



De weg naar veilig datadelen

Een onderzoek naar de adoptie van PETs in Nederland

INNOPAY
A business of Oliver Wyman



Ministerie van Economische Zaken

Auteurs
Douwe Lycklama
Maarten Bakker
Pieter Verhagen
Leon Kluiters
Maikel Abiskharoun

Inhoudsopgave

1. Management samenvatting	4
2. Introductie	7
2.1 Aanleiding en context	7
2.2 Doel en onderzoeksvragen	13
2.3 Onderzoeksopzet en methodiek	14
2.4 Leeswijzer	15
3. Overzicht van het PET-landschap & stand van zaken in Nederland	17
3.1 Introductie PETs	17
3.2 Overzicht van PET toepassingen	19
3.3 Dominante PET-technologieën in de Nederlandse praktijk	24
4. Succesfactoren en barrières voor de adoptie van PETs	27
5. Conclusies en aanbevelingen	45
5.1 Conclusies	45
5.2 Aanbevelingen	49
5.3 Vervolgonderzoek	52
5.4 Afsluiting	52
5.5 Dankwoord	52
Appendix A. Uitwerking PET use-case	53
Appendix B. Begrippenlijst	56
Appendix C. Afkortingen	57
Appendix D. Lijst geïnterviewde partijen	58

Management samenvatting

Nederland heeft een sterke uitgangspositie in PETs

Uit het uitgevoerde onderzoek blijkt dat Nederland een sterke uitgangspositie heeft in Privacy Enhancing Technologies (PETs). De innovatieinfrastructuur is goed ontwikkeld en kennisinstellingen werken actief aan nieuwe PET-innovaties. Nederlandse PET aanbieders leveren inmiddels technologisch rijpe oplossingen en er bestaan meerdere samenwerkingsnetwerken waarin de technologie wordt toegepast. In de zorg, financiële dienstverlening en de publieke sector neemt PET adoptie langzaam toe. Deze sectoren werken veel met gevoelige persoonsgegevens en lopen bij incidenten tegen grote gevolgen aan. In sectoren als energie, industrie en landbouw is die urgentie kleiner. Daar wordt minder met privacygevoelige data gewerkt en zijn de gevolgen van incidenten vaak minder groot.

Door tegenvallende adoptie van PETs laat EZ onderzoek doen naar de oorzaken

De afgelopen jaren hebben PETs veel aandacht gekregen als nieuwe technologieën om datadelen binnen en tussen organisaties veiliger te maken. PETs bieden mogelijkheden om nieuwe inzichten te genereren door data van meerdere organisaties te combineren, zonder de onderliggende brondata te hoeven delen. Hiermee worden (juridische) drempels voor het delen van data potentieel weg genomen. Ondanks hoge verwachtingen blijft brede adoptie van PETs in Nederland achter bij wat eerder werd voorzien. Om te begrijpen waar dit door komt, heeft het ministerie van Economische Zaken (EZ) onderzoek laten uitvoeren naar de overwegingen, kansen en barrières die organisaties ervaren bij de adoptie van PETs.

Datadeelproblemen en gepercipieerde complexiteit houden adoptie tegen

Hoewel PETs technisch voldoende volwassen lijken, blijft brede adoptie dus achter. Organisaties lopen bij de inzet van PETs tegen dezelfde structurele knelpunten aan die bij datadelen in het algemeen spelen, daarbij zijn PETs niet een “silver bullet” die deze problemen zomaar oplossen. Daarbovenop komt dat PETs vaak als juridisch en technologisch complex worden ervaren. Veel betrokkenen begrijpen niet goed hoe de technologie werkt en/of hoe deze zich verhoudt tot relevante wetgeving, waardoor het lastig blijft om in te schatten of PETs juridisch verantwoord kunnen worden toegepast. Deze combinatie van algemene datadeelproblemen en PET-specifieke complexiteit houdt organisaties terughoudend, zelfs wanneer de technologie veilig en betrouwbaar is.

Bij succesvolle toepassingen is er een business case, goede data, een juridische grondslag en vertrouwen

Succesvolle toepassing van PETs blijkt in de praktijk afhankelijk van vier cruciale randvoorwaarden: (1) een positieve financiële businesscase met een evenredige verdeling van kosten tussen deelnemers, (2) goede kwaliteit van de brondata, (3) een duidelijke juridische grondslag om data te mogen delen en tot slot (4) onderling vertrouwen tussen de verschillende organisaties. Daarnaast komen uit een aantal succesvolle praktijkcases een aantal “enablers” naar voren die de adoptie versterken. Deze organisatorische en samenwerkingsgerichte “enablers” bestaan onder andere uit: heldere governance, duidelijke verdeling van verantwoordelijkheden, het verspreiden van verhalen van succesvolle PET-toepassingen en het hebben van een modern IT-landschap.

Een actieve rol van de overheid draagt ook bij aan de adoptie van PETs

Overheidsfactoren spelen een belangrijke rol bij de adoptie van PETs. Een actieve overheid die PET-oplossingen afneemt, duidelijk voorschriften formuleert over wanneer datadelen met PETs is toegestaan en subsidies richt op toepassing en opschaling (in plaats van alleen onderzoek) versnelt vertrouwen en marktontwikkeling. Daarnaast moet financiering gericht worden ingezet voor maatschappelijke use cases, gecombineerd met sectorgerichte communicatie en implementatiesupport voor domeinen waar adoptie achterblijft. Tenslotte helpt het om aandacht te besteden aan de bescherming van bedrijfsgevoelige informatie, niet alleen aan privacy van personen, zodat organisaties beter kunnen inschatten welke concrete meerwaarde PETs bieden. Samen vormen deze maatregelen gunstige voorwaarden voor bredere en effectievere inzet van PETs.



Introductie

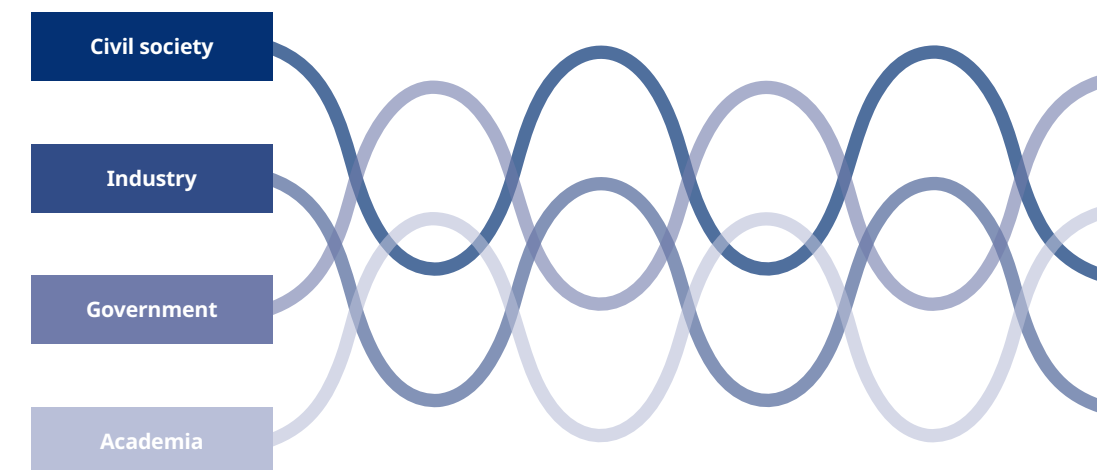
2.1. Aanleiding en context

Inleiding

Wereldwijd groeit sinds 2016¹ de aandacht voor PETs als oplossing voor het veilig delen en benutten van data. Internationale organisaties, zoals de OECD², benadrukken dat deze technologieën niet alleen bijdragen aan privacybescherming, maar ook aan verantwoord datagebruik en maatschappelijk vertrouwen. Deze technologieën omvatten onder meer synthetische data, differential privacy, federated learning, zero-knowledge proofs (ZKP), homomorphic encryption & secure multiparty computation (MPC) en trusted execution environments (TEE). In hoofdstuk 3 zal verder in worden gegaan op deze PET-technologieën.

In Nederland is een groeiend ecosysteem ontstaan waarin kennisinstellingen, bedrijven, overheden en maatschappelijke organisaties elk een eigen rol vervullen (het zogenaamde “quadruple-helixmodel” in figuur 1). Binnen het Nederlandse PET-ecosysteem illustreert dit hoe uiteenlopende initiatieven elkaar versterken en gezamenlijk bijdragen aan innovatie, beleid en maatschappelijke acceptatie van privacy-vriendelijke datatechnologieën.

figuur 1: Quadruple Helix model³



Bron: Oliver Wyman, INNOPAY analyse

¹ OW/INNOPAY analyse

² https://www.oecd.org/en/publications/managing-digital-security-and-privacy-risk_5jlt49ccklt-en.html

³ <https://digicampus.tech/het-quadruple-helix-partnerschap/>

Onderzoek

De ontwikkeling van Privacy Enhancing Technologies (PETs) in Nederland heeft haar oorsprong in de academische en onderzoekswereld. Nederlandse kennisinstellingen, waaronder de Technische Universiteit Eindhoven (TU/e), Technische Universiteit Delft (TUD), Universiteit Twente (UT), Centrum Wiskunde & Informatica (CWI) en de Nederlandse Organisatie voor Toegepast Natuurwetenschappelijk Onderzoek (TNO) behoren tot wereldklasse op zowel fundamentele als toegepaste cryptografische technieken en andere methoden voor veilige gegevensverwerking. Sectorspecifiek speelt Maastrø (onderdeel van Maastricht UMC) een wereldwijde voortrekkersrol in privacy-by-design kankeronderzoek met nieuwe technologische oplossingen. Jarenlange investeringen in fundamenteel en toepast onderzoek bij deze instituten hebben een sterke kennisbasis gelegd voor de valorisatie van Privacy Enhancing Technologies.

Bedrijven

Deze solide kennisbasis vormt de voedingsbodem voor innovatief ondernemerschap. In de tabel hieronder⁴ zijn er een aantal Nederlandse PET aanbieders en infrastructuren te zien. Sommige van de huidige partijen die PETs ontwikkelen zijn ontstaan als directe spin-out van dergelijk onderzoek, zoals Linksight en BluegenAI als spin-offs van TNO en TU Delft. Soms is er een sterke link, zoals Roseman Labs die voortbouwt op open source ontwikkeling vanuit de TU/e, Medical Data Works die nauw samenwerkt met Maastrø Clinics, of Circularise die ontstaan is vanuit het incubatieprogramma Yes!Delft.

Deze bedrijven hebben in Nederland een divers ecosysteem opgebouwd waarin zij uiteenlopende geavanceerde technologische oplossingen (zoals secure multiparty computation, federated learning en synthetische data) aanbieden en inzetten in diverse sectoren in Nederland en steeds meer in het buitenland. Naast deze partijen zien we ook partijen die zelf geen PETs ontwikkelen maar een meer ondersteunende, infrastructurele rol spelen om PET diensten van deze aanbieders gemakkelijk beschikbaar te maken, zoals ZorgTTP, anDREa, Suresync en NLCom.

4 Dit overzicht is mogelijk niet-uitputtend. De auteurs komen graag in contact met andere PET-aanbieders actief op de Nederlandse markt.

PET-aanbieder	Korte beschrijving
Bluegen.AI	Biedt een generiek platform voor het genereren van synthetische data
Branchkey	Biedt een generieke oplossing voor “federated learning as a service”
Circularise	Biedt een oplossing voor digitale product paspoorten gebaseerd op Zero Knowledge Proofs
Linksight	Biedt een generiek platform voor datasamenwerking, gebaseerd op MPC/ Homomorfe Encryptie en Federated Learning
Medical Data Works	Biedt een platform voor medisch onderzoek gebaseerd op Federated Learning
Roseman Labs	Biedt een generiek platform voor datasamenwerking, gebaseerd op MPC/ secret sharing
OASYS NOW	Biedt een platform voor medisch-genetisch onderzoek, waaronder ook modules gebaseerd op Federated Learning en Trusted Execution Environments
Syntho	Biedt een generiek platform voor het genereren van synthetische data

PET-ondersteuner	Korte beschrijving
anDREa	Biedt een veilige softwareomgeving voor gezamenlijk onderzoek, waarbinnen PETs eenvoudig ingezet kunnen worden
NLCom	Biedt datastations waarmee hun klanten PETs eenvoudiger kunnen inzetten
SureSync	Biedt datastations waarmee hun klanten PETs eenvoudiger kunnen inzetten
ZorgTTP	Levert een beheerd datastation waarmee het in PET-datasamenwerkingen optreedt als processor namens 3 ^e partijen.

Aan de vraagzijde zien wij dat PET toepassingen in Nederland vooral gebruikt worden bij zorgorganisaties, in de financiële sector, bij (semi)publieke uitvoeringsinstanties, en door big-tech in hun wereldwijde advertentienetwerken.⁵ PETs worden op dit moment minder toegepast in andere sectoren zoals de energiesector, industrie, logistiek, telecom of landbouw. In de overige hoofdstukken van dit rapport gaan wij hier dieper op in.

5 Buiten scope van dit onderzoek

Overheid

Tegelijkertijd met de opkomst van de PET aanbieders groeit, mede door internationale en Europese ontwikkelingen, ook in Nederland de beleidsmatige aandacht voor PETs. Met de inwerkingtreding en toepassing van de Algemene Verordening Gegevensbescherming (AVG) werden privacy-by-design en dataminimalisatie verplichte uitgangspunten voor systemen en diensten die persoonsgegevens verwerken. Daarnaast is Nederland steeds bewuster van de gevaren van cybercriminaliteit en hacks en is er ook meer nadruk op het veilig omgaan met gevoelige gegevens die geen persoonsgegeven zijn, zoals bijvoorbeeld bedrijfsvertrouwelijke informatie.⁶

De rijksoverheid benadrukt dat verantwoord datagebruik een randvoorwaarde is voor innovatie en economische groei. Zo stelde de Data Agenda Overheid⁷ dat data kunnen bijdragen aan betere publieke dienstverlening, mits organisaties dit doen met behoud van privacy en publieke waarden. Het Strategisch Actieplan voor Artificiële Intelligentie⁸ benoemde het gebruik van sleuteltechnologie die privacy respecteert als randvoorwaarde voor betrouwbare AI-toepassingen. De Strategie Digitale Economie⁹ benadrukte dat veilige datadelen en bescherming van persoonsgegevens cruciale voorwaarden zijn voor een concurrerende en inclusieve digitale economie. Tot slot benoemt de Algemene Inlichtingen- en Veiligheidsdienst (AIVD) dat de inzet van PETs de digitale beveiliging bij gezamenlijke gegevensverwerking kan verhogen.¹⁰

Tegen deze achtergrond positioneerden beleidsmakers PETs als veelbelovende technologieën om de spanning tussen de noodzaak voor datadelen en de behoefte aan bescherming van gevoelige gegevens te overbruggen en nieuwe vormen van datagedreven innovatie mogelijk te maken. Diverse organisaties binnen de overheid hebben dit concreet opgepakt via kennisinfrastructuur, programma's en subsidieregelingen.

Vanuit diverse ministeries heeft de Nederlandse overheid bijgedragen aan het opzetten van verschillende ecosystemen en initiatieven voor de ontwikkeling en toepassing van PETs, waar kennisinstellingen, aanbieders en afnemers bij elkaar komen en kennis uitwisselen. Gezamenlijk versterken zij de nationale capaciteit voor veilig en privacyvriendelijk datadelen. De onderstaande voorbeelden tonen de belangrijkste, mede door de overheid geïnitieerde of gefinancierde initiatieven in dit landschap.

