Deutsche Stiftung für Recht und Informatik

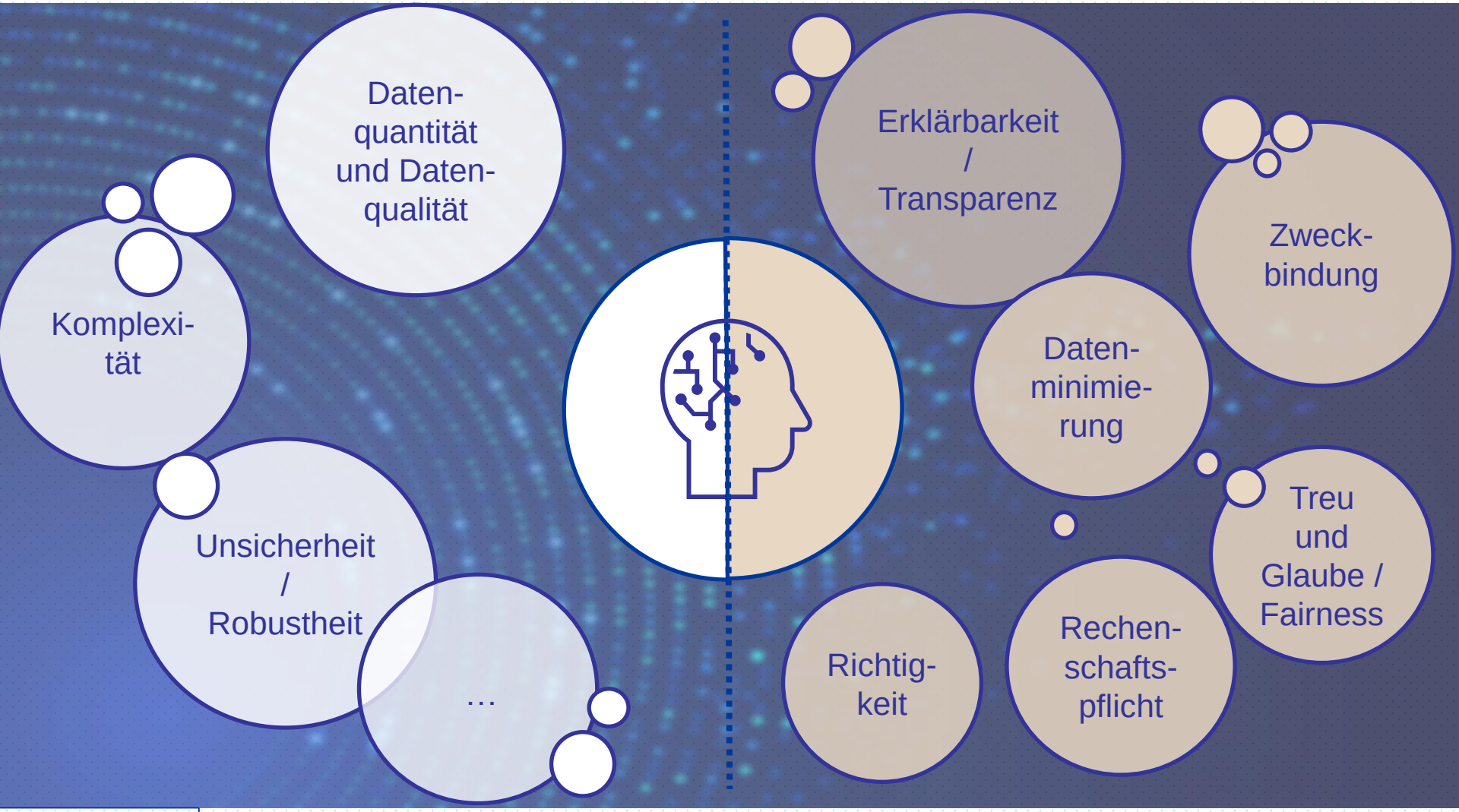
Privacy Enhancing Technologies – Ein Ansatz zur Minimierung datenschutzrechtlicher Risiken beim Einsatz Künstlicher Intelligenz

Nadia Schaff & Dragana Dujak

Pinsent Masons Rechtsanwälte Steuerberater Solicitors Partnerschaft mbB

Herbstakademie 2023

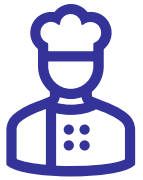
Spannungsfeld: Künstliche Intelligenz & Datenschutz



Privacy Enhancing Technologies (PETs) als Lösung?

Was sind PETs überhaupt?

