

# Reisgids voor PET implementatie in de zorg

## Auteurs

Sarah van Drumpt, Bastiaan van Schijndel, Joris Holtrop, Jannick Dorrestijn,  
Onno van der Galien, John de Vries, Steven Noorlander, Martine van de Gaar,  
Eric Boersma, Rogier Barendse, Isabella Kardys, Henk Marquering, John Jacobs

# Inhoud

|                                                |           |                                                       |           |
|------------------------------------------------|-----------|-------------------------------------------------------|-----------|
| <b>Inleiding</b>                               | <b>3</b>  | <b>4. Checklist voor onderweg</b>                     | <b>12</b> |
| <b>1. Vertrekhal – Waarom deze reis maken?</b> | <b>5</b>  | <b>5. De Praktijk: reizen door onbekend terrein</b>   | <b>13</b> |
| <b>2. De Routekaart: structuur en lijnen</b>   | <b>6</b>  | <b>6. Bestemming: nieuwe inzichten veilig gedeeld</b> | <b>14</b> |
| 2.1 Persona's onderweg                         | 8         | <b>7. Klaar voor vertrek: call-to-action</b>          | <b>16</b> |
| 2.2 Stations                                   | 9         |                                                       |           |
| 2.3 Beslismomenten bij elk station             | 10        |                                                       |           |
| <b>3. Reisdocumenten &amp; instrumenten</b>    | <b>11</b> |                                                       |           |
| 3.1 Regulerend Perspectief                     | 11        |                                                       |           |
| 3.2 Organisatorisch perspectief                | 11        |                                                       |           |
| 3.3 Samenwerkingsperspectief                   | 11        |                                                       |           |

The background of the slide is a deep blue with abstract, glowing light blue and white wavy lines that create a sense of motion and data flow. Scattered throughout are numerous circles of varying sizes, some solid blue and others with a soft, glowing white or light blue center, resembling bokeh or data points.

# Inleiding

Deze gids is voor zorgprofessionals die data-gedreven (willen) samenwerken over organisatiegrenzen heen, waarbij zowel het beschikbaar maken van data als het waarborgen van privacy centraal staan. Het biedt een duidelijke routekaart voor de succesvolle implementatie van Privacy-Enhancing Technologies (PETs). Op basis van praktijkervaring uit het Secur-e-Health project beschrijven we zowel organisatorische, juridische als technische stappen, met persona's en beslismomenten. De nadruk ligt op situaties waarin dataverrijking wenselijk of noodzakelijk is, maar lastig te realiseren blijkt vanwege technische beperkingen, privacyregelgeving (zoals de AVG), commerciële belangen of een gebrek aan onderling vertrouwen.

# Privacy-gedreven samenwerking in de gezondheidszorg

## Doelstelling

Het Secur-e-Health-project richt zich op het mogelijk maken van veilige, privacybeschermende analyses van gezondheidsdata over verschillende organisaties heen. Door gebruik te maken van geavanceerde technieken zoals multi-party computation en digitale identiteitsoplossingen, kunnen medische instellingen samenwerken zonder gevoelige patiëntgegevens direct te delen. Dit bevordert de ontwikkeling van voorspellende modellen, efficiëntere behandelingen en versnelt klinisch onderzoek.

**Looptijd:** November 2021 – December 2025

**Programma:** ITEA 4 (Eureka Cluster voor software-innovatie)

**Internationale samenwerking:** Het project verenigt 30 partners uit vijf landen: Canada, Finland, Duitsland, Portugal en Nederland

- > **Canada:** Kelvin Zero, DENTOS Inc., Perceiv Research Inc.
- > **Finland:** Bittium, CSIT, MediConsult, Nordic Healthcare Group, Solita Oy, SUCCESS CLINIC, VTT
- > **Duitsland:** OFFIS, Oncare, Stryker, University Hospital Aachen
- > **Portugal:** Fundação Fernando Pessoa, ISP, MTG Research & Development Lab, University of Porto
- > **Nederland:** Amsterdam UMC, Achmea, Almende, TU/e, Erasmus MC, Linksight, Medrecord, Ortec, PS-Tech, Stichting ZorgTTP, UMC Utrecht, TNO

## Gebruikscases:

Het project omvat diverse gebruikscases, waaronder:

- > **Canada:** Gebruik van veilige en gebruikersgerichte digitale identiteitsoplossing ter ondersteuning van 's werelds grootste virtuele klinische studie, waarbij innovatieve authenticatiemethoden en betrokkenheid van patiënten in elke fase worden geïntegreerd.
- > **Finland:** Gebruik van federated learning om risicomodellen voor hartrevalidatie te ontwikkelen, waarbij gegevens van verschillende zorgaanbieders worden gecombineerd.
- > **Duitsland:** Implementatie van een gedigitaliseerd patiënttraject voor de behandeling van dijbeenbreuken, inclusief computerondersteunde chirurgie en revalidatie met sensoren, waarbij federated learning wordt gebruikt om gegevens te analyseren
- > **Portugal:** Inzet van federated learning ter ondersteuning van slimme pediatrie zorg, met focus op klinische uitdagingen zoals de aanpak van obesitas bij kinderen en herstel na operaties, waarbij de privacy van patiëntgegevens tussen instellingen wordt gewaarborgd.
- > **Nederland:** Gebruik van privacy-enhancing technologies om gepersonaliseerde risicoscores voor hart- en vaatziekten te ontwikkelen, gebaseerd op elektronische gezondheidsdossiers.

Secur-  
e-Health 



## **Secur-e-Health:**

***“de toekomst van datagebruik in de gezondheidszorg ligt in investeringen en samenwerking op het gebied van privacy”***

## **1. Vertrekhal – Waarom deze reis maken?**

Privacy-Enhancing Technologies (PETs) zijn niet meer weg te denken uit het moderne datagebruik in de gezondheidszorg. Deze technologieën maken het mogelijk gegevens te (her)gebruiken voor onderzoek, beleid en vernieuwing, zoals het meten van effectiviteit, het vergelijken van zorginstellingen en het ontwikkelen van slimme AI-oplossingen. Voor beleid kunnen gegevens bijvoorbeeld worden ingezet om trends in zorggebruik te analyseren en op basis daarvan landelijke richtlijnen of financieringsmodellen aan te passen. Tegelijkertijd beschermen PETs de privacy van gevoelige (gezondheids) gegevens. Deze technologieën faciliteren de naleving van Europese privacyregels (zoals de AVG/GDPR), door middel van het beperken van directe data-inzage en het gebruik van gegevens voor een duidelijk doel. Ze maken niet alleen veilig (her)gebruik van gegevens mogelijk – zoals bedoeld in de nieuwe Europese wetgeving, de European Health Data Space (EHDS) – maar verbeteren ook de digitale weerbaarheid door het risico op datalekken te verkleinen.