6 Nationaal Coördinator Terrorismebestrijding en veiligheid (2024), Cybersecuritybeeld Nederland 2024
7 <https://zoek.officielebekendmakingen.nl/blg-930354.pdf>
8 <https://publiekdenken.nl/wp-content/uploads/2019/10/RapportSAPAI.pdf>
9 <https://open.overheid.nl/documenten/ronl-c6a3495a523bef54ca41011f629b77b7b611045f/pdf>
10 Algemene Inlichtingen- en Veiligheidsdienst (2025), Databescherming met Privacy Enhancing Technologies

Initiatieven actief in het PETs landschap

Nicpet	Nationaal Innovatie Centrum Privacy Enhancing Technologies wil ervoor zorgen dat er binnen de overheid voldoende kennis en ervaring is om PETs effectief in te zetten. Daarvoor organiseert zij bijeenkomsten, start en begeleid zij praktijkproeven, en deelt ze kennis en resultaten. NICPET wordt gefinancierd door de Ministeries van J&V en BZK. TNO voert het programma uit. ¹¹
CoE-DSC	Center of Excellence Data Sharing & Cloud (CoE-DSC) richt zich op datadelen en soevereine cloud. Als sub-onderdeel van dit grotere programma is er aandacht voor datadelen via PETs. CoE-DSC wordt gefinancierd door het Ministerie van EZ, en het programma wordt uitgevoerd door TNO in samenwerking met marktpartijen INNOPAY, Nimble-Nova en Davinci-Conclusion. ¹²
AIC4NL	AI Coalition for the Netherlands (AIC4NL) richt zich op het verantwoordelijk gebruik van AI. PETs zijn geen specifiek onderdeel van dit programma maar een aantal PET-startups met een AI-focus zijn wel onderdeel van dit ecosysteem, bijvoorbeeld voor match-making tussen startups en potentiële klanten of investeerders. ¹³ AIC4NL wordt gefinancierd door het Nationaal Groeifonds en het Ministerie van EZ en heeft een eigen uitvoeringsorganisatie, in samenwerking met enkele consortiumpartners zoals TNO en SURF. ¹⁴
Brightlands	Brightlands Techruption is een ecosysteem op de Brightlands Smart Services Campus in Heerlen, waarin bedrijven, overheid en kennisinstellingen samenwerken aan data-innovaties. PETs zijn specifiek onderdeel van dit programma. Techruption wordt gefinancierd via een combinatie van deelnemersbijdragen en lokale en nationale publieke financiering. Onderzoekers van TNO en Universiteit Maastricht zijn onderdeel van dit programma. ¹⁵
LIFES	Leiden Institute for FAIR and Equitable Science (LIFES) is een ecosysteem dat zich richt op het veilig beschikbaar maken van data voor onderzoek en innovatie via “data visiting”, zoals Federated/Swarm Learning. LIFES heeft geen directe overheidsfinanciering maar is wel sterk verbonden met diverse publiek gefinancierde onderzoeksprojecten in met name de gezondheidszorg. ¹⁶

Naast deze landelijk opererende initiatieven zijn er ook diverse regionale initiatieven actief waar gebruikt wordt gemaakt van PETs. Met name in de zorg zien de onderzoekers steeds meer “datawerkplaatsen”¹⁷ ontstaan waarin regionale zorgpartijen datagedreven samenwerken aan de uitvoering van het Nationaal Zorgakkoord. Daarin is ook steeds meer aandacht voor het gebruik van PETs.

11 <https://nicpet.pleio.nl/>
12 <https://coe-dsc.nl/>
13 <https://aic4nl.nl/en/>
14 <https://aic4nl.nl/over-ons/onze-organisatie/>
15 <https://www.brightlands.com/en/smart-services-campus/overview-innovation-projects>
16 <https://www.lifes.institute>
17 <https://datawerkplaats.net>

Maatschappelijke organisaties

Naast overheden en kennisinstellingen spelen ook burgers c.q. maatschappelijke organisaties een rol in het kennis-ecosysteem rondom PETs. Zij articuleren een behoefte of zorg, en dragen bij aan de maatschappelijke legitimatie van oplossingen. Bovendien benadrukken zij dat privacybescherming niet enkel een juridische of technische, maar ook een publieke en ethische opgave is.

In Nederland vervult Privacy First een vergelijkbare rol door privacy vriendelijke innovaties maatschappelijk zichtbaar te maken. Via de jaarlijkse Dutch Privacy Awards stimuleert de organisatie de ontwikkeling en toepassing van technologieën die bijdragen aan de bescherming van persoonsgegevens. In zowel 2024 als 2025 werden PET-toepassingen van Roseman Labs bekroond, waarmee de awards de maatschappelijke erkenning van deze technologieën verder hebben versterkt.¹⁸

Ook het ECP, Platform voor de InformatieSamenleving droeg bij aan het vergroten van maatschappelijke aandacht voor PETs. In samenwerking met het ministerie van Binnenlandse Zaken en Koninkrijksrelaties (BZK) organiseerde ECP in 2024 de conferentie: Waardengedreven dialogen — Algoritmen in het openbaar bestuur.¹⁹ Tijdens deze bijeenkomst werd de inzet van PET-technologie besproken vanuit maatschappelijke en ethische perspectieven, met nadruk op publieke waarden zoals vertrouwen, effectiviteit, autonomie en privacy.

Het probleem

Hoewel kennisinstellingen, commerciële partijen, de overheid en maatschappelijke organisaties actief bijdragen aan onderzoek, beleid, marktontwikkeling en maatschappelijke legitimatie van PETs, is brede toepassing in de praktijk nog beperkt. Zoals de op de website van de Digitale Overheid²⁰ wordt gesteld:

“PETs bieden veel voordelen. Toch worden deze technologieën nog niet door iedereen toegepast. Dit komt doordat organisaties onvoldoende weten hoe PETs passen binnen de privacywetgeving en goed bestuur. Ook zijn er organisatorische uitdagingen, zoals het vergroten van draagvlak binnen organisaties.”

18 <https://privacyfirst.nl/privacyawards/>

19 <https://ecp.nl/agenda/conferentie-waardengedreven-dialogen-algoritmen-in-het-openbaar-bestuur/>

20 <https://www.digitaleoverheid.nl/nieuws/roadmap-privacyvriendelijke-dataverwerking/>

In 2024 vond in de Tweede Kamer²¹ een discussie plaats rondom het veilig omgaan met gezondheidsdata. Daarin werd door TNO benadrukt dat PETs al technisch beschikbaar zijn, maar dat beleid, bekendheid en vertrouwen nodig zijn om brede toepassing mogelijk te maken.

Ook EZ benadrukt het belang van PETs als sleuteltechnologie voor veilig en betrouwbaar datadelen en het behoud van privacy in een digitale economie. Tegelijkertijd erkent EZ dat de toepassing in de praktijk nog beperkt blijft en dat de overgang van pilotprojecten naar structurele inzet in de markt en publieke sector langzaam verloopt.

2.2. Doel en onderzoeksvragen

Om beter inzicht te krijgen in de meerwaarde, kansen en belemmeringen rondom de inzet van PETs heeft het ministerie van EZ dit onderzoek laten uitvoeren. Dit onderzoek richt zich op het verkennen van de huidige stand van zaken, de factoren die de adoptie beïnvloeden en de potentiële bijdrage van PETs aan de Nederlandse digitale economie.

Doelstellingen van het onderzoek

Dit onderzoek kent 3 doelstellingen

- 1. De praktische en economische meerwaarde van PETs voor organisaties in Nederland in kaart brengen
- 2. De factoren te identificeren die de brede adoptie van PETs in de Nederlandse markt stimuleren of juist belemmeren
- 3. Op basis van deze bevindingen heldere conclusies te formuleren over de rol en het potentieel van PETs in de Nederlandse context

21 <https://nicpet.pleio.nl/news/view/b3a43d34-8b8b-4a73-ba28-2008bdd698ff/hoe-pets-veilige-inzet-van-gezondheidsdata-mogelijk-maken-freek-bomhof-sprekt-in-tweede-kamer>

Hoofdvraag

De adoptie van PETs wordt bepaald door een complex samenspel van verschillende factoren. Om te begrijpen hoe PETs in Nederland breder toegepast kunnen worden, is inzicht nodig in de kansen die de technologieën bieden, de overwegingen van organisaties en barrières die zij ervaren.

Daarom staat in dit onderzoek de volgende hoofdvraag centraal:

“Welke strategische overwegingen, kansen en barrières beïnvloeden de inzet van PETs door private- en publieke organisaties in Nederland?”

Deelvragen

1. Wat zijn de praktische en economische meerwaarden van PETs voor organisaties in Nederland?
2. Welke succesfactoren dragen bij aan de adoptie van PETs?
3. Welke barrières belemmeren de adoptie van PETs?

2.3. Onderzoeksopzet en methodiek

Onderzoeksopzet

Dit onderzoek combineert kwalitatieve en kwantitatieve methoden om inzicht te krijgen in de toepassingen, meerwaarden, en de adoptie van PETs in Nederland. De aanpak bestaat uit drie hoofdelementen: interviews, kwantitatieve inventarisatie en documentanalyse.

Selectie van PETs en ecosystemen

De eerste stap was het opstellen van een longlist met relevante PET-leveranciers, gebruikers, niet-gebruikers en ecosystemen. Deze lijst is samengesteld op basis van marktrapporten, openbare bronnen en expertise. Vervolgens is uit deze longlist een shortlist geselecteerd voor interviews en nadere analyse.

Dataverzameling

Voor het kwalitatieve deel van het onderzoek zijn half-gestructureerde interviews gehouden met een breed scala aan betrokkenen van de shortlist. De gesprekken richtten zich op praktische ervaringen met PETs, succesfactoren, belemmeringen, businessmodellen en de rol van de overheid bij de adoptie van PETs.

Aanvullend is een enquête verspreid binnen de geselecteerde ecosystemen en andere kanalen zoals LinkedIn. De enquête is aanvullend ingezet om de bevindingen uit de interviews te toetsen en te valideren.

Beperkingen

Bij de interpretatie van de resultaten zijn enkele beperkingen in acht genomen:

- Het aantal respondenten is beperkt, waardoor het beeld niet volledig representatief is voor de gehele markt.
- De interviews betroffen vooral early adopters, en geen “laggards”. Dat geeft een vertekening in de resultaten.
 - Om dat te verminderen zijn ook organisaties bevraagd waarvoor het gebruik van PETs “logisch” te verwachten zou zijn maar die dat in de praktijk (nog) niet toepassen.
- Voor specifieke data, zoals marktomvang, is gebruikgemaakt van externe bronnen.
- De omvang van de enquête-dataset (N=26) was onvoldoende voor statistische analyses. Hierdoor moet de enquête primair worden gezien als steun voor de kwalitatieve bevindingen.

2.4. Leeswijzer

Dit rapport biedt inzicht in de strategische, organisatorische en juridische factoren die de adoptie van PETs door Nederlandse organisaties beïnvloeden. Het rapport is opgebouwd om de lezer stap voor stap van context naar analyse en conclusies te leiden.

Hoofdstuk 2 beschrijft de aanleiding van de opdracht, de centrale onderzoeksvragen en gehanteerde onderzoeksaanpak.

Hoofdstuk 3 geeft een overzicht van de belangrijkste PET-technologieën en actuele toepassingen in verschillende sectoren.

Hoofdstuk 4 presenteert de bevindingen uit interviews en enquêteonderzoek. Hierbij worden zowel adoptiedrivers als zes kern barrières voor de inzet van PETs geanalyseerd.

Hoofdstuk 5 bevat de conclusies van het onderzoek en benoemt aandachtspunten voor mogelijk vervolgonderzoek.



Overzicht van het PET-landschap & stand van zaken in Nederland

3.1. Introductie PETs

PETs bieden een nieuwe manier om veilig en verantwoord met data om te gaan. Ze maken het mogelijk dat organisaties waardevolle inzichten uit gegevens halen, zonder dat de onderliggende ruwe data gedeeld of zichtbaar wordt voor anderen. Daardoor kunnen partijen samenwerken aan analyses en gezamenlijke projecten, terwijl ze voldoen aan wet- en regelgeving en zowel de privacy van individuen als de vertrouwelijkheid van bedrijfsinformatie beschermen.

Er bestaan verschillende typen PETs, elk met hun eigen benadering en toepassingsgebied. Figuur 3 hieronder geeft een sterk versimpeld overzicht van de belangrijkste categorieën en de onderliggende technologieën. In de volgende paragrafen worden deze technieken nader toegelicht en worden relevante use-cases besproken.

figuur 2: Overzicht PET categorieën en de onderliggende technologieën

PETs die nieuwe data genereren



Synthetic Data

Genereert een artificiële dataset met vergelijkbare statistische eigenschappen als de originele dataset



Differential Privacy

Voegt ruis toe aan de originele dataset zodat het moeilijker wordt om originele datapunten te identificeren, terwijl het nog steeds mogelijk is om statistische analyses uit te voeren

PETs die alleen modellen of bewijzen delen



Federated Learning

Creëert een gezamenlijk AI model door het trainen en combineren van locale sub-modellen zonder de onderliggende data te delen



Zero-Knowledge Proofs

Levert een bewijs voor een bepaalde bewering aan, zonder de onderliggende brondata te delen

PETs die data verhullen tijdens het gebruik



Homomorphic Encryption & Secure Multiparty Computation

Maakt het mogelijk om berekeningen uit te voeren op versleutelde data zonder deze eerst te moeten ontsleutelen



Trusted Execution Environment

Maakt het mogelijk om analyses uit te voeren op data die opgeslagen staat in veilige geïsoleerde hardware/software componenten

Ruwe data

Data minimale persoonlijke data

Genereert synthetische data

AI model

Encryptie

Inzichten

Ruis toevoegen

Veilige hardware

Bron: Oliver Wyman, INNOPAY analyse

3.2. Overzicht van PET toepassingen

Synthetische data

Synthetische data zijn kunstmatig gegenereerde datasets die dezelfde structuur en statistische verbanden volgen als de oorspronkelijke data, maar geen herleidbare persoonsgegevens bevatten. De gegevens worden gegenereerd op basis van een AI model dat het oorspronkelijke datapatroon nabootst.

Doordat een synthetische dataset dezelfde opbouw en kenmerken heeft als de brondataset is ze geschikt voor het ontwikkelen, testen en analyseren van modellen zonder dat echte persoonsgegevens of vertrouwelijke informatie worden prijsgegeven. Synthetische data kunnen binnen een organisatie worden gebruikt om bestaande datasets te vergroten ter bevordering van modelontwikkeling en IT-testing, maar kan ook worden toegepast om veilig data te delen met onderzoekers, ketenpartners of andere derden.

Synthetische data voor datadelen in praktijk: onderwijsonderzoek²²

Sinds 2022 stelt DUO (Dienst Uitvoering Onderwijs) synthetische datasets beschikbaar voor onderzoek, naast haar geaggregeerde, anonieme open data. Omdat de oorspronkelijke gedetailleerde onderwijsdata persoonsgegevens van studenten bevat en herleidbare informatie (zoals informatie over diploma's, studiefinanciering en opleidingsroutes), mogen deze data niet rechtstreeks met onderzoekers worden gedeeld. Om onderzoek toch mogelijk te maken genereert DUO op verzoek synthetische datasets die dezelfde statistische kenmerken hebben als de oorspronkelijke data, maar geen herleidbare persoonsgegevens bevatten. Onderzoekers kunnen deze datasets gebruiken voor het trainen van modellen en het creëren van statistische inzichten.

