamelen, een interventie aan te passen, een beslissing uit te stellen of niet op basis van het bestaande beeld te interveniëren. Daarbij moeten ook de mogelijke gevolgen van uitstel of niet-handelen worden meegewogen.

Een impactbeoordeling op ketenniveau maakt inzichtelijk welke gevolgen uit de gezamenlijke werking voortvloeien en of de beoogde maatschappelijke resultaten daadwerkelijk worden bereikt. Zij vervangt geen wettelijke DPIA van de betrokken verwerkingsverantwoordelijken, maar levert relevante inzichten voor de beoordeling van risico’s voor de rechten en vrijheden van betrokkenen (artikel 35 AVG).

Een beoordeling op ketenniveau houdt rekening met de betrouwbaarheid van afleidingen, de mogelijke verspreiding van fouten en de uitvoerbaarheid van waarborgen. Een fout of onzekerheid die in één organisatie beheersbaar lijkt, kan gevolgen hebben wanneer andere organisaties daarop voortbouwen.

Voor een verantwoorde inrichting moet duidelijk zijn hoe ketenpartners fouten en onjuiste interpretaties signaleren, terugkoppelen en corrigeren, welke omstandigheden tot herbeoordeling of ingrijpen leiden en hoe daarover wordt besloten.

De betrokken FG’s dienen tijdig en onafhankelijk te worden betrokken bij de beoordeling van gevolgen voor rechten en vrijheden. Waar passend wordt ook het perspectief van betrokkenen meegewogen. Procesregie ondersteunt de afstemming zonder de wettelijke verantwoordelijkheden van de afzonderlijke organisaties over te nemen.

Een waarborg die op papier toereikend is, maar in de praktijk niet kan worden uitgevoerd of gehandhaafd, biedt onvoldoende bescherming.

De maatschappelijke opgave, de noodzakelijke informatieverwerking, de rechtmatigheid van de gegevensverwerking, de verantwoordelijkheden en de impact op betrokkenen hangen onderling samen. Hoofdstuk 7 brengt deze onderdelen bijeen in een stappenplan voor de inrichting en beoordeling van gegevensverwerking in complexe ketens.

7 Stappenplan voor gegevensverwerking in complexe ketens

De voorgaande hoofdstukken hebben laten zien dat rechtmatige en verantwoorde gegevensverwerking in complexe ketens niet begint bij de keuze voor een technische voorziening, een juridische grondslag of een verdeling van AVG-rollen. Het vertrekpunt is de maatschappelijke opgave waarvoor organisaties samenwerken en de informatie die nodig is om die opgave gezamenlijk te kunnen aanpakken.

Vanuit dat vertrekpunt ontstaat een samenhangende beoordeling. Eerst wordt duidelijk welk probleem de samenwerking moet oplossen en welke informatie daarvoor noodzakelijk is. Vervolgens komt aan de orde hoe die informatie beschikbaar kan komen, welke juridische voorwaarden daarvoor gelden en welke verantwoordelijkheden bij de betrokken partijen liggen. De beoordeling van risico's voor betrokkenen maakt zichtbaar of de gekozen inrichting voldoende waarborgen biedt.

Dit hoofdstuk brengt deze afwegingen samen in een stappenplan. Het biedt een werkwijze om van een maatschappelijke opgave tot een rechtmatige, uitvoerbare en controleerbare inrichting van de gegevensverwerking te komen. Daarbij blijft het onderscheid tussen het grondvlak van de afzonderlijke organisaties en het ketenniveau van de gezamenlijke informatiepositie van belang.

Het stappenplan bestaat uit vier fasen:

1. De maatschappelijke opgave en de keten.
2. De noodzakelijke informatieverwerking en de beoordeling van de rechtmatigheid.
3. De rechten, risico's en waarborgen.
4. De inrichting en blijvende verantwoording.

De stappen vormen geen strikt lineair proces. Nieuwe inzichten over de informatiebehoefte, de juridische mogelijkheden of de risico's kunnen aanleiding geven om eerdere keuzes te herzien. Ook de analyse van de impact op ketenniveau, zoals behandeld in hoofdstuk 6, is geen afzonderlijke eindcontrole. De risicobeoordeling loopt mee tijdens de ontwikkeling van de samenwerking en kan leiden tot aanpassing van het ontwerp.

7.1 Fase 1: De maatschappelijke opgave en de keten

Vooraf: Vaststellen of sprake is van een ketenvraagstuk

Niet ieder maatschappelijk probleem waarvoor persoonsgegevens worden verwerkt, is een ketenvraagstuk. De eerste beoordeling betreft daarom de vraag of het probleem binnen de taken en mogelijkheden van één organisatie kan worden opgelost, of dat de bijdrage van meerdere autonome organisaties noodzakelijk is.