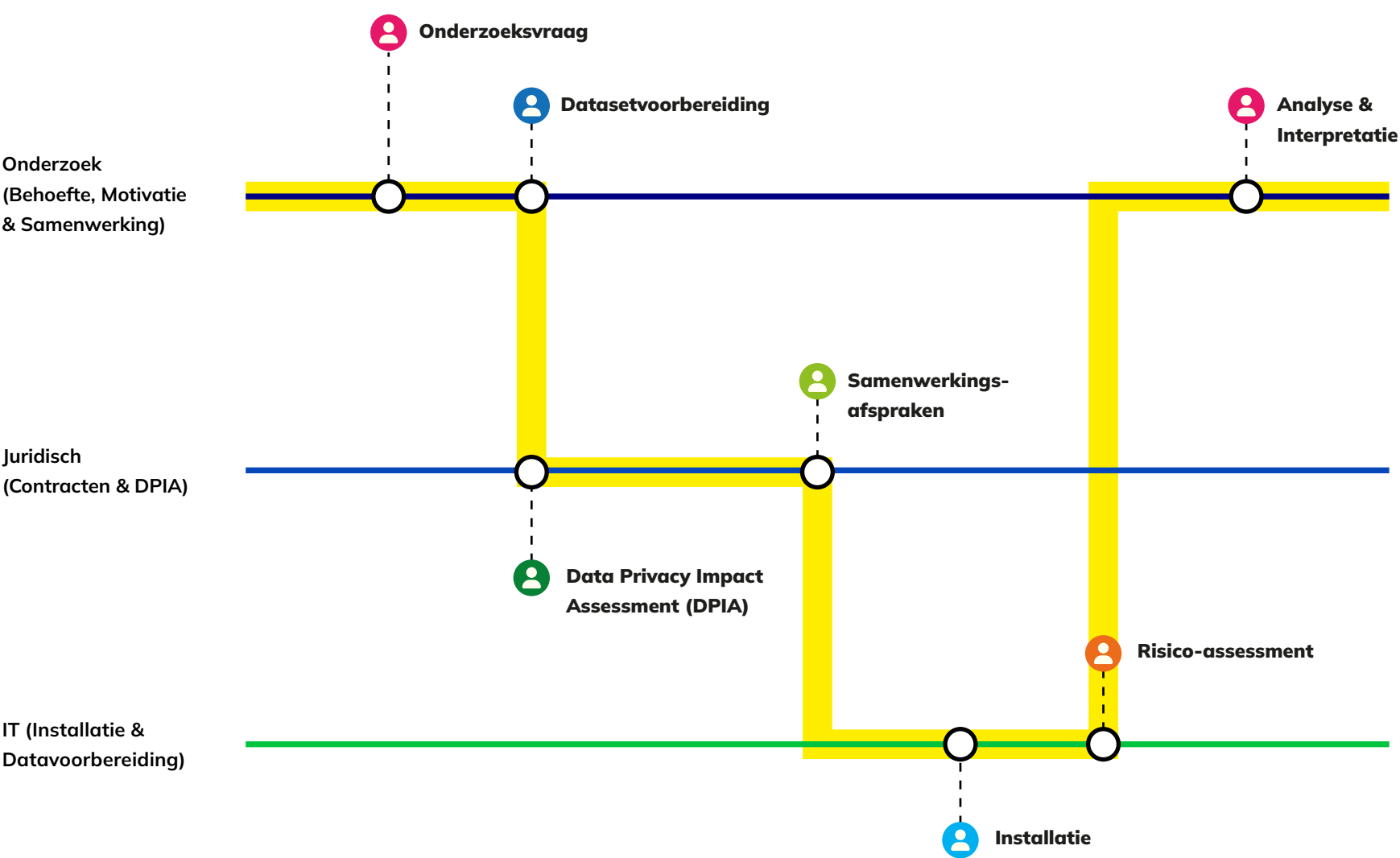
Voor meer informatie over de technieken zelf verwijzen wij graag naar: [Information Commissioner's Office – Privacy-Enhancing Technologies](#).



## 2. De Routekaart: structuur en lijnen

Het proces van PET-implementatie kan worden vergeleken met een reis langs een zorgvuldig uitgestippelde routekaart, waarbij verschillende sporen samenkomen en elkaar kruisen. Elk spoor vertegenwoordigt een belangrijk aspect van de implementatie, van IT en technische voorbereiding tot juridische vereisten en onderzoek. De onderstaande routekaart biedt een overzicht van de drie belangrijkste lijnen die de reis door dit proces vormen: IT (Installatie & Datavoorbereiding), Juridisch (Contracten & DPIA) en Onderzoek (Behoefte, Motivatie & Samenwerking). De routekaart toont een gestructureerde route, maar in de praktijk is het geen strikt watervalmodel: er vinden regelmatig terugkoppelingen en extra communicatie plaats tussen stations om tot een juist besluit te komen en door te kunnen rijden. We beginnen bij het startpunt, de ambitie om samen te werken, en reizen door verschillende stations naar het eindstation: de structurele inbedding van privacyvriendelijke datadeling.

# Stations PET datasamenwerking



## Wat regelt de reisleader?

-  **Onderzoeker**  
Datamanagementplan; variabelen, definities, bronafspraken
-  **Databeheerder**  
Specificaties dataset; tools, format- en kwaliteitseisen
-  **Privacy Officer**  
DPIA, privacyprincipes
-  **Jurist**  
Verwerkers- of samenwerkings-overeenkomst
-  **IT/Systeembeheerder**  
Technische requirements, installatieplanning, DMZ-architectuur (eventueel)
-  **Security Officer**  
Risk assessments, pentests (eventueel), vergelijkingsmateriaal

| Station                          | Beslismoment                 | Wat te beslissen?                                                                                                                        |
|----------------------------------|------------------------------|------------------------------------------------------------------------------------------------------------------------------------------|
| Onderzoeksvraag                  | Vooronderzoek                | Zijn PETs geschikt (let op: het antwoord is mede afhankelijk van de databeschikbaarheid)?<br>Welke alternatieven en risico's spelen mee? |
| Datasetvoorbereiding             | Na definiëren databehoefte   | Is de data beschikbaar en in juiste vorm? Voldoet het aan juridische en ethische criteria?                                               |
| DPIA                             | Na DPIA en ethische toetsing | Gaan we door? Zijn risico's acceptabel en is dekking juridisch geregeld?                                                                 |
| Installatie en risico-assessment | Na technische voorbereiding  | Is installatie haalbaar? Voldoet aan security- en infra-eisen?                                                                           |
| Analyse & Interpretatie          | Voor uitvoering              | Zijn contracten, goedkeuringen en security checks afgerond?                                                                              |

