

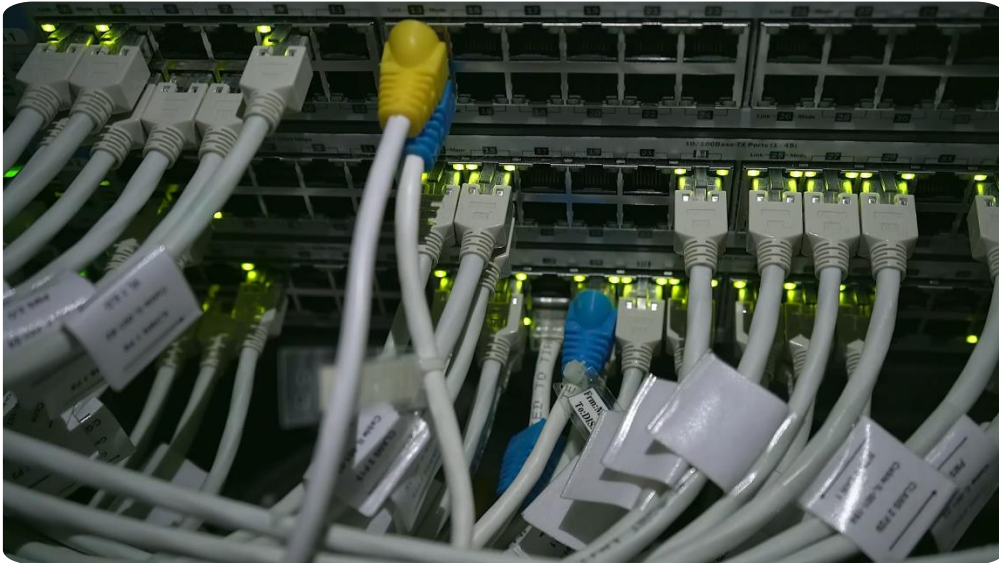
PET's, Data soeveriniteit en Data autonomie

Workshop CIO-dag 2026

Lotte Pater, *DUO*

Sulaika Duijsings-Mahangi, *IenW*





The connection tussen Privacy Enhancing Technologies, data soevereiniteit en data autonomie

Spelregels:

- Dit spel heeft 3 vragenrondes.
- Elke vragenronde bestaat uit 3 vragen.
- Elke ronde duurt 15 minuten.
- Elke groep mag 30 seconden met elkaar overleggen.
- De antwoorden uit elke vragenrondes vormen een link of ook wel een 'connection' tot 1 centraal begrip

Raden jullie waar het om draait?!???

$$F = G \frac{m_1 m_2}{d^2}$$

De drie vragenrondes

- Ronde 1: Techniek
- Ronde 2: Publieke Waarden
- Ronde 3: Use case

$$-E + V = 2$$

$$i\hbar \frac{\partial}{\partial t} \psi = \hat{H} \psi$$

$$\phi(x) = \frac{1}{\sqrt{2\pi\sigma}} e^{-\frac{x^2}{2\sigma^2}}$$

$$E = mc^2$$

$$\frac{\partial^2 u}{\partial t^2} = c^2 \frac{\partial^2 u}{\partial x^2}$$

$$\frac{df}{dt}$$



Ronde 1: vraag 1

Hoe wordt de technologie genoemd die gebruikt wordt voor het versleutelen van informatie zodat het gedeeld kan worden?

Ronde 1: vraag 1 en het antwoord is...

Cryptografie

Beoogde PET	Voor wie	Voorbeeld
Fully Homomorphic Encryption Maakt het mogelijk om berekeningen uit te voeren op versleutelde gegevens, zonder dat deze ooit hoeven te worden gedecodeerd.	Deze technologie maakt het mogelijk om gevoelige informatie zoals medische dossiers, financiële transacties of persoonlijke communicatie te analyseren en te verwerken zonder de onderliggende data te compromitteren. Dit biedt een extra laag van beveiliging en privacy die verder gaat dan traditionele encryptiemethoden.	▪ Gezondheidszorg ▪ Financiële sector ▪ Cloud computing ▪ Onderwijs en onderzoek ▪ Overheid en beleid
Multi-party computation Samenwerken met meerdere partijen om gezamenlijke gegevens te analyseren zonder deze gegevens daadwerkelijk met elkaar te delen.	MPC is niet alleen bedoeld voor organisaties waar privacy cruciaal is, maar ook voor elke entiteit die de voordelen van gezamenlijke data-analyse wil benutten zonder de risico's die gepaard gaan met het delen van gevoelige informatie. Het is een bekende techniek binnen het zorgdomein.	▪ Gezondheidszorg ▪ Financiële sector ▪ Overheid en veiligheid ▪ Supply chain
Zero-knowledge proof Aantonen dat een persoon aan een voorwaarde voldoet (bijvoorbeeld leeftijdscategorie of inkomensgrens), zonder het onderliggend gegeven (geboortedatum of inkomen) te delen.	Door de inzet van Zero Knowledge Proof kunnen zowel individuen als organisaties hun privacy en veiligheid behouden in een breed scala aan toepassingen. Het is een veelzijdige technologie die bijdraagt aan het beschermen van privacy zonder in te boeten aan functionaliteit of veiligheid.	▪ Online stemmen ▪ Leeftijdsverificatie ▪ Financiële transacties ▪ Gezondheidszorg