Wanneer één organisatie het probleem zelfstandig kan aanpakken, ligt de beoordeling van de gegevensverwerking in beginsel op organisatieniveau. Een aanvullende beoordeling op ketenniveau is dan doorgaans niet aan de orde. Dat laat onverlet dat voor de betreffende verwerking een reguliere DPIA verplicht kan zijn op grond van artikel 35 AVG.

Wanneer de oplossing afhankelijk is van de samenhang tussen handelingen, informatie of beslissingen van meerdere organisaties, kan sprake zijn van een ketenvraagstuk. Daarbij is niet doorslaggevend of

organisaties al gegevens uitwisselen, maar of de maatschappelijke opgave een gezamenlijke informatiepositie of onderlinge afstemming noodzakelijk maakt.

De uitkomst van deze stap is een onderbouwde afbakening van het vraagstuk en de vaststelling of een beoordeling op ketenniveau nodig is.

7.1.1 *Stap 1: Beschrijven van het centrale maatschappelijke probleem*

De maatschappelijke opgave wordt beschreven zonder deze bij voorbaat te vertalen naar een ICT-oplossing of een behoefte aan gegevensuitwisseling. Centraal staat welke schade of welk maatschappelijk risico moet worden voorkomen, beperkt of aangepakt.

Daarbij zijn onder meer de ernst en omvang van het probleem, de mogelijkheid van herhaling of escalatie en de gevolgen voor betrokkenen en de samenleving relevant. Ook wordt inzichtelijk waarom de afzonderlijke inzet van organisaties onvoldoende is en welke gevolgen te verwachten zijn wanneer gezamenlijke actie uitblijft.

Deze probleembeschrijving vormt het referentiepunt voor de verdere beoordeling. Zij maakt het mogelijk om later vast te stellen of de voorgestelde informatieverwerking daadwerkelijk bijdraagt aan het oplossen van het probleem en of de daarmee gepaard gaande inbreuken op de persoonlijke levenssfeer gerechtvaardigd kunnen worden.

De uitkomst is een gedeelde en toetsbare omschrijving van de maatschappelijke opgave, inclusief de noodzaak van samenwerking.

7.1.2 *Stap 2: Onderscheiden van organisatie- en ketenniveau*

Vervolgens wordt de bestaande situatie op het grondvlak in kaart gebracht. Daarbij gaat het om de betrokken organisaties, hun wettelijke taken en bevoegdheden, de beschikbare bronregistraties en de gegevensuitwisseling die al tussen organisaties plaatsvindt.

Afzonderlijk wordt beschreven welke informatie of functionaliteit op ketenniveau nodig is. Dat kan bijvoorbeeld gaan om het kunnen vinden van relevante informatie, het verifiëren van een gegeven, het leggen van een verband tussen signalen of het ondersteunen van een gezamenlijke beoordeling.

Dit onderscheid voorkomt dat bestaande organisatiegrenzen automatisch bepalend worden voor de inrichting van de samenwerking. Het maakt ook zichtbaar welke informatie al rechtmatig beschikbaar is, welke aanvullende verwerking wordt voorgesteld en waar nieuwe afhankelijkheden of risico's kunnen ontstaan.

Een gezamenlijke informatiepositie hoeft daarbij niet te berusten op een centrale gegevensverzameling of een uniform informatiemodel. Ook een gedistribueerde inrichting kan de benodigde informatie beschikbaar maken, mits de betekenis, herkomst en bruikbaarheid van de informatie voldoende duidelijk zijn.

De uitkomst is een beschrijving van de bestaande gegevensverwerkingen op organisatieniveau en van de aanvullende informatiebehoefte op ketenniveau.

7.2 Fase 2: De noodzakelijke informatieverwerking en de beoordeling van de rechtmatigheid

7.2.1 *Stap 3: Bepalen van de noodzakelijke informatie-uitwisseling*

Vanuit de maatschappelijke opgave wordt vastgesteld welke informatie daadwerkelijk nodig is om de samenwerking mogelijk te maken. Daarbij staat niet de beschikbaarheid van gegevens centraal, maar de vraag welke onzekerheid moet worden weggenomen of welke beslissing door de informatie kan worden ondersteund.

Vervolgens wordt beoordeeld welke vorm van informatie-uitwisseling daarvoor passend is. Soms is het voldoende om te weten dat bij een andere organisatie relevante informatie beschikbaar is. In andere gevallen kan een verwijzing, verificatie, beperkte set metadata of inhoudelijke gegevensuitwisseling noodzakelijk zijn.