## 2.1 Persona's onderweg

Hieronder worden de verschillende rollen en verantwoordelijkheden beschreven die noodzakelijk zijn voor het beheer van data en het waarborgen van privacy binnen een organisatie. Het is belangrijk om te benadrukken dat de rollen per organisatie kunnen variëren en dat bepaalde rollen mogelijk door één of meerdere personen kunnen worden bekleed, afhankelijk van de organisatiestructuur en de specifieke behoeften van het project. Rollen en verantwoordelijkheden vastleggen helpt niet alleen voor een efficiënte uitvoering van processen, maar ook voor naleving van wet- en regelgeving. De volgende persona's zijn van belang binnen dit domein, elk met hun specifieke verantwoordelijkheden:



### Onderzoeker

Als onderzoeker formuleer ik de onderzoeksvraag en bepaal ik de databehoeftes. Ik stel variabelenspecificaties op, maak afspraken over databronnen en voer de analyses uit. Binnen een PET-omgeving zorg ik ervoor dat de analytische integriteit gewaarborgd blijft, ondanks de beperkingen van de technologie. Dit vraagt om zorgvuldige voorbereiding, duidelijke afstemming en robuuste validatiemethoden om de betrouwbaarheid van de resultaten te waarborgen, waarbij ik idealiter de [FAIR-principes](#) (Findable, Accessible, Interoperable, Reusable) toepas om de waarde en herbruikbaarheid van data en analyses te versterken. De uitkomsten vertaal ik naar heldere inzichten die bijdragen aan betere besluitvorming of zorgverbetering.



### Databeheerder

Als databeheerder ben ik verantwoordelijk voor de extractie, transformatie en harmonisatie van data. Ik zorg ervoor dat de datasets van hoge kwaliteit zijn, ze volgens standaard dataformaten worden opgeslagen en zorgvuldig worden gecureerd – zodat ze eenduidig, bruikbaar en toekomstbestendig blijven. Daarnaast onderhoud ik de communicatie met onderzoekers en andere datapartners om ervoor te zorgen dat de gegevens consistent en goed gecoördineerd worden gedeeld, zodat het onderzoeksproces soepel verloopt.



### Privacy Officer

Als privacy officer ondersteun ik bij het uitvoeren van de Data Protection Impact Assessments (DPIA) en monitor ik de privacyprincipes binnen het project. Ik geef advies over maatregelen die de onderzoeker kan nemen om privacyrisico's te mitigeren. Wanneer mijn organisatie een functionaris gegevensbescherming heeft aangesteld vraag ik deze om advies bij een DPIA. Ik vul samen met de onderzoeker de privacy matrix in en evalueer de herleidbaarheid van gegevens. Daarnaast werk ik nauw samen met juridische en IT-teams om te zorgen voor naleving van privacywetgeving en het waarborgen van de bescherming van persoonsgegevens.



### Jurist

Als jurist stel ik verwerkersovereenkomsten en datatransferovereenkomsten op en zorg ik ervoor dat formele rollen en risicokenmerken correct zijn vastgelegd in contracten. Ik adviseer over juridische kaders zoals de AVG/GDPR en de Europese Gezondheidsdata Strategie (EHDS) en zorg ervoor dat

het project voldoet aan de geldende wet- en regelgeving, zodat juridische risico's op het gebied van compliance worden geminimaliseerd.



### IT/Systeembeheerder

Als IT- of systeembeheerder zorg ik voor de technische inrichting en het onderhoud van de PET-omgeving binnen onze infrastructuur. Ik ben verantwoordelijk voor installatie, configuratie en het monitoren van de systemen. Daarbij bewaak ik de beschikbaarheid en betrouwbaarheid van de infrastructuur en zorg ik dat deze aansluit bij bestaande architecturen (zoals DMZ en netwerksegmentatie). Samenwerking met security- en privacy collega's is essentieel om ervoor te zorgen dat de PET-software niet alleen werkt, maar ook veilig en schaalbaar is.