Synthetische data voor intern gebruik in praktijk: Alliander²³

Alliander heeft gedetailleerde verbruiksdata nodig om analyses uit te voeren voor het beheer van het elektriciteitsnet. Deze gegevens zijn echter privacygevoelig en mogen niet vrij binnen de organisatie worden gebruikt. Daardoor is het lastig om intern te experimenteren, nieuwe modellen te ontwikkelen of scenario's te testen zonder in conflict te komen met privacywetgeving.

Door synthetische data te gebruiken kan Alliander realistische datasets genereren die lijken op de oorspronkelijke verbruiksdata, maar geen persoonsgegevens bevatten. Met deze privacyveilige data kan het bedrijf intern analyses en modellen ontwikkelen, terwijl de uitkomsten vrijwel gelijk blijven aan die met echte data en de privacy gewaarborgd blijft.

22 https://duo.nl/open_onderwijsdata/synthetische-data.jsp

23 <https://bluegen.ai/case-studies/alliander/>

Differential Privacy

Differential privacy is een wiskundige methode om te voorkomen dat individuele datapunten kunnen worden herleid uit geaggregeerde data of analyses. De techniek werkt door gerichte ruis (bewuste, willekeurige verstoring van de data) toe te voegen aan een dataset of aan de resultaten van een berekening. Daardoor blijven de algemene patronen en trends in de dataset behouden, maar kunnen eigenschappen van individuele records niet met zekerheid worden geïdentificeerd.

Het uitgangspunt van differential privacy is dat de uitkomst van een analyse nagenoeg hetzelfde blijft, ongeacht of de gegevens van een enkel persoon wel of niet in de dataset zijn opgenomen. Op het moment dat een dataset met en zonder deze persoon erin wordt vergeleken, is niet duidelijk of het verschil in uitkomst komt door de echte gegevens van die persoon, of wordt veroorzaakt door de ruis. Hierdoor kunnen organisaties betrouwbare statistieken en inzichten publiceren, terwijl de privacy van betrokkenen gewaarborgd blijft.

Differential privacy in praktijk: Apple Device Analytics²⁴

Apple past differential privacy toe binnen het programma Device Analytics, waarmee geaggregeerde gebruikersstatistieken worden verzameld zonder individuele gebruikersdata zichtbaar te maken. Op elk apparaat wordt vooraf ruis toegevoegd, waardoor Apple alleen trends op groepsniveau ziet en geen individuele handelingen of voorkeuren kan herleiden.

Deze methode wordt gebruikt om patronen te herkennen in bijvoorbeeld emoji-gebruik, toetsenbordwoorden, zoekopdrachten en stabiliteitsstatistieken van apps. Deze inzichten verbeteren functies zoals autocorrectie, siri-suggesties en zoekresultaten.

Federated learning

Federated Learning is een technologie waarmee meerdere partijen gezamenlijk een model kunnen trainen zonder hun onderliggende data met elkaar te delen. In plaats van dat data naar een centrale locatie wordt gestuurd, wordt het AI- of machine learningmodel lokaal op elke dataset getraind. Alleen de bijgewerkte modelparameters worden vervolgens gedeeld en samengevoegd tot een verbeterd gezamenlijk model.

Op deze manier blijven alle originele gegevens binnen de eigen omgeving van de deelnemende partijen, terwijl de voordelen van samenwerking, zoals betere modellen en representatievere inzichten, behouden blijven. Federated Learning biedt zo een manier om gedistribueerd te leren zonder dat gevoelige data hoeft te worden uitgewisseld.

²⁴ https://images.apple.com/privacy/docs/Differential_Privacy_Overview.pdf

Federated Learning in praktijk: Personal Health Train (PHT)²⁵

Maastricht UMC leidde een consortium van acht instellingen in vijf landen dat via de PHT infrastructuur een model voor overlevingskansen bij longkanker ontwikkelde. Door middel van Federated Learning konden onderzoekers inzichten genereren uit de data van meer dan 20.000 patiënten verspreid over 8 ziekenhuizen in verschillende landen, zonder dat die ziekenhuizen hun patiëntdata met de onderzoekers of elkaar hoefden delen.

In dit model blijft brondata binnen de IT omgeving van elke deelnemende zorginstelling; alleen het algoritme werden tussen de verschillende instellingen gedeeld om getraind te worden. De lokale resultaten worden vervolgens samengevoegd tot één gezamenlijk model, wat daarmee gebaseerd is op inzichten uit de data van alle deelnemende zorginstellingen.

Zero-knowledge proofs (ZKP)

Zero-knowledge Proofs zijn cryptografische technieken waarmee iemand kan bewijzen dat een bewering waar is, zonder de onderliggende gegevens te onthullen. Een partij kan dus aantonen dat zij over bepaalde informatie beschikt, of dat een berekening correct is uitgevoerd, zonder die informatie prijs te geven.

De werking is gebaseerd op wiskundige constructies waarbij een “bewijs” wordt gegenereerd dat alleen geldig kan zijn als de oorspronkelijke bewering klopt. De ontvangende partij hoeft alleen dat bewijs, en niet de ruwe data te zien om te verifiëren dat de claim juist is.

Zero Knowledge Proofs in praktijk: Samsonite Circular Collection²⁶

Samsonite introduceerde een limited edition circular koffercollectie met een Digital Product Passport (DPP) om de herkomst en traceerbaarheid van materialen inzichtelijk te maken. Hierbij wordt gebruikgemaakt van Zero Knowledge Proofs (ZKP), waarmee leveranciers kunnen aantonen waar hun materialen vandaan komen of dat ze voldoen aan vastgestelde herkomstcriteria, zonder hun onderliggende bedrijfsgevoelige data te delen.

Dankzij ZKP's blijft detailinformatie, zoals exacte samenstelling of leveranciersgegevens, bij de bron, terwijl alleen cryptografisch verifieerbare bewijzen binnen het DPP worden gedeeld. Zo kan Samsonite betrouwbare en verifieerbare informatie over materiaalherkomst aan consumenten aanbieden, met behoud van vertrouwelijkheid binnen de toeleveringsketen.

²⁵ <https://pubmed.ncbi.nlm.nih.gov/31911366/>

²⁶ <https://www.circularise.com/case-studies/samsonite-circularise>

Secure Multiparty Computation: Secret Sharing & Homomorphic Encryption

Secure Multi-Party Computation is een verzamelnaam voor cryptografische methoden waarmee partijen berekeningen kunnen uitvoeren op gezamenlijke data, terwijl die data zelf onleesbaar (versleuteld) blijft tijdens de berekeningen. Binnen deze groep zijn Secret Sharing en Homomorfe Encryptie de bekendste varianten. Bij Secret Sharing wordt een dataset in drie onleesbare stukken opgeknipt, de zogenaamde “shares”. Deze shares bevatten afzonderlijk geen betekenisvolle informatie. Elke share wordt bij een andere partij geplaatst. Deze partijen kunnen nu gezamenlijk berekeningen uitvoeren over de drie shares, zonder dat één van deze partijen de onderliggende data kan inzien. De uitkomsten van de berekening kunnen vervolgens worden vrijgegeven. Bij Homomorfe Encryptie wordt een dataset op een speciale manier versleuteld, zodat de data onleesbaar is, maar er wel berekeningen op kunnen worden uitgevoerd. Hierdoor kan homomorf versleutelde data gedeeld worden binnen een datasamenwerking, en kunnen partijen daar onderling berekeningen op uitvoeren. Ook hier kan geen van de partijen de brondata lezen, en wordt er vervolgens een eindresultaat vrijgegeven.

MPC in praktijk: cyberdreigingen delen via secret sharing²⁷

Digitale dreigingen, zoals ransomware-aanvallen, zijn een toenemend probleem voor Nederlandse bedrijven en overheden. Organisaties zijn van nature zeer terughoudend om actuele incidentinformatie te delen. Het Nationaal Cyber Security Centrum (NCSC) biedt met SecureNed-initiatief een manier om deze gevoelige informatie veilig te kunnen uitwisselen, zodat cyberdreigingen sneller kunnen worden opgespoord en aangepakt. Doordat SecureNed gebruik maakt van secret sharing kunnen organisaties veilig meldingen doen zonder directe details prijs te geven. De uitwisseling van geanonimiseerde inzichten stelt het NCSC in staat om sneller trends en potentiële acties te identificeren, waardoor de algehele cyberweerbaarheid van Nederlandse organisaties aanzienlijk toeneemt en cybercrime netwerken sneller kunnen worden opgerold. Inmiddels delen meer dan 100 organisaties structureel cyberrisico-informatie via SecureNed.

MPC in praktijk: valrisico voorspellen met Homomorfe Encyptie²⁸

Zorgorganisaties beschikken elk over slechts een deel van de informatie die nodig is om valrisico's bij ouderen goed te kunnen voorspellen. Thuiszorg- en verpleeghuisorganisaties registreren wel of iemand is gevallen, maar vaak niet of (en wat voor) letsel er was. Ziekenhuizen registreren juist alleen met welk letsel patiënten worden opgenomen, maar registreren niet of, en onder welke omstandigheden de val heeft plaatsgevonden. Deze gescheiden datastromen maken het moeilijk om een volledig beeld te vormen en transmuraal beleid te formuleren om de ziektelast en kosten door vallen effectief te verminderen.

In deze toepassing worden twee datasets samengevoegd:

1. Thuiszorg/verpleeghuisdata: registraties van gevallen/niet gevallen
2. Ziekenhuisdata: binnen 24 uur opgenomen patiënten met valgerelateerd letsel

Door deze informatie te koppelen, ontstaat inzicht in welke cliënten en zijn gevallen en letsel hebben opgelopen. Op basis daarvan kan een voorspelmodel worden getraind dat kenmerken identificeert van cliënten met een verhoogd risico op ziektelast door vallen. Zo wordt het mogelijk om risico's beter te voorspellen en preventieve maatregelen eerder te nemen, zonder dat gevoelige persoonsgegevens tussen organisaties worden uitgewisseld.

Trusted Execution Environments (TEE)

Trusted Execution Environments zijn afgeschermd delen binnen een computer of server waarin data veilig kan worden verwerkt, los van het reguliere besturingssysteem. Binnen een TEE worden berekeningen uitgevoerd in een beveiligde hardware omgeving die is geïsoleerd van de rest van het systeem. Hierdoor is de data beschermd tegen toegang door gebruikers, applicaties of systeembeheerders.

De werking van een TEE berust op fysieke (hardware-matige) isolatie. Gevoelige gegevens en berekeningen worden verwerkt in een afgesloten omgeving. In die omgeving is een geheime (private) sleutel opgeslagen, die geen enkele partij kent. Data die naar de TEE wordt verzonden, wordt versleuteld met een publieke sleutel, waarna de TEE deze ontsleutelt met een interne private sleutel om veilige operaties uit te voeren. Resultaten worden opnieuw versleuteld met de publieke sleutel voordat ze de TEE verlaten, zodat ze alleen toegankelijk zijn voor bevoegde partijen. Omdat zelfs de partijen die de server waarop de TEE staat beheren geen toegang hebben tot wat er binnenin de TEE gebeurt, is het bij TEE's erg belangrijk dat bewijs wordt geleverd waarmee aangetoond kan worden welke handelingen binnen de TEE daadwerkelijk zijn uitgevoerd, zoals digitale handtekeningen en rapportages.

²⁷ <https://rosemanlabs.com/en/blogs/secureded-important-building-block-for-public-private-information-sharing>

²⁸ <https://datawerkplaats.net/2025/06/11/opsporen-valrisico-en-verminderen-valletsel-bij-ouderen/>

TEE in praktijk: vertrouwelijke verwerking van geolocatiedata van telecomaanbieders²⁹

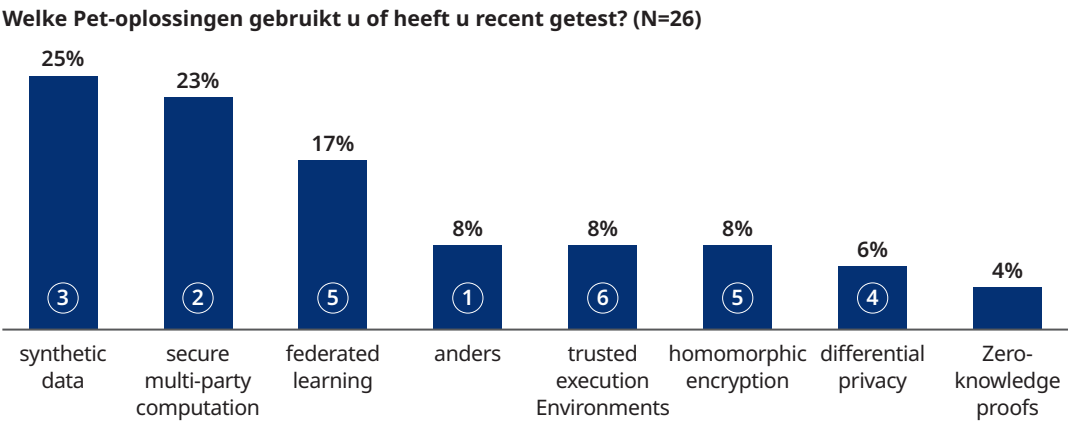
Eurostat werkte samen met Cybernetica AS aan de veilige verwerking van locatiegegevens uit data van mobiele netwerkaanbieders. Met deze gegevens kunnen verplaatsingspatronen van mensen worden geanalyseerd voor statistische doeleinden. De verwerking vond plaats binnen een Trusted Execution Environment (TEE), een beveiligde hardware omgeving op een server waarin data tijdelijk ontsleuteld en verwerkt kan worden zonder dat systeembeheerders of andere partijen toegang hebben tot de zeer gevoelige ruwe informatie.

De TEE fungeerde hier als vertrouwde verwerkingsomgeving, niet als samenwerkingsplatform tussen partijen. Mobiele aanbieders leverden gepseudonimiseerde datasets die binnen de TEE werden geanalyseerd om geaggregeerde mobiliteitsstatistieken te genereren. Zo konden Eurostat en nationale statistiekbureaus betrouwbare analyses uitvoeren op telecomdata, terwijl persoonsgegevens beschermd bleven.

