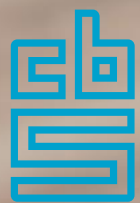


PPA project met



Population Health Data

28 januari 2022

Inhoud

- Succes
- Project
 - Use case
 - Oplossing
 - Doel
 - Aanpak
- Platform
- Lessons Learned

Succes

Eerste toepassing in NL van MPC op echte patiëntgegevens!

- Uitgangspunt echte data: technisch en juridisch gevalideerd
- Volledig decentraal
- Alle partijen analyses gedaan
- >2 partijen in MPC protocol

Succes: oprichting TNO spinoff



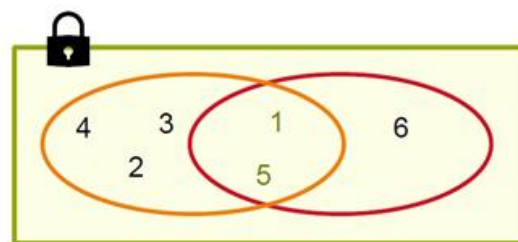
Project: use case 'validatie effectiviteit IBD coach'



ID	Gebruikt Coach?	PROMS
1	J	1
2	N	3
3	J	2
...

'Wat is de **gemiddelde PROMS score** voor **lager opgeleiden**?'

ID	Zorgsoort	Kosten
1	E	100.000
2	B	5.000
3	A	300
...	..	



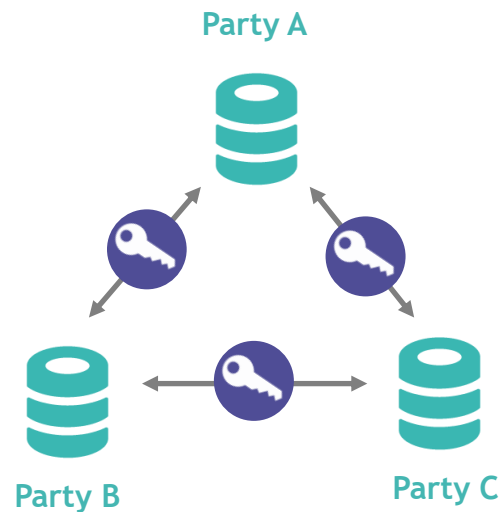
'Wat is het **aantal coach gebruikers** met een **hogere opleiding**?'

'Wat zijn de **gemiddelde zorgkosten** van **coach gebruikers** met een **hoger inkomen**?'

ID	Opleidings-nivo	Inkomen
1	1	25.000
2	5	100.000
3	3	33.000
...	..	



Oplossing: analyseren **zonder** data delen



- Berekeningen op volledig versleutelde data
 - secure Multi Party Computation, (MPC)
- Decentrale governance
 - Business rules & audit trail

Project: doel

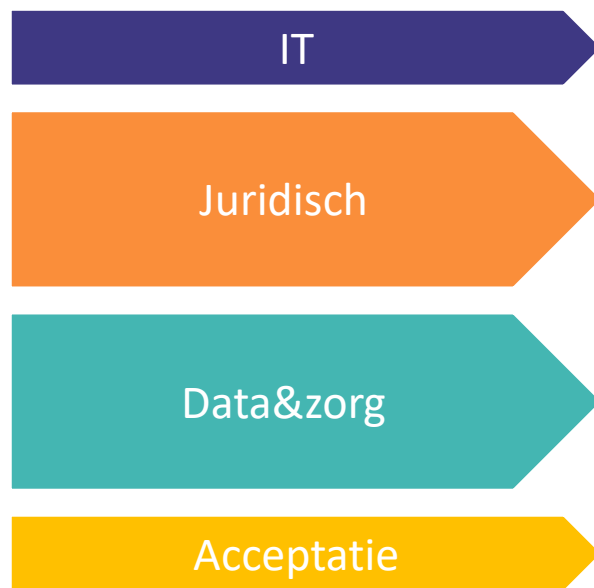
● Validatie van de technologische en juridische aspecten van PPA platform:

- Technisch → Kan het?
- Juridisch → Mag het?
- Acceptatie → Hoe leg je het uit?

● Aan de hand van een concrete use case met echte data!

