



Governance bij toepassing MPC

ten behoeve van pandemische paraatheid

7 november 2025

Door:

Kerngroep GERDA (Nicole Rommens, Astrid van Haastert)

Met hulp van:

Gerard van den Berg, Ivonne Knopert, Ron Allard

Voor:

FG & PO van GGD'en in geval van een pandemie

Dit paper is onderdeel van het project Pandemische Paraatheid gefinancierd door ZonMw. Dit is het eindproduct van een van de zes werkpakketten van het project.

Partners in dit ZonMW project zijn: TNO, Linksight, Topicus, GGD Noord-Oost Gelderland, GGD Brabant-Zuidoost, GGD Utrecht, GGD GHOR Nederland en regionale datawerkplaats GERDA.

INHOUDSOPGAVE

1. Aanleiding	3
1.1. Introductie	3
1.2 Uitleg PET & MPC	4
1.3 Structuur whitepaper	5
1.4 Take-away whitepaper	5
2. Vraagstukken wet- en regelgeving	6
2.1 Best practices & geleerde lessen	7
3. Relevante wetgeving	10
3.1 Vaststellen toepasselijkheid AVG	11
3.2 Bepalen verwerkingsverantwoordelijkheden	11
a) Is leverancier op te merken als verwerker?	12
b) Zijn de deelnemende leden van de datasamenwerking gezamenlijk verantwoordelijk?	12
3.3 Beoordelen doelmatigheid	13
4. Rollen	14
4.1 Rollen van verschillende organisaties	14
4.2 Rollen binnen een organisatie	16
5. Ethische overwegingen	18
6. Referenties	20

1. Aanleiding

1.1. Introductie

De COVID-19-pandemie heeft het belang van data bij het bestrijden van wereldwijde gezondheids crises onderstreept, maar tegelijkertijd ook de uitdagingen blootgelegd in het effectief verzamelen, delen en gebruiken van deze data. Enerzijds is snelle en nauwkeurige informatie essentieel voor vroegtijdige detectie van besmettingen en het nemen van gerichte maatregelen. Anderzijds stuiten datadeling en -analyse vaak op zorgen rondom privacy, ethiek en wetgeving.

Om deze balans te bewaken, winnen **privacy-bevorderende technologieën (Privacy-Enhancing Technologies, PET's)** aan belang. Nieuwe technieken maken het mogelijk om gevoelige gezondheidsdata te benutten zonder dat deze centraal worden opgeslagen of individueel herleidbaar zijn. Dit draagt bij aan een veiligere en efficiëntere aanpak van pandemieën. Een concreet voorbeeld van het gebruik van PET's is het **GERDA-project** in de regio Achterhoek, waarin ervaring is opgedaan met MPC om privacy te waarborgen bij data-analyse.

Het toepassen van PET's kan bijdragen aan **pandemische paraatheid**, oftewel de mate waarin we voorbereid zijn op toekomstige uitbraken van infectieziekten. Door deze innovatieve technologieën in te zetten, kunnen we:

1. **Vroegtijdig clusters van besmettingen detecteren**, bijvoorbeeld in specifieke wijken, werkplekken, scholen of verpleeghuizen. Dit stelt gezondheidsautoriteiten zoals de GGD in staat om snel en gericht maatregelen te nemen, zoals bron- en contactonderzoek, het adviseren van quarantaine of isolatie, het opschalen van testcapaciteit en het informeren van kwetsbare groepen.
2. **Kwetsbare groepen beter beschermen**. Ouderen, mensen met onderliggende aandoeningen en mensen met een lage sociaaleconomische status (SES) lopen een verhoogd risico op ernstige ziekte en sterfte. Bovendien hebben zij vaak minder mogelijkheden om zich tegen besmetting te beschermen, bijvoorbeeld door woonomstandigheden of financiële beperkingen. PET's kunnen helpen om deze groepen beter te identificeren en ondersteunen, zonder hun privacy in gevaar te brengen.

Op basis van deze analyses kan er effectief ingespeeld worden op de pandemie:

- **GGD NOG** kan effectieve maatregelen inzetten. Voorbeelden zijn; inzetten bron en contactonderzoek of hygiënemaatregelen, vaccinaties, isolatie, quarantaine,

beroepsverbod en sluiting van terreinen of gebouwen

- Bij toename van de infectieziekte (warme fase) neemt het **LFI** over als crisisorganisatie. Zij bepalen landelijk beleid om de pandemie effectief te bestrijden. Voorbeelden zijn: routekaart, afstand houden, beperken van groepsgrootte en communicatie naar inwoners
- Deskundige infectiepreventie helpt de **Zorgorganisaties** bij het voorkomen en beheersen van de besmetting. Zorgorganisaties kunnen maatregelen nemen zoals bijvoorbeeld geen handen schudden, meer digitaal organiseren. Bij toename van de infectieziekte reguliere zorg op- of afschalen om een potentiële brandhaard op te vangen. Capaciteit kan vrij gemaakt worden voor acute zorg en er kunnen aanvullende materialen ingekocht worden: mondkapjes, testen, medicijnen, etc.

Om de potentie van PET's in pandemische paraatheid verder te verkennen, heeft ZonMw subsidie toegekend voor onderzoek naar de inzet van deze technologieën. Dit onderzoek richt zich op de vraag hoe PET's kunnen bijdragen aan snellere en effectievere interventies bij toekomstige pandemieën, met behoud van privacy en ethisch verantwoord gebruik van gezondheidsdata. Binnen dit kader belicht dit document de **juridische en ethische overwegingen** van PET's, en in het bijzonder van MPC, in de context van pandemische paraatheid. Het dient als praktische leidraad voor een nieuwe regio, zodat deze overwegingen direct kunnen worden meegenomen en de implementatie van PET's versneld kan plaatsvinden.