### Security Officer

Als security officer beoordeel ik de beveiligingsrisico's die verbonden zijn aan het gebruik van PETs. Ik voer risicoanalyses uit, beoordeel dreigingen en laat waar nodig penetratietesten uitvoeren. Mijn taak is om te waarborgen dat de gekozen technische en organisatorische maatregelen passen bij de gevoeligheid van de data en de use-case. Ik adviseer over aanvullende maatregelen en blijf de securitypositie monitoren, zodat de samenwerking over organisatiegrenzen heen voldoet aan hoge standaarden van informatiebeveiliging.

## 2.2 Stations

Uit ervaring blijkt dat het proces van PET-implementatie bestaat uit verschillende stations, waarbij in elke fase een andere reisleader het voortouw neemt. De reisleader zorgt ervoor dat de benodigde acties worden uitgevoerd om het station met vertrouwen te passeren en de reis voort te zetten. In de onderstaande tabel staat voor elk station de reisleader, het doel van de reisleader, en een inzicht dat de reisleader helpt om bewust om te gaan met de specifieke uitdaging van de betreffende fase.

| Stations                | Reisleader                                                                                              | Lijn      | Doel                                                                                   | Let op                                                                                     |
|-------------------------|---------------------------------------------------------------------------------------------------------|-----------|----------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------|
| Onderzoeksvraag         |  Onderzoeker           | Onderzoek | Heldere databehoeftes definiëren en PET-analyse mogelijk maken zonder herleidbare data | Kennis van de beschikbare databronnen en hun structuur noodzakelijk                        |
| Datasetvoorbereiding    |  Databeheerder         | Onderzoek | Data extraheren, harmoniseren en in de juiste formaten klaarzetten                     | Fouten in de data zijn lastig te ontdekken in een later stadium                            |
| DPIA                    |  Privacy Officer       | Juridisch | Privacyrisico's in kaart brengen en mitigeren via DPIA's en privacyprincipes           | PETs beperken risico maar vervangen geen juridische zorgvuldigheid                         |
| Samenwerkingsafspraken  |  Jurist                | Juridisch | Verantwoordelijkheden en risico's contractueel vastleggen                              | Techniek is niet genoeg; formele afspraken voorkomen misverstanden                         |
| Installatie             |  IT/Systeem-beheerder | IT        | PET-software veilig integreren in de infrastructuur                                    | Maatwerkinstallatie vereist samenwerking tussen afdelingen                                 |
| Risico-assessment       |  Security Officer    | IT        | Beveiligingsrisico's beoordelen binnen specifieke use-cases                            | Risico's variëren per use-case; herbeoordeling is nodig per case                           |
| Analyse & Interpretatie |  Onderzoeker         | Onderzoek | Analyse uitvoeren binnen PET-beperkingen, resultaten interpreteren en valideren        | Subtiele fouten blijven makkelijk onopgemerkt; extra validatie en duiding zijn essentieel. |

## 2.3 Beslismomenten bij elk station

Bij elk station raden wij aan een weloverwogen beslissing te nemen, waarbij rekening wordt gehouden met verschillende factoren zoals beschikbaarheid van data, juridische en ethische overwegingen, technische haalbaarheid en security-eisen. De onderstaande tabel geeft een overzicht van deze beslismomenten en de bijbehorende vragen die beantwoord moeten worden om het proces succesvol door te zetten.

| Station                          | Beslismoment                 | Wat te beslissen?                                                                          |
|----------------------------------|------------------------------|--------------------------------------------------------------------------------------------|
| Onderzoeksvraag                  | Vooronderzoek                | Zijn PETs geschikt? Welke alternatieven en risico's spelen mee?                            |
| Datasetvoorbereiding             | Na definiëren databehoeft    | Is de data beschikbaar en in juiste vorm? Voldoet het aan juridische en ethische criteria? |
| DPIA                             | Na DPIA en ethische toetsing | Gaan we door? Zijn risico's acceptabel en is dekking juridisch geregeld?                   |
| Installatie en risico-assessment | Na technische voorbereiding  | Is installatie haalbaar? Voldoet aan security- en infra-eisen?                             |
| Analyse & Interpretatie          | Voor uitvoering              | Zijn contracten, goedkeuringen en security checks afgerond?                                |

# 3. Reisdocumenten & instrumenten

Tijdens de PET-implementatie zijn er verschillende documenten en instrumenten die van belang zijn vanuit drie perspectieven: regulerend, organisatorisch en samenwerkingsperspectief. Deze documenten helpen bij het waarborgen van naleving van wet- en regelgeving, het efficiënt organiseren van processen en het faciliteren van samenwerking tussen verschillende partijen. In dit hoofdstuk worden de belangrijkste documenten en instrumenten besproken die nodig zijn om de reis succesvol te doorlopen en de implementatie van PETs te realiseren.