3.3. Dominante PET-technologieën in de Nederlandse praktijk

Uit de voor dit onderzoek uitgevoerde survey blijkt dat in de Nederlandse praktijk vooral Secure Multi-Party Computation, Synthetische Data, en Federated Learning actief worden toegepast. Dit beeld wordt bevestigd in figuur 4, waarin zichtbaar is dat deze drie technologieën het vaakst worden gebruikt of getest en het meest worden aanbevolen aan collega's/andere organisaties. Daarmee vormen zij op dit moment de kern van het Nederlandse PET-landschap.

figuur 3: Recent gebruikte of geteste PET-oplossingen

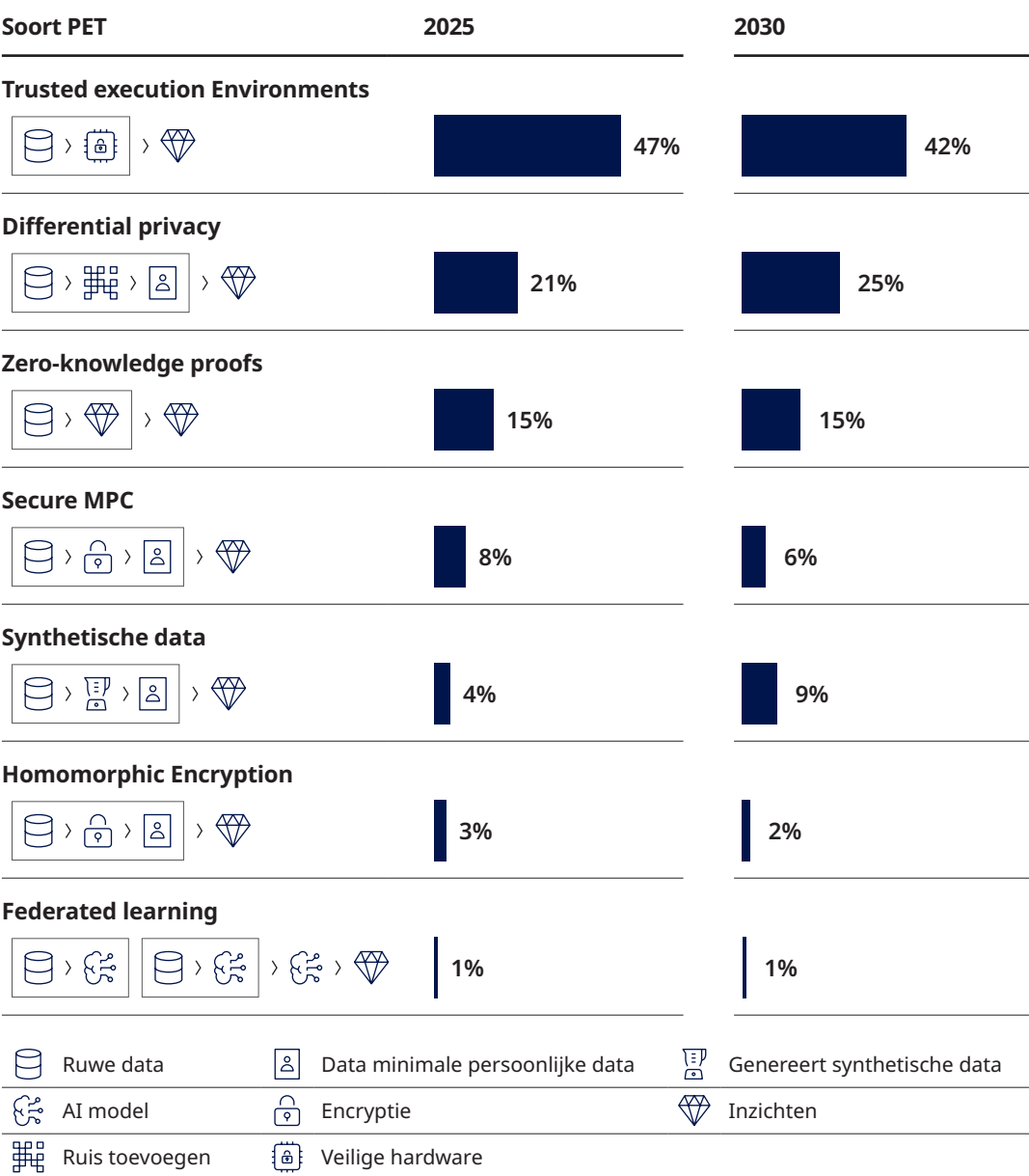


Cijfers geven weer in welke volgorde respondenten de PET zouden aanbevelen (1 = meest aanbevolen, 6 = minst aanbevolen)
Bron: Oliver Wyman, INNOPAY analyse

29 <https://cros.ec.europa.eu/project-ESTAT-2019-0232>

Er bestaan verschillende typen PETs, elk met hun eigen benadering en toepassingsgebied. Figuur 3 hieronder geeft een sterk versimpeld overzicht van de belangrijkste categorieën en de onderliggende technologieën. In de volgende paragrafen worden deze technieken nader toegelicht en worden relevante use-cases besproken.

figuur 4: Marktanalyse van het gebruik van PETs wereldwijd³⁰



Bron: Oliver Wyman, INNOPAY analyse

30 INNOPAY analyse, Grandviewresearch, Mordor Intelligence, Precendence Research, MarketsandMarkets, Nextmsc



Succesfactoren en barrières voor de adoptie van PETs

De belangstelling voor PETs is de afgelopen jaren toegenomen. Deze technologieën maken het mogelijk om data te delen en te analyseren op een manier die zowel de privacy van personen als de vertrouwelijkheid van bedrijfsinformatie waarborgt. Daarmee bieden ze belangrijke kansen voor samenwerking in sectoren waar datadelen nu nog gevoelig of risicovol is.

Toch blijft de daadwerkelijke toepassing in de praktijk achter bij de verwachtingen die onderzoekers, PET-aanbieders en beleidsmakers hadden. Dit betreft impliciete, persoonlijke verwachtingen en niet duidelijk geformuleerde beleidsverwachtingen. Tijdens dit onderzoek vonden wij geen aanwijzingen om aan te nemen dat Nederland daadwerkelijk achterloopt ten opzichte van het buitenland, er heerst bij de geïnterviewde partijen met name het “sterke gevoel” dat Nederland zijn goede uitgangspositie niet voldoende te gelde weet te maken en dat PETs hun belofte nog niet op de schaal hebben kunnen waarmaken die zij zelf verwacht hadden.

In veel sectoren worden pilots en verkenningen uitgevoerd, maar slechts een beperkt aantal initiatieven leidt tot structurele toepassingen. Met structurele toepassingen bedoelen we gebruik van PETs waarbij minimaal aan de volgende criteria wordt voldaan:

-
1. Er wordt gebruik gemaakt van echte gevoelige gegevens
 2. Er wordt gebruik gemaakt van productie-software in een productie-omgeving
 3. De uitkomsten uit de analyses worden daadwerkelijk gebruikt in bedrijfsprocessen
 4. Er wordt structureel betaald voor gebruik van de software, bijvoorbeeld in de vorm van een licentie
-

De kloof tussen technologische mogelijkheden en brede adoptie heeft meerdere oorzaken. Soms ligt de uitdaging in technische complexiteit, maar vaker spelen organisatorische of juridische factoren een grotere rol.

“De technologie is al heel ver doorontwikkeld, maar de markt worstelt nog. Nederland had op een heel ander punt kunnen zijn qua adoptie.”

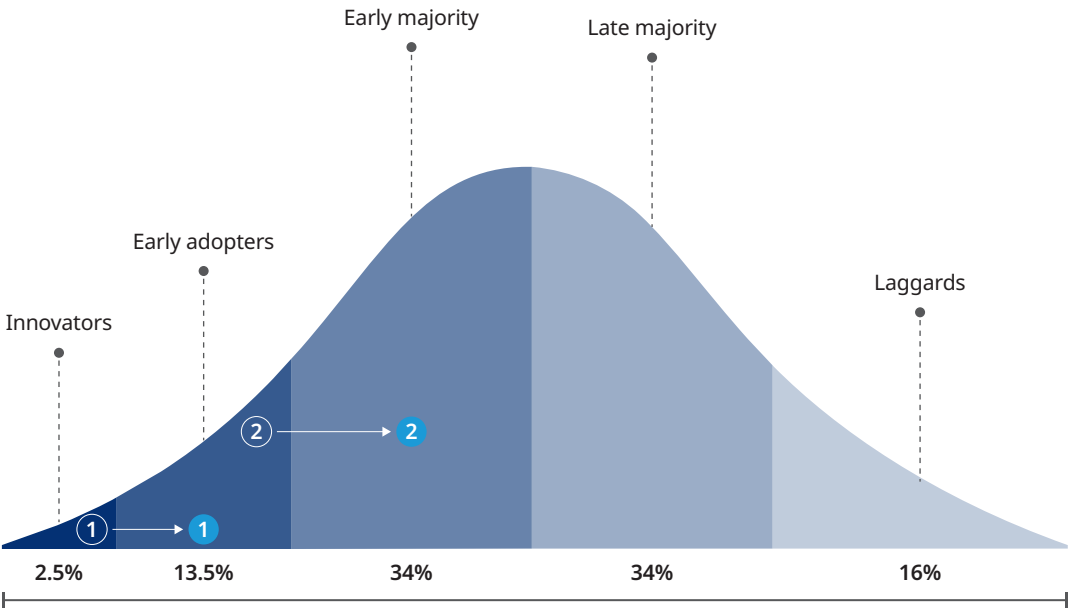
In de volgende paragrafen worden succesfactoren en barrières nader uitgewerkt. Daarbij wordt onderscheid gemaakt tussen zes aspecten die de adoptie van nieuwe technologieën beïnvloeden. Deze aspecten sluiten aan bij het diffusion of innovation-model³¹ (figuur 5), dat beschrijft hoe innovaties zich verspreiden van een kleine groep innovators naar een bredere groep gebruikers. Het gaat hier om vijf aspecten uit het model en één extra aspect, dat wij hebben toegevoegd op basis van onze waarnemingen uit interviews:

1. **Ervaren meerwaarde:** de adoptie neemt toe wanneer organisaties een duidelijke praktische, economische of strategische meerwaarde ervaren.
2. **Aansluiting op bestaande werkwijzen:** de adoptie neemt toe wanneer de nieuwe technologie goed past binnen bestaande processen, systemen en manieren van werken.
3. **Complexiteit:** de adoptie wordt vertraagd wanneer een technologie als complex, moeilijk of risicovol wordt ervaren.
4. **Mogelijkheid om te experimenteren:** de adoptie neemt toe wanneer organisaties laagdrempelig kunnen experimenteren
5. **Zichtbaarheid van resultaten:** de adoptie neemt toe wanneer succesvolle voorbeelden zichtbaar zijn en de impact van de technologie aantoonbaar wordt.
6. **Cultuur van samenwerking en adoptie (additionele factor):** de adoptie neemt toe wanneer er een open samenwerkingscultuur is, vertrouwen tussen partijen en bereidheid om data te delen. Dit is een aanvullende factor op het model, die in Nederland sterk bepalend lijkt.

31 https://www.academia.edu/1988400/Diffusion_of_innovations_by_Everett_Rogers_1995_

De zes aspecten helpen te verklaren waar in deze adoptiecurve PETs zich momenteel bevinden. In Nederland lijkt PET-adoptie zicht te bewegen van de fase van innovators richting early adopters. In domeinen zoals zorg en cybersecurity is de adoptie al verder ontwikkeld; deze domeinen bewegen richting de fase van de early majority.

figuur 5: het diffusion of innovation-model



- 1 De algemene trend duidt erop dat PET-adoptie nu van innovators naar early adopters gaat
- 2 Op basis van interviews stellen wij vast dat de adoptie in specifieke zorg- en cybersecuritycases sneller verloopt en er minder innovatieve partijen deel nemen

Bron: Oliver Wyman, INNOPAY analyse

Uit de analyse komen uiteenlopende knelpunten naar voren die de adoptie van PETs vertragen. Het tegenovergestelde is doorgaans ook waar: Wanneer deze factoren juist positief aanwezig zijn, fungeren zij als succesfactoren die de adoptie van PETs kunnen versnellen. Deze knelpunten sluiten nauw aan bij de zes eerder beschreven adoptie aspecten. De tabel hieronder geeft een overzicht van de belangrijkste belemmeringen genoemd door de respondenten, geordend naar deze zes aspecten.

Aspect van adoptie	Geconstateerde barrières
1. Ervaren meerwaarde	A. De urgentie voor “extra veilig” datadelen wordt in veel organisaties nog onvoldoende gevoeld B. Onduidelijke businesscases maken het moeilijk om de waarde van PETs te bepalen C. PETs leveren vaak maatschappelijke meerwaarde, maar bieden dan beperkte directe prikkels voor individuele organisaties D. Kosten voor PETs worden hoog ingeschat en ongelijk verdeeld binnen en tussen organisaties
2. Aansluiting op bestaande werkwijze	A. Lage digitaliseringsgraad en verouderde IT-systemen maken het technisch moeilijk om PET-oplossingen toe te passen B. Organisaties hebben moeite om PET resultaten te interpreteren en te vertalen naar bruikbare inzichten en acties C. Traditionele werkprocessen staan effectieve toepassing van PETs in de weg D. Organisaties spreken verschillende data-talen, zeker wanneer datasamenwerking cross-sectoraal is
3. Complexiteit	A. Uiteenlopende juridische kaders vergroten onzekerheid en terughoudendheid B. Gebrekkige kennis bij sleutelpersonen binnen organisaties remt draagvlak voor PETs C. Cross-sectoraal samenwerken creëert extra governance- en afstemmingscomplexiteit
4. Mogelijkheid om te experimenteren	A. Hoge coördinatielast tussen partijen maken pilots moeilijk uitvoerbaar B. Koudwatervrees en voorkeur voor gecontroleerde omgevingen beperken de uitvoering van pilots in operationele setting C. Onderzoeksgerichte subsidies stimuleren het opdoen van kennis, maar niet de praktische, snelle experimenten met toepassingen van PETs
5. Zichtbaarheid van resultaten	A. Beperkt zicht op succesvolle praktijkcases remt adoptie van PETs, met name in het publieke domein B. Zelfbouw van PET toepassingen door overheden belemmert adoptie en zichtbaarheid van bestaande oplossingen
6. Cultuur van samenwerking en adoptie	A. De Nederlandse focus op gezamenlijke innovatie vertraagt de adoptie van kant-en-klare oplossingen

Hieronder volgt een nadere toelichting van de zes aspecten die adoptie beïnvloeden, en de bijbehorende barrières die adoptie belemmeren die wij hebben geïdentificeerd in ons onderzoek.

1. Ervaren meerwaarde

De ervaren meerwaarde verwijst naar de mate waarin organisaties PETs zien als een duidelijke verbetering ten opzichte van hun huidige werkwijze voor datadelen en data-analyse. PETs bieden in theorie meerdere voordelen: ze maken samenwerking mogelijk zonder gevoelige gegevens te delen, versterken de naleving van privacywetgeving en ondersteunen het principe van dataminimalisatie zoals vastgelegd in de AVG.³² Bovendien maken PETs het mogelijk om vertrouwelijke of voorheen ontoegankelijke data te benutten, wat kan leiden tot nieuwe inzichten, innovatie en efficiëntere samenwerking.

In de praktijk is de meerwaarde echter niet altijd direct zichtbaar of overtuigend voor alle betrokken partijen. De inzet van PETs wordt pas aantrekkelijk wanneer de verwachte baten duidelijk opwegen tegen de benodigde investeringen. De volgende barrières verhinderen een positieve uitkomst van deze kosten-batenafweging bij veel organisaties.

A. De urgentie voor “extra veilig” datadelen wordt in veel organisaties nog onvoldoende gevoeld

Bestaande beveiligingsmaatregelen worden vaak als voldoende beschouwd om aan wettelijke verplichtingen te voldoen. Zolang er geen concrete incidenten of formele verplichtingen zijn, ontbreekt de druk om te investeren in aanvullende technologieën zoals PETs. Daarnaast speelt mee dat de verantwoordingsdruk, de mogelijkheid om organisaties of bestuurders daadwerkelijk aan te spreken op het zorgvuldig omgaan met gevoelige data, vaak beperkt is. Zonder duidelijke prikkels, toezicht of afrekenbaarheid blijft de urgentie laag en verschuift de aandacht naar andere prioriteiten binnen organisaties.

“Als je bestuurders niet afrekent op veiligheid van data, gebeurt er ook niets.”