1.2 Uitleg PET & MPC

Privacy-Enhancing Technologies (PETs) zijn technieken en methoden die helpen om persoonsgegevens te beschermen tijdens het verwerken, delen en analyseren van data. Ze zorgen ervoor dat gevoelige informatie bruikbaar blijft zonder privacy te schenden. Een vorm van PET is **Multi Party Computation (MPC)**.

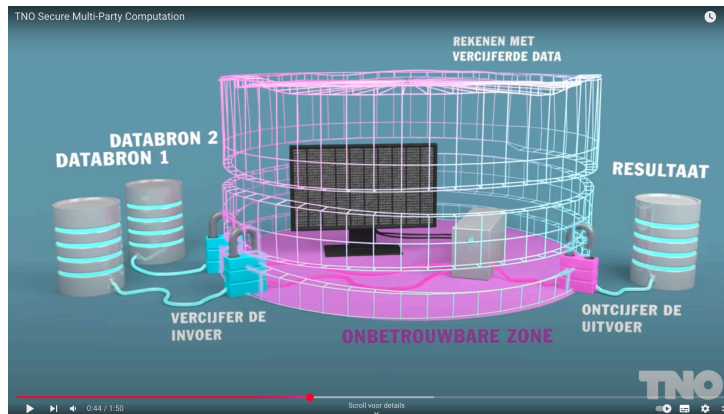
Multiparty Computation (MPC) is een cryptografische techniek waarmee meerdere partijen samen berekeningen kunnen uitvoeren op hun gezamenlijke data, zonder dat ze hun individuele gegevens aan elkaar hoeven bloot te geven.

Hoe werkt het?

- Gegevens worden versleuteld en verdeeld in delen over meerdere partijen.
- Elke partij voert berekeningen uit op deze versleutelde data, zonder de originele gegevens ooit te zien.
- Aan het einde krijgen ze alleen het eindresultaat, zonder dat iemand de invoer van een ander heeft kunnen inzien.

- Daar bovenop worden governance rules afgedwongen. Dit zijn regels binnen een datasamenwerking die beschrijft waar elke analysevraag aan moet voldoende. Denk aan de minimale groeps grootte waarover uitkomsten teruggegeven mogen worden.

Onderstaande film legt op een eenvoudige wijze uit wat MPC is:



1.3 Structuur whitepaper

In deze whitepaper zullen we stil staan bij:

- H2: Welke vraagstukken zijn er rondom wet- en regelgeving? Wat zijn best practices en geleerde lessen die toegepast kunnen worden?
- H3: Overzicht van relevante wetten
- H4: Rollen & verantwoordelijkheden binnen de datasamenwerking
- H5: Ethische overwegingen

1.4 Take-away whitepaper

In een pandemie is het aannemelijk dat op regionaal niveau gegevens op persoonsniveau gedeeld moeten worden. Op landelijk niveau kan doorgaans worden volstaan met geaggregeerde gegevens, waardoor geen persoonsgegevens worden gedeeld en de AVG niet van toepassing is. Voor regionale gegevensdeling geldt de AVG wél. De **Wet publieke gezondheid** biedt hiervoor een passende grondslag, waarbij de betrokken organisaties **gezamenlijk verwerkingsverantwoordelijk** zijn.

Door vooraf duidelijke ethische kaders te formuleren kan de balans worden bewaakt tussen een effectieve crisisrespons en de bescherming van individuele rechten en privacy. Waarden zoals goede gezondheid, betrouwbaarheid, daadkracht, vertrouwen en autonomie zijn van belang. Verschillende handelingsopties zijn verkend en worden deels al opgepakt, maar **structurele voorbereiding blijft essentieel om tijdens een pandemie snel en zorgvuldig te kunnen handelen.**

2. Vraagstukken wet- en regelgeving

Bij het opzetten van een datasamenwerking met MPC spelen diverse juridische en governance vraagstukken. Om de opstart hiervan tijdens een pandemie te versnellen, zijn lessen uit het GERDA-project verzameld. GERDA richt zich op het ontwikkelen van een data-infrastructuur die domeinoverstijgend gegevens samenbrengt met behulp van MPC. Binnen GERDA heeft een werkgroep Governance deze vraagstukken geanalyseerd en uitgewerkt in relatie tot het MPC-product van Linksight. Daarnaast zijn al meerdere datavraagstukken uitgevoerd binnen de datasamenwerking. Dit heeft inzicht gegeven in de belangrijkste vraagstukken die spelen bij het opzetten van een nieuwe datasamenwerking.

1. **Vraagstukken rondom AVG vereisten:**

Ook bij het gebruik van MPC is er sprake van verwerken van persoonsgegevens en is daarom de AVG van toepassing.

- a. Bepalen van verwerkingsverantwoordelijkheid
- b. Is de verwerking van persoonsgegevens in relatie met het doel? Op basis van welke rechtsgrond? En wat is de doelbinding?

2. **Welke juridische structuur is passend?**

Bij het opzetten van een datasamenwerking is het belangrijk om vooraf goed te bepalen onder welke voorwaarden de samenwerking wordt ingericht en welke juridische structuur daarbij passend is. Denk hierbij aan het oprichten van een gezamenlijke entiteit of het vastleggen van afspraken in een samenwerkingsovereenkomst. Tijdens een pandemie is er echter vaak weinig tijd en ruimte om dergelijke afwegingen nog uitgebreid te maken en moet er vooral gehandeld worden. Daarom is het essentieel om deze keuzes al in de voorbereiding op een pandemie doordacht te hebben. In het geval van GERDA bleek een samenwerkingsovereenkomst voldoende; deze vraagt minder formaliteiten en brengt lagere kosten met zich mee dan het oprichten van een juridische entiteit.