Ronde 1: Vraag 2

Met welke beveiligde hardware kan een organisatie veilig rekenen met data?

Ronde 1: Vraag 2 en het antwoord is...

Beoogde PET	Voor wie	Voorbeeld
Trusted Execution Environment (TEE) Een afgesloten omgeving inrichten om daarbinnen gevoelige data te berekenen. Dit maakt de kans op een privacylek minimaal.	TEE's zijn geschikt in situaties waar een extra laag van beveiliging nodig is rond de verwerking van gegevens. Dit is met name relevant voor overheidsorganisaties en individuen die werken met gevoelige of bedrijfskritische informatie.	▪ Medische gegevens ▪ Financiële transacties ▪ Overheid en verkiezingen ▪ Persoonlijke gegevensbescherming ▪ Veiligheidsdiensten



Ronde 1: vraag 3

Welke methodiek wordt gebruikt om aan de hand van patronen te leren en te delen uit data?

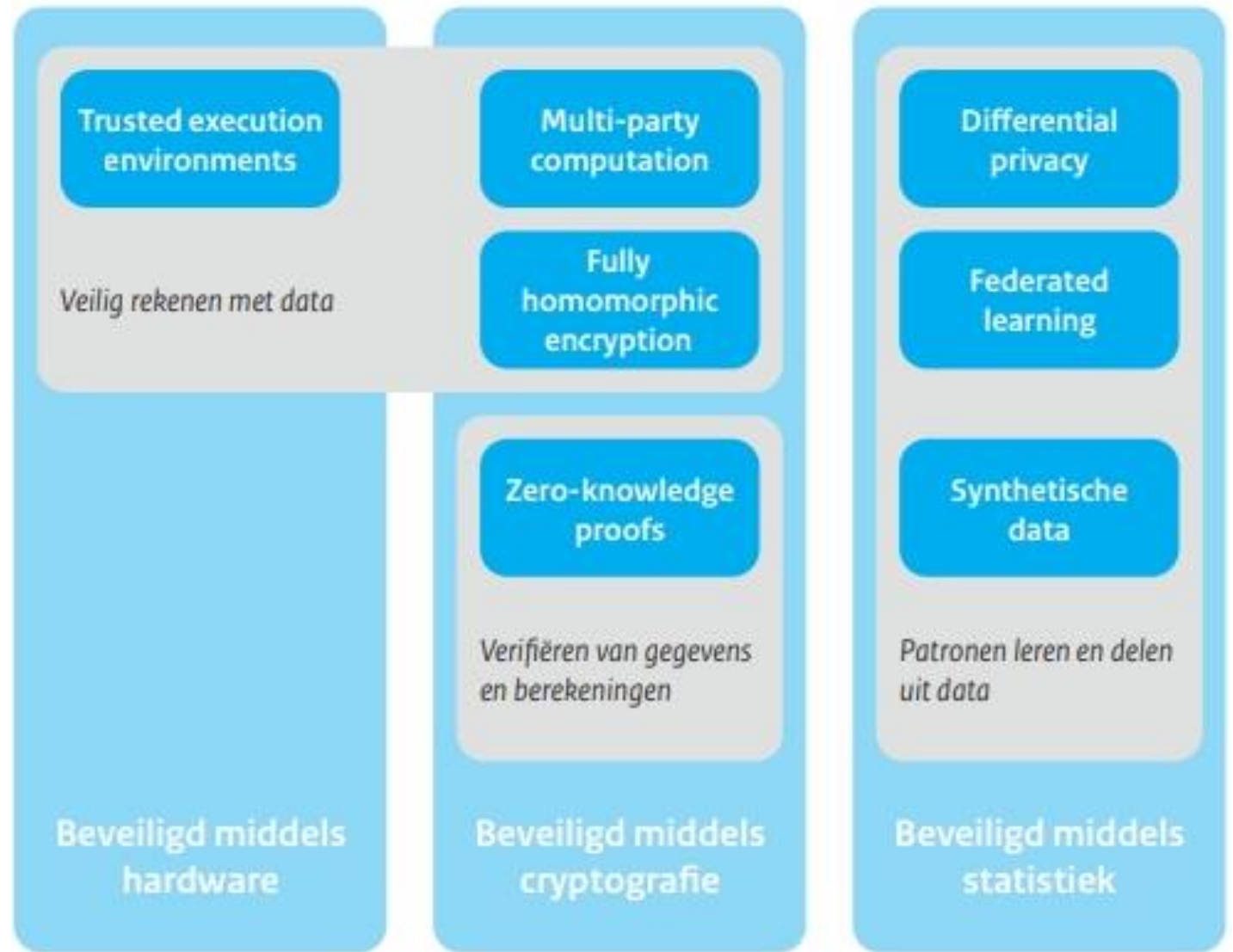
Ronde 1: vraag 3 en het antwoord is...

