



# Workshop Data Delen Onvindbare Deelnemers

21 juni 2023

# Welkom

## Introductie



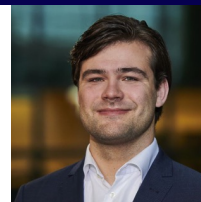
## Gefaciliteerd door



**Maarten Bakker**  
maarten@datasharingcoalition.eu






**Ruben van den Goorbergh**  
ruben@datasharingcoalition.eu



**Freek van Logtestijn**  
freek@datasharingcoalition.eu

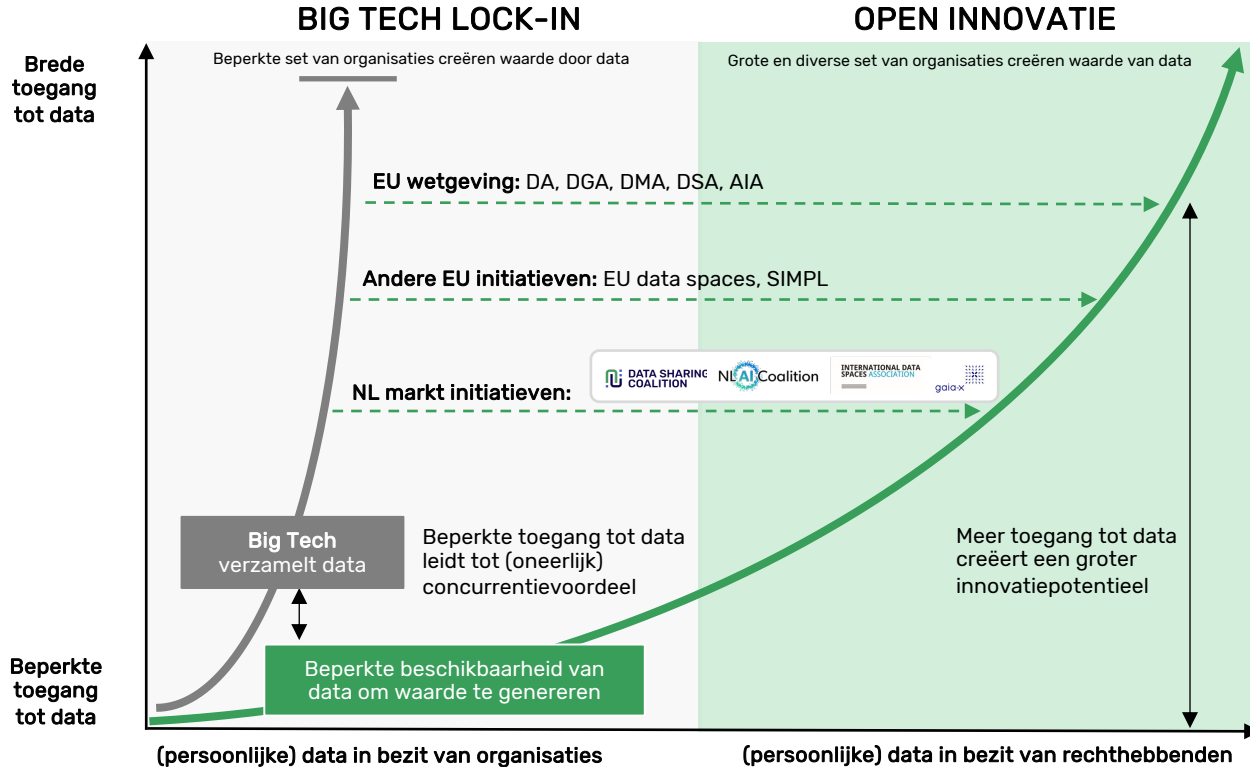
# Doelen van vandaag

-  Inzicht bieden in werkwijze en CoE-DSC en hoe dit aansluit bij het doel van de 'onvindbaren' use case
-  Inzicht bieden in de mogelijkheden van PET's en op welke manier deze kunnen bijdragen aan het uitwisselen van data
-  Bepalen vervolgstappen

# Agenda

	<i>Tijd</i>	<i>Spreker(s)</i>	<i>Opmerkingen</i>
<b>1. Welkom en introductie van het CoE-DSC</b>	<b>20 min</b>	Freek v L.	
2. Ons begrip van de 'onvindbaren' usecase	10 min	Freek v L.	
3. Inleiding en applicatie Privacy Enhancing Technologies	30 min	Ruben vd G.	
<i>Pauze</i>	<i>15 min</i>		
4. Relevantie van PET's voor onvindbaren	30 min		Open discussie
5. Vervolgstappen	30 min		Open discussie
	Totaal: 135 min		

# Het op grote schaal delen van gegevens onder controle van de rechthebbende partij stimuleert innovatie en waardecreatie





# Data delen wordt gestimuleerd door NL digitaliseringsstrategie, opkomende EU wet- en regelgeving en andere EU-initiatieven

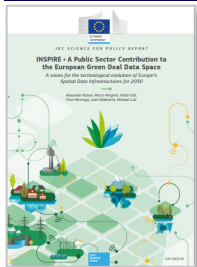


Bron: CoE-DSC analyse

# Volgend op de EU Data Strategie zijn verschillende initiatieven ontstaan om op EU schaal data spaces en infra te ontwikkelen

Niet-uitputtend

## Initiatieven met directe financiering van DIGITAL Europe



### European Common Data Spaces

Gemeenschappelijke Europese data spaces zorgen ervoor dat er meer gegevens beschikbaar komen voor gebruik in de economie en de maatschappij, terwijl de bedrijven en personen die de gegevens genereren de controle behouden.



### SIMPL

SIMPL ontwikkelt gemeenschappelijke middleware die cloud-to-edge federaties mogelijk maakt en alle belangrijke gegevensinitiatieven ondersteunt die door de Europese Commissie worden gefinancierd.



### European Alliance for Industrial Data, Edge and Cloud

De Alliance wil relevante belanghebbenden uit de private en publieke sector op het gebied van cloud en edge samenbrengen om gezamenlijk strategische routekaarten voor investeringen op te stellen.