Bij het opstarten van een nieuwe datasamenwerking is het wenselijk om de volgende producten uit te werken:

1. [Data Protection Impact Assessment](#) (DPIA)
om de risico's van te beoordelen en zo nodig maatregelen te nemen.
2. [Beschrijving van de Governance](#)
 - a. technische governance rol, rollen in de samenwerking en beleggen van deze rollen.
3. [Gezamenlijke verwerkingsovereenkomst](#) of andere benodigde samenwerkingsvorm
4. [Aanpak voor vraagarticulatie](#) & [template voor vraagarticulatie](#)
 - a. om te komen tot een analyseopzet voor beoordeling door de learning community data stewards
 - b. en waarmee de data scientists na akkoord de juiste input hebben om met de analyses te starten
5. [Ethisch beleidsprotocol / overwegingen](#)

2.1 Best practices & geleerde lessen

De werkgroep Governance¹ van het project GERDA heeft onderstaande lessen en best practices geformuleerd²:

1. **Onderscheid tussen regionaal netwerk en datasamenwerking**

Er is een onderscheid tussen het regionale netwerk dat je wilt opbouwen en de datasamenwerking die daarin plaatsvindt. Het is belangrijk om elkaar eerst beter te leren kennen en afspraken te maken over de wijze van samenwerking. De techniek moet hierbij ondersteunend zijn.

Best practice: In nieuwe samenwerkingsverbanden is het belangrijk om eerst kennis te maken, een gezamenlijk doel te formuleren en duidelijke afspraken te maken over de wijze van samenwerken.

Lesson learned: Bij niet elke analyse vraagstuk hoeft elke partij van de regionale datasamenwerking betrokken te zijn. Maak duidelijk per vraagstuk wie er betrokken dient te worden.

2. **Betrek Functionarissen Gegevensbescherming (FG's) en Privacy Officers (PO's) vanaf het begin**

Het betrekken van FG's of PO's bij het opstarten van een datasamenwerking is

¹ Bestaande uit afvaardiging van alle specialisten (privacy officers / functionaris gegevensbescherming) van alle organisaties en bijgestaan door een jurist vanuit een van de betrokken organisaties.

² Alle inzichten van de werkgroep van GERDA zijn terug te lezen in de [Whitepaper Governance bij de toepassing van MPC](#).

cruciaal. Zij kunnen gezamenlijk vragen over het gebruik van Privacy-Enhancing Technologies (PET's) formuleren en oppakken.

Lesson learned: Neem de FG's of PO's vanaf het begin mee in de werking van de techniek. Laat de productleverancier uitleg geven en vraag om relevante artikelen die als input kunnen dienen. Uit ervaring blijkt dat het tijd kost voordat iedereen zich comfortabel voelt met de techniek en de koppeling kan maken met privacy vraagstukken.

Best practice: Het gezamenlijk optrekken van verschillende partijen helpt om complexe materie beter te doorgronden.

3. **Duidelijkheid over de rol van de Data Steward**

Binnen het inzetten van Privacy Enhancing Technology kunnen nieuwe rollen ontstaan zoals de rol van data steward (zie ook [sectie 5.2](#)). De rol van data steward was nieuw binnen de bij GERDA betrokken organisaties en dit bleek een complex vraagstuk, zowel inhoudelijk als organisatorisch.

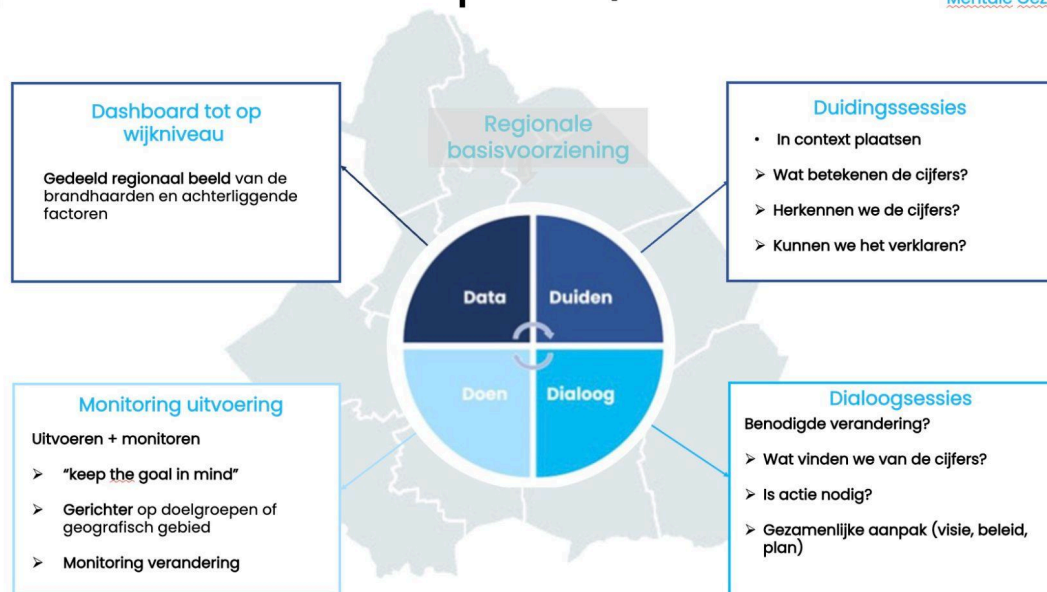
Lesson learned: Maak organisatorische vereisten, zoals de nieuwe rol van data steward, tijdig en duidelijk bekend bij alle deelnemende partijen inclusief een heldere rolomschrijving en benodigde uren (en financiering hiervan).

4. **Investeer in vraagarticulatie met inzichtvragers**

Het formuleren van de doelstelling waaraan gezamenlijk wordt gewerkt is essentieel om impact te kunnen maken. Het bepalen van de juiste vraag, het bepalen van de benodigde data en wat er gedaan kan worden met inzichten (data, duiden, dialoog, doen) is niet vanzelfsprekend. Het is echter essentieel om daadwerkelijk data te gebruiken om verder te komen. Deze vraagarticulatie helpt de data stewards en data scientists om data op de juiste manier in te zetten.

