Whitepaper
Governance bij toepassing MPC

Datum:
25 april 2023

Door:
Werkgroep GERDA (Jerry Fortuin, Ilona Oude Nijhuis en Nicole Rommens)

Met hulp van:
Gerard van den Berg (Slingeland Ziekenhuis & Sensire - inhoudelijk trekker werkgroep Governance), Bilal Hashmi (ZCN - NAAST), Ivonne Knopert (GGD Noord-Oost Gelderland), Jelle Jonker (Marga Klompé), Erna Ruiter (Huisartsenzorg Oude IJssel), Martine van de Gaar (Linksight), Philip den Hartog (Sensire - Jurist) en Lotte van Dieren (GGD Noord-Oost Gelderland)

Voor:
Domeinoverstijgende samenwerkingsverbanden in (andere) regio's, met name werkgroepen die zich bezig houden met de governance-aspecten rondom decentrale data(analyse).

Over dit document

Contactpersoon: ilonaoudenijhuis@room-to.nl

Inhoudsopgave

1. Aanleiding

1.1 Uitgangssituatie domeinoverstijgend onderzoek

In Nederland is het vertalen van gezondheidsdata naar inzichten en informatie een uitdaging door de wijze waarop de (preventieve) gezondheidszorg georganiseerd is. Zorgwetten zijn verdeeld over diverse domeinen, met een ander uitvoeringsniveau (landelijk of regionaal) en andere verantwoordelijke en/of uitvoerende partijen. Om te komen tot integrale gezondheidsbevordering is het nodig om gegevens op persoonsniveau *over* wetten, organisaties en disciplines heen inzichtelijk te maken. In Nederland wordt op dit moment in verschillende regio's en voor diverse thema's in afzonderlijke onderzoeksprojecten gewerkt aan het domeinoverstijgend bij elkaar brengen van gegevens.

In de Achterhoek is de werkgroep GERDA (GEïntegreerde Regionale Data-infrastructuur Achterhoek) bezig met dit onderwerp vanuit uit een gecombineerde opdracht van de Vereniging Digitale Zorg Achterhoek en 8RHK Gezond. GERDA richt zich op het inrichten van een data-infrastructuur waarmee domeinoverstijgend data bij elkaar gebracht wordt voor primair en secundair gebruik. In een eerder beschreven whitepaper 'Geïntegreerde Regionale Data-infrastructuur Achterhoek' (GERDA) zijn diverse beschikbare technieken voor een geïntegreerde data-infrastructuur onderzocht. Op basis van dit whitepaper is vastgesteld dat voor de regio Achterhoek een gefedereerde data-infrastructuur nodig is (data blijft bij de bron), waarmee beschikbare data op een aggregatieniveau van n=1 (persoonsniveau) verwerkt kan worden en waarmee verticaal onderzoek (het verrijken van gegevens van een patiënt met gegevens van andere (zorg)organisaties) kan worden verricht. Multi-Party Computation (hierna: MPC) is hiervoor een geschikte en veilige techniek. Voor GERDA is besloten om een proof of concept (PoC) uit te voeren naar domeinoverstijgend onderzoek op basis van MPC via het Linksight-platform.

Bij domeinoverstijgend onderzoek komen naast het inrichten van de techniek en het werken aan de gezamenlijke onderzoeksvraag ook heel veel (gezamenlijke) afspraken kijken. Doel van dit whitepaper is om projectleden van andere domeinoverstijgende datawerkplaatsen (op basis van MPC) en andere geïnteresseerden inzicht te geven in governance-gerelateerde vraagstukken en de aanpak hiervan binnen de GERDA PoC. Daarbij is het belangrijk om de hoofdstukken in onderlinge samenhang te zien.

1.2 Aanpak governance vraagstukken

Bij domeinoverstijgend onderzoek op basis van MPC komen meerdere juridische en governance vraagstukken kijken, zoals AVG vereisten, de juridische structuur, benodigde governance en de uitwerking van een DPIA. Om deze vraagstukken in kaart te brengen en uit te werken is een werkgroep governance gestart. De governance werkgroep bestond uit een afvaardiging van specialisten (privacy officers/functionaris gegevensbescherming) van alle betrokken organisaties, twee werkgroepleden vanuit GERDA en één werkgroeplid vanuit de leverancier. Zij werden voor het vraagstuk rondom de juridische structuur bijgestaan door een juridisch expert. De werkgroep had een inhoudelijke trekker

(één van de functionarissen gegevensbescherming) en een procesbegeleider, verantwoordelijk voor voortgang en besluitvorming. In tweewekelijkse werksessies zijn de diverse governance vraagstukken en gewenste aanpak besproken en zijn benodigde (eind)producten ontwikkeld, met als scope 'Acute Zorg Kwetsbare Ouderen in West-Achterhoek' (onderwerp van de PoC). De focus van de werkgroep governance lag voor de PoC op AVG-vereisten, informatiebeveiliging en de juridische governance. Op termijn zullen waarschijnlijk ook andere aspecten van governance uitgewerkt moeten worden, onder andere op het gebied van data governance of onderzoeksgovernance.

De GERDA PoC is uitgevoerd in de periode november 2022 - maart 2023. De inzichten hieruit zijn verwerkt in dit whitepaper, waarbij het whitepaper governance is geschreven vanuit het perspectief van opschaling naar andere organisaties in de regio en nieuwe use cases. In het gehele whitepaper staat de toepassing van decentrale data-analyse op basis van MPC centraal en is gekozen voor terminologie zoals gebruikt binnen het Linksight-platform.

Separaat aan de whitepaper heeft de werkgroep de volgende (eind)producten opgeleverd:
(1) Data Protection Impact Assessment (DPIA)
(2) Beschrijving Governance (technische governance rules en benoemde data stewards)
(3) Gezamenlijke verwerkingsovereenkomst en
(4) voorstel voor de juridische structuur.

1.3 Structuur whitepaper

De whitepaper start met een algemene productuitleg (H2) die achtergrond biedt voor de interpretatie van andere hoofdstukken. Waar in latere hoofdstukken extra technische informatie nodig is over het Linksight-platform, wordt dit uitgelegd in een kader zoals hieronder te zien. Terminologie in de tekst wordt dik gedrukt en de definities hiervan staan H8.

Kader uitleg Linksight-platform
In een kader zoals deze wordt aanvullende uitleg over het Linksight-platform (hierna: product) gegeven, om de uitwerking van de Governance vraagstukken goed te kunnen begrijpen.

Na de algemene productuitleg gaat het whitepaper in op de diverse governance vraagstukken die zijn uitgewerkt: het inzichtelijk maken van benodigde governance rules, rollen & verantwoordelijkheden (H3), AVG vereisten (H4), risico's en maatregelen in een DPIA (H5), juridische structuur & overeenkomsten (H6) en de nog te nemen vervolgstappen (H7).

2. Product uitleg

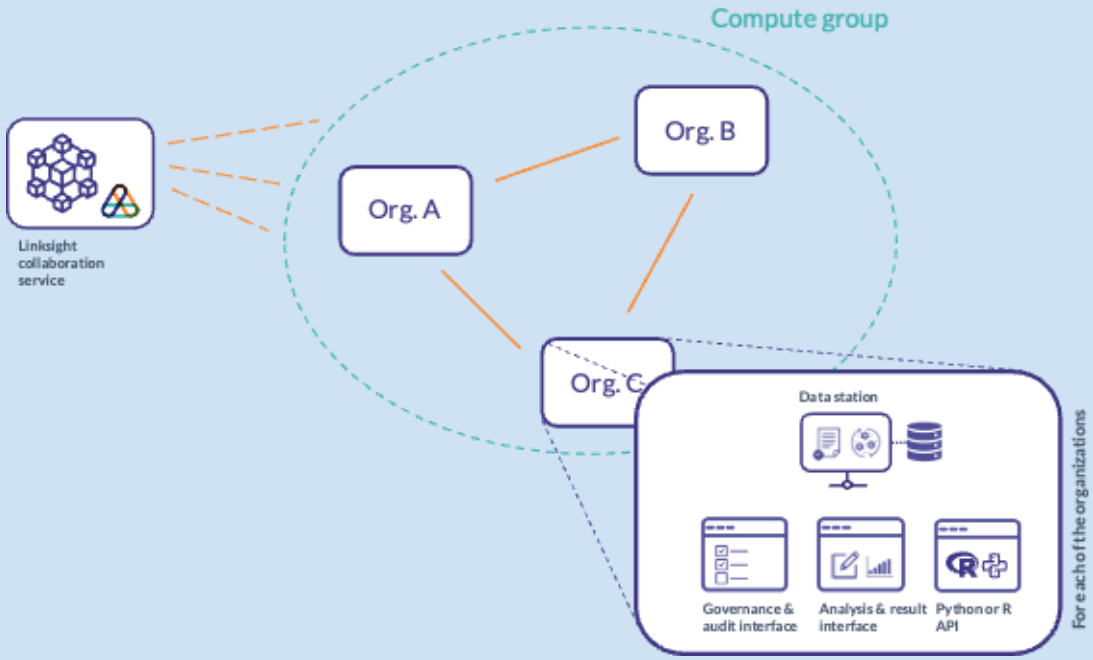
2.1 Datasamenwerking in een MPC-product

In het Linksight-platform krijgt een datasamenwerking invulling. Na het opstellen van een onderzoeksopzet wordt een **compute group** ingericht. Dit is een groep waarin partijen gezamenlijk analyses kunnen doen.

Binnen een compute group heeft elke aangesloten partij een tweetal rollen: **data scientist** en **data steward**. Elke partij wijst deze rollen toe aan één of meerdere personen. De invulling van deze rollen wordt verder beschreven in H3.2 Rollen binnen elke aangesloten organisatie.

