So geht neuer Datenschutz!

Technische Lösungen für mehr digitale Privatsphäre & leistungsfähige KI.

Professor Michael Huth
Co-Founder & Chief Research Officer Xayn
Head of Department of Computing at Imperial College London

23. November 2021
DATEV-BFB Digital2gether

Das Datenschutz-KI-Dilemma

Künstliche Intelligenz

Je mehr gute Daten

- desto besseres Training
- desto leistungsfähigere KI

Leistungsfähige KI und ausreichender Datenschutz scheinen unvereinbar

Gewöhnliche, zentralistische KI-Ansätze kommen an ihre Grenzen

Datenschutz

Je mehr gesammelte Daten, desto größere Gefahr von

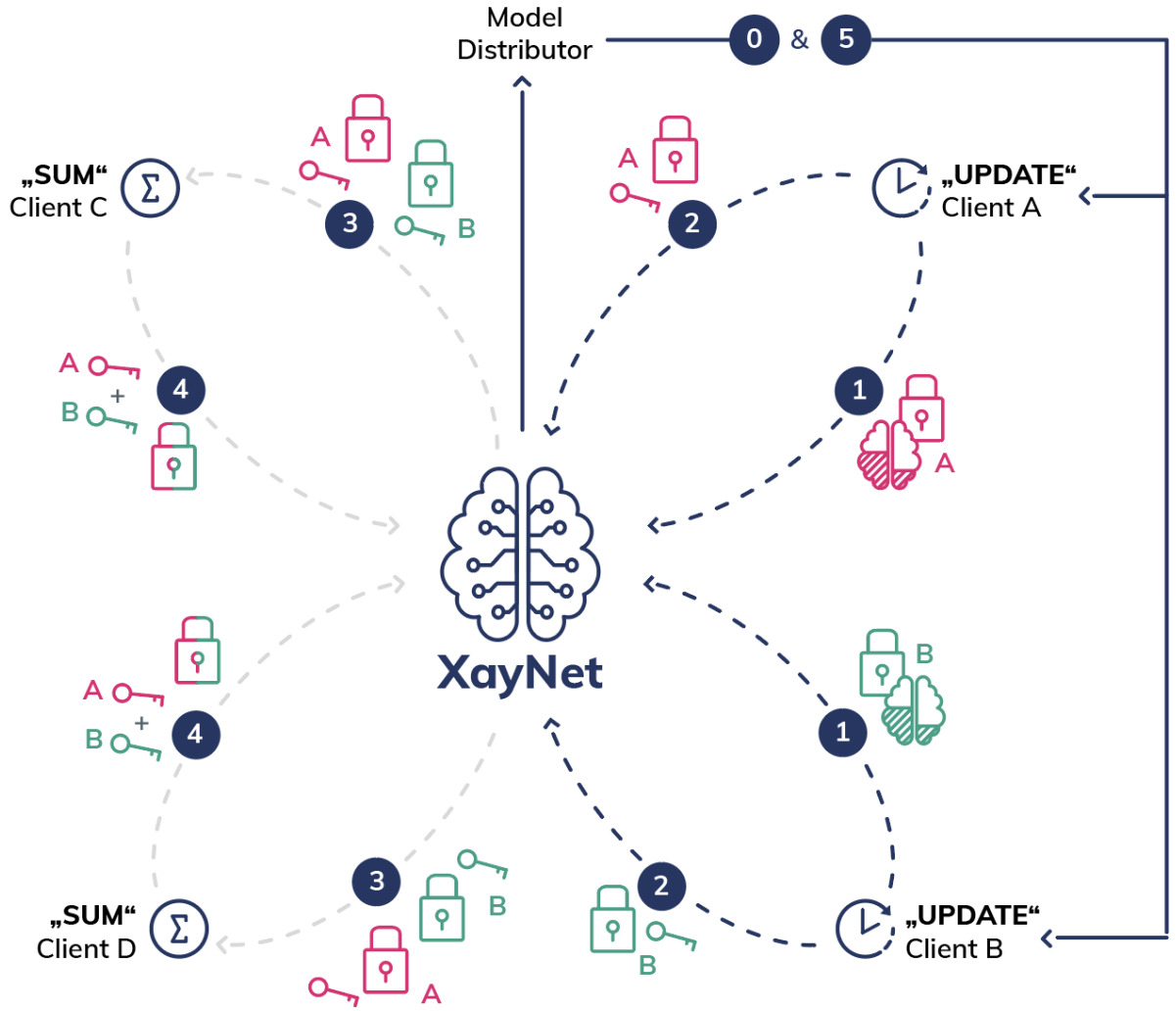
- unlauterem Datenmissbrauch
- unzureichender Datenschutztechnologie
- potenziellen Hacks/Datendiebstähle