Best practice: Investeer in vraagarticulatie en zorg voor duidelijke communicatie met inzichtvragers om tot relevante en goed gedefinieerde vraagstukken te komen. Dit kan via het [template vraagarticulatie](#) vanuit het project GERDA of de data, duiden, dialoog, doen cyclus vanuit het project Datawerkplaats Drenthe. De stappen hiervan zijn geduid in figuur 1.

Aanpak van de Datawerkplaats | Hoe?



Figuur 1: Onderdeel raamwerk voor de toepasselijkheid van de AVG

Binnen GERDA is nog geen ervaring opgedaan met het gebruik van MPC in de context van pandemische paraatheid. Een belangrijk verschil tussen de onderzoeksvragen binnen GERDA en die voor pandemische paraatheid is dat GERDA zich richt op regionale vraagstukken, terwijl een pandemie regionale en bovenregionale of nationale uitdagingen met zich meebrengt.

3. Relevante wetgeving

In het gebruik van PET's kunnen verschillende wetten van toepassing zijn:

- **Algemene Verordening Gegevensbescherming (AVG)**

De AVG stelt regels voor het verwerken van persoonsgegevens.

Relevantie:

- Vereist een rechtmatige grondslag voor gegevensverwerking.
- Dwingt tot Data Protection Impact Assessment (DPIA) bij grootschalige of gevoelige dataverwerking.

- **Data Governance Act (DGA) & Data Act – Europese wetgeving**

De DGA en Data Act regelen hoe data binnen de EU gedeeld en gebruikt mogen worden. In Nederland blijft de AVG de belangrijkste wet voor de verwerking van persoonsgegevens.

- **Wet kwaliteit, klachten en geschillen zorg (WKKgz)**

Deze wet waarborgt de kwaliteit en veiligheid van zorg en gegevensgebruik in de zorgsector. De wet stelt zorgorganisaties in staat gegevens te gebruiken ter verbetering van de kwaliteit van zorg. Dit is dus een mogelijke rechtsgrond onder de AVG.

- **Wet publieke gezondheid (WPG)**

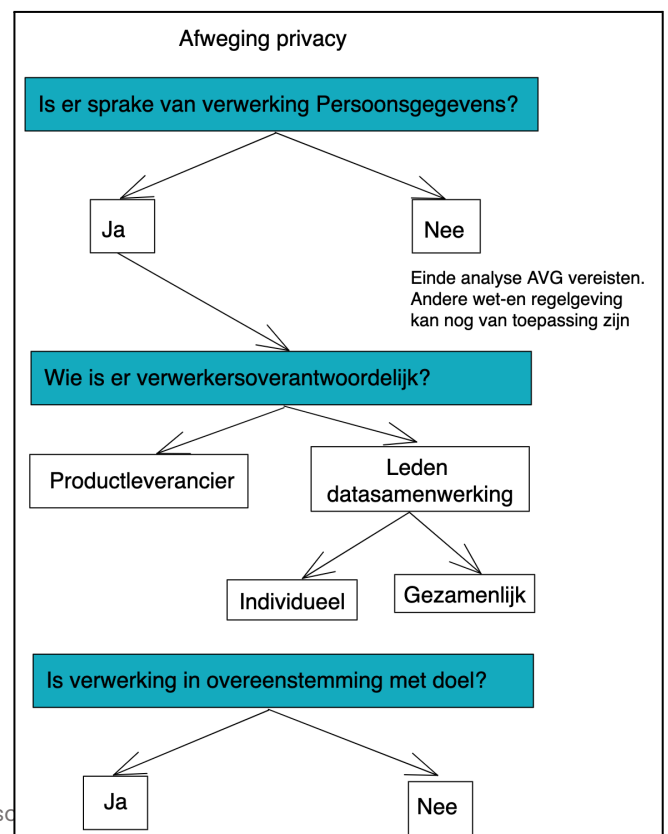
De Wpg geeft GGD's en het RIVM bevoegdheden om infectieziekten te bestrijden.

- **European Health Data Space act (EHDS)**

De EHDS is een verordening vanuit de EU dat tot doel heeft een gestandaardiseerde en veilige uitwisseling van gezondheidsgegevens mogelijk te maken.

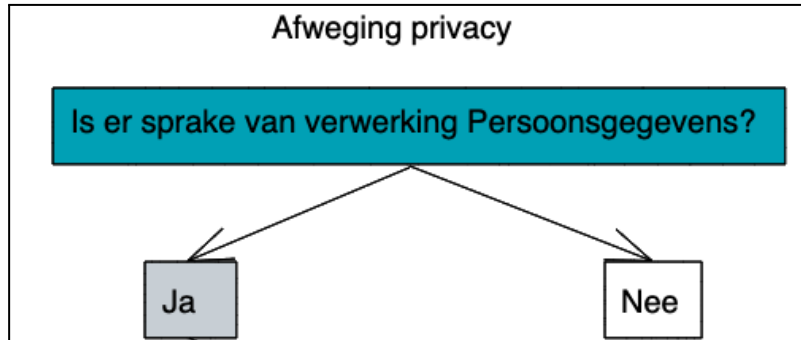
Om vast te stellen aan welke wet- en regelgeving voldaan moet worden, kunnen de volgende stappen doorlopen worden:

- 1) Vaststellen of er sprake is van verwerking van persoonsgegevens?
- 2) Bepalen van verwerkingsverantwoordelijkheid/heden:
 - a) Leden van de datasamenwerking individueel / gezamenlijk
 - b) Productleverancier
- 3) Beoordelen doelmatigheid van de verwerking van (bijzondere) persoonsgegevens voor de deelnemende (zorg)organisaties.



Visueel ziet het gehanteerde raamwerk er uit zoals het figuur hiernaast.