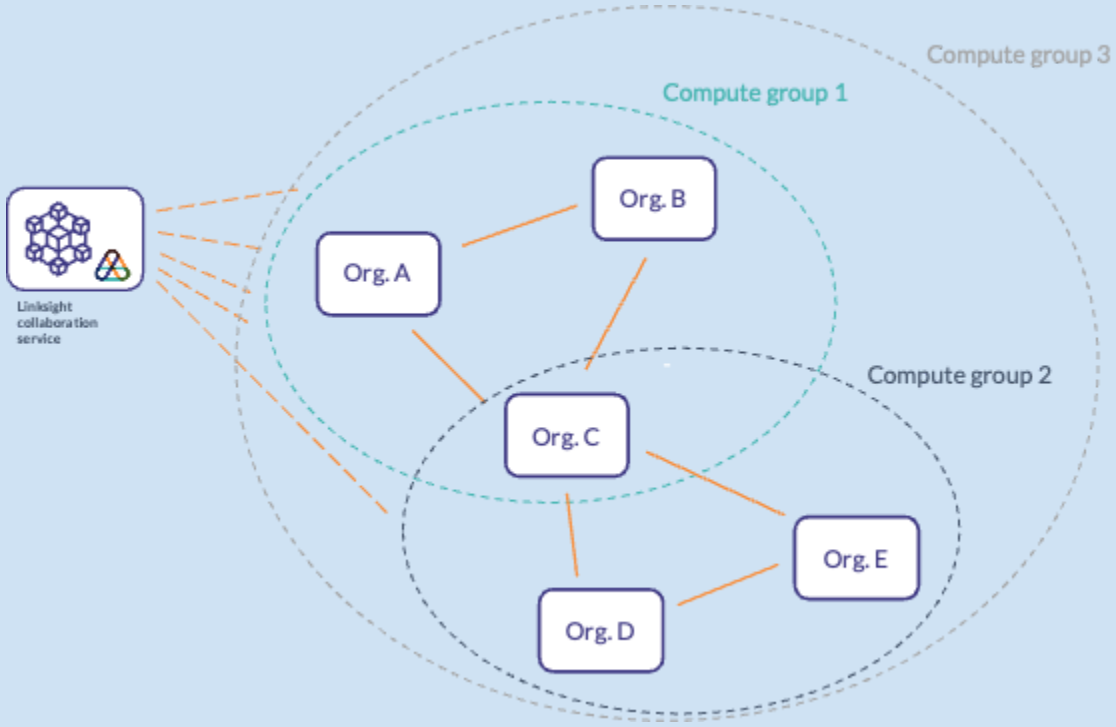
Daarbij wordt per compute group **governance rules** ingeregeld. Dit zijn de regels binnen een compute group over de samenwerking en beschrijven bijvoorbeeld waar elke analysevraag aan moet voldoen. Denk aan de minimale groepsgrootte waarover uitkomsten teruggegeven mogen worden aan de data scientist. De governance rules worden verder beschreven in H3.5 Governance rules.

Binnen een ingerichte compute group kan een data scientist de data analyseren via de analysis & result interface of via Python of R. De datasets blijven binnen de eigen omgeving (**data station**). De data steward kan de data analyse handhaven via de governance & audit interface.



Figuur 1: Versimpelde weergave van de architectuur van het Linksight platform, bestaande uit een compute group met organisatie A, B en C. Elk van de organisaties heeft een datastation en gebruikersinterfaces geïnstalleerd.

Binnen een datasamenwerking kunnen meerdere compute groups ingericht worden. De verwachting is dat voor elke analysevraagstuk een aparte compute group gestart wordt. In onderstaande figuur is een voorbeeld getoond van meerdere compute groups in de datasamenwerking. Per compute group worden datasets gekoppeld en governance rules ingeregeld, zodat alleen de data onderzocht kan worden van het desbetreffende data vraagstuk volgens de opgestelde regels.



Figuur 2: Illustratie van 3 compute groups binnen 1 datasamenwerking in het Linksight platform.

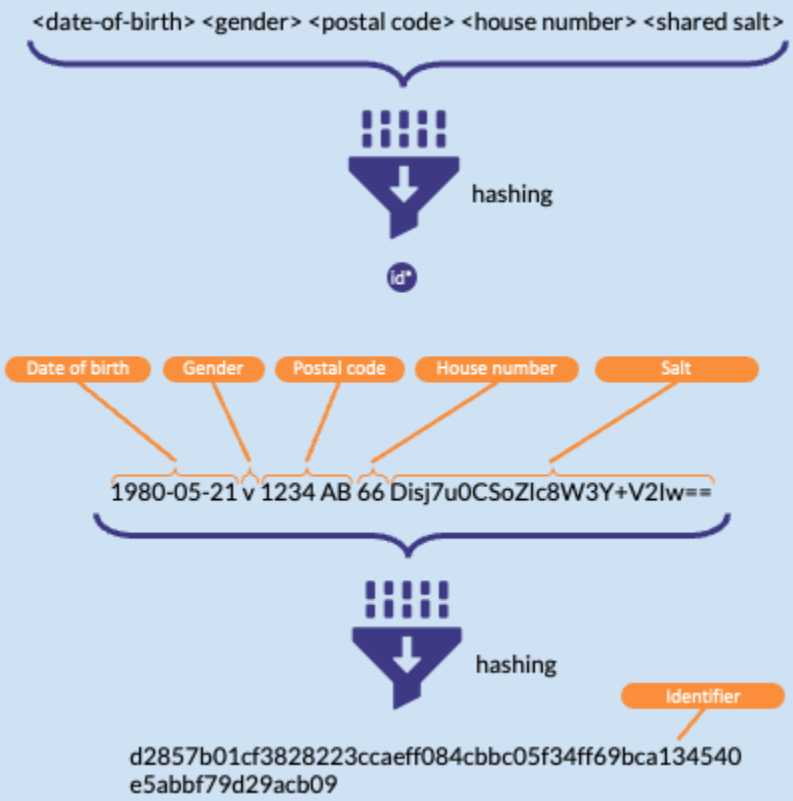
2.2 Gegevensverwerkingen binnen het MPC-product

Voor de invulling van governance rules in H3.5 Governance rules is het zinvol om meer kennis te hebben van de werking en toepassing van governance rules. Kennis van het algehele proces van gegevensverwerking is noodzakelijk voor H5 DPIA. Een verkorte uitleg bevindt zich in deze whitepaper. De gegevensverwerkingen bestaan uit 3 onderdelen; opstellen van een dataset, opstellen & accorderen van governance rules en analyses starten.

2.2.1 Opstellen dataset

Bij het opstellen van een dataset vinden de volgende stappen plaats:

1. Er wordt overeengekomen welke methode gebruik gaat worden om personen uniek te identificeren. Als er geen natuurlijke identifier beschikbaar is, dan kan een identifier gevormd worden bijvoorbeeld op basis van een **(salted) hash** van meerdere attributen, zie figuur 3 voor meer informatie.
2. Er wordt overeengekomen wat de overkoepelende populatie is voor de datasamenwerking.
3. De set van identifiers voor de overkoepelende populatie wordt met elk van de samenwerkingspartijen in de datasamenwerking gedeeld.
4. Elk van de samenwerkingspartijen in de datasamenwerking selecteert de attributen die zij beschikbaar wil stellen in de datasamenwerking, en stelt met behulp van de eerder gedeelde identifiers van de overkoepelende populatie en haar eigen databronnen een dataset samen.
5. Elk van de samenwerkingspartijen stelt de dataset in haar datastation beschikbaar (zie ook figuur 1 voor de versimpelde weergave van de decentrale architectuur).
6. Het datastation van elke samenwerkingspartij hasht de geüploade dataset en deze hash wordt vastgelegd in de auditlog voor de datasamenwerking.



Figuur 3: Illustratie hoe een unieke identifier wordt gemaakt op basis van een verzameling persoonsgegevens (attributen). Om te zorgen dat de persoonsgegevens niet zomaar af te leiden zijn, worden de attributen, in combinatie met een gedeelde 'salt', door een zogenaamde hash-functie gehaald. Dit resulteert nog steeds in unieke identifiers, maar deze zijn niet terug te herleiden tot persoonsgegevens.

2.2.2 Opstellen & accorderen governance rules

Bij het opstellen en accorderen van governance rules vinden de volgende stappen plaats:

7. De samenwerkingspartijen stemmen onderling af welke governance rules van toepassing zijn in deze data samenwerking. Dit kunnen governance rules op diverse gebieden zijn en hoeven niet allemaal technisch van aard te zijn.
8. Een van de samenwerkingspartijen stelt in de governance interface de juiste data-governance rules in die technisch wordt afgedwongen.
9. De andere samenwerkingspartijen stemmen op de voorgestelde governance rules. De stemming wordt per partij vastgelegd in het auditlog.
10. Wanneer alle samenwerkingspartijen hebben ingestemd met de data-governance rules, wordt de nieuwe set aan regels actief, dit moment wordt ook vastgelegd in de auditlog. Zolang er geen unaniem besluit is over een nieuwe regelset, blijven analyses uitgevoerd worden volgens de oude regelset. Er kunnen geen analyses worden uitgevoerd als er geen regelset actief is.

2.2.3 Analyses starten

Wanneer de data governance correct ingesteld en geaccordeerd is door alle samenwerkingspartijen, kunnen partijen analyseverzoeken opstellen en insturen.