### Data Spaces Support Centre (DSSC)

Het DSSC wil de ontwikkeling van interoperabele data spaces stimuleren door de behoefte aan data spaces te onderzoeken

## Andere private & publieke initiatieven

INTERNATIONAL DATA SPACES ASSOCIATION

### International Data Spaces Association (IDSA)

IDSA wil het bouwen van internationale data spaces mogelijk maken en stimuleren

IDSA ondersteunt data spaces in veel sectoren en ontwikkelt een referentiearchitectuur voor data spaces om het delen van data interoperabel te maken.



### Gaia-X

Gaia-X streeft naar een veilig, open en soeverein gebruik van data.

Gaia-X ontwikkelt een ecosysteem waar data kan worden gedeeld en toegankelijk is in een veilige omgeving.



### Open DEI

Open DEI stimuleert afstemming tussen EU data spaces architectuur, platforms and pilots

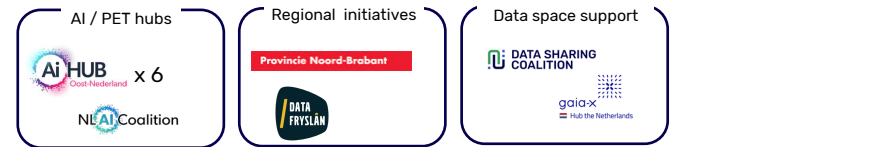
# NL data space landschap staat nog in zijn kinderschoenen, maar toenemende financiering en interesse versnellen ontwikkeling

Niet uitputtend en indicatief

## Nederlandse initiatieven gecategoriseerd per sector



## Andere Nederlandse initiatieven



## Key figures

- Ongeveer 50 NL data space initiatieven zijn in ontwikkeling in relatie tot de Common Data Spaces zoals geschetst door de Europese Commissie
- NL autoriteiten and marktpartijen hebben meer dan > EU 450 mln vrijgegeven voor de ontwikkeling van data spaces.
- NL organisaties dragen meer dan EU 96 mln € in-kind investeringen per jaar bij
- Momenteel zijn ongeveer 500 NL organisaties aangesloten op 'live' data spaces (voornamelijk door [HDN](#) en [SCSN](#))
- Slechts ongeveer 0,3% van NL organisaties zijn momenteel betrokken bij de ontwikkeling van data spaces



# CoE-DSC ondersteunt ontwikkeling van data spaces, benut harmonisatiepotentieel en onderhoudt een actieve community

## CoE-DSC programmaonderdelen

- 1 Data Spaces**



Het ondersteunen van datadeel initiatieven in verschillende stadia van ontwikkeling van een (cross-) sectorale use case
- 2 Harmonisatie**



Onderzoek en ontwikkeling om te komen tot generieke datadeelinfrastructuur
- 3 Community**



Het uitbreiden van de community met nieuwe participanten, het ontwikkelen van nieuwe partnerships en het valoriseren van resultaten

## Welke waarde willen we leveren voor initiatieven?

- **Eén centrale hub** voor support bij datadeel-uitdagingen
- **Schaarse expertise met betrekking tot datadelen** gemakkelijk vindbaar en beschikbaar maken voor de markt en initiatieven
- **Maximaal hergebruik van bestaande kennis en oplossingen**, waarbij op elkaar wordt voortgebouwd in plaats van telkens het wiel opnieuw uit te vinden
- **Zorgen voor interoperabiliteit** zodat data hergebruikt kan worden tussen organisaties, maar ook tussen sectoren
- **Inzicht in EU-ontwikkelingen en het bieden van een kanaal** naar EU-initiatieven

### Oprichtingspartners CoE-DSC:



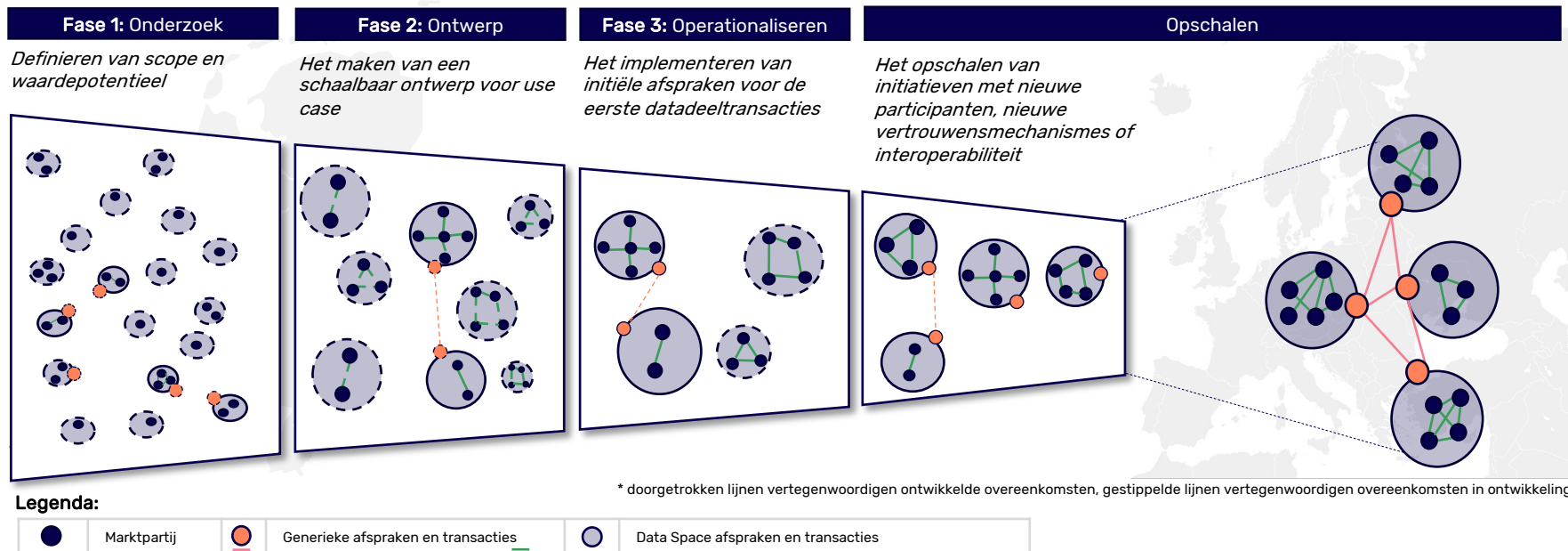
### Samenwerkingspartners:



# CoE-DSC ondersteunt initiatieven met het verkennen, ontwerpen, operationaliseren en opschalen van use cases

## Aanpak:

CoE-DSC heeft resources, tools and expertise om (AI) data space initiatieven te ondersteunen in verschillende fases van ontwikkeling



# Agenda

	<i>Tijd</i>	<i>Spreker(s)</i>	<i>Opmerkingen</i>
1. Welkom en introductie van het CoE-DSC	20 min	TBD	
<b>2. Ons begrip van de 'onvindbaren' use case</b>	<b>20 min</b>	TBD	
3. Inleiding en applicatie Privacy Enhancing Technologies	20 min	TBD	
<i>Pauze</i>	<i>15 min</i>		
4. Relevantie van PET's voor onvindbaren	45 min		Open discussie
5. Vervolgstappen	15 min		Open discussie
	Totaal: 135 min		

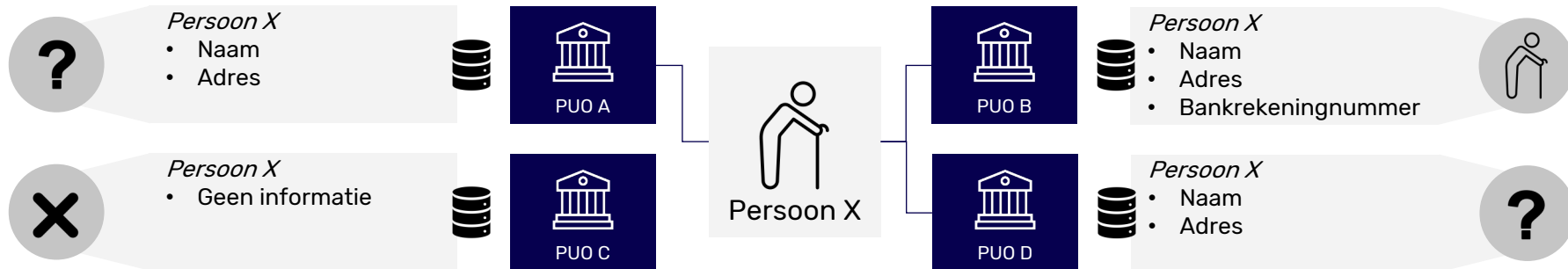
# Agenda

	<i>Tijds</i>	<i>Spreker(s)</i>	<i>Opmerkingen</i>
1. Welkom en introductie van het CoE-DSC	20 min	Freek v L.	
<b>2. Ons begrip van de 'onvindbaren' usecase</b>	<b>10 min</b>	Freek v L.	
3. Inleiding en applicatie Privacy Enhancing Technologies	30 min	Ruben vd G.	
<i>Pauze</i>	<i>15 min</i>		
4. Relevantie van PET's voor onvindbaren	30 min		Open discussie
5. Vervolgstappen	30 min		Open discussie
	Totaal: 135 min		

# Onvindbare deelnemers zijn personen van wie de benodigde informatie ontbreekt om een uitkering te doen

## Onvindbare deelnemers

- Onvindbaren zijn deelnemers die recht hebben op een uitkering maar van wie een pensioenuitvoerder niet over de juiste gegevens beschikt om tot uitkering over te gaan
- Voor het kunnen doen van een uitkering is minimaal een combinatie nodig van:
  - Naam
  - Adres
  - Bankrekeningnummer
- Pensioenuitvoerders hebben een inspanningsverplichtingen om rechthebbenden van pensioenen op te sporen en uitkeringen te verstrekken aan een deelnemer of diens erfgenaam
- Daarbij kunnen postcode en huisnummer maar ook emailadres en sociale media profielen een uitkomst bieden indien benodigde gegevens niet in volledigheid beschikbaar zijn





# Voor matching tussen pensioenuitvoerders zijn afspraken nodig en moet een technologische oplossing worden gekozen



## Uitdagingen met betrekking tot de onvindbare deelnemers

Voor discussie

- Data-uitwisseling kan het traceren van onvindbaren bevorderen, omdat data over onvindbaren soms beschikbaar is bij andere pensioenuitvoerders
- Er niet wordt getwijfeld aan de technische haalbaarheid van data-uitwisseling tussen pensioenuitvoerders. Uitdagingen voor het delen van data liggen voornamelijk op het gebied van governance, juridisch en de business case (kosten)



## Technologische oplossingsrichting

Om onvindbaren te traceren ontbreekt nog kennis over:

- **Technische oplossingsrichting:** Het is nog niet bekend welke technische oplossing het meeste waarde toevoegt in de praktijk. Ook is het gebruik van *Privacy Enhancing Technologies* nog niet verkend in eerder onderzoek
- **Business case (kosten):** Wat de kosten zijn van iedere oplossing en hoe deze in verhouding staan tussen tot de waarde van de oplossing in de praktijk

**Welke technische oplossing is het meest geschikt voor efficiënte data-uitwisseling ten behoeve van het opsporen van onvindbaren?**

- In hoeverre zijn Privacy Enhancing Technologies geschikt voor het organiseren van efficiënte data-uitwisseling?