3.1 Vaststellen toepasselijkheid AVG



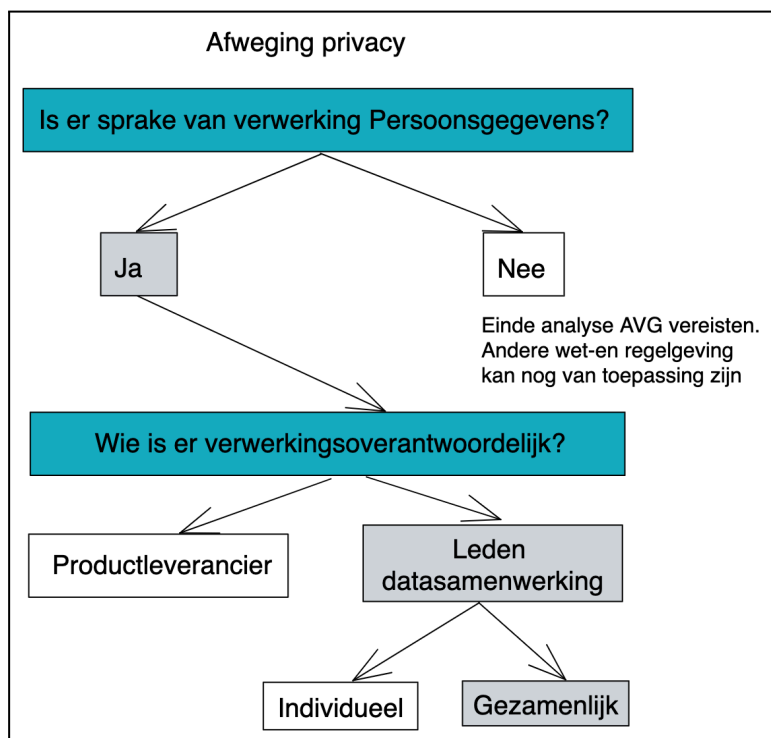
Figuur 2: Onderdeel raamwerk voor de toepasselijkheid van de AVG

In het gebruik van PET's is er sprake van het verwerken van persoonsgegevens. Dat persoonsgegevens gepseudonimiseerd zijn doet hier niets aan af. (Pels Rijcken)

Het is belangrijk op te merken dat het Europese Hof van Justitie in twee rechtszaken heeft bepaald dat pseudonimisering in bepaalde gevallen beschouwd mag worden als anonimisering van persoonsgegevens. Tegen deze beslissing loopt nog een hoger beroep. Als het standpunt van het Hof stand houdt, betekent dit waarschijnlijk dat de AVG niet langer van toepassing is op, gezien de aard van de pseudonimisering overeenkomt met de situatie in de rechtszaak.

3.2 Bepalen verwerkingsverantwoordelijkheden

Om vast te stellen waar de plichten rondom verwerkingsverantwoordelijkheid ligt moet helder zijn welke betrokken partijen verwerkingsverantwoordelijk of verwerker zijn. Het verwerken van persoonsgegevens is niet het primaire doel van de datasamenwerking. Het doel is gericht op het creëren van domein-overstijgende inzichten.



Figuur 3: Onderdeel raamwerk voor het bepalen van de verwerkingsverantwoordelijkheden

a) Is leverancier op te merken als verwerker?

Het grote voordeel van de techniek MPC is dat deelnemende partijen gefaciliteerd worden om op privacy-vriendelijke wijze analyses uit te voeren, zonder dat de leverancier toegang heeft tot de data. Als verwerkingen van persoonsgegevens door gebruik te maken van MPC volledig buiten de leverancier om plaatsvinden, valt de leverancier niet als verwerker aan te merken.

In het geval van leverancier 'Linksight' kan geconcludeerd worden dat Linksight geen verwerker is omdat (1) Linksight niet bij de data kan en (2) de deelnemende partijen via de governance rules zelf bepalen wat wel en niet kan met hun eigen data.

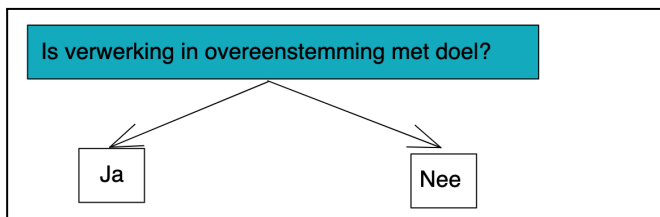
b) Zijn de deelnemende leden van de datasamenwerking gezamenlijk verantwoordelijk?

De leden van de datasamenwerking kunnen geduid worden als gezamenlijk verantwoordelijk wanneer de data als de doelen waarvoor de verwerking plaatsvindt in gezamenlijkheid worden bepaald. Voor zover bij de aanlevering van de data en bij de uitwisseling daarvan geen sprake is van een hiërarchische relatie (en in dat kader ook geen afspraken zijn gemaakt) is iedere partij gelijk. Iedere partij is vrij en daarmee verantwoordelijk voor het verwerken en uitwisselen van de door hen ingeladen informatie. (Pels Rijcken)

In de context van een reguliere datasamenwerking wordt vaak gezamenlijk bepaald welke data geanalyseerd wordt ten einde van welk doel. In dat geval is het aannemelijk dat de deelnemende leden gezamenlijk verantwoordelijk zijn.

3.3 Beoordelen doelmatigheid

Het laatste aspect van het het raamwerk is of de verwerking van de bijzondere persoonsgegevens in overeenstemming is met het door de (zorg)organisaties vastgelegde doel.



Figuur 4: Onderdeel raamwerk voor het bepalen van de doel van de verwerking

Voor het verwerken van persoonsgegevens zijn zes grondslagen mogelijk:

1. uitvoering van een overeenkomst;
2. toestemming;
3. wettelijke verplichting
4. vitaal belang van betrokkene of andere personen;
5. algemeen belang of
6. gerechtvaardigd belang.