Project: aanpak

Vorbereidende fase

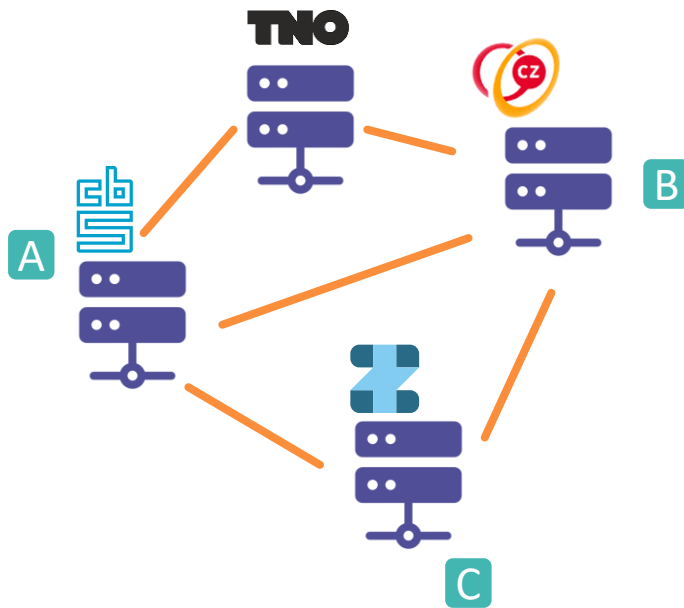


Analyse fase



Platform: versimpelde architectuur

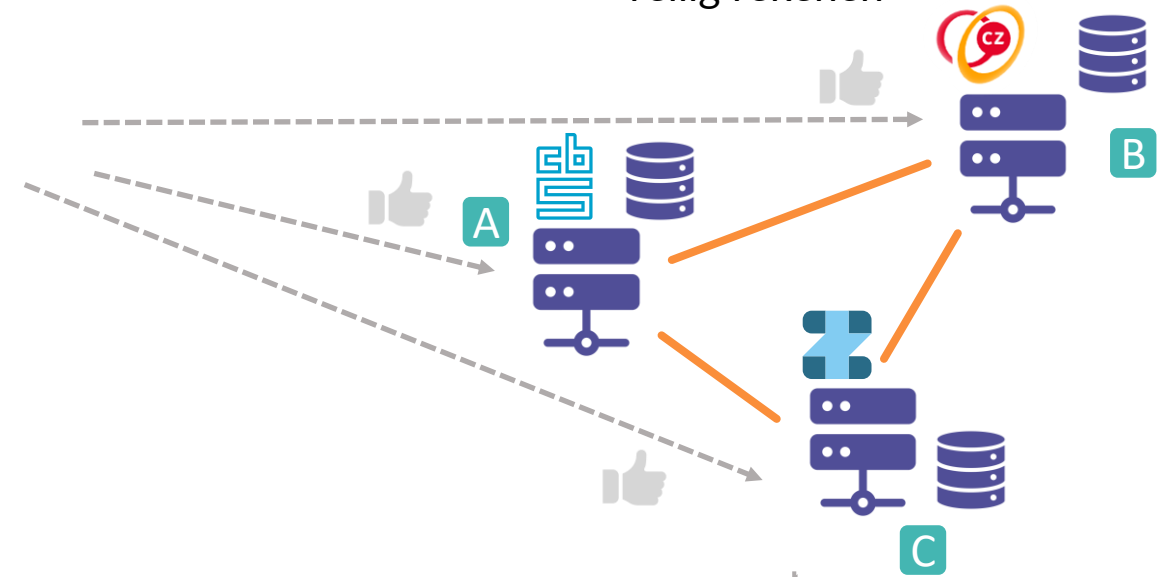
Blockchain netwerk t.b.v. governance & auditlog



Smart contract met governance regels



MPC netwerk t.b.v. veilig rekenen



Resultaat berekening



Lessons learned: juridisch

Versleutelde gegevens zijn pseudoniemen → AVG van toepassing

- Stap 1: Grondslag
- Stap 2: Gezamenlijke DPIA
- Stap 3: Joint controller agreement
- Stap 4: Governance borgen
- Stap 5: Ethisch perspectief

Lessons learned: acceptatie

$$\ell_i = \left(\prod_{j \in T, j \neq i} (-j) \right) \cdot \left(\frac{\nu}{\prod_{j \in T, j \neq i} (i - j)} \right)$$

$$\lambda := \text{lcm}(p-1, q-1),$$

$$\mu := (L(g^\lambda \bmod n^2))^{-1} \bmod n,$$

$$L(x) := (x-1)/n.$$

Lessons learned: technisch

- Schaalbaarheid
- Algoritmen
- Technische governance

Op naar meer datasamenwerkingen!

Vertel ons je uitdaging: martine@linksight.nl

Curious to learn more?

martine@linksight.nl

0615621883

www.linksight.nl