## Afspraken

Ook ontbreken nog afspraken op het gebied van:

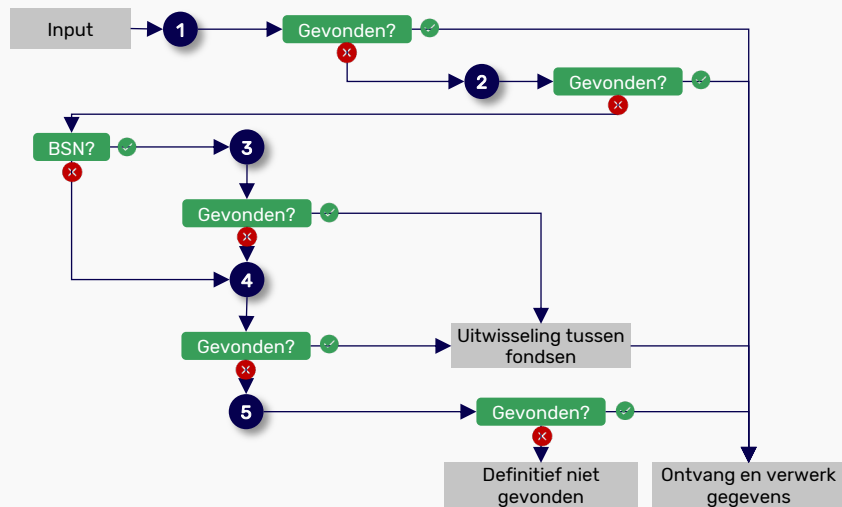
- **Governance:** Hierbij gaat het o.a. over bestuurlijke inbedding rond datadelen, taken en bevoegdheden en een nog op te richten coördinerende samenwerkingsverband
- **Juridisch:** Afspraken over contracten en juridische kaders voor gegevensuitwisseling. Dit kent een belangrijk privacy-aspect omdat de AVG van toepassing is

**Welke afspraken zijn er nodig voor efficiënte data-uitwisseling ten behoeve van het opsporen van onvindbaren?**

- Welke afspraken zijn er nodig voor een efficiënte governance m.b.t. data-uitwisseling?
- Welke afspraken zijn er nodig over contracten en juridische kaders (o.a. op het gebied van de AVG)

# Technologie bestaat om privacy bij uitwisseling van data tussen fondsen te kunnen waarborgen

In rapportage onderzoek delen data "onvindbare" deelnemers worden 5 mogelijke scenario's geschetst binnen een stroomschema



## Legenda

- 1 Zoeken tussen de verschillende pensioenuitvoerders binnen één pensioenuitvoeringsorganisatie
- 2 Zoeken bij één specifieke andere pensioenuitvoerder

## Matching in relatie tot privacygevoeligheid

- Een aantal scenario's is uitgewerkt waarin mogelijke oplossingsrichtingen worden aangedragen voor het traceren van onvindbare deelnemers
- De meest effectieve scenario's hebben betrekking tot het delen van data van deelnemers over één of meerdere andere fondsen heen om gegevens van deelnemers te matchen
- Deze scenario's waarin veel-op-veel data gedeeld wordt kennen mogelijke nadelen met betrekking tot privacy gevoeligheid
- AVG-wetgeving lijkt in eerste instantie nadelig te zijn voor toepassing van centrale matching
- Gezien de relevantie en mogelijke uitdagingen van AVG-wetgeving met betrekking tot het uitwisselen van data voor het traceren van onvindbaren moet gekeken worden naar mogelijke maatregelen

- 3 Zoeken met BSN bij Stichting Pensioenregister (SPR)
- 4 Zoeken bij meerdere andere fondsen
- 5 Zoeken met behulp van externe partijen

# Agenda

	<i>Tija</i>	<i>Spreker(s)</i>	<i>Opmerkingen</i>
1. Welkom en introductie van het CoE-DSC	20 min	TBD	
2. Ons begrip van de 'onvindbaren' use case	20 min	TBD	
<b>3. Inleiding en applicatie Privacy Enhancing Technologies</b>	<b>20 min</b>	TBD	
<i>Pauze</i>	<i>15 min</i>		
4. Relevantie van PET's voor onvindbaren	45 min		Open discussie
5. Vervolgstappen	15 min		Open discussie
	Totaal: 135 min		

# PET's kunnen helpen bij datadelen door barrières te verlagen rondom privacy, commercie en reputatie

## 3 barrières voor datasamenwerking

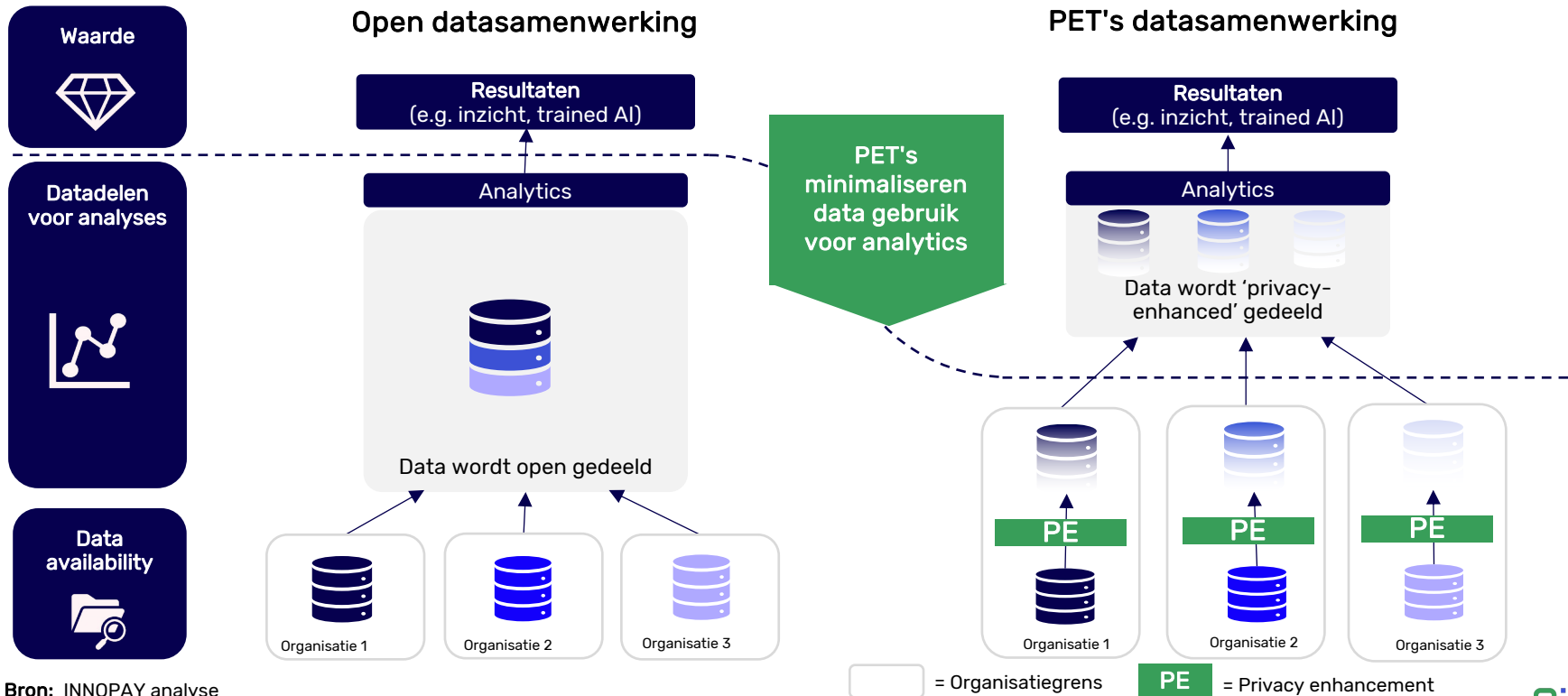
	1. Privacy barrière	2. Commerciële barrière	3. Reputatie barrière
			