De omvang en detaillering van de informatie worden afgestemd op de beoogde functie. Daarbij wordt ook beoordeeld of informatie bij de bron kan blijven en alleen beschikbaar hoeft te komen wanneer daarvoor een concrete aanleiding bestaat.

De uitkomst is een onderbouwde beschrijving van de noodzakelijke informatieverwerking, inclusief de gegevenscategorieën, de betrokken partijen en de voorwaarden waaronder informatie beschikbaar komt.

7.2.2 *Stap 4: Beoordelen van de rechtmatigheid op beide niveaus*

De juridische beoordeling betreft zowel de gegevensverwerkingen van de afzonderlijke organisaties als de aanvullende verwerking die voor de samenwerking noodzakelijk is.

Op organisatieniveau wordt beoordeeld voor welke doeleinden persoonsgegevens worden verwerkt, welke taken en bevoegdheden daarbij relevant zijn en op welke AVG-grondslag de verwerking berust. Bij bijzondere categorieën persoonsgegevens (artikel 9 AVG) of strafrechtelijke persoonsgegevens gelden aanvullende voorwaarden. Ook wettelijke geheimhoudingsverplichtingen en sectorale regels kunnen bepalend zijn voor de mogelijkheden tot verstrekking of gebruik.

Op ketenniveau staat de vraag centraal of de gezamenlijke informatieverwerking binnen de toepasselijke wettelijke kaders kan plaatsvinden. Daarbij worden de gezamenlijke doelstelling, de noodzakelijkheid en evenredigheid van de verwerking en de grenzen aan het gebruik van de informatie beoordeeld.

De rechtmatigheid van gegevensverwerking op ketenniveau kan niet zonder meer worden afgeleid uit de rechtmatigheid van de afzonderlijke bronverwerkingen. Tegelijkertijd is niet voor iedere samenwerking een zelfstandige wettelijke grondslag of één gezamenlijke verwerkingsverantwoordelijke vereist. Welke wettelijke basis en aanvullende waarborgen nodig zijn, hangt af van de aard van de verwerkingen, de betrokken partijen en het toepasselijke wettelijke kader. Waar wetgeving een zwaarwegend algemeen belang vereist, maakt ook die eis deel uit van de beoordeling.

De uitkomst is een samenhangende juridische onderbouwing van de noodzakelijke gegevensverwerkingen en de voorwaarden waaronder de samenwerking kan plaatsvinden.

7.2.3 *Stap 5: Beoordelen van het koppelmechanisme*

Wanneer informatie uit verschillende organisaties met elkaar in verband wordt gebracht, is de betrouwbaarheid van het koppelmechanisme bepalend voor de kwaliteit van de gezamenlijke informatiepositie.

De beoordeling omvat de wijze waarop personen, gebeurtenissen of andere relevante objecten worden geïdentificeerd en hoe wordt vastgesteld dat gegevens daadwerkelijk betrekking hebben op dezelfde persoon of situatie. Daarbij zijn onder meer betrouwbaarheid, integriteit, actualiteit, beschikbaarheid en autorisatie van belang.

Ook de gevolgen van foutieve koppelingen verdienen aandacht. Een foutpositieve koppeling kan ertoe leiden dat informatie ten onrechte aan een persoon wordt toegeschreven. Een foutnegatieve koppeling kan juist verhinderen dat relevante informatie wordt herkend. Beide kunnen gevolgen hebben voor de maatschappelijke opgave en voor de rechten van betrokkenen.

Het koppelmechanisme wordt daarom beoordeeld in relatie tot het probleem dat de samenwerking moet oplossen. Een technisch mogelijke koppeling is niet zonder meer een noodzakelijke of geschikte koppeling.

De uitkomst is een beoordeling van de geschiktheid en betrouwbaarheid van de gekozen wijze van identificatie, verwijzing of koppeling.

7.2.4 *Stap 6: Beoordelen van contextbehoud*

Gegevens ontlenen hun betekenis mede aan de omstandigheden waarin zij zijn vastgelegd. Wanneer informatie wordt gedeeld met andere organisaties of voor een andere beslissing wordt gebruikt, kan een deel van die context verloren gaan.

Daarom wordt beoordeeld welke informatie de ontvanger nodig heeft om een gegeven correct te interpreteren. Daarbij kan het gaan om de herkomst, de datum, de status, de mate van zekerheid, de omstandigheden waaronder het gegeven is ontstaan en eventuele beperkingen aan het gebruik ervan.

