

Privacy Enhancing Technologies



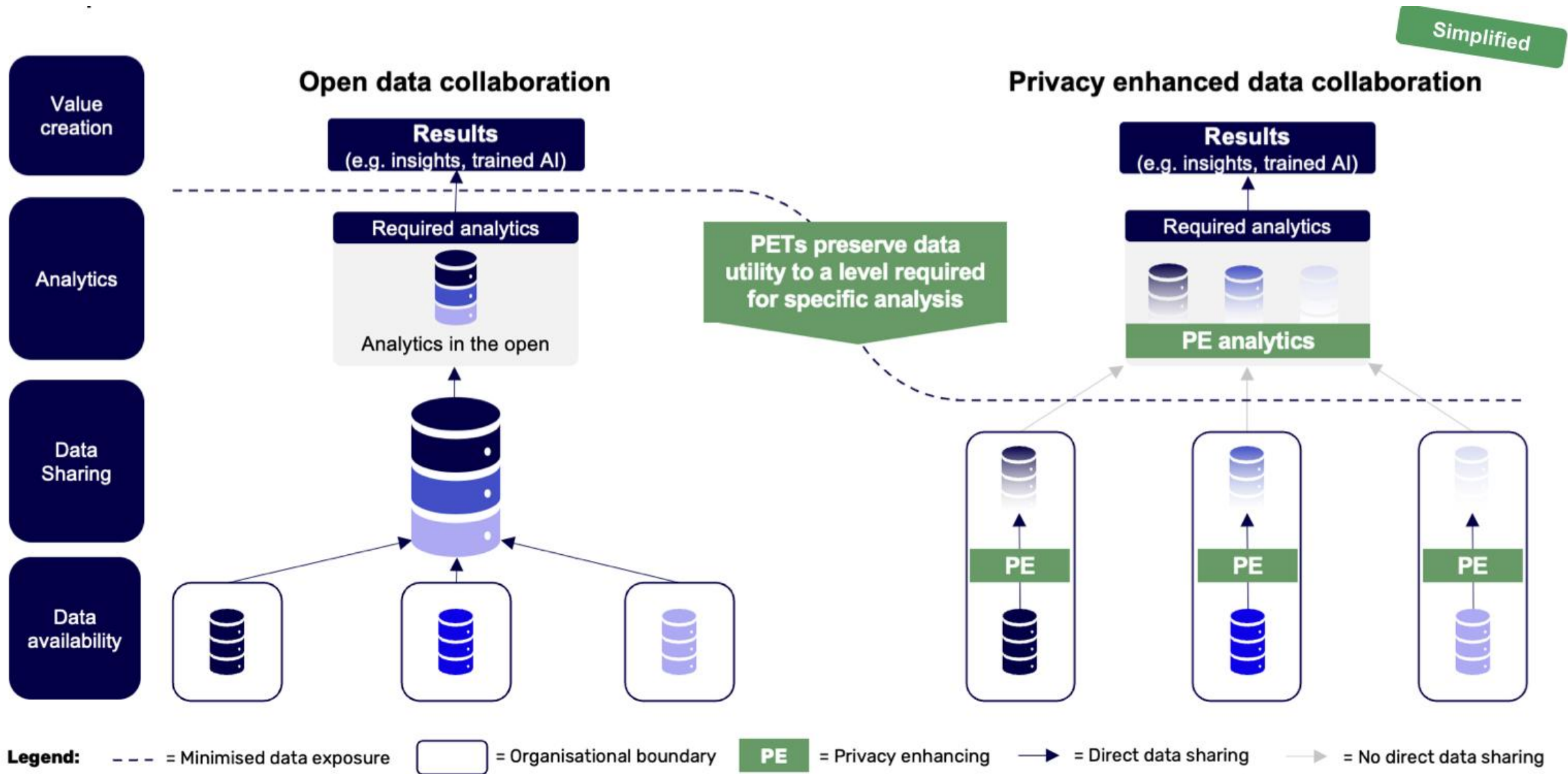
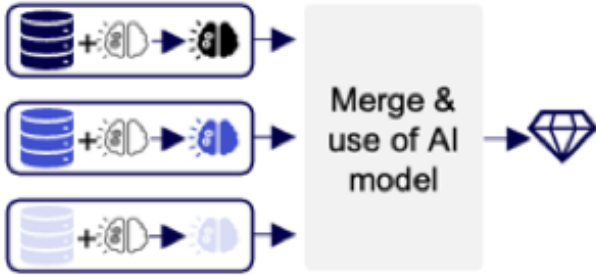
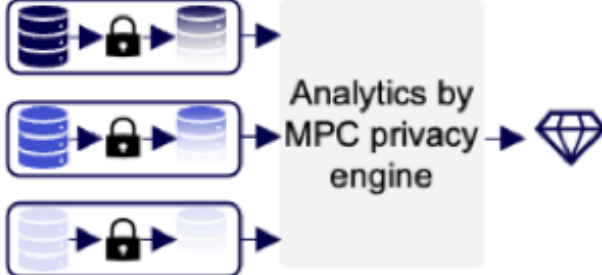