<b>Beschrijving</b>	Gegevens die persoonlijk identificeerbare informatie (PII) bevatten, zijn moeilijk te delen onder de AVG	Organisaties zijn terughoudend om data te delen omdat deze commerciële waarde vertegenwoordigen en daarom worden beschouwd als belangrijke asset	Organisaties zijn terughoudend om gegevens te delen vanwege reputatieschade, waaronder schade als gevolg van het misbruik van gegevens
<b>Voorbeeld context</b>	Kenmerkend voor usecases waar gevoelige data bij betrokken zijn, zoals medische dossiers van patiënten, reispatronen van een individu, etc.	Kenmerkend voor usecases waar concurrerende partijen bij betrokken zijn. Bijvoorbeeld verzekeraars, banken, etc.	Kenmerkend voor usecases waarbij data worden hergebruikt voor andere doeleinden dan waarvoor ze oorspronkelijk zijn verzameld, zoals het monitoren van sectorprestaties, duurzaamheidsmetingen, etc.

## PET's kunnen deze barrières verlagen

- **Privacy Enhancing Technologies (PET's)** is een verzameling technieken die het mogelijk maken inzicht uit data te verkrijgen zonder de ruwe data prijs te geven
- Dit resulteert erin dat deelnemers in een datasamenwerking volledige controle houden over hun data

# Inzichten worden verkregen zonder ruwe data te delen bij het gebruik van PET's

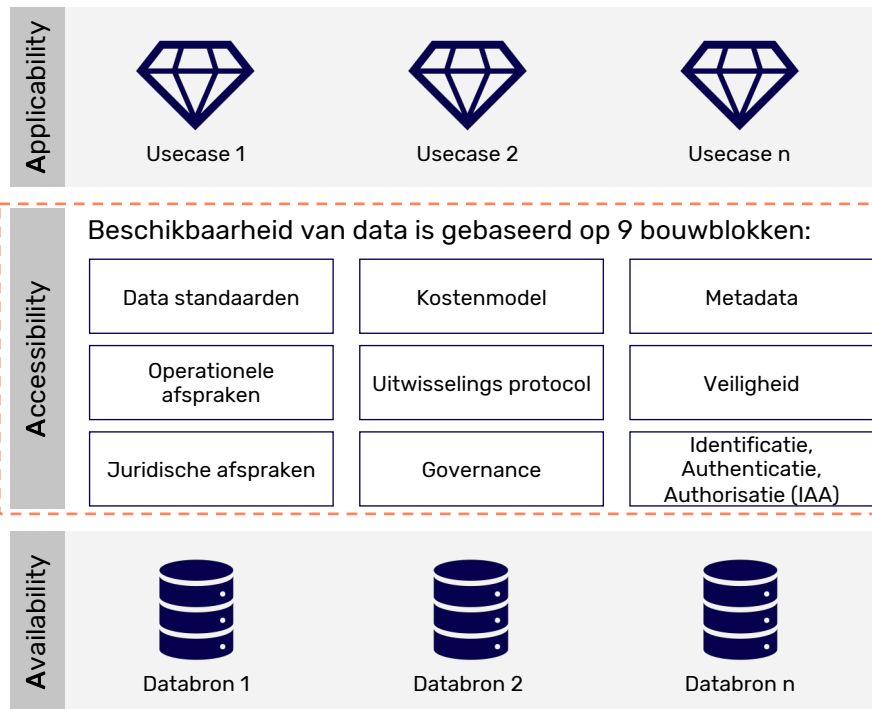
Privacy Enhancing Technologies (PET's) is een verzameling technieken die het mogelijk maken inzicht uit data te verkrijgen zonder ruwe data prijs te geven





# PET's zijn onderdeel van een bredere set afspraken om vertrouwen voor datadelen te organiseren

## Visualisatie Triple A model



- Het gebruik van PET's geeft invulling aan en beïnvloed een deel van de bouwblokken om datadelen mogelijk te maken
- PET's zijn op zichzelf nooit voldoende om datadelen te organiseren, zo bieden ze bijvoorbeeld geen antwoord op governance-vraagstukken
- Hierom zijn PET's altijd onderdeel van een bredere set afspraken om vertrouwen voor datadelen te organiseren

# MPC is de focus van vandaag omdat deze PET geschikt is voor matchingsuitdagingen

Indicative

	Privacy assessment tech	Privacy enhancing tech	
	Differential Privacy	Synthetic Data	Multi-Party Computation
<b>Beschrijving</b>	Differential Privacy (DP) geeft een maatstaf voor de mate waarin persoonlijke gegevens worden blootgesteld door een specifiek gegevensanalyse-algoritme. Het toont wiskundige parameters met betrekking tot privacy.	Synthetische data-tools transformeren datasets in nieuwe datasets met vergelijkbare statistische eigenschappen, terwijl privacygevoelige informatie uit de oorspronkelijke dataset wordt verwijderd.	MPC (Multi-Party Computation) stelt organisaties in staat berekeningen uit te voeren op gegevens op een zodanige manier dat geen enkele partij iets leert wat verder gaat dan zijn eigen input en output van deze berekeningen.
<b>Visualisatie</b>			
<b>Legend:</b>	Raw data Data with minimised PII AI model Synthetic data generation Encryption Value Measure of privacy parameter		