Masked Federated Learning

Funktionsweise:

- alle Rohdaten bleiben auf den Endgeräten
- KI-Modelle lernen lokal und werden verschlüsselt verschickt (homomorphe Verschlüsselung)
- Verschlüsselte Modelle werden zu globalem Modell aggregiert

Mehr Informationen zur Open-Source-Plattform **XayNet**: https://www.xaynet.dev/



Computing on the edge

Vorteile

Schützt digitale Privatsphäre (DSGVO-konform)

Funktioniert asychnron

Leichter hoch skalierbar

Resilienter gegenüber potenziellen Angreifern

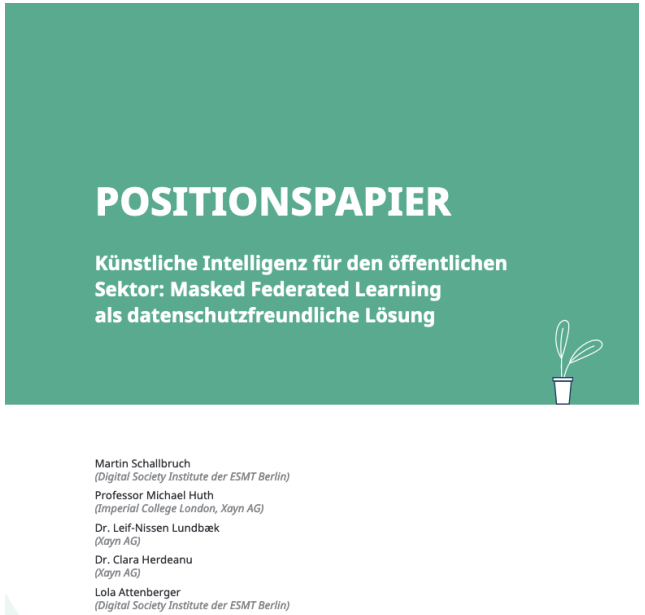
Cross-silo und cross-device Anwendungen möglich

Potenzielle Anwendungen

Positionspapier

Gemeinsames **Positionspapier** des **Digital Society Institute** der ESMT und **Xayn**

- Potenzielle Anwendungen datenschutzfreundlicher KI im öffentlichen Sektor
  - **Gesundheitswesen**:
    - Kombination aus cross-silo/device Anwendungen für bessere Pandemiebelämpfung
  - **Strafverfolgung**:
    - Früherkennung von Straftaten durch datenschutzfreundliche Datenanalyse



Kostenfreier Download, Juni 2021

Probleme der Suchmaschinen

Datenschutz

Convenience

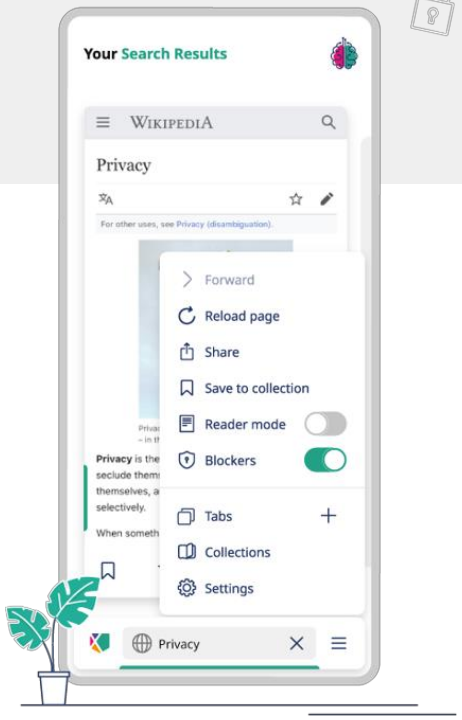
Startpage.com & DuckDuckGo	**Anbieter**	Google & Bing
Datenschutz, da keine Tracker	**Fokus**	**Convenience** & UX durch Datenmengen (z.B. für Personalisierung)
- **Rückschritt** in Technologie - **Schlechtere** Nutzererfahrung & Ergebnisse	**Probleme**	- **Missbrauch** von Nutzerdaten - **Geschäftsmodell** unvereinbar mit Datenschutz