- Technische Grundbausteine
- *Data protection by design or by default*



Kategorien von PETs

Input Privacy
Steuerung Zugang zu personenbezogenen Daten

Output Privacy
Steuerung Zuordnungs-möglichkeiten Daten-Output

Ansätze

- Datenminimierung
- Verbergen / Verwischen
- Teilen / Steuern

Beispiele für PETs

Datenminimierung

- Differential Privacy; Anonymisierung
- Synthetische Daten

Verbergen / Verwischen

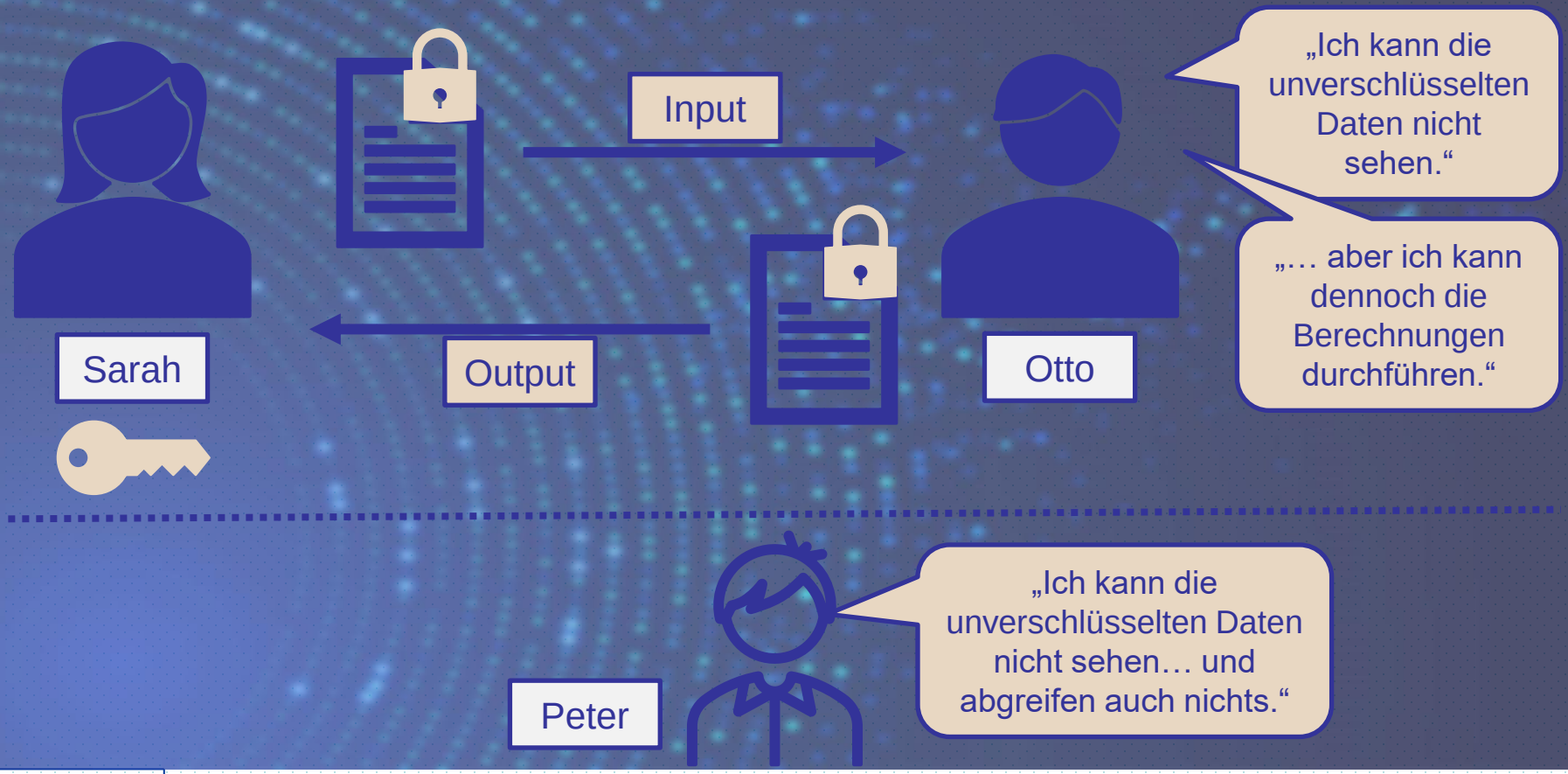
- Homomorphe Verschlüsselung
- Hashing
- Zero-Knowledge Proof
- Trusted Execution Environments

Teilen / Steuern

- Secure Multi-Party Computation; Private Set Intersection
- Federated Learning

Homomorphe Verschlüsselung

- Übertragung und anschließende Berechnung erfolgt verschlüsselt
- Auslagerung von Daten und Berechnungen; Gesundheits- / Sozialwesen