In geval van het ontstaan van bovenregionale besmettingshaarden is de grondslag: 'Algemeen belang' van toepassing. De GGD heeft hiernaast ook de wettelijke verplichting o.b.v. Wet Publieke Gezondheid.

4. Rollen

4.1 Rollen van verschillende organisaties

In het geval van een pandemie zal een data samenwerking gestart moeten worden om besmettingshaarden te detecteren en kwetsbare groepen te identificeren. Naar verwachting is een regionale en een landelijke datasamenwerking noodzakelijk.

Regionale datasamenwerking

In het uitgewerkt scenario van het detecteren van besmettingshaarden en identificeren van kwetsbare groepen is een **regionaal** datasamenwerking nodig met o.a. GGD, Huisartsen, Ziekenhuis en Apotheek. Binnen deze datasamenwerking wordt op basis van MPC data gedeeld terwijl;

- Data bij de bron (geen centrale opslag)
- Data-integratie op individueel niveau
- Domeinoverstijgende inzichten / acties
- Data soevereiniteit bij de bron (en dus ook eigenaarschap datakwaliteit)

Het algoritme om besmettingshaarden te detecteren en kwetsbare groepen te identificeren wordt regionaal getraind door data van deze organisaties te combineren. Het gaat om actuele data van de regio en door de regio.

Landelijke datasamenwerking

Op **landelijk niveau** is er geen directe uitwisseling van persoonsgegevens tussen regio's of met landelijke instanties. De door regio's getrainde modellen worden landelijk samengevoegd tot een geoptimaliseerd model middels *federated learning*. Het model kan vervolgens beschikbaar gesteld worden, zodat zij gebruik kunnen maken van landelijke inzichten zonder data te delen. Dit maakt het mogelijk om overkoepelende patronen te detecteren op basis van gecombineerde model uitkomsten.

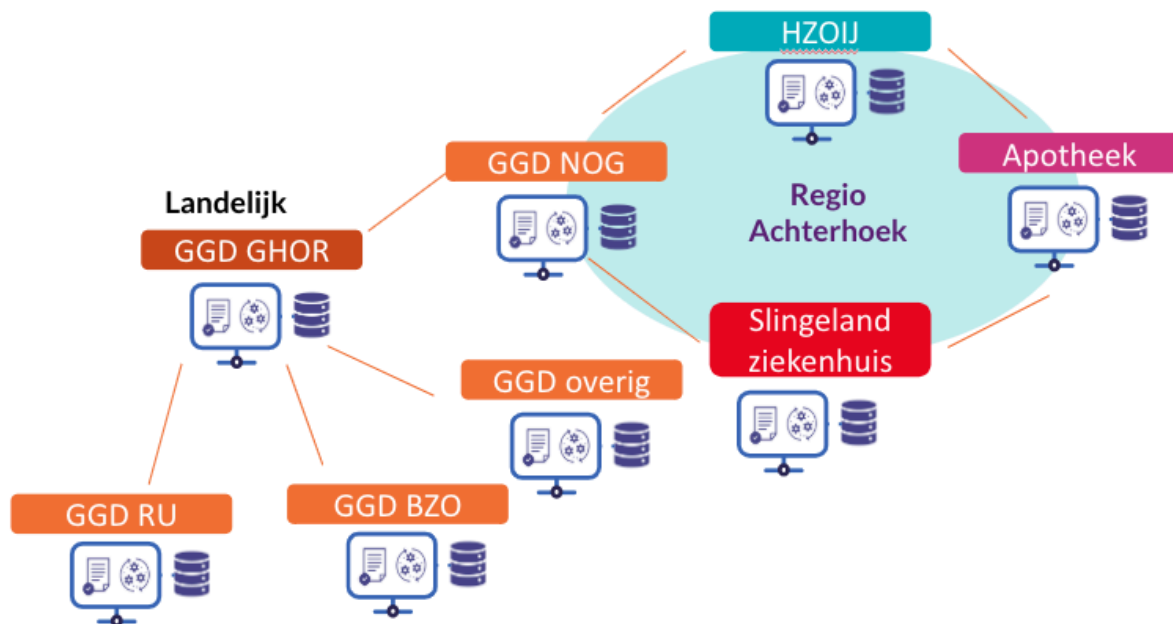
De kernprincipes van de landelijke samenwerking zijn:

- Geen centrale opslag van persoonsgegevens
- Model integratie en -distributie
- Inzichten van o.a. brandhaarden op landelijk niveau



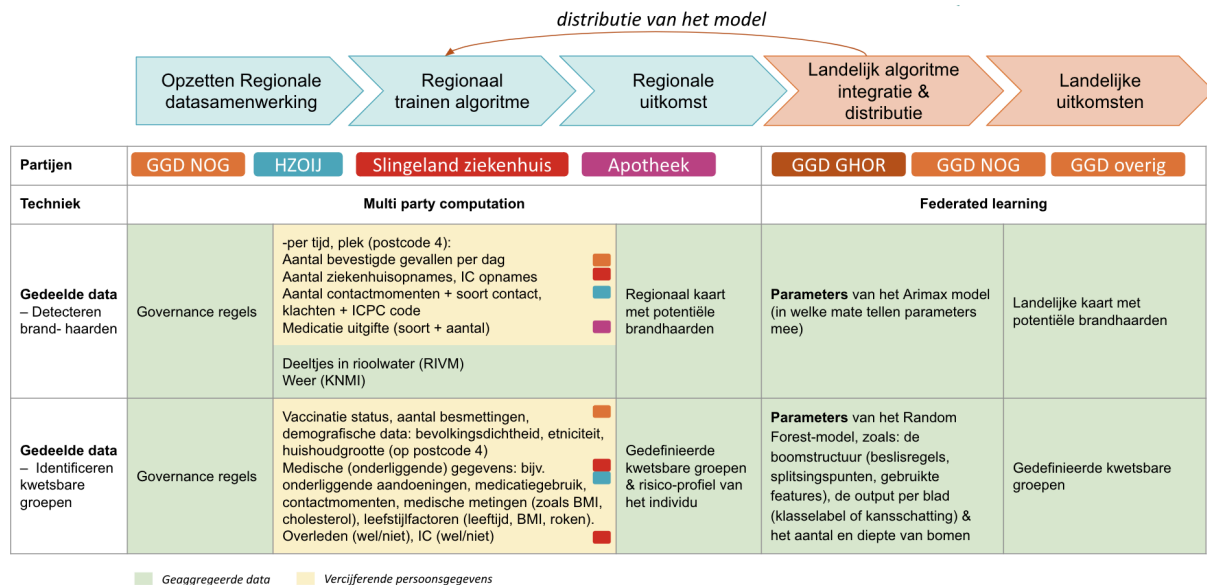
Figuur 5 Voorbeeld van een regionale datasamenwerking in geval van een pandemie