Dit is in het bijzonder relevant wanneer gegevens uit verschillende bronnen worden gecombineerd of wanneer uit die combinatie nieuwe conclusies worden afgeleid. De betekenis van een gegeven binnen de oorspronkelijke organisatie hoeft immers niet gelijk te zijn aan de betekenis die eraan wordt toegekend binnen de samenwerking.

Contextbehoud vraagt niet noodzakelijk om standaardisering van alle brongegevens of om één uniform informatiemodel. Wel moet de uitgewisselde informatie voldoende betekenis en context behouden om binnen de keten verantwoord te kunnen worden gebruikt.

De uitkomst is een beschrijving van de noodzakelijke contextinformatie en de maatregelen die onjuiste interpretatie of ongeoorloofd hergebruik moeten voorkomen.

7.3 Fase 3: De rechten, risico's en waarborgen

7.3.1 *Stap 7: Beoordelen van rechten en zeggenschap van betrokkenen*

De inrichting van de samenwerking moet duidelijk maken welke gevolgen de gegevensverwerking heeft voor de positie van betrokkenen. Daarbij gaat het zowel om de informatie die zij over de verwerking ontvangen als om de mogelijkheden om hun rechten daadwerkelijk uit te oefenen.

Van belang is dat betrokkenen kunnen begrijpen welke organisaties bij de verwerking zijn betrokken, voor welke doeleinden hun gegevens worden gebruikt en waar zij terechtkunnen met vragen of verzoeken. Ook moet duidelijk zijn hoe verzoeken tot inzage, rectificatie, beperking of bezwaar worden behandeld, voor zover deze rechten in de betreffende situatie van toepassing zijn.

Wanneer toestemming een rol speelt, wordt beoordeeld voor welke concrete verwerking zij wordt gevraagd en of toestemming, gelet op de omstandigheden en de verhouding tussen partijen, een geschikte en rechtsgeldige basis kan vormen.

Bij complexe ketens verdient bijzondere aandacht dat betrokkenen niet tussen organisaties terechtkomen zonder dat duidelijk is wie hun verzoek behandelt. De verdeling van verantwoordelijkheden mag de effectieve uitoefening van rechten niet belemmeren.

De uitkomst is een beoordeling van de transparantie, rechtsbescherming en feitelijke mogelijkheden van betrokkenen om invloed uit te oefenen op de verwerking van hun persoonsgegevens.

7.3.2 *Stap 8: Analyseren van ketenspecifieke risico's*

Naast de risico's van afzonderlijke gegevensverwerkingen kunnen bij samenwerking risico's ontstaan die samenhangen met de gezamenlijke informatiepositie.

Daarbij gaat het bijvoorbeeld om het geleidelijk uitbreiden van doeleinden, het cumulatieve effect van gegevens uit verschillende bronnen, foutieve koppelingen, onterechte uitsluiting of stigmatisering en het ontstaan van nieuwe conclusies over personen. Ook kunnen verantwoordelijkheden verschuiven, kunnen betrokkenen hun gedrag aanpassen doordat zij zich voortdurend gevolgd voelen en kunnen incidenten gevolgen hebben voor meerdere organisaties tegelijk.

Bijzondere aandacht verdienen risico's die niet volledig aan één bronverwerking zijn toe te schrijven. De combinatie van gegevens kan immers informatie opleveren die in geen van de afzonderlijke bronnen als zodanig aanwezig was.

De analyse van de impact op ketenniveau, zoals behandeld in hoofdstuk 6, helpt deze gevolgen in samenhang te beoordelen. Een eventuele DPIA op grond van artikel 35 AVG blijft de verantwoordelijkheid van de betrokken verwerkingsverantwoordelijken.

De uitkomst is een overzicht van de relevante ketenspecifieke risico's, hun mogelijke gevolgen en de mate waarin bestaande waarborgen toereikend zijn.

7.3.3 *Stap 9: Beoordelen van uitvoeringsfactoren*

Een juridisch en technisch zorgvuldig ontwerp biedt niet vanzelf voldoende bescherming wanneer de samenwerking in de praktijk niet uitvoerbaar is. De feitelijke omstandigheden waaronder organisaties samenwerken, kunnen risico's versterken of maatregelen minder effectief maken.

De omstandigheden van deelnemers verschillen. Naast capaciteit, deskundigheid, financiering en technische afhankelijkheden gaat het om professionele taken, geheimhoudingsplichten, registratiepraktijken en uiteenlopende eisen aan bewijs en betrouwbaarheid. Politiegegevens kunnen bijvoorbeeld bestaan uit signalen, vermoedens en nog niet geverifieerde informatie. Terughoudendheid

bij verstrekking kan daarom voortkomen uit de bescherming van betrokkenen en de noodzaak om misinterpretatie buiten de oorspronkelijke context te voorkomen.