"Users are always the losers"

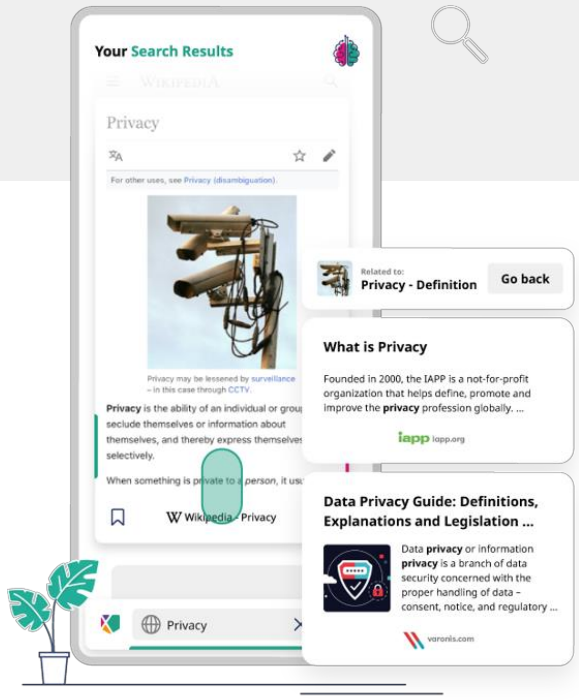
Nutzer verlieren entweder Zeit oder Daten

Xayn App

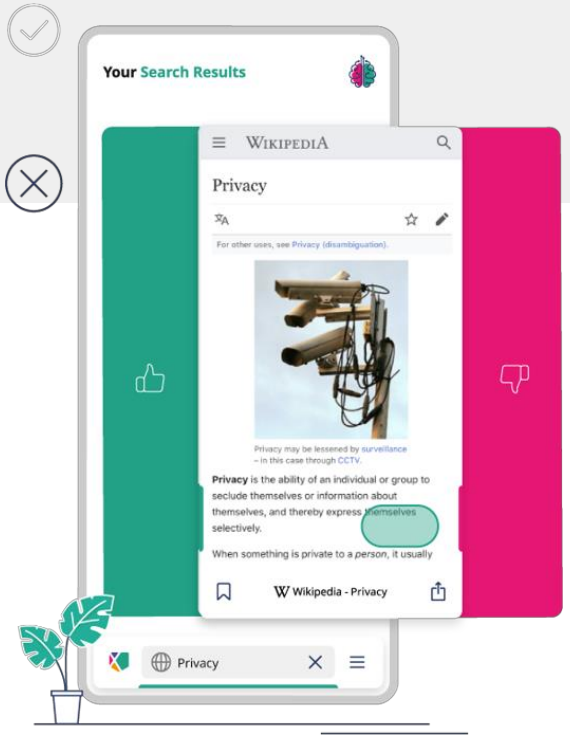
Datenschutz und Nutzerfreundlichkeit durch KI