³² https://autoriteitpersoonsgegevens.nl/uploads/imported/verordening_2016_-_679_definitief.pdf

B. Onduidelijke businesscases maken het moeilijk om de waarde van PETs te bepalen

PETs missen vaak een overtuigende financiële business case voor datadelen tussen alle betrokken organisaties. In samenwerkingen met meerdere partijen is de verdeling van kosten en baten regelmatig ongelijk: degene die data levert haalt niet altijd direct voordeel uit de inzichten die daaruit ontstaan. Veel PET-toepassingen bevinden zich nog in een vroege fase van commercialisatie, hun concrete meerwaarde in termen van efficiëntie, risicoreductie of nieuwe verdienmodellen is nog onvoldoende aangetoond. Zolang deze baten niet duidelijk zijn, is het moeilijk om een onderling verrekenmodel te vinden om partijen aan te sluiten voor wie de meerwaarde niet evident aanwezig is, en komen veel projecten niet van de grond.

“Vaak investeert een andere partij dan degene die uiteindelijk de voordelen behaalt. Deze mismatch in de verdeling van kosten en baten doet zich niet alleen bij PETs voor, maar bij veel initiatieven voor datasamenwerking.”

C. PETs leveren vaak maatschappelijke meerwaarde, maar bieden dan beperkte directe prikkels voor individuele organisaties

Zeker in omgevingen waar opbrengsten indirect of collectief zijn, is de commerciële haalbaarheid van PETs niet vanzelfsprekend. Veilig datadelen binnen en tussen sectoren kan aanzienlijke maatschappelijke meerwaarde opleveren. Toepassingen van PETs kunnen bijdragen aan betere dienstverlening, meer transparantie of effectievere fraudepreventie. Deze opbrengsten zijn echter vaak publiek of collectief van aard en vertalen zich niet zonder meer in tastbare voordelen voor individuele organisaties.

Voor veel partijen wegen de kosten en inspanningen om data toegankelijk te maken en te investeren in gezamenlijke PET-oplossingen niet op tegen de voordelen die zij zelf direct ervaren. Organisaties die de meeste inspanning moeten leveren voor deze maatschappelijke baten, bijvoorbeeld door databronnen open te stellen of governance te organiseren, zien zelden directe financiële baten terug. Daardoor ontbreekt vaak de prikkel om actief deel te nemen, ook wanneer het maatschappelijke belang groot is. Wanneer organisaties wel een directe financiële meerwaarde zien, verandert dit beeld. In zulke gevallen blijkt het doorgaans vooral een kwestie van onderhandelen over kosten, baten en verantwoordelijkheden. Partijen weten hier meestal goed uit te komen en de samenwerking tot stand te brengen.

“Banken hebben geen direct belang bij het bestrijden van zorgfraude. Het delen van data voor zorgfraudeonderzoek zien zij als een extra risico en als een kostenpost waarvan de directe baten voor hen beperkt zijn.”

D. Kosten voor PETs worden hoog ingeschat en ongelijk verdeeld binnen en tussen organisaties

Niet alleen de totale kosten spelen een rol bij de adoptie van PETs, maar vooral ook de perceptie van deze kosten en hoe deze kosten gedragen worden. Hoewel de PET-oplossingen door aanbieders vaak als relatief betaalbaar worden gepositioneerd, ervaren organisaties de kosten verschillend. Voor sommige grote organisaties vallen de kosten mee, terwijl kleinere organisaties dezelfde bedragen als zwaar belastend zien.

“PETs worden over het algemeen als relatief goedkoop gezien, maar betaalbaarheid hangt sterk van de organisatiegrootte af: €25,000-30,000 per jaar is voor een ziekenhuis makkelijk te dragen, maar voor een huisartsenpraktijk is dat onhaalbaar.”

De grootste kosten van een PET-traject zitten niet in de licenties of technologie zelf, maar in het interne werk om de oplossing operationeel te maken. Dit omvat afstemming en inzet van IT-, data-science-, security-, juridische- en privacy-teams evenals het opzetten van een governancestructuur.

Op totaalniveau kan de investering in PETs beperkt lijken, maar zodra de uitgave uit een specifiek budget moet komen (bijvoorbeeld IT, business of innovatie) wordt deze al snel als duur ervaren. Bovendien vloeien de baten vaak verspreid terug naar meerdere afdelingen. Daardoor blijft de waargenomen meerwaarde laag, zelfs wanneer de werkelijke kosten relatief beperkt zijn.

“Een belangrijk knelpunt is wie de licentiekosten voor PETs draagt. Nu wordt dat op projectniveau geregeld, terwijl de licentie voor de hele organisatie relevant kan zijn. Door die projectmatige kostentoedeling beginnen veel partijen hier liever niet aan.”

2. Aansluiting op bestaande werkwijze

Een tweede belangrijke factor voor de adoptie van PETs is de mate waarin de technologie aansluit op bestaande werkwijzen, processen en juridische kaders. PETs bieden in theorie kansen om binnen die bestaande structuren gevoelige data te benutten zonder ze te delen en daarmee de naleving van privacywetgeving en dataminimalisatie te versterken.

In de praktijk blijkt die aansluiting echter niet vanzelfsprekend. Organisaties verschillen sterk in hun juridische bevoegdheden, processen en digitale volwassenheid, waardoor PETs moeilijk inpasbaar zijn in de dagelijkse praktijk. Dit beperkt het gebruik, zelfs wanneer de technologie technisch betrouwbaar en juridisch goedgekeurd is.

A. Lage digitaliseringsgraad en verouderde IT-systemen maken het technisch moeilijk om PET-oplossingen toe te passen

De inzet van PETs vereist een bepaald niveau van digitalisering: brondata moeten kwalitatief, betrouwbaar, gestandaardiseerd, en technisch toegankelijk zijn. In veel sectoren ontbreekt die basis nog. Versnipperde databases en lage datakwaliteit bemoeilijken de integratie van PET-oplossingen. De technologie werkt het meest effectief wanneer organisaties beschikken over moderne data infrastructuur en heldere processen voor databaseer. Daarnaast zijn ook moderne IT-systemen nodig voor effectieve toepassing van PETs. De wijdverbreide aanwezigheid van legacy IT-systemen binnen organisaties verhindert versnelde adoptie.

“De ketens waar wij mee werken zijn nog vaak op on-prem-systeemniveau, de digitale volwassenheid en datavolwassenheid zijn onvoldoende om PETs breed toe te passen.”

B. Organisaties hebben moeite om PET resultaten te interpreteren en te vertalen naar bruikbare inzichten en acties

Veel organisaties kunnen de uitkomsten van PET-toepassingen nog niet goed interpreteren of vertalen naar concrete acties. Dat heeft meerdere oorzaken. Ten eerste ontbreekt in veel organisaties nog een datagedreven manier van werken: er zijn geen rollen, processen of verantwoordelijkheden ingericht om nieuwe informatiestromen te benutten. Ten tweede ontbreekt vaak de benodigde kennis en capaciteit om PET-resultaten te analyseren en om te zetten in bruikbare inzichten.

De prikkel om in PETs te investeren ontbreekt bij organisaties die zelf weinig directe en meetbare voordelen ervaren van datadelen. Bestaande werkprocessen zijn niet afgestemd op het verwerken van andere typen informatie, en er is weinig organisatorische wendbaarheid om de benodigde veranderingen door te voeren. Als gevolg blijft de potentiële waarde van PETs vaak onbenut en zien organisaties weinig aanleiding om datadelen actief te ondersteunen.

“Veel kleinere organisaties hebben geen data-scientist in dienst. Daardoor ontbreekt de capaciteit om datasets te analyseren en te vertalen naar bruikbare inzichten, waardoor de potentiële waarde van datadelen of PET-toepassingen onbenut blijft.”

C. Traditionele werkprocessen staan effectieve toepassing van PETs in de weg

Binnen organisaties is te zien dat medewerkers gewend zijn om gegevens op een bepaalde manier te registeren en deze werkwijze het liefst behouden. In sectoren zoals de zorg wordt informatie vastgelegd op een wijze die niet bedoeld of gericht is op hergebruik of analyse. Dit leidt tot wisselende datakwaliteit en maakt PET-toepassingen afhankelijk van brondata die niet altijd uniform of gestructureerd is. De opkomst van AI voor dataverwerking (bijv. AI-assistenten die een verslag schrijven van een medisch consult) kan helpen bij het verhogen van de datakwaliteit zonder veel extra administratieve last te creëren.

“Ik heb wel eens te horen gekregen van een arts: ik registreer uitsluitend voor de directe patiëntenzorg en niet met het oog op later hergebruik, een dure infrastructuur verandert daar niets aan.”

D. Organisaties spreken verschillende data-talen, zeker wanneer datasamenwerking cross-sectoraal is

Tussen sectoren en zelfs binnen een sector bestaan grote verschillen in terminologie, definities en registratiestandaarden voor datapunten. Hierdoor sluiten datasets inhoudelijk niet vanzelf op elkaar aan, ook wanneer ze over vergelijkbare processen gaan.

Deze variatie is het gevolg van jarenlang gegroeide werkprocessen, systemen en gewoontes. Organisaties zijn gewend aan hun eigen manier van registreren en hechten waarde aan hun eigen vertrouwde datamodel. Daardoor kost het tijd en inspanning om overeenstemming te bereiken over wat bepaalde variabelen betekenen.

“Het spreken van verschillende data-talen is een van de grote uitdagingen. Neem bijvoorbeeld een veld met de behandelstatus: daarvoor is eenduidige definitie en standaardisatie nodig. In één dataset ontbrak de kolomtitel en stonden cellen alleen gevuld met een streepje of met de zin ‘patiënt naar huis’. Voor het eigen zorgpersoneel is dat begrijpelijk, maar voor externe partijen is onduidelijk wat zulke notaties precies betekenen.”

3. Complexiteit

De ervaren complexiteit van PETs vormt een belangrijke factor die de adoptie vertraagt. Die complexiteit zit niet primair in de technologie zelf, want PETs zijn inmiddels volwassen, gebruiksvriendelijk en technisch betrouwbaar. De complexiteit ligt vooral in het begrijpen van de technologie en organisatorische en juridische randvoorwaarden voor implementatie.

A. Uiteenlopende juridische kaders vergroten onzekerheid en terughoudendheid

Een belangrijke belemmering voor de toepassing van PETs is dat organisaties binnen uiteenlopende juridische kaders kunnen opereren die verschillen in grondslag en bevoegdheden. Zelfs binnen één sector variëren regels en verantwoordelijkheden, bijvoorbeeld over het bewerken, combineren of delen van data, waardoor juridische compatibiliteit vaak beperkt is. Interpretaties van wat juridisch is toegestaan lopen per organisatie uiteen. Die onzekerheid leidt tot terughoudendheid en kan ertoe leiden dat partijen helemaal afzien van samenwerking, ook wanneer technische oplossingen beschikbaar zijn.

Tussen sectoren bestaan bovendien verschillende wetten en toezichtkaders (zoals de Wet op het financieel toezicht en de Zorgverzekeringswet). Elk domein kent eigen regels, terminologie en procedures, wat cross sectorale afstemming extra complex maakt. PETs kunnen deze verschillen deels overbruggen, maar ze vervangen niet de noodzaak om duidelijke, gezamenlijke afspraken te maken over verantwoordelijkheden, juridische grondslag en governance.

Deze juridische onduidelijkheid versterkt de terughoudendheid, vooral wanneer privacygevoelige informatie wordt gedeeld. Partijen vrezen juridische consequenties en kiezen daarom vaak voor geen datadelen, ook al zijn PETs bedoeld om veilige datadelen binnen bestaande juridische grenzen mogelijk te maken.

“Zorgverzekeraars vinden het juridisch risicovol om data van verzekerden te analyseren, ook wanneer die data geanonimiseerd beschikbaar is. Juristen geven niet altijd hetzelfde advies, waardoor bestuurders huiverig zijn omdat zij zelf aansprakelijk kunnen worden gesteld door toezichthouders.”

B. Gebrekkige kennis bij sleutelpersonen binnen organisaties remt draagvlak voor PETs

Binnen veel organisaties is de kennis over PETs nog beperkt en versnipperd. Vaak kennen alleen enkele specialisten de technologie en de mogelijkheden ervan. Personen in sleutelrollen (bijv. juristen, privacy officers, managers of directieleden) hebben doorgaans weinig kennis van PETs, maar wel de bevoegdheid om projecten te stoppen of goed te keuren. Omdat zij beslissingsmacht hebben, speelt hun perceptie en begrip een grote rol in de vraag of een initiatief doorgaat.

Door het gebrek aan gedeeld begrip ontstaat zelden een gezamenlijke visie op de inzet van PETs. Afdelingen spreken niet dezelfde taal, juridische en compliance zorgen van besluitvormers kunnen doorslaggevend zijn en leiden tot stagnatie in besluitvorming over toepassingen en investeringen. Daardoor worden PETs vaak gezien als experimenteel of te technisch, in plaats van als praktisch hulpmiddel voor veilige samenwerking met data. Deze beperkte bekendheid versterkt de perceptie van complexiteit en houdt organisaties terughoudend.

“Voor de gemiddelde manager binnen onze organisatie zijn Privacy Enhancing Technologies te complex om goed te begrijpen.”

C. Cross-sectoraal samenwerken creëert extra governance- en afstemmingscomplexiteit

Samenwerken over sectoren heen vergroot de complexiteit van het toepassen van PETs aanzienlijk. Cross sectoraal datadelen vraagt niet alleen technische afstemming, maar ook overeenstemming over uiteenlopende wettelijke kaders, verantwoordelijkheden en belangen. Elke sector kent eigen juridische vereisten en interpretaties van regelgeving, wat de afstemming tussen partijen bemoeilijkt.

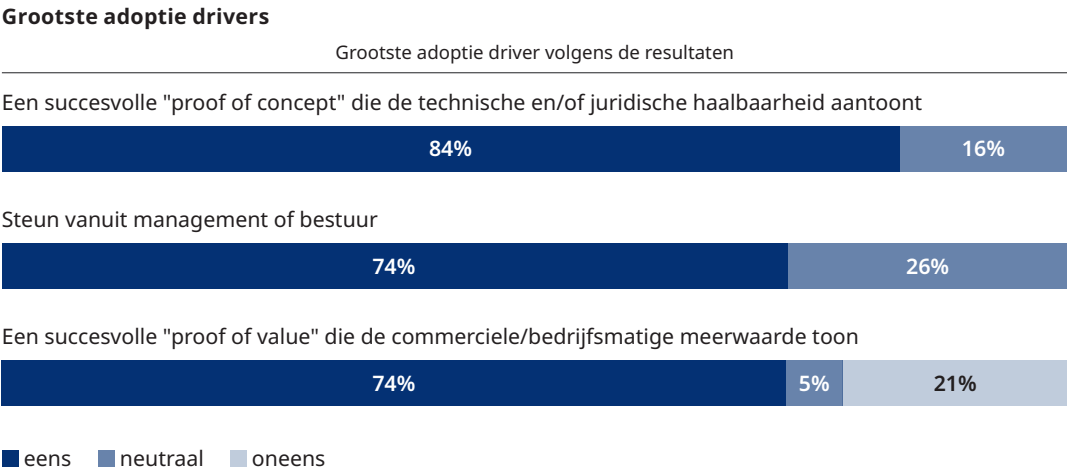
Daarnaast moet voor cross sectoraal gebruik vaak een nieuwe governancestructuur worden ingericht die duidelijk maakt wie verantwoordelijk is voor besluitvorming, beheer en naleving van juridische verplichtingen. Dit proces vergt tijd en coördinatie en vormt daardoor een extra drempel voor samenwerking. De noodzaak om consensus te bereiken tussen partijen met verschillende belangen en bevoegdheden maakt de implementatie van PETs over sectoren heen extra lastig.