De keten moet rekening houden met die verschillen: leg herkomst, status, onzekerheid en gebruiksbeperkingen vast en maak duidelijk welke verificatie nodig is voordat een signaal tot een interventie kan leiden. Een maatregel die niet uitvoerbaar is of waarvoor geen capaciteit bestaat, biedt in de praktijk onvoldoende bescherming.

De uitvoeringsfactoren maken daarom deel uit van de beoordeling van de haalbaarheid en effectiviteit van de voorgestelde waarborgen.

De uitkomst is een overzicht van de omstandigheden die de uitvoerbaarheid en betrouwbaarheid van de samenwerking beïnvloeden, inclusief de maatregelen die nodig zijn om deze risico's te beperken.

7.3.4 *Stap 10: Ontwerpen van maatregelen per niveau*

Op basis van de voorgaande beoordelingen wordt vastgesteld welke maatregelen nodig zijn om de gegevensverwerking rechtmatig, betrouwbaar en verantwoord te laten plaatsvinden.

Bepaal bij ieder risico waar het ontstaat, waar het effectief kan worden beheerst en wie daarvoor verantwoordelijk is. Bij de bron kan een organisatie bijvoorbeeld de status en onzekerheid van een politiegegeven registreren. Op ketenniveau zijn afspraken nodig om te voorkomen dat een andere deelnemer hetzelfde signaal als vaststaand feit behandelt. Beide maatregelen vullen elkaar aan.

Ook foutieve koppelingen vragen om een gezamenlijke correctie- en terugkoppelprocedure. Bij informatie onder beroepsgeheim kan de bron beoordelen welke beperkte professionele terugkoppeling rechtmatig mogelijk is, terwijl de keten vastlegt hoe die terugkoppeling wordt gebruikt. Maatregelen op ketenniveau betekenen niet dat gegevens of verantwoordelijkheden moeten worden gecentraliseerd.

Een maatregel op ketenniveau hoeft niet te betekenen dat de verwerking of de verantwoordelijkheid wordt gecentraliseerd. De gekozen oplossing moet aansluiten bij de aard van het risico en de inrichting van de samenwerking. Centrale voorzieningen zijn niet vanzelfsprekend aangewezen voor problemen die bij de bron kunnen worden opgelost.

De uitkomst is per risico een overzicht van de bronmaatregel, de eventuele aanvullende ketenmaatregel, de verantwoordelijke partij, de uitvoerbaarheid en de wijze waarop de werking wordt gecontroleerd.

7.4 Fase 4: De inrichting en blijvende verantwoording

7.4.1 *Stap 11: Inrichten van procesregie, verantwoordelijkheden en besluitvorming*

Voor de uitvoering van de samenwerking is duidelijkheid nodig over de procesregie, de besluitvorming en de verantwoordelijkheden van de betrokken partijen.

Procesregie is daarbij niet hetzelfde als hiërarchisch opdrachtgeverschap of verwerkingsverantwoordelijkheid. De procesregisseur bewaakt de samenhang van de analyse en de besluitvorming, maakt afhankelijkheden zichtbaar en draagt bij aan de traceerbaarheid van besluiten. Daarbij is van belang dat het belang van één deelnemende organisatie niet zonder meer als het gezamenlijke ketenbelang wordt gepresenteerd.

De procesregisseur bewaakt de samenhang van het gezamenlijke analyse- en besluitvormingsproces, maakt afhankelijkheden zichtbaar, voorkomt dat het organisatiebelang van één partij zonder meer als ketenbelang wordt gepresenteerd en waarborgt dat besluiten navolgbaar zijn.

De procesregisseur hoeft niet de eigenaar van de gebruikte voorzieningen te zijn en is evenmin automatisch verwerkingsverantwoordelijke voor alle gegevensverwerkingen binnen de samenwerking. De procesregie moet zodanig zijn ingericht dat conflicterende organisatie- of leveranciersbelangen de gezamenlijke beoordeling niet onevenredig beïnvloeden.

De AVG-rollen volgen uit de feitelijke en juridische inrichting van de verschillende gegevensverwerkingen. De daaruit voortvloeiende verantwoordelijkheden en onderlinge afspraken worden overeenkomstig de toepasselijke AVG-verplichtingen vastgelegd. Daarbij wordt onderscheid gemaakt tussen de oorspronkelijke verwerking bij de bron, het beschikbaar stellen of opvragen van gegevens, eventuele gezamenlijke voorzieningen en het gebruik van de ontvangen informatie. Bij gezamenlijke verwerkingsverantwoordelijkheid is artikel 26 AVG van toepassing; bij verwerking namens een verantwoordelijke artikel 28 AVG.