Datenschutz durch computing on the edge – **alle Daten bleiben auf dem Gerät.**



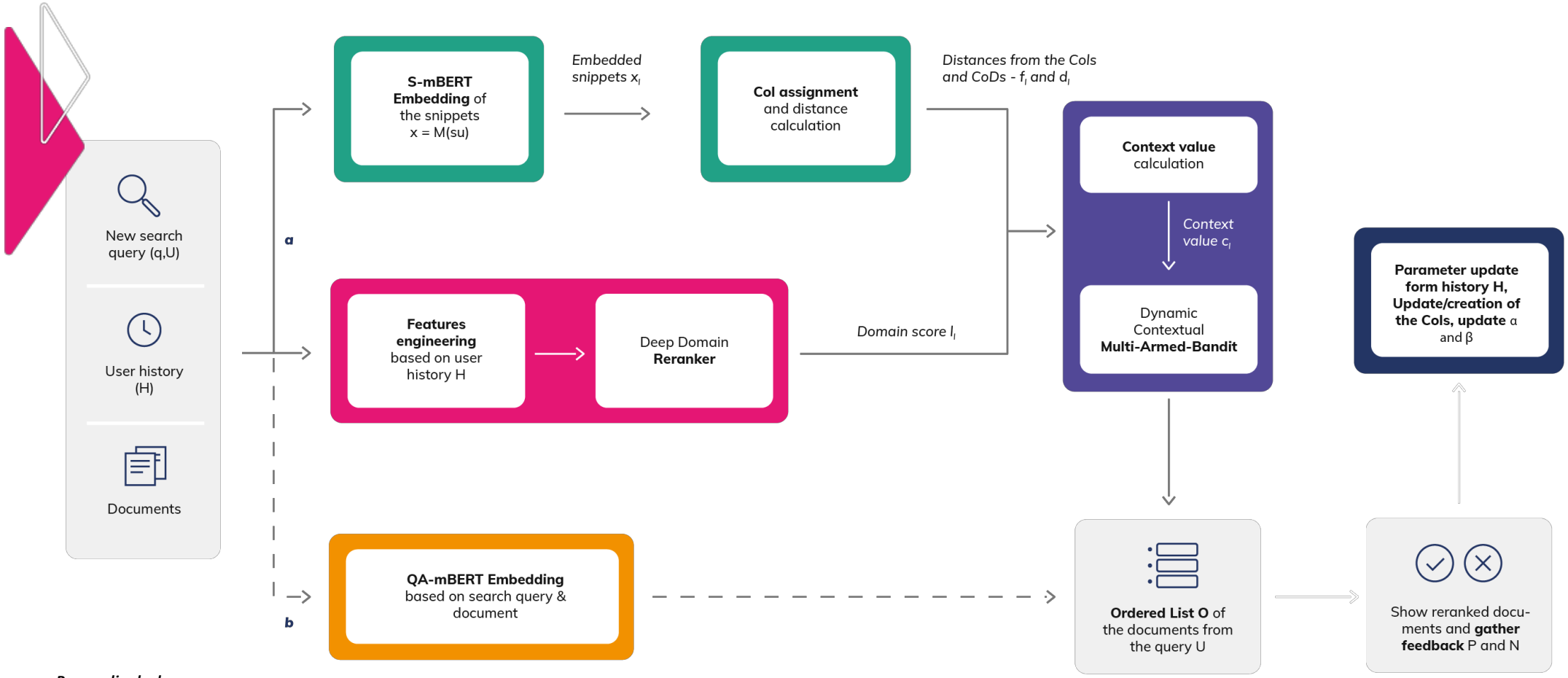
Personalisierung der Suchergebnisse durch Komination von KI-Modellen.



Kontrolle über Algorithmen durch Wischen der Suchergebnisse.