## 3.1 Regulerend Perspectief

Binnen het regulerend perspectief staan juridische en beleidsmatige vereisten centraal die de inzet van PETs kaderen. Deze documenten zorgen voor naleving van privacywetgeving en bieden houvast bij het vastleggen van verantwoordelijkheden. Ze vormen de basis voor een rechtmatige en transparante gegevensverwerking.

- > **DPIA:** verplichte risicoanalyse bij waarschijnlijk hoge privacyrisico's
- > **(Gezamenlijke) verwerkersovereenkomst:** formaliseren rollen en verantwoordelijkheden met betrekking tot de dataverwerking. Hierin wordt onder andere ook beschreven welke data en onder welke voorwaarden deze data verwerkt zal gaan worden.

## 3.2 Organisatorisch perspectief

Vanuit organisatorisch oogpunt zijn er verschillende elementen die bijdragen aan een gestructureerde en veilige implementatie van PETs. Deze hebben betrekking op de inrichting van processen, beschikbaarheid van expertise, en technische randvoorwaarden. De onderstaande documenten en maatregelen ondersteunen een robuuste uitvoering en borging binnen de organisatie.

- > **Risicoassessment:** inschatting van dreigingen, kwetsbaarheden en impact
- > **IT-architectuur & documentatie:** DMZ, netwerksegmentatie, toegangsprotocollen
- > **Datamanagementplan:** rollen, definities, classificatie, datastromen en FAIR-principes
- > **Capaciteit & expertise:** beschikbaarheid van data-, privacy-, security- en technische specialisten

## 3.3 Samenwerkingsperspectief

Effectieve samenwerking tussen betrokken partijen is belangrijk voor de inzet van PETs. Dit perspectief richt zich op afspraken, afstemming en gezamenlijke werkwijzen die nodig zijn om een gedeeld begrip en goede coördinatie te waarborgen. De volgende instrumenten ondersteunen een transparante en afgestemde samenwerking.

- > **Gezamenlijke privacy matrix:** afspraken over herleidbaarheid en gebruik waarin gezamenlijk geëvalueerd wordt op de privacy principes en maatregelen die van toepassing zijn bij de datasamenwerking.
- > **Datatransfer agreement:** bij uitwisseling van gevoelige data
- > **IT-afstemming:** infrastructuur, monitoring, onderhoud via architectuurkaarten
- > **Onderzoekersoverleg:** gezamenlijk bespreken van de eindresultaten.

## 4. Checklist voor onderweg

Voor een succesvolle implementatie van PETs is het belangrijk om onderweg een aantal zaken te regelen. In deze checklist per persona worden de belangrijkste verantwoordelijkheden en acties op een rij gezet die elke persoon in het proces moet uitvoeren. Door de juiste stappen op tijd te nemen, wordt ervoor gezorgd dat privacy, security en andere benodigde aspecten efficiënt kunnen worden beheerd. In de onderstaande checklist vind je de taken die per rol moeten worden uitgevoerd om de reis soepel te laten verlopen.

### Checklist per persona

| Persoon                                                                                                  | Te regelen                                                                 |
|----------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------|
|  Onderzoeker            | Datamanagementplan; variabelen, definities, bronafspraken                  |
|  Databeheerder          | Specificaties dataset; tools, format- en kwaliteitseisen                   |
|  Privacy Officer      | DPIA, privacyprincipes                                                     |
|  Jurist               | Verwerkers- of samenwerkingsovereenkomst                                   |
|  IT/Systeem-beheerder | Technische requirements, installatieplanning, DMZ-architectuur (eventueel) |
|  Security Officer     | Risk assessments, pentests (eventueel), vergelijkingsmateriaal             |

**Tip:** Verzamel alle technische en inhoudelijke details vooraf, zodat privacy & security efficiënt kunnen worden beoordeeld.

# 5. De Praktijk: reizen door onbekend terrein

Omdat PETs nog relatief nieuw zijn, bevindt de implementatie zich vaak in een onbekend terrein. Dit betekent dat je je extra bewust moet zijn van verschillende aspecten om de reis veilig en succesvol te voltooien. Hieronder gaan we dieper in op de belangrijke overwegingen en bieden we praktische handvatten om effectief met de uitdagingen van PETs om te gaan.