Daarnaast wordt bepaald hoe besluiten worden voorbereid en genomen, hoe conflicten worden behandeld, hoe escalatie plaatsvindt en hoe wijzigingen in de samenwerking worden beheerst.

De ketenpartners spreken af hoe ongewenste ketenbrede gevolgen worden gesignaleerd en hersteld, wie actie kan ondernemen en wanneer een nieuwe beoordeling nodig is. De FG’s adviseren onafhankelijk over de bescherming van persoonsgegevens; waar passend wordt het perspectief van betrokkenen betrokken (artikelen 35, negende lid, 38 en 39 AVG).

De uitkomst is een navolgbare inrichting van de procesregie, de besluitvorming en de juridische en organisatorische verantwoordelijkheden.

7.4.2 *Stap 12: Beoordelen van restrisico's en organiseren van herijking*

Na het bepalen van de noodzakelijke maatregelen wordt beoordeeld welke risico's voor de rechten en vrijheden van betrokkenen resteren en of de verwerking met die restrisico's verantwoord kan plaatsvinden.

Daarbij wordt vastgelegd welke risico's blijven bestaan, welke partijen daarvoor verantwoordelijk zijn en welke besluiten over de aanvaardbaarheid ervan zijn genomen. De beoordeling vindt plaats binnen de toepasselijke wettelijke verantwoordelijkheden. Een gezamenlijk besluit over restrisico's neemt de eigen verplichtingen van de betrokken verwerkingsverantwoordelijken niet weg.

Onzekerheden die nog niet zijn onderzocht, zijn geen aanvaarde restrisico’s. Als het beschikbare beeld onvoldoende betrouwbaar is of de gevolgen onvoldoende zijn beoordeeld, moet ook worden overwogen de verwerking of interventie aan te passen, uit te stellen of achterwege te laten, met aandacht voor de gevolgen van niet-handelen.

Wanneer voor een concrete verwerking een gegevensbeschermingseffectbeoordeling op grond van artikel 35 AVG verplicht is, moet die worden uitgevoerd. Indien de verwerking ondanks maatregelen een hoog risico zou opleveren en de verantwoordelijke dat risico niet kan beperken, is voorafgaande raadpleging op grond van artikel 36 AVG vereist. De bredere ketenanalyse staat naast deze wettelijke verplichtingen en vervangt ze niet.

De beoordeling eindigt niet bij de ingebruikname van de samenwerking. Veranderingen in de maatschappelijke opgave, de deelnemende organisaties, de juridische kaders, de technologie, de

informatiebehoefte of de schaal van de gegevensverwerking kunnen aanleiding geven om eerdere keuzes te herzien.

De herijking betreft niet alleen de technische en organisatorische maatregelen, maar zo nodig ook de noodzakelijkheid en rechtmatigheid van de gegevensverwerking, de analyse van de impact op ketenniveau en de verdeling van verantwoordelijkheden.

De uitkomst is een onderbouwd besluit over de voorgenomen verwerking, met inzicht in de restrisico's en afspraken over de momenten en omstandigheden waarin een nieuwe beoordeling noodzakelijk is.

7.5 Het stappenplan als samenhangende beoordeling

Het stappenplan brengt de verschillende onderdelen van deze handreiking bijeen, maar vormt geen afvinklijst waarmee rechtmatigheid automatisch kan worden vastgesteld. De kwaliteit van de beoordeling hangt af van de onderbouwing van de gemaakte keuzes en van de samenhang tussen de maatschappelijke opgave, de informatiebehoefte, de beoordeling van de rechtmatigheid en de getroffen waarborgen.

Daarbij zijn twee uitgangspunten bepalend. Ten eerste is niet iedere verwerking binnen een keten een verwerking op ketenniveau. Veel gegevensverwerkingen blijven onderdeel van de eigen taken en verantwoordelijkheden van de deelnemende organisaties. Ten tweede kunnen op ketenniveau informatie, afhankelijkheden en risico's ontstaan die niet volledig zichtbaar worden vanuit de afzonderlijke organisaties.

De beoordeling moet beide niveaus recht doen. Zij voorkomt daarmee zowel dat verantwoordelijkheden onnodig naar het ketenniveau worden verplaatst als dat ketenspecifieke gevolgen buiten beeld blijven doordat uitsluitend naar afzonderlijke gegevensverwerkingen wordt gekeken.