11. Een datascientist van een samenwerkingspartij stelt een analyseverzoek op in de analyse interface, en stuurt deze naar een datastation.
12. Het datastation verifieert of het binnenkomende analyseverzoek toegestaan is. Dit gebeurt op basis van de overeengekomen governance regels binnen de datasamenwerking. Analyseverzoeken die hier niet aan voldoen, worden onmiddellijk afgebroken.
13. Het datastation stuurt het analyseverzoek door naar de andere datastations in de datasamenwerking, en deze datastations voeren ook de verificatie uit beschreven in de vorige stap.
14. Als alle datastations het analyseverzoek hebben goedgekeurd, beginnen de datastations het protocol voor het gezamenlijk berekenen van het antwoord op het verzoek.
15. Gedurende het MPC protocol wisselen de datastations in meerdere stappen berichten uit. In deze berichten staan alleen versleutelde gegevens. Uit deze versleutelde gegevens is niets af te leiden.
16. Als er een (tussen)resultaat ontsleuteld moet worden, dan kan dat alleen als alle datastations samenwerken, wat alleen gebeurt als alle datastations aangeven dat nog aan de afgesproken regels wordt voldaan (zie ook volgende punt). Afhankelijk van de afgesproken regels wordt het (tussen)resultaat bij een aangewezen datastation ontsleuteld of bij alle datastations.
17. Gedurende het MPC protocol worden er door de datastations van de samenwerkingspartijen de in de governance rules afgesproken outputcontroles uitgevoerd op de ontsleutelde (tussen)resultaten.
18. Wanneer het protocol is afgerond en aan alle governance rules is voldaan, wordt het resultaat beschikbaar gesteld aan de (analyse interface) van de samenwerkingspartijen die deze volgens de afgesproken governance regels mogen inzien.

3. Governance

3.1 Samenwerking in het datasamenwerkingsverband

Voor GERDA is gekozen voor een constructie waarin de Vereniging Digitalisering Zorg Achterhoek de datasamenwerking binnen de GERDA-datawerkplaats faciliteert. In die hoedanigheid is de Vereniging Digitale Zorg Achterhoek contractant van het Linksight-platform. Ook speelt de Vereniging een rol bij het ophalen, formuleren en prioriteren van domeinoverstijgende onderzoeksvragen, het aanmaken van de benodigde compute groups, het opstellen van governance rules en het uitvoeren van data analyses. Een deel van deze activiteiten kan uitbesteed worden, bijvoorbeeld op het gebied van het uitvoeren van de data analyses. Het verdient de aanbeveling om deze rol te (blijven) evalueren en waar nodig anders in te vullen naar behoefte.

Voor de proof of concept is voor GERDA een eerste gezamenlijke compute group 'Acute Zorg' ingericht, met daarin alle organisaties die deelnemen aan de PoC. Richting de toekomst is het idee dat voor nieuwe domeinoverstijgende onderzoeksvragen deelnemende organisaties zelf nieuwe compute groups inrichten. Binnen een compute group is standaard elke organisatie die deelneemt aan de datasamenwerking inzicht-vrager en toegang-verstrekker. Hierop zijn uitzonderingen mogelijk. Bijvoorbeeld als een partij wel data levert (toegang-verstrekker), maar geen inzichten mag opvragen (inzicht-vrager). Iedere organisatie kent binnen de compute group twee rollen toe voor hun organisatie: data scientist en data steward. Deze rollen zullen verder beschreven worden in sectie 3.2.

De deelnemende partijen worden geadviseerd om met personen die toegang hebben tot de servers waar het Linksight platform op draait (en waar onversleutelde data op staat) afspraken te maken over geheimhouding. Elke organisatie uit de datasamenwerking geeft hieraan individueel invulling, passend binnen de kaders van de eigen organisatie. Linksight heeft als ontwerpprincipe geen toegang tot de data en derhalve geen verwerkingsverantwoordelijke of verwerker is (zie ook paragraaf 4.3.1). Wel heeft zij een rol in het faciliteren van het technische governance-netwerk.

3.2 Rollen binnen elke aangesloten organisatie

Om binnen een datasamenwerking goed samen te kunnen werken met het Linksight platform moeten per deelnemende organisatie twee rollen ingevuld worden, die van data scientist en data steward. Iedere aangesloten partij besluit zelf in hoeverre de personen die deze rollen invullen zelfstandig mogen acteren of waar (op onderdelen) andere personen te consulteren of informeren.

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 datasteward 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.

Een rol als data steward was voorafgaand aan het proof of concept nog niet ingevuld in de regio. Om deze rol invulling te kunnen geven, is deze rol verder uitgewerkt in bijgevoegd document[1].

Activiteiten op het Linksight platform - governance & audit interface:

- Aanmaken van een nieuwe compute group
- Invoeren van de governance rules
- Besluiten over nieuw voorgestelde governance rules
- Koppelen van beschikbare dataset aan compute group
- Bepalen wie toegang heeft tot de analyse-interface (eigen data scientists)
- Optioneel: nieuwe organisaties uitnodigen

Kader context:
Datastewardship is een relatief nieuw beroep, ontstaan om onderzoekers te ondersteunen bij het omgaan met data voor, tijdens en na een onderzoeksproject. Datastewards worden opgeleid om data zo FAIR (Findable, Accessible, Interoperable, Reusable) mogelijk te maken en te adviseren over datadeling. Met de ondersteuning van data stewards worden data duurzamer en blijven ze waardevol na afloop van een onderzoeksproject.

De groei in dit functieprofiel wordt verder ondersteund met de Health-RI Data Stewardship community, met als doel om datastewardship versneld te implementeren, ervaringen te delen en krachten te bundelen om problemen aan te pakken.

Voor meer informatie:
https://www.health-ri.nl/about-health-ri/organisation/fair-data/health-ri-data-stewardship-community

Data Scientist

De data scientist is de "speler" die inzichten uit data haalt, binnen de door de data steward opgestelde "spelregels". Als een analyse niet past binnen de "spelregels" wordt deze door het Linksight platform gedetecteerd en wordt de analyse niet uitgevoerd.

Let op! De door ons gebruikte definitie van een data scientist is breder dan gemiddeld. In dit geval is de data scientist elke beoogde gebruiker van de datawerkplaats (BI, beleidsmaker of modelontwikkelaar).

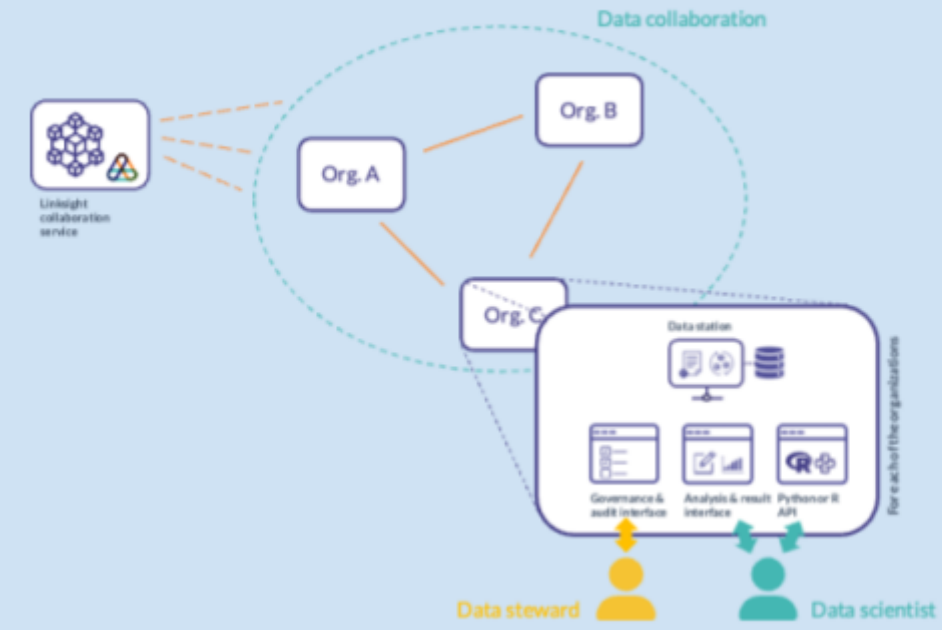
Activiteiten op het Linksight platform - analysis & result interface:

- Een analyse starten en uitvoeren via R of Python-package of analysis & result interface
- Metadata beschrijvingen raadplegen via de analyse interface

[1] Rolbeschrijving_DataSteward

- Geldende governance rules raadplegen in de analyse interface

Kader Product uitleg:
In het Linksight platform ziet deze rolverdeling er als volgt uit:



Figuur 4: Data scientist en data steward geplot op het Linksight platform

3.3 Samenwerking tussen de rollen

Voor de GERDA-PoC werden de rollen data steward en data scientist geïntroduceerd bij en ingevuld door alle betrokken organisaties. Omdat het gaat om nieuwe functies met nieuwe taken, is het van belang bij de introductie van de rollen de bevoegdheden en verantwoordelijkheden helder te hebben. Ook is het relevant om de samenhang van de rol van data steward en data scientist met andere rollen binnen of buiten de organisaties te beschrijven. Vraagstukken die hierbij spelen zijn onder andere in hoeverre een data steward zelfstandig mag handelen en de mate waarin de data steward vooral zorg draagt voor het Linksight-platform of een meer algemene, brede verantwoordelijkheid heeft rondom datakwaliteit.

Opgedane inzichten zijn uitgewerkt in een verantwoordelijkheidsmatrix (RACI) voor de werkzaamheden die plaatsvinden binnen een datasamenwerking. Daarnaast zijn rolbeschrijvingen gemaakt (voor wat betreft verantwoordelijkheden en competenties) voor de rol van data steward en data scientist.

Werkzaamheden	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

Verantwoordelijkheden data steward

- Zorgdragen dat compute groups inclusief governance rules worden gebruikt volgens wet en regelgeving en interne regels.
- Monitoren van naleving van governance rules.
- Zorgdragen dat actuele databeschrijvingen aanwezig zijn
- Aankaarten van vraagstukken rondom de datakwaliteit van de eigen organisatie.

Competenties data steward

- Als liaison tussen IT, business (inzichtvrager) en legal/compliance is hij/zij communicatief vaardig richting verschillende type medewerkers.
- Zowel kennis van relevante wet- en regelgeving, als de organisatiespecifieke & regionale afspraken.
- Hij/zij weet technische rapportages te lezen en vertalen, maar kan ook meedenken met eindgebruikers.