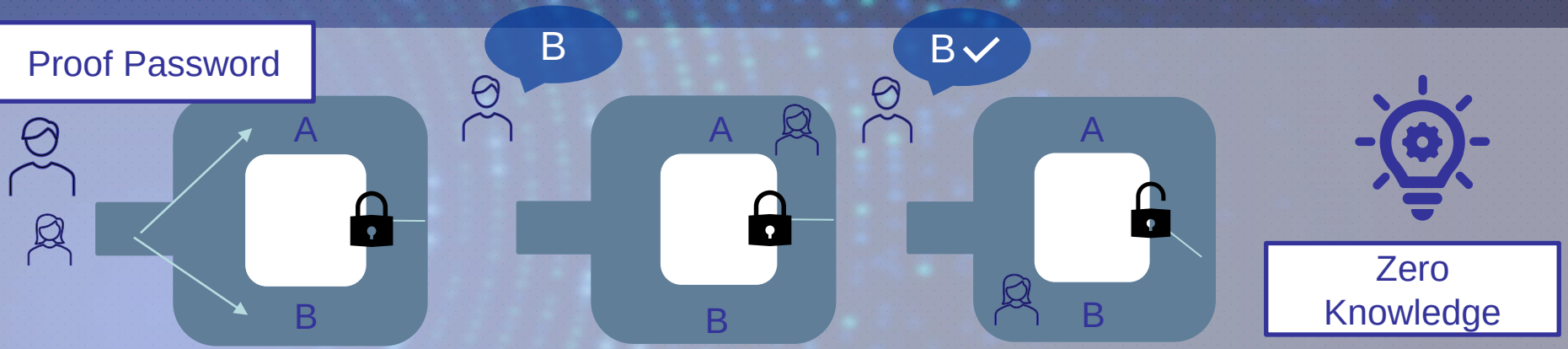
Zero-Knowledge Proof

Proof Age

Zero Knowledge

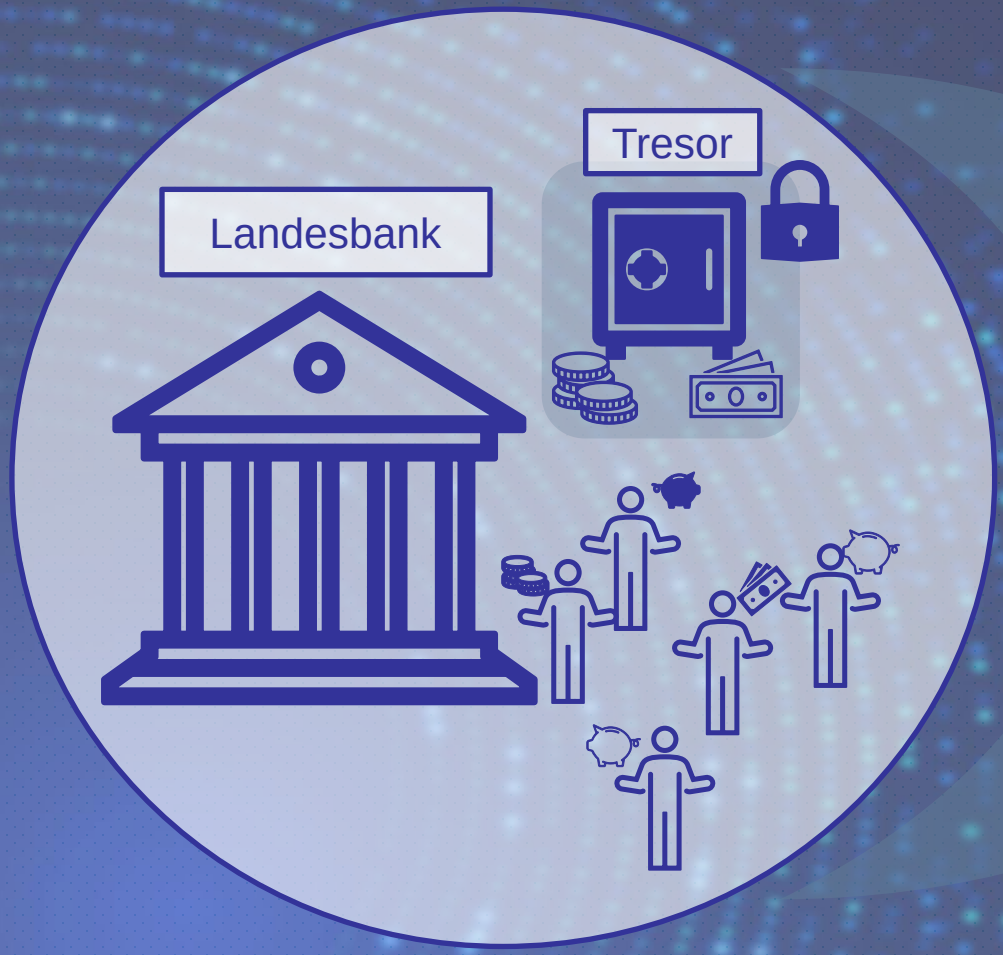
Beweisverfahren zur Bestimmung der Gültigkeit einer Aussage

Proof Password



Zero Knowledge

Trusted Execution Environments



Sicherer, von dem übrigen System isolierter, Bereich

Federated Learning

- Training erfolgt lokal
- Übermittlung Ergebnis (!) an zentrale Instanz → Weiterentwicklung zu globalem Modell
- Aggregierung an lokale Systeme