De verschillende stappen blijven bovendien met elkaar verbonden. Wanneer bijvoorbeeld blijkt dat de noodzakelijke informatie niet rechtmatig beschikbaar kan worden gesteld, kan dat aanleiding geven om de informatiebehoefte of de inrichting van de samenwerking opnieuw te bezien. Wanneer de analyse van de impact op ketenniveau onaanvaardbare risico's zichtbaar maakt, kunnen aanvullende maatregelen nodig zijn of kan blijken dat een andere werkwijze aangewezen is.

Zo ondersteunt het stappenplan niet alleen de ontwikkeling van nieuwe ketensamenwerkingen, maar ook de beoordeling en verbetering van bestaande samenwerkingen. Het doel is een inrichting waarin de noodzakelijke informatie beschikbaar kan komen zonder dat de juridische grenzen, de verantwoordelijkheden van de betrokken organisaties of de rechten van betrokkenen uit het oog worden verloren.

8 Conclusies

Gegevensverwerking in complexe ketens vraagt om een andere benadering dan gegevensverwerking binnen één organisatie. De betrokken organisaties beschikken ieder over eigen taken, bevoegdheden en verantwoordelijkheden, terwijl het maatschappelijke probleem waarvoor zij samenwerken zich niet noodzakelijk binnen die afzonderlijke grenzen laat oplossen.

De centrale vraag is daarom niet welke gegevens organisaties kunnen uitwisselen, maar welke informatie nodig is om een maatschappelijk probleem gezamenlijk aan te pakken. Vanuit die informatiebehoefte kan worden beoordeeld welke gegevensverwerkingen noodzakelijk en rechtmatig zijn en welke inrichting daarbij passend is.

Het onderscheid tussen het organisatieniveau van de afzonderlijke organisaties en het ketenniveau van de samenwerking is daarbij essentieel. Op het organisatieniveau worden gegevens verzameld en verwerkt binnen de taken en verantwoordelijkheden van afzonderlijke organisaties. Op ketenniveau kan door het beschikbaar maken, combineren of interpreteren van informatie een gezamenlijke informatiepositie ontstaan. Die informatiepositie hoeft niet centraal te worden opgeslagen en valt niet noodzakelijk samen met de bestaande gegevensverwerkingen of verantwoordelijkheden van één organisatie.

Daarin schuilt ook het risico van een niveauvergissing. De rechtmatigheid van afzonderlijke gegevensverwerkingen betekent niet zonder meer dat ook het gebruik van informatie in de samenwerking rechtmatig is. Omgekeerd kan het maatschappelijke belang van de samenwerking niet zelfstandig de juridische voorwaarden voor gegevensverwerking door de afzonderlijke deelnemers vervangen. Beide niveaus moeten in hun onderlinge samenhang worden beoordeeld.

De kwaliteit van de informatieverwerking is daarbij minstens zo belangrijk als de beschikbaarheid van gegevens. Betrouwbaarheid, integriteit, actualiteit en behoud van context bepalen mede of informatie geschikt is voor het doel waarvoor zij binnen de keten wordt gebruikt. Wanneer gegevens uit hun oorspronkelijke context worden gehaald of met andere gegevens worden gecombineerd, kunnen nieuwe betekenissen en risico's ontstaan die bij de afzonderlijke bronverwerkingen niet zichtbaar waren.

De juridische en organisatorische inrichting volgt uit deze analyse. AVG-rollen en privacyafspraken zijn geen vrij te kiezen vertrekpunt voor de samenwerking, maar geven uitvoering aan de verantwoordelijkheden die voortvloeien uit de feitelijke en juridische inrichting van de gegevensverwerking. De analyse van de impact op ketenniveau maakt vervolgens inzichtelijk welke risico's uit de samenhang tussen de verwerkingen ontstaan en of de gekozen maatregelen in de praktijk voldoende bescherming bieden.

Daarmee is de inrichting van gegevensverwerking in complexe ketens geen eenmalige exercitie. Veranderingen in de maatschappelijke opgave, de informatiebehoefte, de wetgeving of de samenwerking kunnen aanleiding geven tot herbeoordeling van eerdere keuzes.

9 Aanbevelingen

Uit deze handreiking volgen de volgende uitgangspunten voor het ontwerpen, beoordelen en onderhouden van gegevensverwerking in complexe ketens.

1. **De maatschappelijke opgave vormt het vertrekpunt.** De noodzaak van samenwerking wordt bepaald door het probleem dat afzonderlijke organisaties niet zelfstandig kunnen oplossen. Gegevensuitwisseling, infrastructuur en juridische afspraken zijn middelen om die opgave te ondersteunen en vormen geen doel op zichzelf.