Verantwoordelijkheden data scientist

- Uitvoeren van data bewerking, analyse, modellering, communicatie met inzicht-vrager en visualisatie van inzichten en voorspellingen in informatieproducten.
- Correct uitoefenen van onderzoeksprotocol en procedures, als ethisch en integer te werk te gaan.
- Geheimhouding in acht nemen rondom de opgedane inzichten.

Competenties data scientist

- Heeft kennis van statistiek en het opzetten van onderzoek , waarvan de mate van kennis afhankelijk is van het analysevraagstuk & methodiek conform onderzoeksopzet.
- Kan analyses uitvoeren middels R of Python-package of in de analysis & result interface.

3.4 Invulling van de rollen

Voor wat betreft de rol van data scientist zijn binnen iedere deelnemende organisatie de benodigde competenties aanwezig om inzichten te creëren gericht op basisstatistiek. Er zijn binnen de organisaties grote verschillen in de hoeveelheid (beschikbare) analysecapaciteit. Een goede invulling van de rol data scientist binnen de organisaties in een datasamenwerking lijkt daarmee vooral een prioriteits- en capaciteitsvraagstuk.

De rol van data steward bestond binnen de organisaties die deelnamen aan de PoC nog niet. Om de rol goed te kunnen introduceren en beleggen bij de deelnemers was het daarom essentieel deze rol nader af te stemmen en te beschrijven binnen de werkgroep Governance. Daarna hebben de werkgroepleden de invulling van deze rol vanuit de eigen organisatie bespreekbaar gemaakt en een voorstel gedaan voor invulling. Hieruit ontstond een gevarieerde groep van medewerkers, met als gemene deler een

focus op (methodologisch) onderzoek en BI/Analytics, al dan niet in nadrukkelijke samenwerking met de functionaris gegevensbescherming.

De data stewards en data scientists hebben tijdens een gezamenlijke sessie een zogenaamde ‘playground’ voor Acute Zorg ingericht. Daarbij is ieder vanuit zijn eigen rol ingelogd (data steward of data scientist), hebben ze gezamenlijk een compute group opgestart, (fake) data ingeladen en de (concept) governance rules opgesteld en ingeregeld.

3.5 Governance rules

Belangrijk onderdeel van een compute group is dat er ‘spelregels’ zijn waaraan een data-analyse moet voldoen. Deze governance rules worden door de data stewards onderling afgesproken en ingesteld in het Linksight platform. Denk bijvoorbeeld aan de minimale groepsgrootte waarover uitkomsten teruggegeven mogen worden aan de data scientist. Omdat het technisch inregelen van goverance rules nieuw is binnen de regio wordt in de paragraaf hieronder wat meer toelichting gegeven.

3.5.1 Algemene governance rules

De werkgroep Governance kiest er richting de toekomst voor om de invulling van governance rules over te laten aan de data stewards. Per compute group kunnen de data stewards onderling bepalen welke voorwaarden zij stellen aan de data-analyses. Alle data stewards moeten de voorgestelde governance rules accepteren, voordat een (nieuwe) compute group actief wordt.

Bij elke compute group kan uit onderstaande governance rules gekozen worden:

1. Toegestane analyse - De analysemethode {{analysemethode}} is toegestaan in deze compute group
2. Regelset vervaldatum - Deze regelset is geldig tot {{datum}}, daarna moet het opnieuw door alle partijen bevestigd worden.
3. Analyses starten - Partijen die de analyses mogen starten: {{partijen}}
4. Grootte anonimiteitsset - Het aantal items in de resultaatset van de analyse moet minstens {{n}} zijn.
5. Attribuut in query-select - Het attribuut {{attr}} mag niet als selectiecriterium gebruikt worden
6. Attribuut in query-where - Het attribuut {{attr}} mag niet als filtercriterium gebruikt worden
7. Attribuut in query-group-by - Het attribuut {{attr}} mag niet als group-by criterium gebruikt worden
8. Minimum genormaliseerde std dev - Wanneer gerekend wordt met attribuut {{attr}}, moet de genormaliseerde standaarddeviatie minstens {{minimum}} zijn.

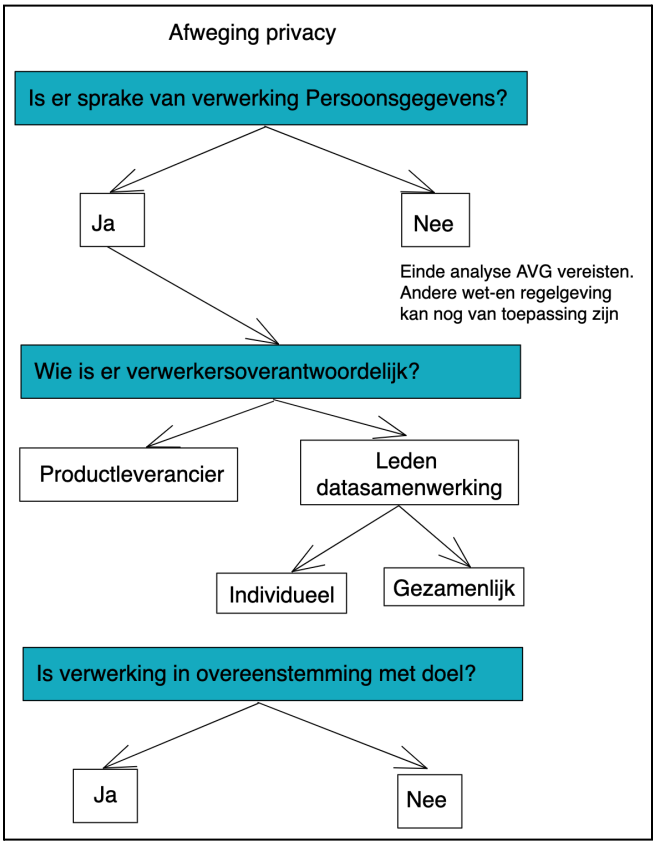
4. AVG Vereisten

4.1 Raamwerk voor afwegingen over privacy

Bij het verwerken van persoonsgegevens is de AVG van toepassing. Vanuit deze wet zijn er meerdere vereisten beschreven. Om vorm te geven aan de AVG vereisten in relatie tot de GERDA-PoC zijn de volgende aspecten bekeken:

a) Vaststellen van de toepasselijkheid van de AVG
b) Bepalen verwerkingsverantwoordelijkheid/heden voor
    i) Leden van de datasamenwerking individueel/gezamenlijk;
    ii) Linksight als productleverancier
c) Beoordelen doelmatigheid van de verwerking van bijzondere persoonsgegevens voor de deelnemende (zorg)organisaties

Visueel ziet het gehanteerde raamwerk er uit zoals in figuur 5.



Figuur 5: Raamwerk voor afwegingen over privacy

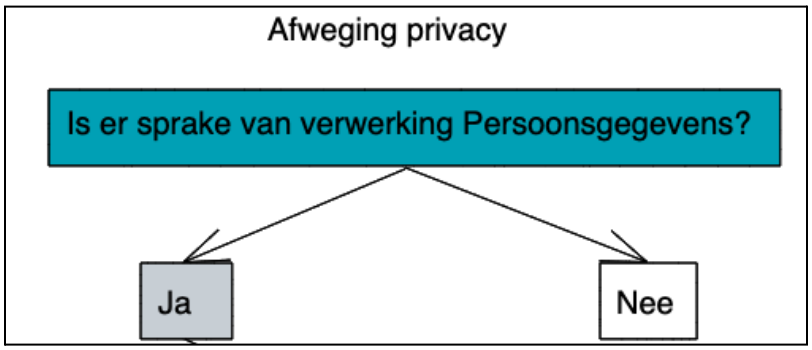
De verschillende aspecten uit het raamwerk worden in de volgende paragrafen verder beschreven en uitgewerkt. Hiervoor gebruikte de werkgroep governance onder andere documenten die door Linksight (leverancier) beschikbaar zijn gesteld.

De beschikbaar gestelde documenten waren:

- 11-09-2022 - *Hooghiemstra* - Herbeoordeling-Linksight-Platform
- 13-10-2021 - *Moerel & Hooghiemstra* - Linksight-Juridisch-Advies
- 30-03-2022 - *ICTRecht* - Linksight - Advies rolverdeling AVG

4.2 Vaststellen toepasselijkheid AVG

Om te bepalen of de AVG van toepassing is, moet vastgesteld worden of persoonsgegevens verwerkt worden.

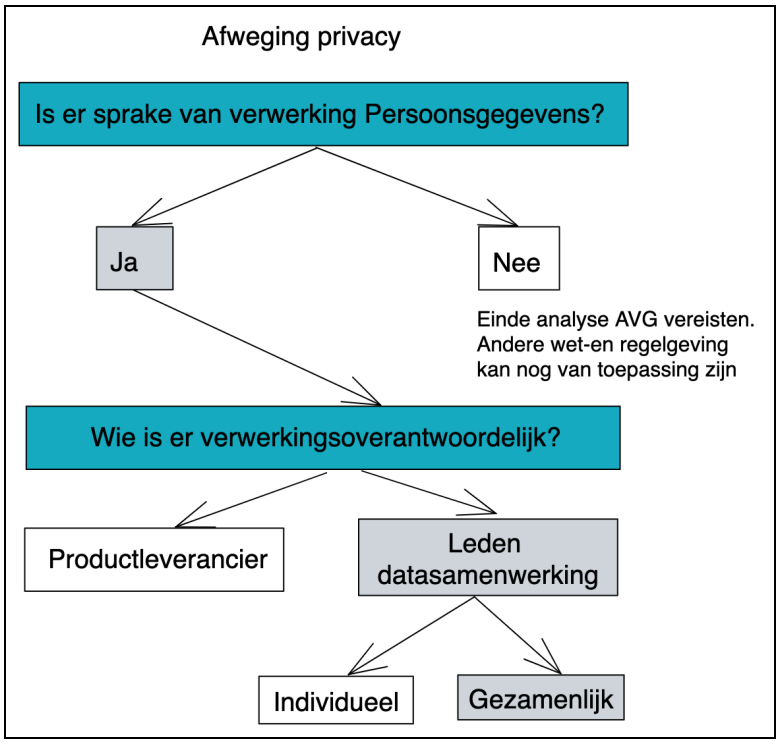


Figuur 6: Onderdeel raamwerk voor de toepasselijkheid van de AVG

In lijn met Moerel & Hooghiemstra concludeert de werkgroep, dat de AVG van toepassing is, omdat bij de verwerking persoonsgegevens gebruikt worden. Dat persoonsgegevens gepseudonimiseerd zijn doet hier niets aan af. In de context van de GERDA-PoC is er sprake van bijzondere persoonsgegevens.