- Statistiek

Beoogde PET	Voor wie	Voorbeeld
Differential Privacy Waardevolle inzichten uit grote hoeveelheden data halen zonder de privacy te schenden.	Differential Privacy is nuttig voor overheidsinstellingen die grote hoeveelheden gevoelige data analyseren. Het is bovendien waardevol voor burgers die willen dat hun persoonlijke informatie privé blijft, zelfs als deze wordt opgenomen in grootschalige data-analyses. Grootschaligheid is daarbij wel een voorwaarde voor succesvolle toepassing van differential privacy.	▪ Volksgezondheid ▪ Marketing ▪ Onderwijs
Synthetische data ‘Echte’ data nabootsen door kenmerken en structuren aan te nemen die lijken op die van de originele data. Gebruik de synthetische data voor analyse en onderzoek zonder de gevoelige data te gebruiken.	Synthetische data zijn geschikt voor elke situatie waarin data-analyse nodig is maar waar privacy een belangrijke overweging is.	▪ Trainen van ingewikkelde datamodellen ▪ Gezondheidsonderzoek ▪ Verkeersplanning ▪ Marktonderzoek
Federated learning Machine learning modellen trainen op data die op verschillende plekken staat, zonder dat de data de bron verlaat.	Federated Learning is vooral nuttig voor organisaties met machine learning toepassingen die te maken hebben met gevoelige of verspreide data.	▪ Gezondheidszorg ▪ Financiële sector ▪ Internet of Things ▪ Telecommunicatie

Om een beeld te krijgen waar we over praten

Bron: AIVD
Databescherming met
Privacy Enhancing
Technologies



Ronde 1: Woord 1



CRYPTOGRAFIE



TRUSTED
EXECUTION
ENVIRONMENT



STATISTIEK

Privacy Enhancing Technology

Ronde 1: Woord 1



CRYPTOGRAFIE



TRUSTED
EXECUTION
ENVIRONMENT



STATISTIEK

Privacy Enhancing Technology

De organisatie kan PET's zelf inrichten naar eigen wensen eisen. Dit draagt bij aan **data autonomie** van de organisatie.

PET's kunnen in meer of mindere mate vallen onder het regime dat gekozen wordt door de organisatie. Dit draagt bij aan **data soevereiniteit** van de organisatie



Ronde 2: vraag 1

Welk publiek goed wordt
nagestreefd door de AVG?

Ronde 2:
vraag 1 en
het antwoord
is...

Privacy





Ronde 2: vraag 2

Welk publiek goed wordt
nagestreefd door de WOO?



Ronde 2:
vraag 2 en
het antwoord
is...

Openheid /
transparantie





Ronde 2: vraag 3

Op basis van welk principe (ook onderdeel van haar titel) heeft staatssecretaris Willemijn Aerdts de overname van Solvinity geblokkeerd?

Ronde 2:
vraag 3 en
het antwoord
is...