# MPC wordt ingezet om financiële criminaliteit op te sporen door data te delen zonder schending van privacy

## Banken worstelen met bestrijding financiële criminaliteit

### Dutch bank ING fined \$900 million for failing to spot money laundering

Special Report | **EU efforts to fight money laundering in the banking sector are fragmented and implementation is insufficient**

**The State of Tax Justice 2020:**  
Tax Justice in the time of COVID-19  
November 2020

**HSBC fined £64m for failures in anti-laundering processes**

**FCA found 'serious weaknesses' in systems used to monitor for possible criminal activity in transactions**

## Uitdagingen

### Situatie:

- Banken hebben moeite om financiële criminaliteit te bestrijden, gedeeltelijk omdat relevante gegevens versnipperd zijn over meerdere bronnen en banken. Het creëren van een gecombineerd overzicht kan banken helpen om meer inzicht te krijgen in transactiepatronen en betrokken organisaties
- Gegevens die verband houden met dezelfde entiteit moeten worden gematcht tussen datasets

### Belangrijkste barrières voor matching binnen deze usecase:

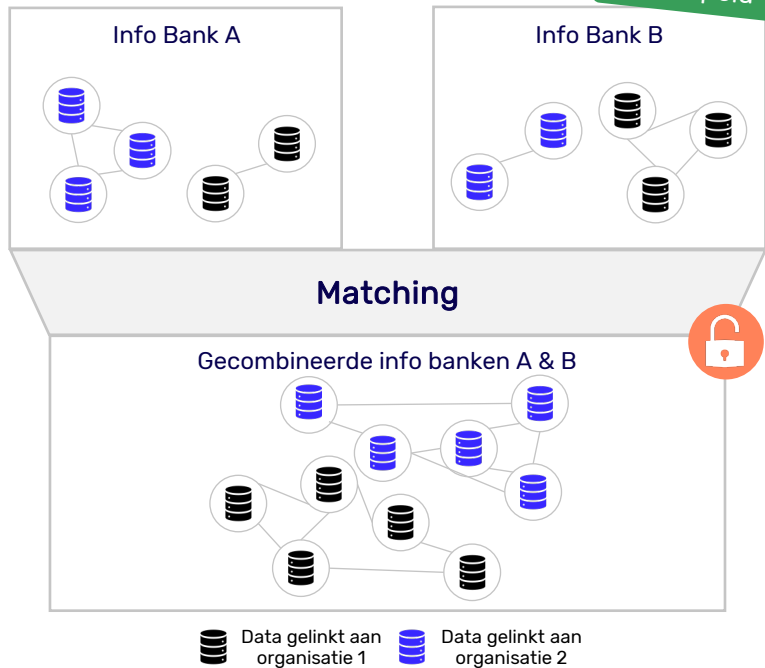
- **Privacy.** Gevoelige of vertrouwelijke informatie over klanten kan vaak niet worden gedeeld vanwege de AVG en contractuele afspraken.
- **Commercieel.** Banken zijn terughoudend om gegevens te delen omdat transactiegedrag commerciële waarde heeft.

Bronnen: [The Guardian](#), [Reuters](#), [European Court of Auditors](#), [World Economic Forum](#), [Tax Justice Network](#)

# In deze usecase stond matching van entiteiten tussen banken centraal om inzicht te krijgen in complexe transactiepatronen

## Creëren van een gecombineerd overzicht

Versimpeld



## Detecteren van verdachte transacties door informatie te combineren

Om een gecombineerd overzicht te creëren, moeten gegevens van meerdere banken worden gekoppeld aan dezelfde entiteit

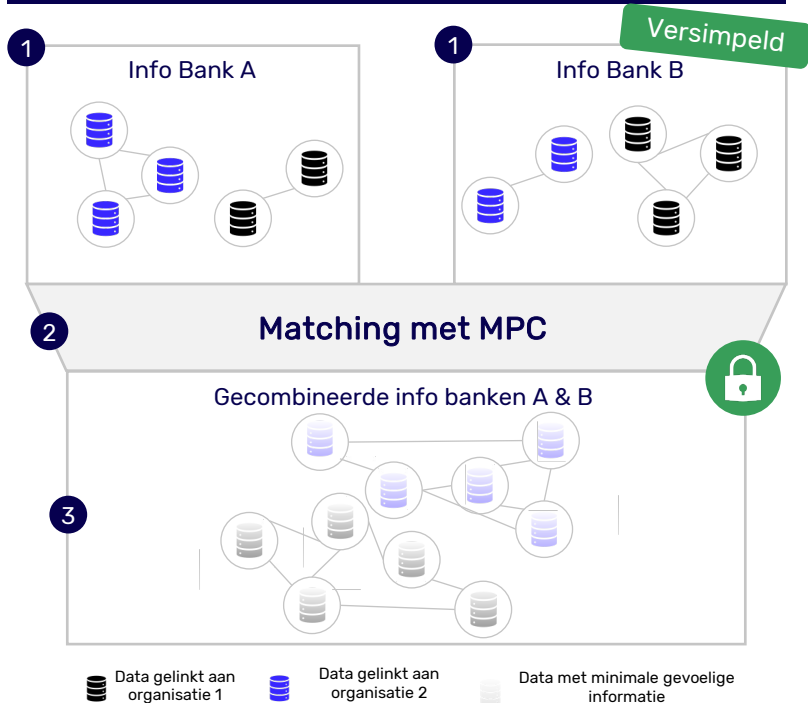
- Banken hebben alleen toegang tot hun eigen data (bijv. transactiegegevens, KYC-gegevens, enz.)
- Om een gecombineerd overzicht te creëren, moeten beschikbare gegevens van verschillende banken worden gekoppeld aan dezelfde organisatie in de echte wereld

Het uitvoeren koppelen van data op interbancair niveau is complex vanwege de gevoeligheid en vertrouwelijkheid van betreffende data