4.3 Bepalen verwerkingsverantwoordelijkhe(i)d(en)

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 7: Onderdeel raamwerk voor het bepalen van de verwerkingsverantwoordelijkheden

4.3.1 Is Linksight aan 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. Hooghiemstra heeft op verzoek van Linksight hun platform beoordeeld. Hieruit blijkt 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. De werkgroep Governance concludeert na een aanvullende uitleg over de werking van het Linksight platform en een controle op dat persoonsgegevens niet gedeeld worden met de leverancier dat de productleverancier geen verwerker is over.

Kader Product uitleg
De diensten die bij Linksight draaien faciliteren enkel de datasamenwerkingen: coördinatie tussen datastations, het technisch vastleggen van governance rules en het ondersteunen van de auditlog. Het Linksight platform ontvangt daarbij geen persoonsgegevens.

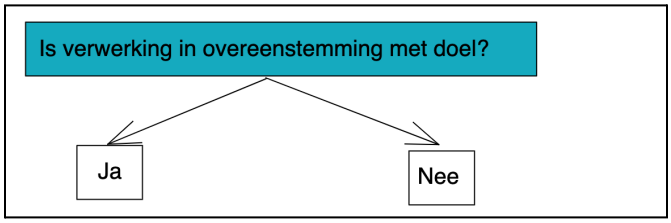
4.3.2 Zijn de deelnemende leden van de datasamenwerking gezamenlijk verantwoordelijk?

Om te bepalen of de deelnemende organisaties individueel of gezamenlijk verantwoordelijk zijn heeft de werkgroep Governance het rapport van Moerel & Hooghiemstra als bron gebruikt. Conclusie op basis van dit stuk en verdere duiding door de werkgroep Governance wordt geconcludeerd dat voor de

GERDA-PoC de (zorg)organisaties gezamenlijk verwerkingsverantwoordelijk zijn, omdat zowel de data als de doelen waarvoor de verwerking plaatsvindt in gezamenlijkheid worden bepaald. [2] Gezamenlijke verantwoordelijkheid start op het moment dat de zorgorganisaties contractueel deelnemen aan een GERDA-datasamenwerking. De data-uitwisseling start als het Linksight platform is geïnstalleerd en de organisatie deelneemt aan één of meerdere compute groups. De individuele organisaties zijn en blijven verantwoordelijk voor hun eigen data.

4.4 Is de verwerking van persoonsgegevens in overeenstemming met het doel?

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 8: 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.

Het is mogelijk dat voor het doel van de domeinoverstijgende onderzoeksvraag een andere grondslag van toepassing is dan voor het oorspronkelijke doel van vastlegging. De grondslag kan daarnaast per deelnemende partij verschillen.

In het Linksight-platform kunnen verschillende soorten verwerkingen uitgevoerd worden. In sommige gevallen is er sprake van wetenschappelijk onderzoek. Echter, uit de analyse van beoogde gebruikers whitepaper 'Regionale Datawerkplaats - Een samenvatting van de wensen van potentiële gebruikers van een regionale datawerkplaats' blijkt dat de meeste gebruikers in de datawerkplaats vanuit beleidsmakers (in het whitepaper inzicht-vragers) vragen ontvangen om de procesuitvoering

[2] Er kan al sprake zijn van een gezamenlijke verwerkingsverantwoordelijkheid indien gezamenlijk het doel van en de middelen van de verwerkingen worden bepaald. In het document "*Richtsnoeren 07/2020 over de begrippen "verwerkingsverantwoordelijke" en "verwerker*" " van de EDPB *staat o.a. het volgen*de: "Een belangrijk criterium is dat de verwerking niet mogelijk zou zijn zonder de deelname van beide partijen".

domein-overstijgend te verbeteren. Dat blijkt ook uit de gekozen onderzoeksopzet voor het proof of concept, waar de analyse zich richt op de acute zorgketen bij de doelgroep ouderen. De werkgroep Governance komt daarom tot het oordeel dat de grondslag 'uitvoering van een overeenkomst' het best passend is.

4.4.1 Rechtsgrond

Voor de verwerking van de persoonsgegevens baseren de deelnemende partijen zich op de grondslag dat de verwerking valt onder het uitvoeren van een (zorg)overeenkomst. Partijen verlenen zorg en zijn wettelijk verplicht dat goed te doen. Daarnaast hebben de organisaties processen ingericht om de kwaliteit van zorg te monitoren en te verbeteren. Deze datasamenwerking stelt de (zorg)organisaties in staat om -op basis van de resultaten- de zorg voor subgroepen zorgvragers en (daardoor) ook van individuen te verbeteren.

Indien er andere use cases ontstaan kan het zijn dat een andere grondslag (meer) van toepassing is. Bij nieuwe use cases wordt het DPIA bijgewerkt en zal beoordeeld worden of een andere grondslag (meer) van toepassing is. Dit wordt ook getoetst wanneer de datasamenwerking uitgebreid wordt met nieuwe organisaties.

4.4.2 Doelbinding

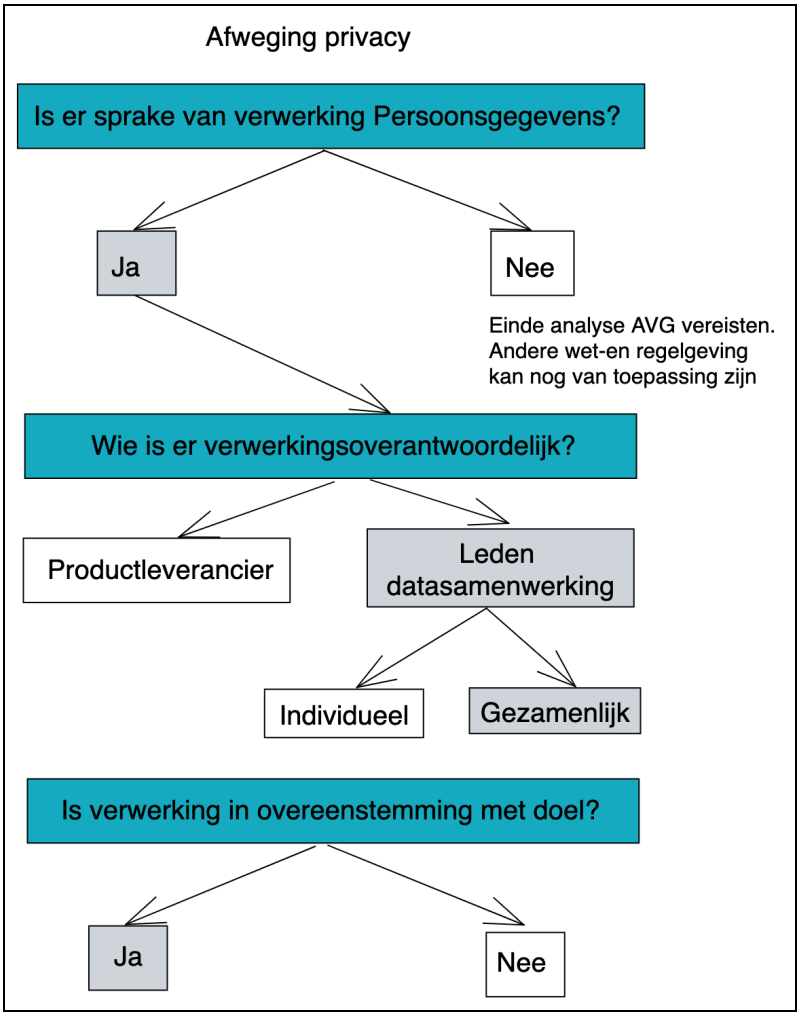
Doelbinding vereist dat de dataverwerking volgens de regels voor de geselecteerde grondslag wordt toegepast. Het doel wordt vastgelegd, zodat data niet zonder meer hergebruikt mag worden voor andere doeleinden.

In de AVG wordt de rechtsgrond 'uitvoeren van een (zorg)overeenkomst; geduid als: preventieve geneeskunde, medische diagnosen, het verstrekken van gezondheidszorg of behandelingen of uit hoofde van een overeenkomst met een gezondheidswerker.

Voor de GERDA-PoC is bovengenoemde doeleinde van toepassing op de gekozen onderzoeksopzet. Als nieuwe onderzoeksvragen opgepakt worden en/of nieuwe compute groups ingericht worden moet goed gekeken worden of het doel van de onderzoeksvraag aansluit bij het huidige (voor de GERDA-PoC beschreven) doel. Deze controle vindt zoals in de paragraaf hierboven beschreven plaats door middel van het nalopen en waar nodig bijwerken van de DPIA.