Digitale soevereiniteit



Ronde 2: Woord 2



PRIVACY

OPENHEID

DIGITALE
SOEVEREINITEIT

Publieke waarden

Synthetische Data





Synthetische Data

- Idee:
 - Privacy: individueel niveau
 - Informatie: structuurniveau
- Synthetische data:
 - Nep op individueel niveau
 - AVG niet van toepassing
 - Zelfde conclusies op structuurniveau
- Use case: Personeelsdata MBO

Geanonimiseerd vs. Synthetisch

Originele data¹

BSN	Werk-gever	Geslacht	Leeftijd	Bruto Salaris
027150926	Albeda	M	58	€5229
770002080	Yuverta	V	40	€3264
202275590	Rijnland	M	64	€4615

Geanonimiseerde data¹

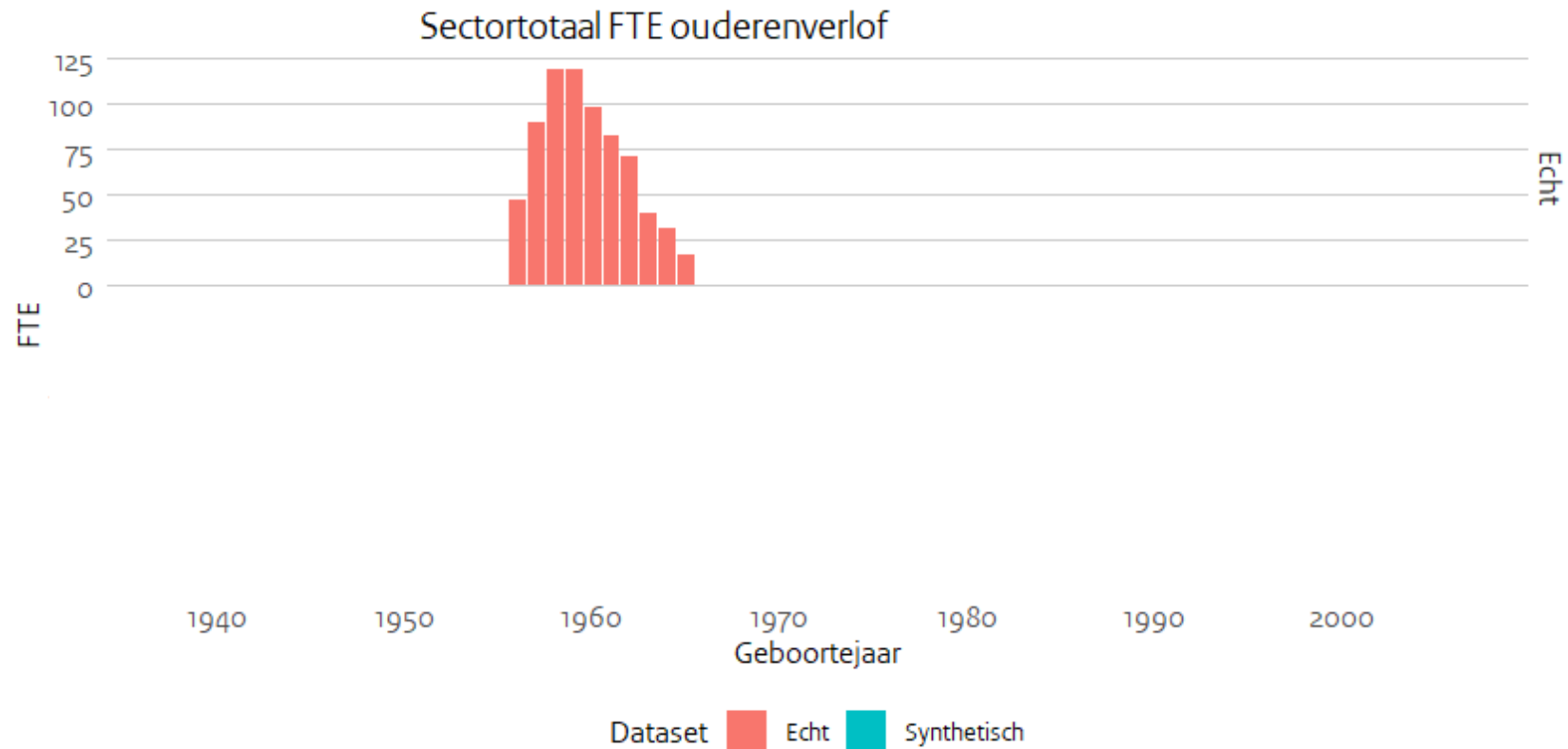
BSN	Werk-gever	Geslacht	Leeftijds-groep	Bruto Salaris
027150926	1	M	56-50	€5000-5500
770002080	2	V	36-40	€3000-3500
202275590	3	M	60-65	€4500-5000

Synthetische data¹

BSN	Werk-gever	Geslacht	Leeftijd	Bruto Salaris
601288208	Rijnland	V	58	€5229
586026228	Albeda	M	28	€2643
329283972	Albeda	V	59	€4615

¹: Fictieve BSNs uit BSN generator zijn gebruikt.

Use case: Data MBO personeel tbv CAO-onderhandelingen



Vragen?