Figure 1. Differences between open and privacy enhanced data collaborations

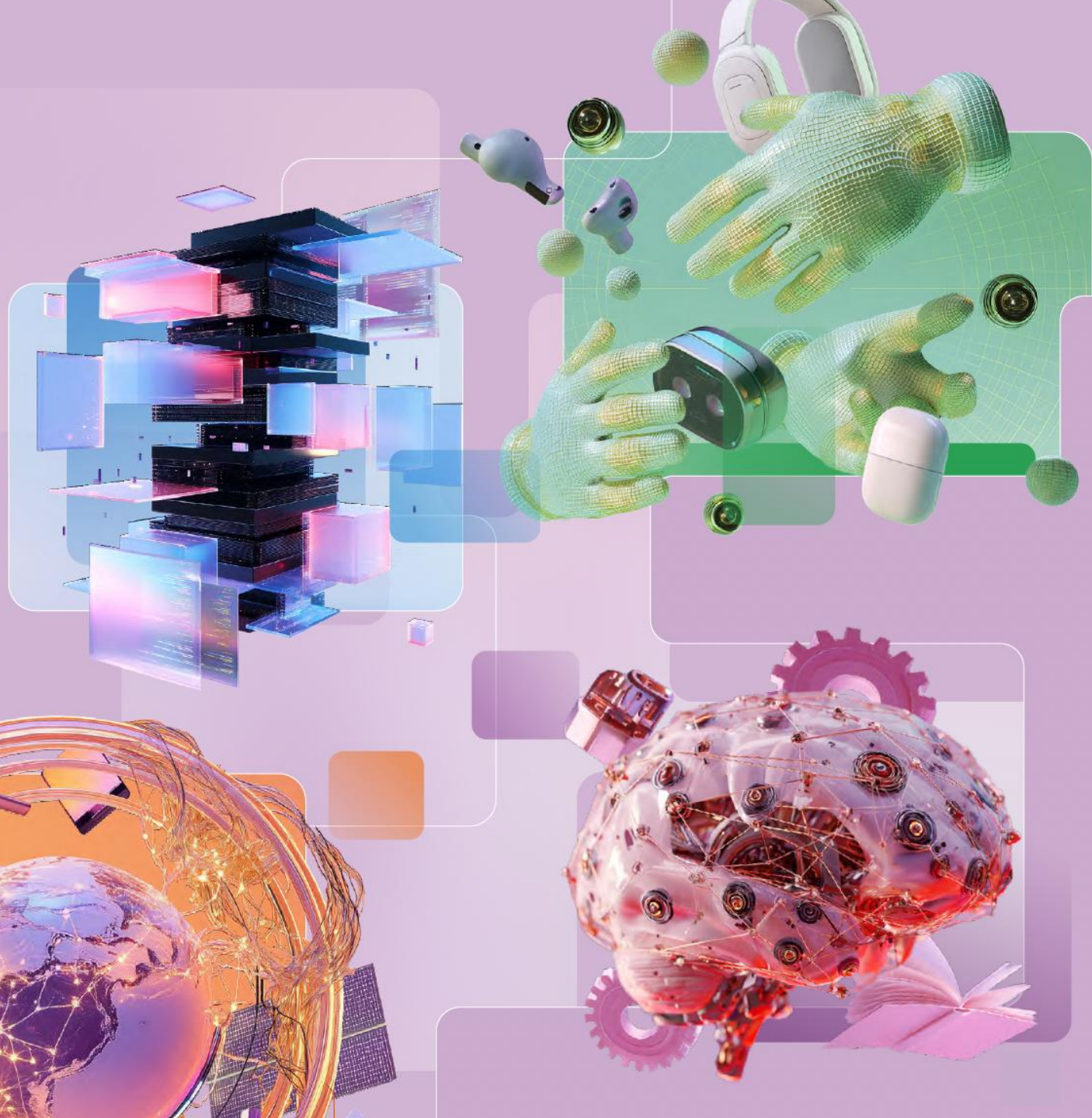
	Privacy Enhancement Technologies		
	Synthetic data	Federated Learning (FL)	Multi-Party Computation (MPC)
Illustration			
Description	Synthetic data tools transform a dataset into a new data set with similar statistical properties while removing privacy sensitive information from the original data set.	Federated learning trains one 'overarching' AI model by locally training 'sub' AI models, removing the need to share & combine the original data sets.	Family of encryption schemes for computation on encrypted data. E.g.: • Secret sharing • Circuit garbling • Homomorphic encryption

SURF TECH TRENDS 2026



Interactieve website
Klik en blader door de
hoofdstukken op
techtrends.surf.nl

SURF



Toegankelijkere privacyverhogende technologieën (PETs) voor datadeling

- Inzet van PETs zoals differentiële privacy, synthetische data sets, federatief leren en homomorfe encryptie
- Biedt kansen voor privacy-gerichte datadeling en data-analyse tussen meerdere partijen
- Vormt een aanvulling op traditionele security-by-design benaderingen met data-centrische controles