4.5 Conclusie AVG

De werkgroep Governance is voor wat betreft de vereisten vanuit de AVG van mening dat in de GERDA-PoC (1) de AVG van toepassing is, (2) de leverancier geen verwerker is, (3) de betrokken partijen gezamenlijk verwerkingsverantwoordelijk zijn en (4) de grondslag 'uitvoering van een overeenkomst' het best passend is. Visueel ziet deze uitwerking er als volgt uit:



Figuur 9: Uitwerking van het raamwerk afwegingen over privacy voor de proof of concept GERDA

5. DPIA

5.1 Aanpak

Om privacy risico's van de gegevensverwerking in de datasamenwerking te beoordelen en passende beheersmaatregelen te bepalen is een Data Protection Impact Assessment (DPIA) uitgevoerd. In de uitwerking van de DPIA is de reikwijdte de GERDA-PoC, gericht op de use case Acute Zorg Kwetsbare Ouderen West-Achterhoek. Voor de DPIA is de onderzoeksopzet van de use case verder uitgewerkt door de werkgroep 'Zorginhoud'.

Als startpunt is een template DPIA vanuit Linksight gebruikt. In deze template zijn de dataverwerking in het platform en de risico's en beheersmaatregelen al uitgewerkt. De template DPIA is doorgenomen door de functionarissen gegevensbescherming van de aan de GERDA-PoC deelnemende organisaties. Zij hebben samen gekeken naar de inhoud en naar de impact van verschillende risico's en de beheersmaatregelen die genomen dienen te worden.

De werkgroep heeft vervolgens de specifieke onderzoeksopzet van de GERDA-PoC en de conclusies van de werkgroep Governance voor wat betreft de AVG vereisten toegevoegd aan het DPIA. Dit DPIA is geaccordeerd door de werkgroep Governance en vervolgens voorgelegd ter akkoord bij de gezamenlijke verwerkingsverantwoordelijken.

5.2 Actualisatie van het DPIA

Ambitie is om het DPIA bij uitbreidingen van de datasamenwerking te kunnen hergebruiken. Daarom is met de functionarissen gegevensbescherming besproken wanneer het DPIA geactualiseerd zou moeten worden. Hoewel geen harde eis, gelden onderstaande uitgangspunten als algemene richtlijn.

1. Bestaande datasamenwerking - bestaande compute group - uitbreiding datasets
    a. Het DPIA hoeft in principe niet aangepast te worden. (Let op: belangrijk hierbij is dat de uitbreiding aansluit bij het geformuleerde onderzoeksdoel van de compute group)
2. Bestaande datasamenwerking - nieuwe compute group
    a. Het DPIA moet geactualiseerd worden
3. Nieuwe datasamenwerking of uitbreiding datasamenwerking met nieuwe partijen
    - Het DPIA moet bijgewerkt worden (net als de samenwerkingsovereenkomst en de gezamenlijke verwerkersovereenkomst)

5.3 Risico's en maatregelen

Elke verwerking van persoonsgegevens brengt risico's met zich mee. Decentrale data-analyse via MPC beperkt dit risico ten opzichte van oplossingen met een centrale data-opslag. Zie voor meer informatie: gelinked whitepaper van TNO.

Het gebruik van het Linksight platform draagt bij aan het voldoen aan de vereisten rondom dataminimalisatie en privacy-by-design. Daarnaast draagt het platform technisch bij aan doelbinding door het (technisch) vastleggen van afspraken tussen organisaties over welke data-analyses plaats mogen vinden. De analyses worden met behulp van een privacy-by-design oplossing (MPC) uitgevoerd om de persoonsgegevens van de betrokkenen adequaat te beschermen. In het DPIA zijn de risico's van de gegevensverwerking voor de GERDA-PoC beschreven en gewogen. Maatregelen zijn benoemd om eventuele risico's te mitigeren naar een acceptabel niveau.

5.3.1 Risico's

De vastgestelde risico's zijn te lezen in het DPIA. In dit whitepaper zijn de drie risico's opgenomen met een gemiddeld tot hoog risico;

A. Risico's als gevolg van een datalek, zoals identiteitsfraude of -diefstal, reputatieschade, verlies van vertrouwelijkheid van persoonsgegevens, die worden beschermd door een beroepsmatige geheimhoudingsplicht.
B. Risico dat rechten van betrokkenen worden ingeperkt of onvoldoende uitgeoefend kunnen worden, bijvoorbeeld doordat betrokkenen onvoldoende worden geïnformeerd of door de gezamenlijke verwerking.
C. Risico op oneigenlijk gebruik van gevoelige persoonsgegevens.

5.3.2 Maatregelen

Onderstaand zijn de maatregelen beschreven om de belangrijkste risico's uit bovenstaande paragraaf te mitigeren. Dit zijn niet de enige maatregelen die zijn genomen. Een overzicht van alle maatregelen is opgenomen in het DPIA.

A. Maatregelen 'risico op een datalek'

Het risico op een datalek wordt beperkt door gebruik te maken van MPC-technologie, aangevuld met diverse technische en niet-technische maatregelen. Deze technische en organisatorische maatregelen staat hieronder kort beschreven.

De belangrijkste technische maatregelen om het risico om datalek te verkleinen zijn:

- Aggregatie naar categorie voor sommige gevoelige attributen
- Onveranderbare auditlog, waarin governance rules zijn vastgelegd
- Diverse controles van het analyseverzoek:
    - Voldoet het analyseverzoek aan de governance rules
    - Voldoet het resultaat van het analyseverzoek aan de governance rules
    - Logging van alle (correcte/gestopte/niet toegestane) analyseverzoeken

- Inzet van MPC en homomorfe encryptie om te rekenen met versleutelde data. Versleuteling van de data-uitwisseling.

Kader Product uitleg:

Het Linksight platform bevat een verzameling technische beveiligingsmaatregelen om de vertrouwelijkheid en integriteit van de gebruikte gegevens te waarborgen. Dit zijn onder andere:

- Rekenen met vercijferde gegevens (MPC)
- Industrie-standaard vercijferde TLS verbindingen met mutual authentication
- Gebruikers-authenticatie
- Onveranderbare auditlog
- Autorisatie-checks voor analyses o.b.v. governance rules
- Geautomatiseerd output controle o.b.v. governance rules

Organisatorische maatregelen:

- Opstellen van een gezamenlijke verwerkersovereenkomst en samenwerkingsovereenkomst.
- Rolscheiding data scientist en data steward.
- Risico bestaat dat zonder heldere afspraken voorafgaand, data onbedoeld voor andere toepassingen wordt ingezet. In deze samenwerking wordt dit risico voorkomen door gebruik te maken van een combinatie van organisatorische en technische governance rules.
- Samenwerkingspartijen hebben een ethisch beleidsdocument opgesteld, waarin expliciet is afgesproken dat uitkomsten van de data-analyse niet gebruikt wordt voor ongewenste profilering en/of geautomatiseerde besluitvorming en/of beleidsformulering waarin mensen worden uitgesloten. Dit is beschreven in het ethisch beleidsdocument.

B. Maatregelen ‘rechten van betrokkenen’

Rechten van betrokkenen blijven binnen de datasamenwerking onverkort van kracht. Alle deelnemende organisaties zijn zelf verantwoordelijk voor een goede uitoefening van de rechten van hun klanten en de communicatie hierover. Het recht op uitsluiting sluit aan bij de privacy statements van de organisatie.

Organisatorische maatregelen:

- Datascientists hebben via het Linksight platform geen toegang tot de directe brondata van de eigen organisatie of van andere deelnemende organisaties.
- Organisaties informeren via hun privacy statements betrokkenen over de verwerking van hun data voor het gekozen doeleinde binnen de datasamenwerking. Ook wordt de compute group toegevoegd aan het verwerkingsregister.
- Deelnemende organisaties in de datasamenwerking hebben in de ‘Overeenkomst gezamenlijke verwerkingsverantwoordelijken’ afspraken gemaakt over het informeren van betrokkenen en de mogelijkheid om de overige AVG rechten uit te oefenen bij de samenwerkende partijen.

C. Maatregel ‘oneigenlijk gebruik van gevoelige persoonsgegevens’

Het oneigenlijk gebruik maken van gevoelige persoonsgegevens kent diverse oorzaken, waaronder het ontbreken van een grondslag voor de verwerking, het gebruiken van meer persoonsgegevens dan nodig, het gebruiken van persoonsgegevens voor andere doeleinden dan waarvoor ze vastgelegd zijn

en het te lang verwerken van persoonsgegevens (niet tijdig vernietigen). Daarom zijn binnen de datasamenwerking op meerdere aspecten maatregelen genomen.

Grondslag
Voor de verwerking van de persoonsgegevens hanteren de samenwerkingspartijen als grondslag dat de verwerking valt onder het uitvoeren van een (zorg)overeenkomst zoals beschreven in onderdeel 3.4.1 van deze whitepaper.

Toegang en autorisatie
Er zijn diverse maatregelen genomen om te zorgen enkel bevoegde medewerkers toegang hebben tot persoonsgegevens. Zo hebben data scientists van de (zorg)organisaties binnen de GERDA-PoC via het Linksight platform geen toegang tot de directe brondata van de eigen partij of die van andere partijen. Daarnaast kunnen alleen bevoegde medewerkers (de data stewards) de technisch afdwingbare data-governance rules beoordelen en accorderen.

Gezamenlijke verwerkingsverantwoordelijkheid
De respectievelijk verantwoordelijkheden zijn in een 'Overeenkomst voor gezamenlijke verwerkingsverantwoordelijken' vastgelegd (Art. 26 AVG). De partij hebben hierin contractueel en organisatorisch geborgd, dat de resultaten van de analyses uitsluitend worden gebruikt ten behoeve goede zorgverlening.

5.3.3 Voorafgaande raadpleging

Door toepassing van de voorgestelde maatregelen is er geen sprake van een hoog risico voor de rechten en vrijheden van betrokkenen, in het bijzonder het recht op de bescherming van de persoonlijke levenssfeer en het recht op gegevensbescherming waardoor voorafgaande raadpleging bij de Autoriteit Persoonsgegevens niet noodzakelijk is.

6. Juridische structuur

Een voorstel voor de juridische structuur is door de - in de werkgroep Governance - aangehaakte jurist geschetst. In dit voorstel zijn twee mogelijke constructies uitgewerkt. Daarbij zijn de uitgangspunten van de samenwerking benoemd en is gekeken naar bestaande samenwerkingsvormen binnen de regio Achterhoek.