Xayn AI Workflow

Kombination verschiedener KI-Modelle

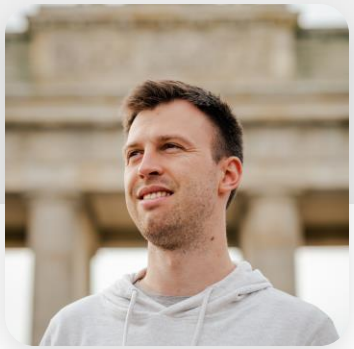


a - Personalised relevance

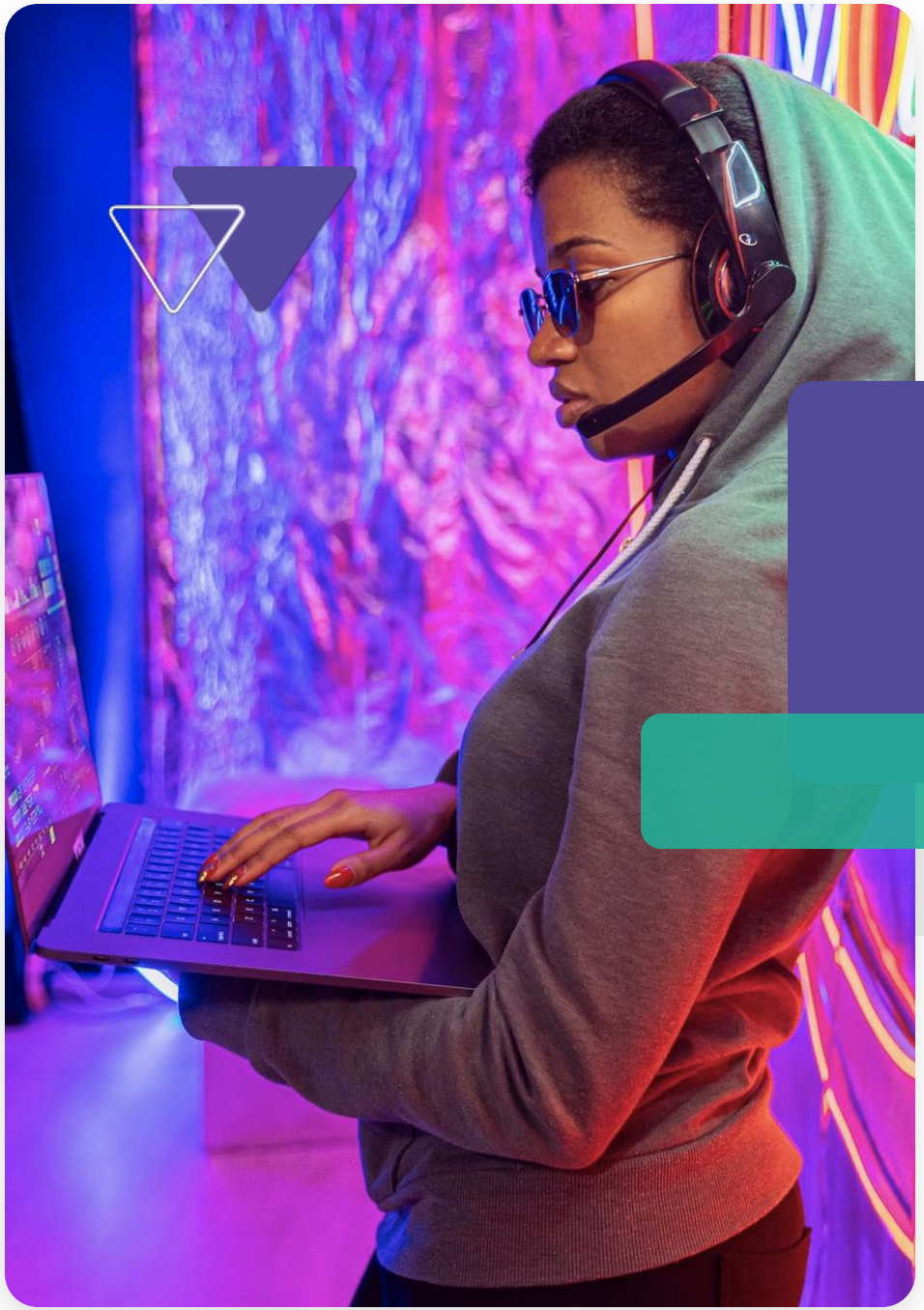
b - Semantic relevance

Über Xayn & das Team






- **Gründer**: Leif-Nissen Lundbæk (Ph.D.), Professor Michael Huth (Ph.D.), Felix Hahmann
- Teamgröße: 33 (**30 % PhD**)
- Wurzeln an der **Oxford University**, Office in **Berlin**
- Entwickler des OS Projekt **XayNet Apache**
- **Investoren**: Global Brain, Earlybird VC, DS.
- **Awards**: Gewinner des 1. Porsche Innovation Contest (2017)
- Unsere **Datenschutzrichtlinie**



Haben Sie Fragen?

Danke für Ihre Aufmerksamkeit!

Xayn AG
Unter den Linden 42
10117 Berlin, Germany

www.xayn.com
michael@xayn.com
+49 (0) 30 896 3199 0