- Regionale autonomie blijft behouden



Figuur 6: Voorbeeld van een landelijke datasamenwerking in geval van een pandemie

Welke data moet er op welk moment gedeeld worden?



Figuur 7: Overzicht van de data die gedeeld wordt en wat hiervan om persoonsgegevens gaat.

4.2 Rollen binnen een organisatie

Voor een effectieve samenwerking binnen een datasamenwerkingsverband is het essentieel dat deelnemende organisaties verschillende rollen invullen. De drie belangrijkste rollen zijn: **data steward**, **data scientist** en **inzichtvrager**.

Data steward

De data steward is de persoon die samen met de andere data stewards de “spelregels” opstelt waarbij zij rekening houden met wat er mag en kan (wet- en regelgeving). Daarnaast is de data steward ook de persoon die controleert (via de audittrail) of de opgestelde regels gehandhaafd worden en kan, na overleg, de een voorstel doen tot aanpassing van de “spelregels” en/of bewaken of voorstellen voor aanpassing voldoen aan wetgeving en interne regels. Ten slotte controleert de data steward periodiek de integriteit van de analyses.

Data Scientist

De data scientist is de “speler” die inzichten uit data haalt, binnen de door de data steward opgestelde “spelregels”. De data scientist is elke beoogde gebruiker van de datawerkplaats en kan verschillende rollen hebben in een organisatie zoals BI, beleidsmaker of modelontwikkelaar.

Inzichtvrager

De inzichtvrager is degene die een specifiek vraagstuk heeft en op basis van data een antwoord of inzicht wil verkrijgen. Dit kunnen beleidsmakers, onderzoekers of zorgprofessionals zijn die data-analyses nodig hebben ter ondersteuning van besluitvorming of strategische keuzes. In het kader van pandemische paraatheid zijn dit met name IZB-artsen, die inzicht willen in bijvoorbeeld infectie patronen, risicogroepen of de effectiviteit van maatregelen.

Om duidelijk te maken wie welke verantwoordelijkheden heeft binnen de datasamenwerking, wordt hieronder een RACI-tabel gepresenteerd.

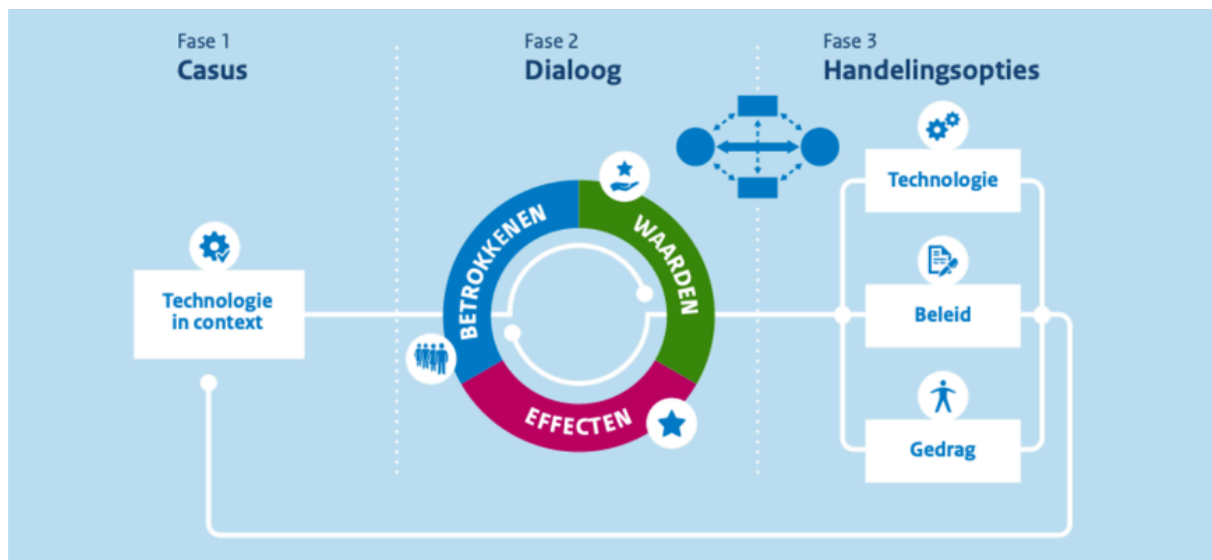
Werzaamheden	Rol	RACI – rol			
		Responsible	Accountable	Consult	Inform
Effectueren van beleid en procedures (governance rules & toegangsrechten)	Data steward	X	X		
	FG, Data scientist, Informatie manager			X	X

Inrichten van een operationele data samenwerkingsstructuur	Data steward	X			
	Data scientist, inzichtvrager				X
Monitoren dat governance rules gevolgd worden	Data steward	X	X		
	Data scientist			X	
	Inzichtvrager			X	X
Aanleveren en actualiseren databeschrijvingen	Data steward	X			
	Data scientist				X
	Informatie manager		X		
Aanspreekpunt zijn voor de datakwaliteit	Data steward	X	X		
	Data scientist			X	X
	Informatie manager			X	
	Inzichtvrager				X
Beschrijven van een onderzoeksopzet	Data steward			X	X
	Inzichtvrager	X	X		
Een analyse uitvoeren door data te structureren, analyseren en visualiseren in informatie-producten	Data scientist	X	X		
	Informatie manager			X	
	Inzichtvrager			X	X