## Juridische en administratieve inbedding is nodig

PETs vereisen vaak een aparte paragraaf in bestaande DPIA's (Data Protection Impact Assessments) en contracttemplates.

**Wat helpt:** het gebruik van **standaardformats**, zoals aangepaste DPIA-sjablonen, en voorbeelden uit eerdere implementaties, bijvoorbeeld **federated learning bij het UMCU**.

## Onzichtbaarheid van datakwaliteit vereist vroege borging

Omdat ruwe data niet tussen partijen wordt gedeeld, zijn fouten in de data-input niet voor iedereen direct zichtbaar. Dat maakt het essentieel om datakwaliteit vooraf goed te borgen.

**Wat helpt:** **vroegtijdige betrokkenheid van domeinexperts** die weten waar ze op moeten letten bij de dataselectie en -interpretatie. Soms kunnen fouten ook worden herkend in afwijkende eindresultaten, dus is een proefanalyse of simulatie zinvol.

## Hogere beveiligingseisen bij samenwerking over organisaties heen

Samenwerking tussen zorginstellingen en externe partijen vraagt om stevige technische en organisatorische beveiligingsmaatregelen. Privacy-verhogende technieken dragen hieraan bij, maar zijn geen volledige oplossing; aanvullende maatregelen blijven nodig om alle risico's af te dekken.

**Wat helpt:** hergebruik van **bestaande security-beoordelingen en audits** waar mogelijk, en het volgen van bewezen technische standaarden.

## Gebrek aan bekendheid en ervaring met PETs vraagt om voorbeelden

Veel organisaties zijn nog niet bekend met de werkwijze en implicaties van PETs, wat kan leiden tot misverstanden of vertraging.

**Wat helpt:** **praktijkvoorbeelden**, toegankelijke uitleg en eventueel een **ondersteuning** (zoals middels het open source [PET-lab](#) of van PET providers) kunnen organisaties helpen sneller vertrouwd te raken met deze technologie.

## 6. Bestemming: nieuwe inzichten veilig gedeeld

Hieronder wordt de meerwaarde van PETs besproken en illustreren wij dit aan de hand van een praktijkvoorbeeld vanuit het Secur-e-Health project.

### Meerwaarde van PETs:

- > **Betere modellen door gecombineerde data**  
Integratie van data uit diverse bronnen leidt tot robuustere en accuratere AI-modellen.
- > **Populatie specifieke finetuning en continue updates**  
Modellen worden voortdurend aangepast aan de unieke kenmerken en behoeften van specifieke patiëntgroepen.
- > **Gegarandeerde privacybescherming**  
Geavanceerde technieken zoals federated learning en multi-party computation waarborgen de vertrouwelijkheid van patiëntgegevens.
- > **Versterkt vertrouwen in datagedreven zorginnovatie**  
Transparantie, veiligheid en effectiviteit bevorderen het draagvlak voor AI in de zorg.

### Praktijkvoorbeeld: Betere risicovoorspellingen bij hart- en vaatziekten, met behoud van privacy

Om patiënten met hart- en vaatziekten beter te kunnen behandelen, is het belangrijk om hun risico op verslechtering of nieuwe aandoeningen zo nauwkeurig mogelijk te voorspellen. In twee verschillende casussen laten we zien hoe PETs het mogelijk maken om data-gedreven modellen te verbeteren, zónder dat privacy of controle over data in gevaar komt.

### Casus 1: Aangepast risicomodel voor patiënten met vaatziekten

In het UMC Utrecht wilden we het bestaande SMART2-model – dat voorspelt hoe groot de kans is dat iemand met een bestaande vaatziekte opnieuw een aandoening krijgt – beter laten aansluiten bij de eigen patiëntengroep. Daarvoor hadden we meer gegevens nodig dan alleen uit het ziekenhuis, bijvoorbeeld over zorg die patiënten elders ontvingen. Verzekeraar Zilveren Kruis heeft zulke aanvullende informatie, maar het delen van data tussen ziekenhuizen en verzekeraars ligt gevoelig en is aan strenge privacyregels gebonden, zoals een passend beveiligingsniveau van de gegevens. Om een beeld te vormen van het niveau van beveiligingsmaatregelen is er een penetratie test uitgevoerd. Een dergelijke test biedt waardevolle inzichten over de gerealiseerde technische inrichting en configuratie van de data-samenwerking. De test heeft er dan ook aan bijgedragen om het beveiligingsniveau verder te verhogen en expliciete keuzes te maken over risico's.