“Binnen de club van deelnemers komt het maar niet van de grond, ondanks een hele succesvolle pilots. Er is veel weerstand vanuit andere deelnemers omdat zij bang zijn dat wij ze op basis van de data kunnen gaan afrekenen. Ze hebben echt het idee dat wij dit kunnen misbruiken.”

4. Mogelijkheid tot experimenteren

De mogelijkheid om nieuwe technologieën eerst op kleine schaal te testen speelt een belangrijke rol bij de adoptie ervan. Een pilot biedt organisaties de kans om ervaring op te doen, risico's te beperken en de meerwaarde in de praktijk te toetsen voordat zij grootschalig investeren. Uit de enquête (figuur 6) blijkt dat juist succesvolle proof-of-concept trajecten (technische en juridische haalbaarheid) en proof-of-value-trajecten (business haalbaarheid) worden gezien als de belangrijkste adoptiedrivers voor PETs. In de praktijk blijkt het echter vaak lastig om dergelijke pilots te organiseren.

figuur 6: Het diffusion of innovation-model



Bron: Oliver Wyman, INNOPAY analyse

A. Hoge coördinatielast tussen partijen maken pilots moeilijk uitvoerbaar

Een pilot (Proof-of-value of proof-of-concept) met PETs vraagt om samenwerking tussen meerdere partijen, omdat PETs pas relevant zijn wanneer gegevens of analyses over organisatiegrenzen heen plaatsvinden. Er moeten afspraken worden gemaakt over onder andere verantwoordelijkheden, beveiliging en kosten, vaak nog voordat duidelijk is wat de pilot precies zal opleveren. Hierdoor worden verkennende initiatieven als tijdrovend en kostbaar ervaren en komen pilots moeilijk van de grond.

Toch zijn juist deze proof-of-values cruciaal om ervaring op te bouwen en vertrouwen in PETs te vergroten. Zonder concrete experimenten blijft de technologie abstract en is het voor organisaties moeilijk om de potentiële meerwaarde te beoordelen. Het beperkte aantal uitgevoerde pilots verklaart mede waarom de opschaling van PETs nog achterblijft, ondanks de groeiende aandacht en technologische vooruitgang.

B. Koudwatervrees en voorkeur voor gecontroleerde omgevingen beperken de uitvoering van pilots in operationele setting

Binnen publieke instellingen bestaat vaak een “koudwatervrees” om daadwerkelijk met PETs aan de slag te gaan. In plaats van te experimenteren met marktpartijen kiezen veel publieke organisaties ervoor samen te werken met kennisinstellingen zoals TNO. Dat wordt gezien als een veiligere en meer gecontroleerde omgeving, waardoor de toepassing van PETs vaak beperkt blijft tot theoretisch of onderzoeksniveau. Hierbij wordt dan gebruik gemaakt van experimentele software, die niet gebruiksvriendelijk is, complex om te installeren, en niet geoptimaliseerd op bijvoorbeeld snelle rekentijden. Als voordeel wordt gezien dat er geen commerciële belangen in het spel zijn. Een nadeel is dat bij een eventueel succes van een pilot de dienst niet eenvoudig in operationeel beheer genomen kan worden, maar nog flink doorontwikkeld moet worden.

Uit de enquête en interviews blijkt juist dat het belangrijk is om proof of concept en proof of value te leveren met echte data in realistische IT-omgevingen. Alleen dan wordt de daadwerkelijke meerwaarde van PETs zichtbaar. Beperken pilots zich tot onderzoekopstellingen met zogenaamde “professorware”, dan komt de praktische waarde niet goed naar voren en blijft het vertrouwen in de technologie beperkt.

“In Nederland bestaat een duidelijke voorkeur voor samenwerking met publieke kennisinstellingen. Bedrijven worden vaak minder snel vertrouwd als directe partners. Door een kennisinstelling te betrekken neemt de perceptie van mogelijke beïnvloeding door commerciële belangen af. Dat verklaart waarom veel partijen er de voorkeur aan geven projecten via of samen met publieke organisaties te organiseren.”

C. Onderzoeksgerichte subsidies stimuleren het opdoen van kennis, maar niet de praktische, snelle experimenten met toepassingen van PETs

De manier waarop subsidies zijn ingericht draagt bij aan terughoudendheid. Veel regelingen richten zich op onderzoek en kennisontwikkeling in plaats van op praktische toepassing en validatie. Daardoor blijven partijen nieuwe varianten van toepassingen bouwen of onderzoeken of en hoe iets werkt, in plaats van daadwerkelijk te testen of er waarde ontstaat in een operationele omgeving. Dit beperkt het leereffect tot onderzoek en kennisontwikkeling, en zorgt ervoor dat veelbelovende ideeën vaak niet verder komen dan de onderzoeksfase.

5. Zichtbaarheid van resultaten

De zichtbaarheid van succesvolle toepassingen speelt een cruciale rol in de acceptatie van nieuwe technologieën. Wanneer organisaties de concrete voorbeelden zien van hoe PETs in de praktijk werken en waarde opleveren, groeit het vertrouwen om zelf deel te nemen. Bij PETs is die zichtbaarheid echter vaak beperkt, veel initiatieven blijven steken in verkenning of kleinschalige experimenten vanwege de bovengenoemde barrières, waardoor de waargenomen meerwaarde gering blijft.

Tegelijkertijd blijkt uit praktijkvoorbeelden dat zodra er eenmaal een “minimal viable ecosystem” bestaat waarin de waarde van PETs is aangetoond, toetreding voor nieuwe partijen aanzienlijk makkelijker wordt. Voorbeelden hiervan zijn SecureNed van NCSC of de datawerkplaats in de Achterhoek. Waar de eerste deelnemers vaak nog maanden nodig hebben om een PET-omgeving op te kunnen zetten, kunnen nieuwe deelnemers later in enkele weken aansluiten. Dit verkort de instapkosten en vergroot de geloofwaardigheid van de technologie, waardoor het ecosysteem sneller kan groeien.

A. Beperkt zicht op succesvolle praktijkcases remt adoptie van PETs, met namen in het publieke domein

Tot nu toe hebben veel PET-pilots, vooral binnen de publieke sector, weinig tastbare resultaten opgeleverd of zijn ze vroegtijdig beëindigd, vanwege de bovengenoemde barrières. Mislukte of onvoltooide pilots wekken het beeld dat PETs te complex of onvoldoende technologisch volwassen zijn, terwijl de oorzaken van het mislukken eerder organisatorisch van aard zijn. Dit gebrek aan meetbare successen maakt publieke en private partijen terughoudend om verder te investeren of pilots op te schalen.

“We zien dat sommige overheidsinstellingen zelf PET-oplossingen proberen te ontwikkelen, terwijl er al bewezen technologie beschikbaar is. Wanneer zulke interne experimenten mislukken, ontstaat al snel het beeld dat de technologie niet werkt. Dat is jammer, want de oplossingen bestaan wel degelijk alleen krijgen wij als aanbieders niet altijd de kans om dat in de praktijk te laten zien.”

B. Zelfbouw van PET toepassingen door overheden belemmert adoptie en zichtbaarheid van bestaande oplossingen

Een bijkomende uitdaging is dat overheidsorganisaties regelmatig zelf PET oplossingen ontwikkelen of testen, terwijl vergelijkbare technologieën al door marktpartijen worden aangeboden. Daardoor starten soms trajecten opnieuw die elders al verder zijn uitgewerkt of zelfs operationeel worden toegepast. Marktpartijen hebben doorgaans meer praktijkervaring en hebben veel van de technische en organisatorische uitdagingen al onderzocht.

Als overheden die externe expertise niet benutten en zelf nieuwe oplossingen proberen te bouwen, leidt dat regelmatig tot vertraging of mislukte pilots. De aandacht verschuift dan van toepassing naar technologieontwikkeling, terwijl het juist belangrijk is om bestaande, bewezen oplossingen te implementeren en te evalueren. Dit veroorzaakt versnippering van kennis, inefficiënt gebruik van middelen en een gebrek aan zichtbare successen.

Het gevolg is dat PETs in de publieke context soms onterecht worden geassocieerd met falende experimenten, terwijl de onderliggende technologie bij marktpartijen vaak al volwassen en toepasbaar is.

“Als je wilt weten hoe een auto werkt moet je onder de motorkap kijken. Je hoeft niet eerst zelf een hele auto te bouwen. Voor PETs geldt hetzelfde.”

6. Cultuur van samenwerking en adoptie

Op basis van de interviews hebben de onderzoekers een extra categorie toegevoegd aan het gebruikte model van de adoptie van innovatie, en dat is innovatiecultuur. Dat is de cultuur die bepaalt hoe organisaties omgaan met vernieuwing en innovatie, hoe ze hierin intern en extern samenwerken, en hoe ze innovatie financieren.

A. De Nederlandse focus op gezamenlijke innovatie vertraagt de adoptie van kant-en-klare oplossingen

De Nederlandse innovatiecultuur kenmerkt zich door gezamenlijk ontwikkelen en verkennen van nieuwe technologieën, vaak in gesubsidieerde pilots en publiek-private samenwerkingen. Veel publieke en private organisaties geven de voorkeur aan co-creatie of zelf experimenteren boven het direct aankopen van kant-en-klare PET-oplossingen van commerciële aanbieders. Dit gebeurt om te voorkomen dat er teveel commerciële belangen en “vendor lock-in” ontstaan. Deze samenwerkingsaanpak is waardevol voor interne kennisopbouw en het opbouwen van onderling vertrouwen. Echter, het leidt er ook toe dat bewezen oplossingen niet worden aangeschaft of serieus worden onderzocht, en dat projecten lang kunnen duren, en moeilijk opschaalbaar zijn.

Vaak worden deze gezamenlijke innovatieprojecten gefinancierd via subsidie-aanvragen. Dit geldt zowel voor publiek-private consortia als voor consortia met alleen overheidspartijen. In de subsidievoorwaarden wordt vaak geëist dat er een zekere technische onzekerheid aanwezig is, wat resulteert in trajecten die meer onderzoekend en minder toepassend van aard zijn.

Uit interviews blijkt dat de tendens van zelf bouwen vooral te vinden is bij projecten met synthetische data, waar eenvoudige open-source toepassingen beschikbaar zijn waarmee een eenvoudige pilot georganiseerd kan worden. Bij samenwerkingsgerichte PETs, met name Multi-Party Computation (MPC), zijn partijen sneller geneigd om TNO in te schakelen om een pilot te begeleiden. Dit komt voort uit het gevoel dat deze technologie complexer te beheersen en te duiden is, en aan de behoefte aan onpartijdige duiding en begeleiding.

Als gevolg hiervan wordt bestaande, technisch uitontwikkelde technologie in Nederland minder benut dan mogelijk is, en beginnen partijen vaak opnieuw met het onderzoeken en ontwikkelen van toepassingen van PET toepassingen waar de markt al oplossingen voor heeft.

“Binnen overheidsorganisaties zie je dat ze niet snel kiezen voor kant-en-klare PET oplossingen. Ze willen er graag eerst zelf mee aan de slag gaan om ervaring en kennis op te bouwen ipv gelijk naar een kant-en-klare oplossing te kijken. Bovendien zijn partijen vaak bang voor een vendor-lock-in effect of willen overheidinstellingen niet gelijk aanbestedingen opzetten, omdat hier veel bij komt kijken.”



Conclusies en aanbevelingen

5.1. Conclusies

De belangrijkste bevindingen uit het onderzoek laten zien dat Nederland beschikt over een sterke uitgangspositie op het gebied van PETs, maar dat brede adoptie achterblijft vanwege meerdere barrières. PETs leveren aantoonbare voordelen op voor risicobeperkingen en datagedreven samenwerking, maar lossen structurele datadeelproblemen niet zelfstandig op. De adoptie wordt vooral bepaald door organisatorische, governance-gerelateerde en juridische randvoorwaarden, evenals door factoren die de toepassing kunnen versnellen zodra deze basis op orde is. Zeven conclusies volgen uit de inzichten over de adoptie van PETs in Nederland:

1. Nederland heeft een sterke uitgangspositie, maar grootschalige adoptie van PETs blijft achter bij het potentieel
2. PETs leveren waarde door risico's in datadelen te beperken en nieuwe kansen te creëren
3. Er bestaan adoptieverschillen tussen sectoren. PETs worden vooral toegepast in zorg, financiële en publieke sector, en minder aan sectoren zoals industrie, energie, of logistiek
4. PETs zijn geen “silver bullet” om alle datadeelproblemen mee op te lossen
5. PET-adoptie wordt geremd door algemene datadeelproblemen en extra juridische en technische complexiteit
6. De adoptie van PETs staat of valt met vier cruciale randvoorwaarden: een positieve businesscase, goede datakwaliteit, juridische grondslag en onderling vertrouwen en samenwerking.
7. Naast randvoorwaarden zijn er verschillende “best practices” die adoptie versnellen. Hierin wordt de markt meer volwassen

1. Nederland heeft een sterke uitgangspositie, maar grootschalige adoptie van PETs blijft achter bij het potentieel

Nederland heeft een sterke innovatiestructuur voor PETs. Dit wordt mogelijk gemaakt door de elkaar versterkende samenwerking tussen onderzoeksinstituten, de overheid, bedrijven (aanbieders en gebruikers) en maatschappelijke organisaties.

In vergelijking met het buitenland blinkt Nederland vooral uit op de praktische toepassing van synthetische data, MPC/HE en federated learning. Er zijn diverse Nederlandse startups en scale-ups actief die ook steeds meer klanten in het buitenland aantrekken, en enkele infrastructurele/ondersteunende partijen nemen PETs op als onderdeel van hun aanbod.

In verschillende sectoren zijn succesvolle toepassingen operationeel, vooral in de zorg, de financiële en publieke sector. Er bestaan daar soms al jaren gespecialiseerde infrastructuren en samenwerkingsverbanden voor veilig datadelen, die momenteel in een duidelijke opschalingsfase zitten.

Toch vertaalt deze solide basis zich (nog) niet in brede, grootschalige toepassingen over alle sectoren van de Nederlandse economie. De daadwerkelijke adoptie van PETs blijft achter bij het potentieel, zeker in verhouding met de voordelige uitgangspositie.

2. PETs leveren waarde door risico's te beperken en nieuwe kansen te creëren

PETs helpen datadelende organisaties de kans op datalekken van persoonsgegevens of commercieel gevoelige data te verkleinen en juridische risico's te verminderen. Ze ondersteunen bij het voldoen aan regels zoals de AVG en het principe van dataminimalisatie door analyses mogelijk te maken zonder het uitwisselen van herleidbare brondata. Dit vergroot de dataveiligheid en het vertrouwen tussen samenwerkende partijen. Dit is vooral van groot belang in sectoren met hoge privacy en compliance gevoeligheid zoals de zorg, de financiële sector en de publieke sector.

Tegelijkertijd bieden PETs kansen die zonder deze technieken niet of nauwelijks realiseerbaar zijn. Door data van meerdere organisaties te combineren zonder ruwe data te delen, ontstaan nieuwe inzichten en wordt besluitvorming efficiënter. Dat opent de deur naar gezamenlijke oplossingen voor (maatschappelijke) vraagstukken zoals betere zorg, effectievere fraudepreventie en sterkere cyberweerbaarheid, terwijl privacy en vertrouwelijkheid gewaarborgd blijven. Hoe deze kansen worden benut verschilt echter per sector.