5. Ethische overwegingen

Bij het inzetten van een datawerkplaats tijdens een pandemie is het cruciaal om vooraf stil te staan bij de ethische implicaties, met name op het gebied van privacy en gegevensbescherming. Tijdens de corona pandemie werd in de haast om gegevens snel te delen en de crisis effectief te managen, onvoldoende rekening gehouden met privacyrichtlijnen. Dit leidde tot ernstige datalekken, waarbij gevoelige informatie van burgers op straat kwam te liggen. Zulke incidenten ondermijnen niet alleen het vertrouwen in overheidsinstanties en zorgorganisaties, maar kunnen de effectiviteit van toekomstige digitale oplossingen belemmeren. Door vooraf goed na te denken over ethische kaders kan worden voorkomen dat dezelfde fouten opnieuw worden gemaakt. Zo blijft de balans gewaarborgd tussen effectieve crisisrespons en het beschermen van de rechten en de privacy van individuen.

In de basis zorgt het inzetten van Privacy Enhancing Technology voor het beter beschermen van de publieke waarde zoals veiligheid, effectiviteit en efficiëntie en het beschermen van de privacy. Om toch de verschillende publieke waarde goed te overwegen is een data dialoog uitgevoerd met gebruikers, beleidsmedewerkers en burgers.



Figuur 8: Overzicht aanpak datadialoog.

De volledige datadialoog is [via de website IBDS](#) te lezen. De belangrijkste **waarde** zijn in de groep gedefinieerd als:

- Goede Gezondheid
- Betrouwbaarheid / Kwaliteit

- Effectiviteit / Daadkracht
- Inclusiviteit / Participatie / Vertrouwen
- Autonomie / Privacy

In de datadialoog zijn veel **handelingsopties** besproken. Een aantal in het bijzonder worden vanuit het projectteam beoordeeld als belangrijk om op te pakken.

Handelingsoptie	Bijbehorende waarde	Actiehouder	In scope project	Wordt al aan gewerkt?
<i>Borgen van datakwaliteit in het systeem (bijvoorbeeld via data schema's)</i>	<i>Betrouwbaarheid</i>	<i>Leverancier MPC (Linksight)</i>	<i>nvt</i>	<i>Ja</i>
<i>Afspraken maken over data uniformiteit</i>	<i>Betrouwbaarheid</i>	<i>LFI</i>	<i>Nee</i>	<i>Ja</i>
<i>Validatie van model</i>	<i>Betrouwbaarheid</i>	<i>Data Scientist</i>	<i>WP 5</i>	
<i>Mogelijkheden creëren tot opt-out</i>	<i>Autonomie</i>	<i>Betrokken organisaties</i>	<i>Nee</i>	
<i>Creëren van plek waar opt-out aangegeven kan worden (bijv. PGO)</i>	<i>Autonomie</i>	<i>Betrokken organisaties</i>	<i>Nee</i>	
<i>Creëren van inzicht welke (eenduidig) gedeeld kan worden met inwoners</i>	<i>Vertrouwen / Participatie</i>	<i>Inzichtvrager</i>	<i>WP 5</i>	
<i>Duiden wat er nodig is aan voorlichting voor inwoners en professionals – gefundeerd op uitkomsten analyse</i>	<i>Vertrouwen / Participatie</i>	<i>Project</i>	<i>Nee</i>	
<i>Verduidelijken wie verantwoordelijk is rondom de data analyse en het aanpassen van beleid in verschillende fases van de pandemie</i>	<i>Effectiviteit</i>	<i>Project</i>	<i>WP 6</i>	<i>Ja</i>

6. Referenties

Digitale Overheid. "Toolbox Ethisch Verantwoorde Interventie." *Toolbox Ethisch*

Verantwoorde Interventie,

<https://www.digitaleoverheid.nl/overzicht-van-alle-onderwerpen/nieuwe-technologieen-data-en-ethiek/publieke-waarden/toolbox-voor-ethisch-verantwoorde-innovatie/>.

Nicpet. "Aandachtspunten bij PET implementaties." *Aandachtspunten bij PET*

implementaties, 2024,

<https://nicpet.pleio.nl/wiki/view/b484fcea-98b5-4849-a1a0-3881a56a00e5/aandachtspunten-bij-pet-implementaties>. Accessed 03 mei 2024.

Nivel. "Vertrouwen in (her)gebruik van gezondheidsgegevens: onderzoek onthult

voorwaarden en overwegingen van burgers en zorgprofessionals." *Vertrouwen in (her)gebruik van gezondheidsgegevens, 22 04 2024,*

[https://www.nivel.nl/nl/nieuws/vertrouwen-hergebruik-van-gezondheidsgegevens-onderzoek-onthult-voorwaarden-en-overwegingen#:~:text=Uit%20onderzoek%20van%20de%20\(inter,leiden%20bij%20he%20tot%20wantrouwen](https://www.nivel.nl/nl/nieuws/vertrouwen-hergebruik-van-gezondheidsgegevens-onderzoek-onthult-voorwaarden-en-overwegingen#:~:text=Uit%20onderzoek%20van%20de%20(inter,leiden%20bij%20he%20tot%20wantrouwen). Accessed 31 03 2025.

Pels Rijcken. "Juridische aspecten van de inzet van Secure Multi-Party Computation

(MPC)." *Juridische aspecten van de inzet van Secure Multi-Party Computation (MPC), 2023,*

<https://pelsrijcken.nl/kennis/juridische-aspecten-van-de-inzet-van-secure-multi-party-computation-mpc>. Accessed 14 April 2025.