- Data uit verschillende gegevensbronnen missen vaak een gemeenschappelijke identificator (UID), wat matching complex maakt
- De resultaten van matching kunnen worden verbeterd door gevoelige en vertrouwelijke gegevens mee te nemen in de analyse
- Gevoelige en vertrouwelijke gegevens kunnen niet eenvoudig worden gedeeld buiten de grenzen van de eigen bank vanwege privacy en commerciële barrières
- Dit vormt een uitdaging voor banken die willen samenwerken om een gecombineerd overzicht te creëren

# De aanpak met MPC leidt tot meer inzicht zonder daarbij gevoelige data te delen in ruwe vorm

## Creëren gecombineerd overzicht zonder gevoelige data



## MPC maakt mogelijk gevoelige data te gebruiken zonder te delen

- Om het maximale resultaat te behalen, moeten gevoelige en vertrouwelijke gegevens worden opgenomen in de analyse
- Bij het uitvoeren van matching zonder MPC betekent dit dat gegevens op één centrale locatie moeten worden samengevoegd, waardoor deze blootgesteld worden aan minstens één andere partij
- Door te matchen middels MPC wordt gedecentraliseerde analyse mogelijk, dit betekent dat gegevens niet worden blootgesteld aan partijen buiten de grenzen van de eigen organisatie

## Uitleg matching middels MPC

- 1** De data (bijv. transactiedata, KYC-data, enz.) bevinden zich binnen elke bank
- 2** Matching m.b.v. MPC wordt gebruikt om een overzicht op interbancair niveau te creëren dat minimale gevoelige en vertrouwelijke informatie bevat
- 3** Dit gecombineerde overzicht kan worden gebruikt om verdachte transacties op interbancair niveau te detecteren zonder dat gevoelige en vertrouwelijke data kan worden ingezien door andere partijen dan de partij die de data beheert



# Agenda

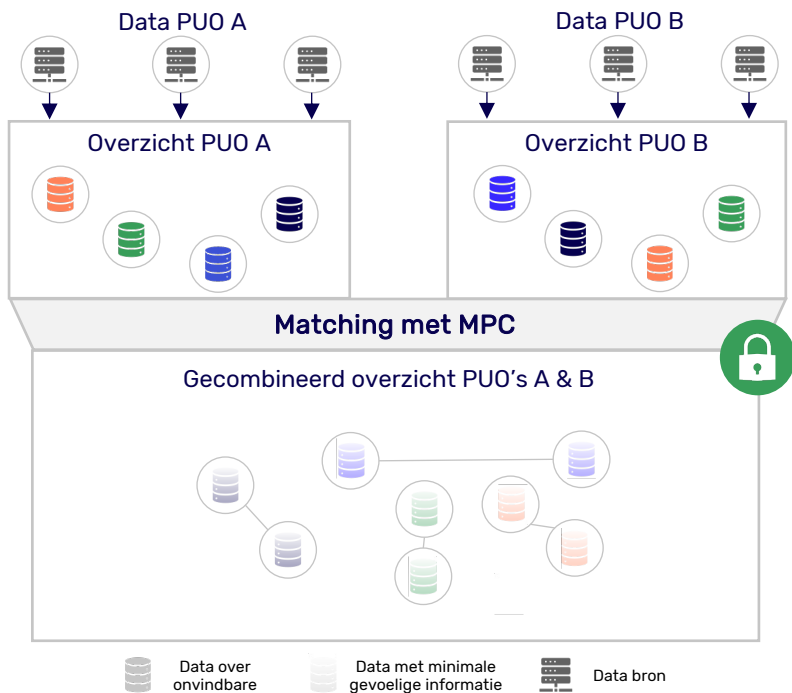
	<i>Tijd</i>	<i>Spreker(s)</i>	<i>Opmerkingen</i>
1. Welkom en introductie van het CoE-DSC	20 min	TBD	
2. Ons begrip van de 'onvindbaren' use case	20 min	TBD	
3. Inleiding en applicatie Privacy Enhancing Technologies	20 min	TBD	
<i>Pauze</i>	<i>15 min</i>		
4. Relevantie van PET's voor onvindbaren	45 min		Open discussie
5. Vervolgstappen	15 min		Open discussie
	Totaal: 135 min		

# Agenda

	<i>Tijd</i>	<i>Spreker(s)</i>	<i>Opmerkingen</i>
1. Welkom en introductie van het CoE-DSC	20 min	TBD	
2. Ons begrip van de 'onvindbaren' use case	20 min	TBD	
3. Inleiding en applicatie Privacy Enhancing Technologies	20 min	TBD	
<i>Pauze</i>	<i>15 min</i>		
<b>4. Relevantie van PET's voor onvindbaren</b>	<b>45 min</b>		Open discussie
5. Vervolgstappen	15 min		Open discussie
	Totaal: 135 min		

# M.b.v. MPC kan data van verschillende PUO's aan elkaar gelinkt worden zonder ruwe data over alle deelnemers prijs te geven

## Interactiemodel (gesimplificeerd)



## Huidig scenario met betrekking tot uitwisseling van data

- Pensioenuitvoerders hebben toegang tot eigen databronnen waarin informatie over onvindbaren beschikbaar is
- Bij het uitvoeren van matching met gedeelde data worden in het gedane onderzoek twee scenario's beschreven:
  - Een decentrale variant waarbij bilaterale connecties ontstaan tussen alle pensioenuitvoerders
  - Een centrale variant waarbij alle data bij één externe partij wordt belegd

## Uitkomst van PET's voor beschermen privacy en delen data

- Bij centrale matching zonder gebruik van MPC wordt data blootgesteld aan ten minste één externe partij
- Met behulp van MPC kunnen databronnen van meerdere pensioenuitvoerders decentraal aan elkaar gelinkt worden zodat bepaald kan worden of PUO's relevante informatie hebben zonder dat gevoelige informatie prijs gegeven wordt

## Ter discussie:

- In hoeverre kan MPC een waardevolle aanvulling zijn binnen de besproken usecase?
- Met welke factoren moet daarvoor rekening gehouden worden?