6.1 Uitgangspunten & deelnemende partijen

Definitie/doelstelling:
GERDA heeft als doel om voor de samenwerkende partijen een Virtual Research Environment (VRE) te realiseren. Hierbij wordt gebruikgemaakt van Multi-Party Computation (MPC).

Uitgangspunten:

1. De doelstelling van de VRE is om de samenwerkende partijen in staat te stellen om, met inachtneming van alle relevante wet- en regelgeving, onderzoek te verrichten in de (zorg)keten aan de hand van de data van de aangesloten samenwerkende partijen.
2. De onderzoeken moeten de kwaliteit van zorg verbeteren.
3. De onderzoeken worden uitgevoerd met behulp van de patiëntgegevens (data) waarover de deelnemende partijen beschikken.
4. Er is geen sprake van de opbouw en/of instandhouding van een, al dan niet gezamenlijk beheerde, database met onderzoeksgegevens. De data zijn en blijven bij de deelnemende partijen.
5. Technisch maakt de VRE gebruik van een externe leverancier, Linksight, die de voor de uitwisseling te gebruiken techniek inbrengt.
6. De samenwerking dient flexibel en schaalbaar te zijn. Dat wil zeggen dat partijen - onder voorwaarden - moeten kunnen toetreden (of uittreden).

Deelnemende partijen:
Vereniging Digitalisering Zorg Achterhoek: vereniging die data-uitwisseling tussen regionale zorgaanbieders ten behoeve van de uitvoering van primaire zorg stimuleert.

8RHK Gezond: is een zogenaamde 'Wettelijk geregelde publiekrechtelijke samenwerking' (Wgr) op regionaal niveau. Er wordt samengewerkt door maatschappelijke organisaties. Vanuit het thema 'De Gezondste Regio' worden initiatieven ontwikkeld om de gezondheid van de burgers binnen het samenwerkingsgebied te verbeteren.

Regionale zorgaanbieders, die bij de start van GERDA de volgende partijen betreffen:

- Sensire (VVT)
- Slingeland Ziekenhuis;

- ZCN-NAAST (aanbieder digitale zorg op afstand);
- Huisartsenzorg Oude IJsselstreek (HZOIJ);
- Marga Klompé (VVT);
- GGD-Noord-Oost Gelderland;

De softwareleverancier: Linksight.

6.2 Mogelijke invullingen & voorstel

De letterlijke vertaling van governance is **bestuur, beheersing en macht of de wijze van besturen**. Governance kan algemeen worden beschreven als 'het uitvoeren van beleid, controle, macht, regels en principes van organisaties'. Een eerste vraag hierbij is of de besturing c.q. de organisatie van de samenwerking op basis van een overeenkomst kan plaatsvinden of moet worden ondergebracht in een entiteit.

Juridische entiteit:
Onderbrenging in een aparte (juridische) entiteit heeft onder meer te maken met het nut en/of de noodzaak van een (van de deelnemende partijen) afgescheiden vermogen, vanwege redenen verband houdend met aansprakelijkheid of commerciële, organisatorische en/of financiële redenen. Een entiteit brengt de nodige formaliteiten en extra kosten met zich mee.
Een juridische entiteit kan een veelheid aan vormen hebben, bijvoorbeeld een BV, stichting, vereniging, Coöperatie, VOF (vennootschap onder firma) of CV (commanditaire vennootschap). Ieder van deze vormen heeft eigen kenmerken en voor- en nadelen.

Samenwerkingsovereenkomst:
Een samenwerkingsovereenkomst is flexibel, goedkoop en eenvoudig(er) qua opzet en inrichting. Wel vraagt een samenwerkingsovereenkomst meer discipline van de deelnemende partijen. Alle activiteiten vinden immers plaats op basis van de samenwerkingsafspraken en vragen daarmee continu medewerking van de deelnemende partijen. Partijen kunnen gemakkelijk toe- en uittreden uit een samenwerkingsverband bij overeenkomst.

Als we beide mogelijkheden naast elkaar zetten, zien we dat een juridische entiteit in vergelijking met een samenwerkingsovereenkomst meer afstemming en administratie vraagt. Ook brengt het oprichten van een juridische entiteit aanvullende kosten met zich mee. Anderzijds biedt een juridische entiteit op het gebied van aansprakelijkheid een betere bescherming. De entiteit is immers de eerste (en vaak ook enige) aan te spreken partij. Daarnaast is de entiteit flexibeler bij een eventuele uitrol/marktbenadering van een product dat door de samenwerking wordt ontwikkeld. Toe- en uittreden is lastiger en brengt meer formaliteiten met zich mee. Een entiteit kan daarnaast bestuurlijk gevoelig liggen en (daardoor) op weerstand stuiten. In de tabel hieronder staat voor een aantal onderwerpen een overzicht van de verschillen tussen een juridische entiteit en samenwerkingsovereenkomst.

Overzicht verschillen samenwerkingsovereenkomst - juridische entiteit:

Onderwerp	**Samenwerkings-overeenkomst**	**Juridische entiteit**
Afgescheiden vermogen	Iedere partij treedt op uit eigen naam.	Entiteit kan optreden in het rechtsverkeer en gaat verplichtingen aan, niet de deelnemende partijen.
Eigendom product	Deelnemers gezamenlijk eigenaar of iedere deelnemer zelf voor het geheel (afhankelijk van de gemaakte afspraken).	Entiteit is de eigenaar.
Aansprakelijkheid (jegens derden)	Deelnemers zijn ieder hoofdelijk aansprakelijk voor het geheel (met regres op andere deelnemers) en voor eigen handelen (eventueel met regres op andere deelnemers). Aansprakelijkheid moet (en kan ook) goed geregeld worden in de overeenkomst.	Entiteit is aansprakelijk, deelnemende partijen in principe* niet. ** hierop zijn uitzonderingen*
Commerciële aspecten	Gezamenlijke exploitatie ligt niet voor de hand of vraagt veel (ingewikkeld) maatwerk.	Het is mogelijk onder naam van de entiteit de markt te betreden en een product te exploiteren.
Organisatie	Deelnemers brengen ieder middelen (mensen, zaken e/o financieel) in om de samenwerking concreet uit te voeren. Er moet een project/samenwerkings-administratie opgezet worden. Vaak is één van de deelnemers penvoerder en dezelfde of een andere organisatie administrateur.	Entiteit beschikt over een eigen organisatie voor uitvoering van de samenwerking.
Financieel	Door bijdragen van de deelnemende partijen in geld, goederen of mensen.	Financiering van de entiteit (door bank of deelnemende partijen) is noodzakelijk.
Vastlegging	Samenwerkingsovereenkomst.	Overeenkomst (bij bijvoorbeeld een personenvennootschap) of via het oprichten van een rechtspersoon (bij de notaris). Er is altijd een inschrijving bij de KvK.
Beëindigen samenwerking	Door opzegging van de overeenkomst of uittreden volgens de vastgelegde	Liquidatie van de entiteit of uittreden uit de entiteit.

Onderwerp	Samenwerkings-overeenkomst	Juridische entiteit
	afspraken.	
Personeel	Door bijdragen van de deelnemende partijen of via detachering met een onderlinge verrekening.	Entiteit kan personeel in dienst nemen.

De keuze voor een samenwerking via een overeenkomst of via een entiteit lijkt het meest afhankelijk van het doel van de datasamenwerking en de vraag of er producten worden gerealiseerd/ontwikkeld met de ambitie ze breder te vermarkten. In onderstaande paragraaf wordt voor GERDA de afweging voorr de best passende juridische vorm gemaakt.

6.3 Regionale context

Vereniging Digitalisering Zorg Achterhoek en de deelnemende zorginstellingen:
De Vereniging en deelnemende (zorg)organisaties werken actief samen binnen de GERDA-PoC. Het gaat om zorgaanbieders die binnen de zorgketen actief zijn en belang hebben bij het onderzoek om de kwaliteit van zorg in de keten te verbeteren.

Linksight:
De rol van Linksight is die van softwareleverancier. Linksight stelt de software beschikbaar waarmee de VRE op een technisch veilige en binnen de privacyregelgeving passende wijze kan worden ingericht. Het belang van Linksight ligt vooral in het gebruik en de toepassing van de software. Deelname aan de GERDA-PoC heeft als voordeel voor Linksight dat zij hun software in de praktijk kunnen testen en zo een (nog beter) werkend product kunnen ontwikkelen, dat hun product door de deelnemende partijen wordt gebruikt en afgenomen en dat hun product vanwege de schaalbaarheid breder kan worden verkocht.

Dit betekent dat de relatie met Linksight primair contractueel kan worden ingestoken, waarbij afspraken gemaakt moeten worden over gebruiksvoorwaarden voor en het onderhoud van het Linksight-platform, over de rechten voor de nieuw ontwikkelde datasamenwerking, protocollen, documenten en governance van de VRE en de marktbenadering na afronding van de GERDA-PoC. Voorkomen moet worden dat een met behulp van zorgorganisaties ontwikkelde invulling uitsluitend aan de softwareleverancier toekomt en zij deze vervolgens tegen commerciële tarieven verkopen aan andere zorginstellingen. Anderzijds moet rekening gehouden worden met de gerechtvaardigde (financiële) belangen van Linksight.

8RHK Gezond:
De rol van 8RHK Gezond lijkt vooralsnog beperkt tot ondersteunen en meekijken. Wel is 8RHK gezond geïnteresseerd in de mogelijkheden om de VRE in te zetten voor (andere) onderzoeksvragen, met name

op het gebied van het ontwikkelen van beleid. Een meer indirecte vorm van onderzoek, maar met een duidelijk maatschappelijk belang.