3. Er bestaan adoptieverschillen tussen sectoren. PETs worden vooral toegepast in zorg, financiële en publieke sector, en minder aan sectoren zoals industrie, energie, of logistiek

De meeste toepassingen van PETs verschijnen momenteel in de zorg-, de financiële- en de publieke sector. Deze domeinen werken intensief met gevoelige persoonsgegevens, vallen onder strenge regelgeving en lopen bij incidenten tegen grote consequenties aan dan andere sectoren. Daardoor is de urgentie om veilig samen te werken groot en is de druk om te voldoen aan compliance hoog. Binnen sommige ecosystemen in de zorg en in cybersecurity is een duidelijke opschaling zichtbaar. Initiatieven die aanvankelijk door een kleine groep voortrekkers worden verkend, worden na succesvolle eerste ervaringen door een bredere groep organisaties opgepakt.

In sectoren zoals energie, industrie en logistiek komt adoptie veel minder op gang. De interne compliancedruk rond privacy of bedrijfsgevoelige data is daar vaak kleiner, de noodzaak tot sectorbreed delen minder direct en de behoefte aan gezamenlijke datadelen beperkt. Bovendien ontbreken in deze sectoren vaak sterke datadeel-ecosystemen en is men minder gewend data met derden te delen. Daardoor wordt in deze sectoren minder gebruik gemaakt van of onderzoek gedaan naar samenwerkingsgerichte technieken zoals MPC, homomorphic encryption en federated learning. Wel wordt er vaker gebruik gemaakt van intern-gerichte PETs, zoals synthetische data voor het vergroten van datasets. De verschillen in adoptie hangen samen met sectorale urgentie, de aanwezigheid van datadeel-ecosystemen en de heersende datacultuur.

4. PETs zijn geen “silver bullet” om alle datadeelproblemen mee op te lossen

Hoewel PETs de afgelopen jaren veel aandacht hebben gekregen, vormen zij geen “silver bullet” die datadelen automatisch mogelijk maakt. In de beginfase van hun ontwikkeling werd soms verwacht dat PETs kansarme datasamenwerkingen alsnog konden laten slagen. Die verwachting blijkt onterecht. PETs lossen geen fundamentele belemmeringen op, zoals het ontbreken van governance, onvoldoende onderling vertrouwen, of een gebrekkige datakwaliteit. PETs bieden extra zekerheid/veiligheid, ten koste van meer complexiteit.

Een andere misvatting is dat PETs het mogelijk maken om bestaande wetgeving te “omzeilen” en zo datasamenwerkingen op te zetten waarvoor bijvoorbeeld geen grondslag in de AVG te vinden is. Ook bij gebruik van PETs moeten organisaties blijven voldoen aan vereisten zoals juridische grondslagen, doelbinding en aansprakelijkheid. Wel zien we dat PETs soms kunnen worden ingezet wanneer er wel een grondslag is, maar het delen van volledige datasets wordt gezien als disproportioneel.

Er is hierbij wel een kanttekening: Rondom de GDPR/AVG ontwikkelt zich een juridische discussie over de vraag in hoeverre en in welke context bepaalde gepseudonimiseerde gegevens niet langer altijd als persoonsgegevens hoeven te worden aangemerkt. De Nederlandse Autoriteit Persoonsgegevens (AP) wordt gezien als conservatief in discussies over dit thema.

5. PET-adoptie wordt geremd door algemene datadeelproblemen en extra juridische en technische complexiteit

PETs lossen de basisproblemen bij datadelen niet op. Bij samenwerkingen met PETs spelen dezelfde structurele obstakels een rol als bij andere datagedreven samenwerkingen. Belangrijke knelpunten zijn onduidelijkheid over governance en verantwoordelijkheden, juridische onzekerheid over grondslagen en risicoverdeling, een ongelijke verdeling van kosten en baten en een gebrek aan vertrouwen. Daarnaast vormen cultuur en de perceptie van risico's terugkerende belemmeringen voor gezamenlijke initiatieven.

PETs kennen extra drempels die de adoptie complexer maken dan bij andere datadelingstechnieken. De technologie is technisch volwassen, maar de onderliggende cryptografische methoden zijn complex en moeilijk uitlegbaar aan bestuurders, juristen, toezichthouders en andere stakeholders. Organisaties vinden het lastig te beoordelen of de technologie juridisch verantwoord kan worden toegepast en vrezen gevolgen wanneer interpretaties achteraf onjuist blijken. Deze combinatie van technische complexiteit en beperkte uitlegbaarheid zorgen ervoor dat de risicoperceptie wordt versterkt.

De combinatie van algemene datadeelproblemen en PET-specifieke complexiteit verklaart waarom grootschalige adoptie achterblijft, ook wanneer de technologie goed werkt.

6. De adoptie van PETs staat of valt met 4 cruciale randvoorwaarden

Allereerst is een positieve financiële businesscase noodzakelijk. Kosten en benodigde inspanningen moeten in verhouding staan tot de voordelen die organisaties ervaren. Daarbij is een evenredige verdeling van kosten en baten in samenwerkingen essentieel. Als één partij substantieel meer moet investeren dan zij terugziet, stukt het draagvlak vrijwel direct.

Een tweede randvoorwaarde is de kwaliteit van de onderliggende gegevens. PET-toepassingen creëren alleen waarde als er betrouwbare brondata beschikbaar zijn die consistent en zorgvuldig worden vastgelegd.

Even belangrijk is het hebben van een duidelijke juridische grondslag. Organisaties moeten begrijpen welke vormen van datadelen en onder welke voorwaarden zijn toegestaan binnen de AVG en andere relevante wetgeving. Bij cross-sectoraal data delen kan het zijn dat aan verschillende juridische kaders tegelijk moet worden voldaan, die soms niet goed samengaan.

Tot slot vormen vertrouwen en samenwerking de basis waarop PETs kunnen worden ingevoerd. PETs vervangen vertrouwen niet, zij ondersteunen het. Pas wanneer partijen vertrouwen hebben in elkaars intenties, het beoogde datagebruik en de onderlinge afspraken, kan PET-technologie op grotere schaal in de praktijk worden toegepast.

7. Naast randvoorwaarden zijn er verschillende versnellers van adoptie

In uiteenlopende projecten ontstaan inmiddels duidelijke voorbeelden van succesvolle PET-toepassingen. In vrijwel alle onderzochte initiatieven komen dezelfde “versnellers” terug, factoren die samenwerking vergemakkelijken en de kans op een geslaagde implementatie vergroten.

- Een belangrijke versneller is het bestaan van heldere governance en concrete samenwerkingsafspraken tussen partijen. Wanneer verantwoordelijkheden, besluitvorming en datagebruik vooraf goed zijn georganiseerd, ontstaat ruimte om de technologie in de praktijk te brengen.
- Binnen die samenwerking spelen sleutelpersonen zoals juristen, privacy officers, managers en bestuurders een cruciale rol. Als deze sleutelpersonen zich hardmaken voor het gebruik van PETs, neemt de slaagkans aanzienlijk toe.
- Daarnaast helpen aantoonbare successen de adoptie vooruit. Zichtbare voorbeelden bij andere vergelijkbare organisaties verlagen de drempel om zelf te starten, omdat zichtbaar wordt dat PETs in de praktijk functioneren.
- Een modern en flexibel IT-landschap draagt eraan bij dat PETs eenvoudiger geïntegreerd, getest en opgeschaald kunnen worden.
- Vroegtijdige betrokkenheid van technologieaanbieders draagt ook bij aan versnelling en vooral ook aan opschaling na een succesvolle pilot.

5.2. Aanbevelingen

Nederland beschikt over een relatief volwassen en veelzijdig PET-ecosysteem, gedragen door het quadruple-helixmodel waarin onderzoeksinstellingen, bedrijven, overheid en maatschappelijke organisaties ieder een eigen en elkaar versterkende rol vervullen.

Dit bestaande fundament biedt een goede uitgangspositie, maar gerichte versterking is nodig om toepassingen sneller op te schalen en de adoptie in verschillende sectoren te vergroten. Het PET-ecosysteem kan doelgericht worden ondersteund en verder uitgebouwd door te focussen op de volgende vijf onderdelen:

1. Verschuif financiering naar toepassing en opschaling (proof-of-concept en proof-of-value)

Veel financieringsinstrumenten richten zich primair op onderzoek en innovatie. De grootste behoefte ligt echter bij het valideren, toepassen en opschalen van PET-toepassingen. Stimuleer financieringsmodellen die proof-of-concept trajecten ondersteunen, zodat organisaties PET-oplossingen daadwerkelijk kunnen testen in productie omgevingen, inclusief integratie met bestaande IT-landschappen en het gebruik van echte gevoelige gegevens.

2. Versterk de rol van de overheid als afnemer van PET-oplossingen

De overheid spreekt veel over PETs (bijvoorbeeld bij NICPET) maar past zelf niet vaak PETs toe in de praktijk. Waar praktijktoepassing wel wordt gevonden ontwikkelt de overheid vaak eigen oplossingen in plaats van bestaande PET-oplossingen af te nemen. Juist een actieve afnemersrol van de overheid versnelt de adoptie en vergroot het marktvertrouwen. Stimuleer modellen waarin de overheid nadrukkelijk optreedt als gebruiker van PETs in datasamenwerkingen en waarbij de overheid PET-oplossingen ook afneemt in plaats van deze zelf ontwikkelt.

3. Richt financiering op use-cases die maatschappelijke waarde creëren

PET-toepassingen die maatschappelijke waarde creëren, leveren de betrokken partijen in de praktijk niet altijd directe baten op. Daardoor hebben zij minder prikkels om hiermee aan de slag te gaan. Zet gerichte financiering in voor use-cases waarbij maatschappelijke belangen niet vanzelf aansluiten op de individuele belangen van organisaties.

4. Overweeg ook een regulatory sandbox op use-cases die maatschappelijke waarde creëren

In enkele landen zoals Singapore³³ en het VK³⁴ heeft de toezichthouder een zogenaamde regulatory sandbox geopend waarbinnen overheidspartijen en bedrijven eenvoudiger met PETs kunnen experimenteren onder versoepelde privacyregelgeving en/of met advies vanuit de toezichthouder vooraf in plaats van toezicht achteraf. In andere landen, zoals Ierland³⁵ heeft de overheid sandboxes ingericht rondom een specifiek maatschappelijk thema, zoals Anti-Money Laundering (AML), waarbinnen ook met PETs geëxperimenteerd wordt. In Nederland zijn geen vergelijkbare sandboxes. Overweeg om naast financiering ook een regulatory sandbox rondom een of meer maatschappelijk relevante use-case te creëren.

33 <https://www.pdpc.gov.sg/news-and-events/announcements/2022/07/launch-of-privacy-enhancing-technologies-sandbox>

34 <https://ico.org.uk/for-organisations/advice-and-services/regulatory-sandbox/>

35 <https://www.centralbank.ie/regulation/innovation-hub/innovation-sandbox-programme/financial-crime>

5. Stimuleer naamsbekendheid en kennis van PETs binnen de Nederlandse economie

Veel organisaties kennen PETs nog onvoldoende en hebben onvoldoende kennis van wat de technologieën kunnen betekenen. Bovendien worden PETs voornamelijk geassocieerd met uitsluitend de bescherming van persoonsgegevens, terwijl het veel bredere toepassing heeft zoals bescherming van gevoelige bedrijfsgegevens. Stimuleer naamsbekendheid en kennis van PETs door te focus op de volgende elementen:

- **Richt communicatie op sectoren waar adoptie achterblijft**

Sectoren zoals (maar niet beperkt tot) energie, bouw, maakindustrie en de agrarische sector zijn momenteel minder gericht op PETs, hebben minder beschikbare kennis en hebben deze technologieën nog onvoldoende verkend. Het is belangrijk om kennis binnen deze sectoren verder op te bouwen en inzichtelijk te maken welke waarde PETs kunnen bieden voor veilig datadelen en welke nieuwe innovatiekansen dit kan opleveren. Maatschappelijke thema's waarbij data delen relevant is zijn in deze sectoren zeker te vinden, te denken valt aan energietransitie, stikstofcrisis en circulaire productieketens. Ontwikkel sectorspecifieke kennisprogramma's, showcases en laagdrempelige experimenten om organisaties te laten zien hoe veilig data delen via PETs kan bijdragen aan innovatie, efficiëntere ketens en versterking van de concurrentiekracht.

- **Vergroot kennis over bescherming van gevoelige bedrijfsgegevens door middel van PETs**

PETs worden in Nederland nog vaak primair geassocieerd met de bescherming van persoonsgegevens. In veel sectoren ligt echter juist grote waarde in het veilig kunnen delen van bedrijfsgevoelige data. De potentie voor niet-persoonsgegevens is daar momenteel nog onvoldoende bekend en benut. Ontwikkel gerichte voorlichting en praktijkvoorbeelden over het gebruik van PETs voor bedrijfsgevoelige en andere niet-persoonsgebonden gegevens, zodat organisaties beter inzicht krijgen in de zakelijke waarden en toepassingsmogelijkheden ervan. Overweeg daarbij ook een andere term te gebruiken in plaats van PETs.

5.3. Vervolgonderzoek

Uit dit onderzoek blijkt dat internationale marktgroei-verwachtingen voor PETs niet aansluiten op de technologieën die Nederlandse organisaties op dit moment toepassen. De internationale marktrapporten voorspellen in verhouding grotere groei voor oplossingen zoals differential privacy, zero-knowledge proofs en trusted execution environments.

In Nederland ligt de praktijk nadrukkelijk bij andere PETs. Organisaties testen en gebruiken vooral synthetische data, multi-party computation en federated learning. Deze afwijking tussen voorspelde marktgroei en feitelijk gebruik roept de vraag op of hier sprake is van een structurele mismatch, of dat Nederland juist een unieke niche-positie heeft opgebouwd die internationaal verder benut kan worden. Het verdient aanbeveling dit verder te onderzoeken en hier een strategie op te ontwikkelen.

5.4. Afsluiting

Samenvattend laat dit onderzoek zien dat PETs in Nederland veelbelovend zijn, maar nog onbenut potentieel hebben. De technologische basis is sterk, het ecosysteem groeit en er bestaan overtuigende voorbeelden van werkende toepassingen. Tegelijkertijd vraagt brede adoptie om het wegnemen van structurele belemmeringen en het versterken van randvoorwaarden. Door deze elementen gericht te versterken kan Nederland de volgende stap zetten naar verantwoord en grootschalig datadelen met PETs

5.5. Dankwoord

Dit onderzoek kwam tot stand dankzij de waardevolle bijdragen van betrokkenen uit overheid, bedrijfsleven, kennisinstellingen en maatschappelijke organisaties. Hun medewerking vormde het fundament voor de analyses en conclusies in dit rapport. Daarnaast wordt dank uitgesproken voor de prettige samenwerking met de opdrachtgevers van het Ministerie van Economische Zaken.

Appendix A. Uitwerking PET use-case

Appendix A bevat een use case waarin meerdere organisaties wilden samenwerken rond gevoelige data maar dit niet van de grond kwam. Er is een duidelijke behoefte aan het delen van inzichten omdat gezamenlijk analyseren kan leiden tot betere signalering, snellere besluitvorming en effectievere interventies. Of samenwerking daadwerkelijk van de grond komt hangt sterk af van organisatorische factoren zoals gedeelde incentives, afspraken over governance en het onderlinge vertrouwen tussen partijen.

Deze use case toont aan dat samenwerking lastig kan zijn wanneer organisaties uiteenlopende belangen hebben, verschillend afgerekend worden op risico's of onder verschillende juridische en organisatorische kaders opereren. Vooral bij samenwerking tussen sectoren ontstaat hierdoor extra complexiteit omdat doelen, incentives en verantwoordelijkheden niet automatisch op elkaar aansluiten.