PETs bieden een mogelijkheid om gegevens op een privacy-vriendelijke manier tussen partijen te delen. Met de techniek *Secure Multi-Party Computation* konden we gegevens van beide partijen veilig combineren, zonder dat de onderliggende patiëntdata werden gedeeld. Elke partij hield controle over zijn eigen data. Zo konden we:

- > Het risicomodel aanpassen op de echte patiënten van het UMC Utrecht
- > De controle over data behouden bij zowel het ziekenhuis als de verzekeraar
- > Semi-automatisch naleven van afspraken over datagebruik via een technische structuur

**Het resultaat:** een verbeterd model dat beter aansluit bij onze patiënten, met een laag risico dat de privacy van die patiënten in gevaar komt. Deze aanpak laat zien hoe PETs kunnen helpen bij het verbeteren van de zorg, zonder dat dit ten koste gaat van vertrouwen of regelgeving.

## **Casus 2: Verbeterde prognose bij hartfalen met federated learning**

Ook bij hartfalen is goede risicostratificatie cruciaal. Deze aandoening kent een slechte prognose en een sterk verminderde kwaliteit van leven. In een samenwerking tussen meerdere universitaire medische centra analyseren we hoe routine-laboratoriumdata uit elektronische patiëntendossiers kunnen helpen bij het voorspellen van ziekteverergering. Hiervoor gebruiken we tijdsafhankelijke Cox-modellen – een statistische methode die in kaart brengt hoe bepaalde factoren samenhangen met de kans dat een patiënt binnen een bepaalde tijd een verslechtering doormaakt.

Omdat de data van verschillende patiënten verspreid zijn over meerdere ziekenhuizen, zetten we *federated learning* in: een PET-techniek waarmee modellen gezamenlijk kunnen worden getraind op data die op locatie blijft. Zo benutten we de kracht van multicenterdata, zonder dat gevoelige informatie uitgewisseld hoeft te worden.

**Het resultaat:** In beide casussen leverden PETs een belangrijke bijdrage aan betere voorspellende modellen voor hart- en vaatziekten. Dankzij deze technieken konden we de kracht van data benutten, zonder in te leveren op privacy, vertrouwen of naleving van regelgeving.



## 7. Klaar voor vertrek: call-to-action

Om PETs effectief in te zetten binnen je data-ecosysteem, is het belangrijk om te starten met kleinschalige, praktische stappen. Dit helpt om inzicht te krijgen in de toegevoegde waarde van PETs voor jouw specifieke situatie. Onderstaande acties bieden houvast om ervaring op te doen en ondersteuning te vinden bij het Secur-e-Health project.

- > **Evalueer je data samenwerkingen:** Waar voegt PET waarde toe?
- > **Start een proefanalyse:** Gebruik formats en adviezen van het Secur-e-Health project
- > **Neem contact op** met het Secur-e-Health team voor templates, demo's en advies:  
Andries Stam (CEO Almende b.v.)  
[Andries@almende.org](mailto:Andries@almende.org);

## Auteurs

- > Sarah van Drumpt, TNO (hoofdauteur), sarah.vandrumpt@tno.nl
- > Bastiaan van Schijndel, Stichting ZorgTTP (hoofdauteur), bastiaan.van.schijndel@zorgttp.nl
- > Joris Holtrop, UMCU, j.holtrop-3@umcutrecht.nl
- > Jannick Dorresteyn, UMCU, j.a.n.dorresteyn-2@umcutrecht.nl
- > Onno van der Galien, Zilveren Kruis, onno.van.der.galien@zilverenkruis.nl
- > John de Vries, Zilveren Kruis, john.de.vries2@zilverenkruis.nl
- > Steven Noorlander, Zilveren Kruis, steven.noorlander@zilverenkruis.nl
- > Martine van de Gaar, Linksight, martine@linksight.nl
- > Eric Boersma, Erasmus MC, h.boersma@erasmusmc.nl
- > Rogier Barendse, Erasmus MC, r.barendse@erasmusmc.nl
- > Isabella Kardys, Erasmus MC, i.kardys@erasmusmc.nl
- > Henk Marquering, Amsterdam UMC, h.a.marquering@amsterdamumc.nl
- > John Jacobs, Ortec, john.jacobs@ortec.com