Voor onderzoeksvragen gericht op de ontwikkeling van beleid is het (waarschijnlijk) wenselijk om een aangepaste set van governance afspraken te maken, die op onderdelen kan afwijken van de huidige set governance rules binnen de GERDA-PoC. Vanwege de aard en de doelstelling van 'onderzoek voor beleidsvorming' zou daarnaast het gebruik van (bijzondere) persoonsgegevens (iets) andere regels kunnen hebben dan voor 'onderzoek ter verbetering van de zorg'. In de algemene branchevoorwaarden van ACTIZ bijvoorbeeld, waar de deelnemende VVT leden bij aangesloten zijn, staat in de voorwaarden dat expliciete toestemming aan cliënten gevraagd moet worden voor het gebruik van hun gegevens anders dan voor wetenschappelijk onderzoek ten behoeve van (verbetering van) de zorg.

Om de GERDA-PoC niet onnodig te compliceren en te vertragen kan overwogen worden om 8RHK Gezond en de beleidsmatiger ingestoken onderzoekswensen (nog) niet verder uit te werken. In dit geval zou 8RHK Gezond alsnog via een intentieverklaring of samenwerkingsovereenkomst kunnen aansluiten, waarbij wordt vastgelegd dat in een volgende fase de datasamenwerking uitgebreid wordt met een VRE voor beleidsmatig onderzoek, inclusief een set (aangepaste) governance rules op basis van kennis en ervaring opgedaan in de GERDA-PoC.

Advies voorgestelde samenwerkingsvorm:
Op basis van bovenstaande informatie is het meest wenselijk initieel een datasamenwerking te starten met de Vereniging en de aan de GERDA-PoC deelnemende (zorg)organisaties. Omdat de deelnemende (zorg)organisaties allemaal lid zijn van de Vereniging is het praktisch om GERDA (als VRE) onder de paraplu van de Vereniging te brengen/laten. De Vereniging en de deelnemende partijen moeten dan gezamenlijk een overeenkomst sluiten om de benodigde afspraken in vast te leggen, inclusief een verwijzing naar de met Linksight en 8RHK Gezond te maken afspraken/sluiten overeenkomsten.

De rol en positie van de GGD in de GERDA-PoC moeten nader worden bepaald. De GGD sluit meer vanuit een beleidsmatige invalshoek (8RHK Gezond) aan, is geen lid van de Vereniging en geen zorgaanbieder in de keten.

6.4 Afstemming & besluitvorming

Het voorstel voor de juridische structuur is doorgenomen in de werkgroep Governance. Op basis hiervan ontstaat een tweesporenbeleid voor de verdere invulling:

1. Voor de GERDA-PoC (met productiedata) wordt de Gezamenlijke Verwerkersovereenkomst en het DPIA aan de deelnemende (zorg)organisaties ter ondertekening aangeboden. Omdat de GGD Noord- en Oost-Gelderland (nog) geen verwerkersverantwoordelijkheid heeft en 'enkel' analyse-capaciteit beschikbaar stelt worden er wel afspraken over geheimhouding gemaakt, maar ondertekent de GGD (in dit stadium) de gezamenlijke verwerkersovereenkomst niet.
2. Voor de structurele oprichting van de datasamenwerking is het voorstel om aanvullend op de

gezamenlijke verwerkersovereenkomst een intentieverklaring tussen de Vereniging Digitale Zorg Achterhoek en 8HRK Gezond op te stellen. De inrichting van de datawerkplaats vindt plaats ‘onder’ de Vereniging Digitalisering Zorg Achterhoek.

De regie over verdere bestuurlijke afstemming ligt bij de Vereniging Digitalisering Zorg Achterhoek.

7. Vervolgstappen

In dit hoofdstuk besteden we aandacht aan 'lessons learned' vanuit de werkgroep governance en mogelijke vervolgstappen, anders dan de vervolgstappen gericht op de juridische structuur (al beschreven in paragraaf 6.3). We sluiten af met een korte inkijk naar inhoudelijke doorontwikkeling.

7.1 Lessons learned vanuit de werkgroep Governance

1. Bij de start van de werkgroep Governance bleek het doorgronden van MPC een flinke uitdaging. Het heeft enige tijd geduurd voordat de werkgroepleden zich comfortabel voelden met de techniek en de relatie konden leggen naar het onderwerp privacy.
   Lesson learned: neem werkgroepleden vanaf het begin mee in de werking van de techniek.

2. De invulling van de rol data steward - een nieuwe rol binnen de betrokken organisaties - bleek een complex vraagstuk. Niet (alleen) inhoudelijk, maar (ook) organisatorisch.
   Lesson learned: maak organisatorische vereisten -zoals een nieuwe rol van de data steward- helder en tijdig bekend bij de deelnemende partijen.

3. Bij verschillende vraagstukken bleek het belangrijk om elkaar eerst beter te leren kennen en afspraken te maken over hoe de verschillende partijen onderling willen samenwerken. De techniek, MPC, moet hier vervolgens in faciliteren.
   Lesson learned: binnen nieuwe samenwerkingsverbanden is het belangrijk eerst kennis te maken en stil te staan bij en afspraken te maken over de wijze van samenwerken.

7.2 Vervolgstappen bij nadere inrichting

1. Na de GERDA-PoC blijft het noodzakelijk om periodiek de **afstemming tussen data scientists en data stewards** van verschillende compute groups te organiseren, zodat de afstemming over inrichting van de VRE (bijvoorbeeld het beschikbaar stellen van data of het bijwerken van de governance rules) periodiek aandacht blijft krijgen. Ook is het belangrijk om helder te maken hoe **toeleiding van nieuwe onderzoeksvragen naar de data stewards** vanuit projecten en/of beleidsmedewerkers in de (zorg)organisaties plaatsvindt.
   Lesson learned: ondersteun de deelnemende partijen bij het organiseren van overleggen en het inrichten van processen.

2. Voor de analyse en invulling van diverse governance vragen zijn de implementatie-adviezen van Moerel & Hooghiemstra doorgenomen. Zij adviseren onder andere ook om een **ethisch beleidskader voor data stewards en data scientists** te schrijven, op basis van de landelijke, reeds beschikbare informatie.

Lesson learned: Het is nodig om de ethische kant van onderzoeksvragen en data-analyse goed uit te werken en toepasbaar te maken voor medewerkers van de (zorg)organisaties.

3. Verder werden de beschreven onderdelen van deze whitepaper als een goede basis ervaren om vanuit governance, informatiebeveiliging en juridische expertise met GERDA te kunnen starten. De verwachting is dat bij (bredere) implementatie en gebruik van MPC nieuwe governance vraagstukken ontstaan. Daarom is **evaluatie over circa een half jaar** nodig om bij te sturen op basis van de opgedane kennis en ervaring.
   Lesson learned: door het opknippen van dit projectonderdeel in overzichtelijke onderdelen met een heldere tijdslijn, werd focus gegeven aan de werkgroepleden. De werkgroepleden vinden het erg belangrijk om het privacy aspect van opgedane ervaringen te evalueren.

4. Vanuit betrokken organisaties is de wens uitgesproken om een **learning community voor governance, informatiebeveiliging en juridische expertise** te starten om zo gezamenlijk complexe vraagstukken uit te werken. Wens is een combinatie van fysieke en digitale bijeenkomsten, met goede ondersteuning en voorbereiding.
   Lesson learned: In deze wereld van toenemende complexiteit van techniek en regelgeving is samenwerking en kennisdeling over de keten heen een 'must'.

7.3 Inhoudelijke doorontwikkeling

De verwachting is dat op termijn doorontwikkeling van de datasamenwerking/VRE plaatsvindt. Denk aan de scenario's waarin externe partijen valide bevragingen mogen doen, data geautomatiseerd vanuit de datastations beschikbaar wordt gesteld en nieuwe analysetechnieken op basis van MPC beschikbaar komen.

8. Definities

Compute group
Een compute group wordt gevormd door organisaties binnen een *datasamenwerking* ten behoeve van het beantwoorden van 1 specifiek analysevraagstuk.

Datastation
Een datastation is het verwerkingslocatie binnen een organisatie die aangesloten is op de compute group. Berekeningen op eigen data-attributen vinden plaats binnen het eigen datastation en alleen het antwoord wordt verstuurd.

Datasamenwerking
Een samenwerking van organisaties die gezamenlijk data willen delen & analyseren. Binnen het project GERDA is de datasamenwerking formeel vastgelegd in een gezamenlijke verwerkersovereenkomst. Binnen een datasamenwerking kunnen meerdere *compute groups* actief zijn.

Homomorfe vercijfering
Dat is een versleutelingsmethode om analyses uit te kunnen voeren op data terwijl die data steeds versleuteld en dus onleesbaar blijft.

Governance rules
Dit zijn de regels binnen een compute group over de samenwerking en beschrijven bijvoorbeeld waar elke analysevraag aan moet voldoen. Denk bijvoorbeeld aan de minimale groepsgrootte waarover uitkomsten teruggegeven mogen worden aan de data scientist. Indien er niet voldaan wordt aan de governance rules, worden uitkomsten niet zichtbaar voor de data scientist.

Hashing
Hashing is een methode waarmee de invoer op een repeteerbare manier versleuteld wordt zodat de originele invoer niet zomaar teruggehaald kan worden. In de context van dit whitepaper wordt hashing onder andere gebruikt om een verzameling attributen om te zetten naar een unieke identifier per persoon, zonder dat de oorspronkelijke attributen herleidbaar zijn.

Playground
De Linksight playground is een online (cloud) omgeving waar organisaties kunnen experimenteren met de mogelijkheden van MPC op basis van fictieve data binnen de organisatie zonder programmatuur te hoeven installeren. Dit omvat zowel de data collaboration governance als de daadwerkelijke analyses.

Salt
Een “salt” is een onvoorspelbare code die als additionele beveiligingsmethode meegenomen kan worden in het hashen zodat zonder kennis van deze salt niet na te gaan is *of* een bepaalde invoer tot dezelfde hash-uitvoer heeft geleid.