Use case: Aanpak zorgfraude

Context & probleemstelling

Het Nederlandse zorgstelsel lijdt jaarlijks grote financiële verliezen door zorgfraude. Volgens de Algemene Rekenkamer³⁶ lopen de kosten op tot enkele miljarden euro's per jaar, onder meer door onterechte declaraties, opzettelijk verhogen van declaraties of declaraties voor niet-geleverde zorg. De opsporing van dergelijke fraude is complex omdat relevante informatie verspreid ligt over meerdere organisaties.

Zo beschikken zorgverzekeraars over declaratiegegevens en medische signalen die op fraude kunnen wijzen, terwijl banken zicht hebben op verdachte financiële transacties en geldstromen van potentieel malafide zorgaanbieders. Door beperkte wettelijke mogelijkheden om informatie te delen, blijft veel gevallen van fraude onder de radar. De huidige privacywetgeving en het ontbreken van een heldere juridische grondslag belemmeren samenwerking tussen toezichthouders en deze partijen.

Aanpak van het probleem

Om dit probleem aan te pakken, hebben TNO, zorgverzekeraar CZ, de Nederlandse Zorgautoriteit en het Informatie Knooppunt Zorgfraude (IKZ) een concept ontwikkeld waarin gebruik wordt gemaakt van Secure Multi-Party Computation.³⁷ Met deze cryptografische technologie kunnen betrokken partijen gezamenlijke analyses uitvoeren, zonder dat zij hun eigen brongegevens leesbaar hoeven te delen of inzicht krijgen in elkaars onderliggende informatie.

³⁶ <https://www.rekenkamer.nl/publicaties/rapporten/2022/04/14/een-zorg-gebrek-aan-daadkracht>

³⁷ <https://ibestuur.nl/data-en-ai/innovatie/cryptografie-als-wapen-in-de-strijd-tegen-zorgfraude>

De voorgestelde werkwijze richtte zich op het combineren van fraudesignalen uit verschillende bronnen. De zorgverzekeraar versleuteld de lijst met zorgaanbieders waarvoor interne fraudesignalen bestaan, terwijl banken hun eigen gegevens over verdachte transacties versleutelen. Binnen het MPC-protocol wordt een gecombineerde risico-score berekend, en wordt aan de zorgverzekeraar teruggegeven welke zorgaanbieders zowel bij zorgverzekeraar als bank een grote kans op fraude laten zien. De zorgverzekeraar heeft daarmee voldoende onderbouwing voor haar verdenking om een diepgravender onderzoek in te stellen, en daarbij meer informatie in te winnen binnen de wettelijke kaders. De bank leert niet welke van haar klanten verdacht zijn bij zorgverzekeraars.

Deze benadering zou het mogelijk maken om op een privacy-by-design manier fraude te signaleren. MPC biedt daarmee een manier om samenwerking tussen zorgverzekeraars, banken en toezichthouders te versterken, zonder dat gevoelige persoonsgegevens of bedrijfsinformatie worden uitgewisseld, en waarbij vooral proportionaliteit hoog in het vaandel staat.

Betrokken partijen

De voorgestelde aanpak brengt verschillende partijen samen:

- **Zorgverzekeraars:** leveren relevante gegevens over zorgaanbieders en ontvangen de uitkomsten van het MPC-protocol. Zorgverzekeraars hebben vanuit hun formele rol een taak en ook een financieel incentive om zorgfraude te beperken.
- **Banken:** leveren financiële transactiedata, en ontvangen geen inzicht in welke zorgaanbieders door de zorgverzekeraar worden onderzocht. Banken hebben geen formele taak om zorgfraude te beperken.
- **Kamer van Koophandel:** biedt bedrijfsinformatie ter ondersteuning van de analyses. KVK heeft een poortwachterstaak om bedrijfsmatige fraude te helpen bestrijden.
- **NZa en IKZ:** vervullen een beleidsmatige en coördinerende rol bij de juridische en ethische borging van de aanpak zorgfraude.
- **TNO:** ontwikkelde het concept en adviseerde over de technische en cryptografische haalbaarheid. TNO speelt alleen een rol in de opzet van dit systeem, niet in de operationele uitvoering.

Resultaten & knelpunten

De gezamenlijke verkenning toonde aan dat MPC technisch geschikt is om deze datasamenwerking tussen partijen mogelijk te maken met het behoud van vertrouwelijkheid en naleving van de AVG. Toch bleef verdere uitvoering vooralsnog uit. De belangrijkste belemmeringen lagen in:

1. Perceptie van juridische complexiteit en angst voor risico's

Hoewel de huidige privacywetgeving samenwerking met PETs juridisch wel mogelijk maakt, heerst onder betrokken organisaties de perceptie dat gegevensuitwisseling via PETs juridisch riskant is. Veel professionals binnen de organisaties ervaren onzekerheid over hoe de technologie werkt en hoe deze zich precies verhoudt tot de AVG. Deze kennis- en vertrouwenskloof leidt tot terughoudendheid. Organisaties willen pas bewegen wanneer alle betrokken afdelingen volledig overtuigd zijn dat de aanpak geen risico's oplevert. De angst voor mogelijke incidenten, toezichtreacties of reputatieschade fungeert als rem.

2. Samenwerking vraagt coördinatie tussen partijen met uiteenlopende belangen

De betrokken partijen hebben elk eigen prioriteiten, juridische risico's en operationele agenda's. Het gezamenlijk organiseren van een datagedreven fraude-aanpak vereist intensieve afstemming, wat in de praktijk moeilijk te realiseren is. Met name aan de kant van de financiële instellingen zijn de belangen niet duidelijk. Banken wordt gevraagd om tijd en geld te investeren en risico te lopen in het aanleveren van data, terwijl banken zelf geen directe probleemhouder zijn van het dossier zorgfraude.

3. Beperkte financiële prikkels voor individuele organisaties

Hoewel zorgfraude een groot maatschappelijk probleem is, zijn de financiële baten voor individuele organisaties vaak indirect. Banken ervaren bijvoorbeeld weinig direct voordeel van de detectie van zorgfraude, terwijl de kosten van deelname en compliance-inspanningen wel hoog zijn. Deze discrepantie maakt het lastig om investeringsbeslissingen te rechtvaardigen.

4. Ervaring met eerdere initiatieven beïnvloedt vertrouwen

Het eerdere grote Nederlandse initiatief rondom datadelen tussen banken voor transaction monitoring bij TMNL is voortijdig beëindigd. De oorzaak hiervan lag niet bij het wel of niet gebruiken van PETs, maar met name bij beeldvorming en discussies met de AP. Deze negatieve ervaringen hebben met name de betrokken banken voorzichtig en sceptisch gemaakt ten aanzien van soortgelijke datadeel projecten, zelfs wanneer doel, domein, en technische opzet verschilt.

Onderstaande tabel geeft de bovengenoemde belangen versimpeld weer, in de vorm van een balans tussen kosten/risico's en verantwoordelijkheid en directe baten van de samenwerking. Uit deze tabel is op te maken dat de balans niet voor alle typen organisaties positief uitpakt, ondanks dat allen het maatschappelijk belang van het bestrijden van zorgfraude ten volle onderschrijven.

Geïnterviewden	Levert gegevens	Maakt kosten	Formele rol verminderen zorgfraude	Financieel incentive verminderen zorgfraude	Balans
Zorgverzekeraars					+
Banken					-
KVK					+/-
NZa en IKZ					+
TNO					+

Veel/groot

Beperkt

Geen

Hier mee laat deze case mooi zien dat er meer nodig is dan adoptie van PETs om grote maatschappelijke problemen op te lossen, en dat de kern van adoptie ook ligt in het vinden van use-cases met een positieve balans voor alle deelnemers.

Appendix B. Begrippenlijst

Datadeel-cultuur	De verzameling normen, gewoontes en overtuigingen binnen een organisatie over de manier waarop en met wie men samenwerkt en data deelt.
Datadeel-ecosysteem	Een georganiseerde netwerk van partijen, afspraken, infrastructuren en governance waarin data veilig, structureel en volgens vaste regels wordt gedeeld.
Differential Privacy	Een wiskundige methode om statistische analyses uit te voeren met garanties dat individuele records in een dataset niet herleidbaar zijn.
Federated Learning	Een methode waarbij modellen worden getraind op gedistribueerde data bij verschillende partijen, waarbij de data lokaal blijft en modelparameters worden gedeeld.
Governance	De afspraken, rollen en verantwoordelijkheden en processen die bepalen hoe samenwerking wordt georganiseerd.
Homomorfe Encryptie	Cryptografische methode om berekeningen uit te voeren op data die tijdens de berekening versleuteld en dus onleesbaar blijft.
Interne PETs	PET-toepassingen die binnen een organisatie worden gebruikt, bijvoorbeeld synthetische data om datasets te vergroten.
Privacy Enhancing Technologies	Technologieën die het mogelijk maken om data te analyseren, te delen of te gebruiken terwijl de privacy en vertrouwelijkheid van die data wordt beschermd.
Proof-of-Concept	Een kleinschalige test die aantoont dat een technologie technisch haalbaar is.
Proof-of-Value	Een pilot die niet alleen technische haalbaarheid, maar ook businesswaarde of maatschappelijke waarde laat zien.
Samenwerkingsgerichte PETs	PET-technieken die samenwerking tussen meerdere partijen mogelijk maken zonder de uitwisseling van brondata, zoals MPC en federated learning.
Secret Sharing	Cryptografische methode om datasets in drie onleesbare shares te verdelen
Secure Multi-Party Computation	Een verzamelnaam voor cryptografische technieken waarmee samenwerkende partijen berekeningen kunnen uitvoeren op elkaars data, zonder dat zij elkaars data kunnen lezen.
Synthetische data	Kunstmatig gegenereerde data die statistisch lijkt op echte gegevens, maar geen direct herleidbare persoonsgegevens bevat. Wordt gebruikt om privacy risico's te vermijden of datasets te vergroten.
Trusted Execution Environment	Een beveiligde hardware-omgeving waarin berekeningen kunnen worden uitgevoerd zonder dat de binnenkomende data zichtbaar is voor het besturingssysteem of andere applicaties.
Zero-knowledge Proofs	Cryptografische bewijzen waarmee een partij kan aantonen dat iets waar is zonder de onderliggende informatie te onthullen.

Appendix C. Afkortingen

AVG	Algemene verordening gegevensbescherming
CISO	Chief Information Security Officer
CoE-DSC	Centre of Excellence for Data Sharing & Cloud
CWI	Centrum Wiskunde & Informatica
DP	Differential Privacy
EZ	Ministerie van Economische Zaken
FL	Federated Learning
HE	Homomorphic Encryption
IKZ	Informatie Knooppunt Zorgfraude
MPC	Multi-Party Computation
NZa	Nederlandse Zorgautoriteit
PETs	Privacy Enhancing Technologies
PoC	Proof-of-Concept
PoV	Proof-of-Value
TEE	Trusted Execution Environment
TNO	Nederlandse Organisatie voor Toegepast-Natuurwetenschappelijk Onderzoek
ZKP	Zero-Knowledge Proof

Appendix D. Lijst geïnterviewde partijen

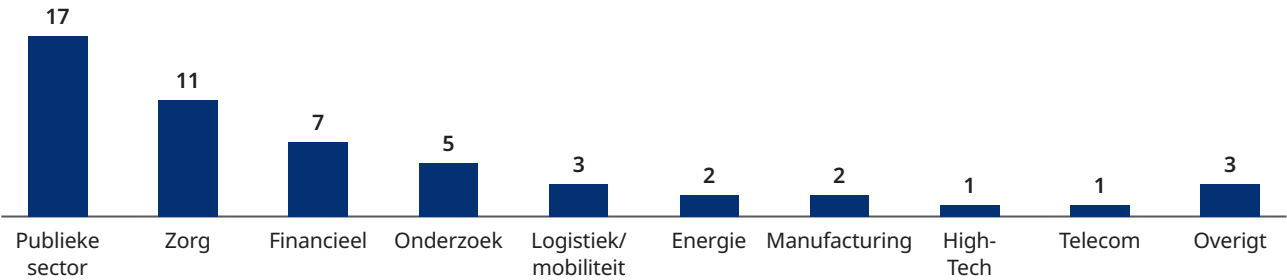
Overzicht van PET aanbieders/partners

Op verzoek van de geïnterviewden zijn sommige partijen geanonimiseerd.

Geïnterviewden	Aanbieder	PET-ondersteuner	Gebruiker	Ecosysteem
1 Bluegen.AI				
2 Circularise				
3 Linksight				
4 Medical Data Works				
5 Roseman Labs				
6 OASYS NOW				
7 Syntho				
8 anDREa				
9 ICT-dienstverlener				
10 Zorgverzekeraar				
11 Logistieke dienstverlener				
12 Farmaceutisch bedrijf				
13 Financiële instelling				
14 Financieel consortium				
15 AI Coalition 4 NL				
16 Centre of Excellence for Data Sharing & Cloud (CoE-DSC)				
17 Datawerkplaats				
18 LIFES				
19 Nicpet				
20 TNO				

figuur 7: Overzicht van de sectoren waarin de enquêterespondenten actief zijn

In welke sector(en) is uw organisatie actief? (N=26)



INNOPAY — a business of Oliver Wyman, advises on strategy, product development, and implementation across four strands of the digital economy: payments, open finance, digital identity, and data sharing. Our service spans not only the planning and operational aspects of our clients' businesses, but the technologies they deploy, and their compliance with local and international regulations.

By promoting collaboration and innovation, we help clients reimagine the complexities of digital transactions, with technology and product-focused approaches. The result is sustainable growth and real-time trust in an increasingly digital-first world.

Oliver Wyman, a Marsh (NYSE: MRSH) business, is a management consulting firm driven by deep industry insight, bold innovation, and a collaborative approach that cuts through complexity to help organizations navigate their most defining transformative moments. Marsh is a global leader in risk, reinsurance and capital, people and investments, and management consulting, advising clients in 130 countries. With annual revenue of over \$24 billion and more than 90,000 colleagues, Marsh helps build the confidence to thrive through the power of perspective.

For more information, visit oliverwyman.com, or follow on LinkedIn and X.

Europe
+44 20 7333 8333

Americas
+1 212 541 8100

Asia Pacific
+65 6510 9700

India, Middle East & Africa
+971 (0) 4 425 7000

AUTEURS

Douwe Lycklama
Senior Vice President
douwe@innopay.com

Maarten Bakker
Vice President
maarten.bakker@innopay.com

Pieter Verhagen
Senior Manager
pieter.verhagen@innopay.com

Leon Kluiters
Manager
leon.kluiters@innopay.com

Maikel Abiskharoun
Consultant
maikel.abiskharoun@innopay.com

Copyright ©2026 Oliver Wyman

All rights reserved. This report may not be reproduced or redistributed, in whole or in part, without the written permission of Oliver Wyman and Oliver Wyman accepts no liability whatsoever for the actions of third parties in this respect.

The information and opinions in this report were prepared by Oliver Wyman. This report is not investment advice and should not be relied on for such advice or as a substitute for consultation with professional accountants, tax, legal or financial advisors. Oliver Wyman has made every effort to use reliable, up-to-date and comprehensive information and analysis, but all information is provided without warranty of any kind, express or implied. Oliver Wyman disclaims any responsibility to update the information or conclusions in this report. Oliver Wyman accepts no liability for any loss arising from any action taken or refrained from as a result of information contained in this report or any reports or sources of information referred to herein, or for any consequential, special or similar damages even if advised of the possibility of such damages. The report is not an offer to buy or sell securities or a solicitation of an offer to buy or sell securities. This report may not be sold without the written consent of Oliver Wyman.