2. **Het onderscheid tussen organisatie- en ketenniveau blijft zichtbaar.** Bij de beoordeling van de informatiebehoefte, de rechtmatigheid, de risico's en de verantwoordelijkheden is duidelijk welke aspecten tot de afzonderlijke organisaties behoren en welke voortvloeien uit hun samenwerking. Daarmee worden zowel onnodige centralisatie als onvoldoende aandacht voor ketenspecifieke gevolgen voorkomen.

3. **De inrichting op ketenniveau blijft beperkt tot wat noodzakelijk is.** Een gezamenlijke informatiepositie vereist niet vanzelfsprekend een centrale gegevensverzameling, uniforme bronregistraties of één technische voorziening. De inrichting sluit aan bij de informatie die nodig is om het maatschappelijke probleem aan te pakken, met behoud van de verantwoordelijkheden en mogelijkheden van de afzonderlijke organisaties.

4. **De betekenis en betrouwbaarheid van informatie zijn onderdeel van de beoordeling van de rechtmatigheid en de inrichting van de gegevensverwerking.** Gegevens zijn niet zonder meer geschikt voor gebruik buiten hun oorspronkelijke context. De herkomst, actualiteit, status, onzekerheid en gebruiksbeperkingen van informatie zijn bepalend voor de wijze waarop deze verantwoord kan worden geïnterpreteerd en gebruikt.

5. **De rechtmatigheid en de passende maatregelen worden op beide niveaus beoordeeld.** Beoordeel de bronverwerkingen, de voorwaarden voor verstrekking en verder gebruik én de gezamenlijke informatieverwerking. Leg per risico vast welke waarborg bij de bron nodig is, welke aanvullende afspraak op ketenniveau noodzakelijk is en wie uitvoering en correctie verzorgt. Toestemming vervangt geen ontbrekende bevoegdheid.

6. **Verantwoordelijkheden, procesregie en risico's worden in samenhang beoordeeld.** Procesregie ondersteunt de gezamenlijke analyse en besluitvorming, zonder de wettelijke verantwoordelijkheden van de deelnemers over te nemen. De analyse van de impact op ketenniveau omvat ook risico's die ontstaan door de combinatie van gegevens en door omstandigheden die de uitvoerbaarheid van waarborgen beïnvloeden. De gemaakte afspraken blijven onderwerp van beheer en periodieke herijking.

10 Tot slot

De meerwaarde van ketensamenwerking ligt niet in het bijeenbrengen van zoveel mogelijk gegevens, maar in het beschikbaar maken van de juiste informatie op het moment en in de context waarin zij nodig is.

Een zorgvuldige inrichting van de informatieverwerking maakt het mogelijk maatschappelijke problemen gezamenlijk aan te pakken zonder de juridische grenzen en verantwoordelijkheden van afzonderlijke organisaties uit het oog te verliezen. Daarvoor is niet noodzakelijk méér gegevensverwerking nodig, maar vooral een beter begrip van welke informatie de samenwerking daadwerkelijk vereist en welke gevolgen het gebruik daarvan met zich meebrengt.

11 Bronnen

Grijpink, J.H.A.M. (1997), Keteninformatisering met toepassing op de justitiële bedrijfsketen. Proefschrift.

Grijpink, J. (2010), Chain Analysis for Large-scale Communication Systems. Methodologie voor ketenanalyse, dominante ketenproblemen en keteninformatiestrategie.

Grijpink, J. (2011), De uitdaging van grootschalige stelsels voor informatie-uitwisseling tussen organisaties. Afscheidsoratie.

Adviescollege ICT-toetsing (26 mei 2026), Advies Programma Implementatie Generieke Functies.

European Data Protection Board (2020), Guidelines 05/2020 on consent under Regulation 2016/679, versie 1.1, 4 mei 2020.

Wet gegevensverwerking door samenwerkingsverbanden (WGS).

Wet elektronische gegevensuitwisseling in de zorg (Wegiz).

Wet aanpak meervoudige problematiek sociaal domein (Wams), wetsvoorstel 36 295.

CIP (2020), Privacyafspraken bij ketensamenwerking, versie 1.1. Voorganger van deze handreiking.

Verordening (EU) 2016/679 (AVG), met name artikelen 4, 5, 6, 9, 25, 26, 28, 35, 36, 38 en 39.

European Data Protection Board (2020), Guidelines 4/2019 on Article 25 Data Protection by Design and by Default, versie 2.0, 20 oktober 2020.