# Agenda

	<i>Tijd</i>	<i>Spreker(s)</i>	<i>Opmerkingen</i>
1. Welkom en introductie van het CoE-DSC	20 min	TBD	
2. Ons begrip van de 'onvindbaren' use case	20 min	TBD	
3. Inleiding en applicatie Privacy Enhancing Technologies	20 min	TBD	
<i>Pauze</i>	<i>15 min</i>		
4. Relevantie van PET's voor onvindbaren	45 min		Open discussie
<b>5. Vervolgstappen</b>	<b>15 min</b>		Open discussie
Totaal: 135 min			

# De volgende stap bestaat uit het definiëren van de benodigde afspraken, waarna deze verder worden ingevuld

## Visualisatie Triple A model



## Benodigde afspraken

- In 'Onderzoek Data Delen Onvindbare Deelnemers' zijn een aantal vraagstukken gedefinieerd m.b.t. het uitwisselen van data voor het traceren van onvindbaren:
  - Inrichtingsvraagstuk
  - Governance vraagstuk
  - Juridisch vraagstuk
  - Investeringsvraagstuk
- Topics voor eerste afspraken worden gezien in:
  - Juridische afspraken (*privacy-voorwaarden, standaard contracten*)
  - Governance (*bestuurlijke inbedding, eventueel op te richten coördinerend samenwerkingsverband*)
  - Uitwisselingsprotocol & data standaarden (*technische realisatie van oplossing*)
  - Kostenmodel (*business case*)

### Ter discussie:

- Op welke topics moeten minimaal afspraken worden gemaakt om tot ontwikkeling van een pilot te komen?
- Op welke topics moeten vervolgens nog afspraken worden gemaakt om tot volledige operationalisering te komen?



# Vervolgstappen- wat kunnen we samen doen?

	 <b>Achieved</b>	 <b>Next Step</b>	 <b>Ter discussie</b>
 <b>Sessie</b>	<b>Sessie 1: Mogelijkheden van PET's</b>	<b>Sessie 2: Uitwerken plan van aanpak</b>	<b>Sessie 3: ...</b>
 <b>Datum</b>	21 juni 2023	TBD	TBD
 <b>Plan (Agenda)</b>	<ul style="list-style-type: none"> <li>Het creëren van inzicht in de activiteiten van CoE-DSC en eerdere projecten PET's een uitkomst boden</li> <li>Mogelijkheden van PET's voor de 'onvindbaren' case</li> </ul>	Definiëren van afspraken die nodig zijn op het gebied van: <ul style="list-style-type: none"> <li>Governance</li> <li>Juridisch</li> <li>Technisch</li> <li>Business</li> <li>...</li> </ul>	TBD
 <b>Doel en Resultaat</b>	Inzicht in de mogelijkheden van PET's en op welke manier deze bijdragen aan het uitwisselen van data	Een opzet voor het maken van afspraken rondom o.a. taken & rollen, governance en kosten	TBD

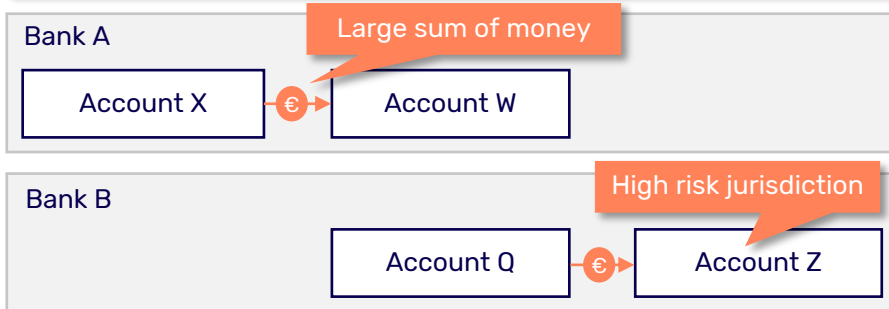
# Appendix



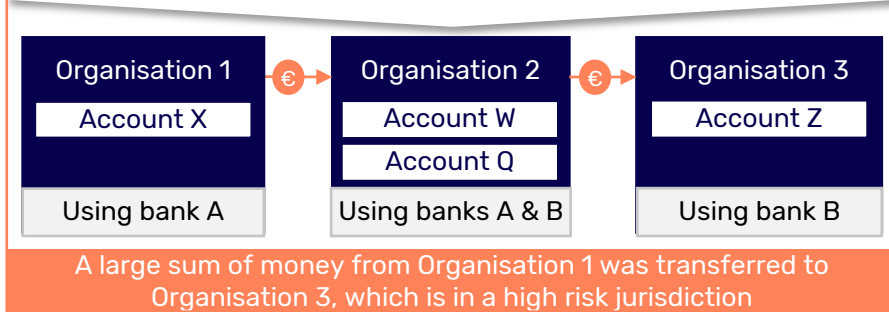
# Introducing a more detailed example of interbank matching helping in the detection of financial crime

## Example situation (simplified)

### I. What is observed by the TTP without entity resolution:



### II. What matching helps the TTP to detect:



## Value of entity resolution for detecting financial crime

- Let's assume three criminal organisations (1, 2 and 3) have set up a chain to cover up transactions. They are using Financial Institution A and Financial Institution B to transact via accounts X, W, Q, and Z:
    - Account X belongs to Organisation 1
    - Accounts W and Q both belong to Organisation 2
    - Account Z belongs to Organisation 3
  - A Trusted Third Party (TTP) conducts AML and CFT analyses. For that the TTP applies business rules to detect suspicious financial activity in the transaction patterns
  - For example, a transaction is marked suspicious if:
    - A large sum of money is transferred; AND
    - This money flows into a high risk jurisdiction
- I. The transaction isn't flagged as suspicious in the scenario where interbank matching is not used:**
- The TTP observes that a high amount of cash has been transferred from account X to account W
  - The TTP knows that account Z is located in the high risk jurisdiction
  - Transactions from X to W and from Q to Z, appear to be unrelated so no flags are raised
- II. The transaction is flagged when entity resolution is used:**
- The TTP can see that accounts W and Z belong to the same Organisation 2. And thus, the TTP can track that Organisation 1 has been transferring a large sum of money to an organisation located in a high risk jurisdiction (Organisation 3)

Legend: Bank account (blue box), Criminal Entity (dark blue box), Bank (grey box), Money flow (€ arrow)