

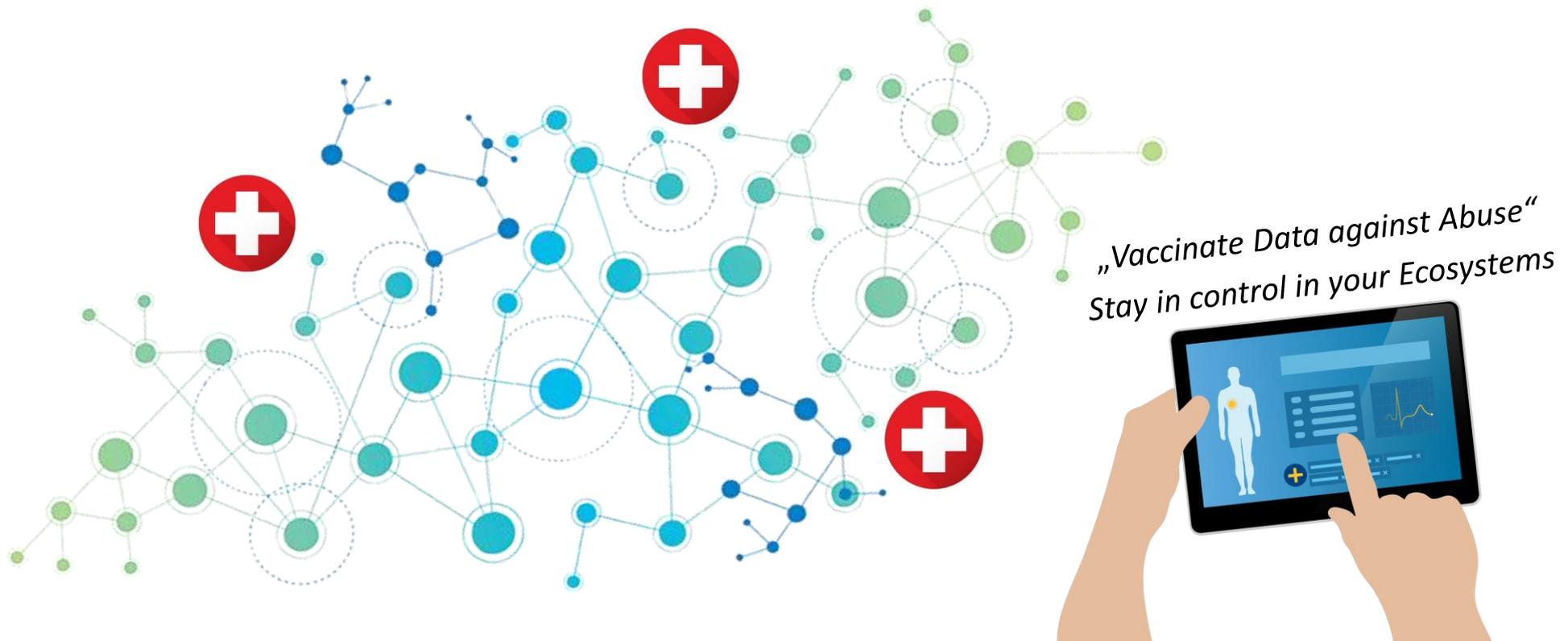


LONDON, MAY 29-30

**DIGITAL  
HEALTH  
CONGRESS2025**



# How to Ensure Sovereignty in Health Data Ecosystems



# The Cloud is just someone else's Computer



Vendors promise the „Sovereign Cloud“ but only if Sovereignty can be enforced by users on all levels at any time, only then users are in control.



**„Believe me“**

... sounds good, but users must control their own destiny.

... and even more so in sensitive data ecosystems.

Source: Computerworld



Data Governance is challenged every single day, mostly unnoticed. The digital world is getting used to headline news like this one on [Computerweekly](#): > pdf 

## „US intelligence chief Tulsi Gabbard probes UK demand for Apple’s encrypted data“

**Data Governance Risks** for just this single event are manifold:

- Apple Cloud subject to US Law (for all users globally)
- US Cloud Act grants US government authorities access:  
NSA, Homeland Security, CIA, Defense Intelligence Agency (no need to notify)
- Multi-lateral accords: The Five Eyes (FVEY) alliance on signal intelligence:  
Australia, Canada, New Zealand, the UK and the US
- FVEY intelligence agencies: CSE (CA), GCHQ (UK), GCSB (NZ), NSA (US)
- Bilateral agreement between UK and US under US Cloud Act
- Constitutional rights of US citizens serve as leverage for enforcement

**And this is among friends! “The bilateral US-UK relationship must be built on trust”.**

# Data Sovereignty in the Era of Cloud

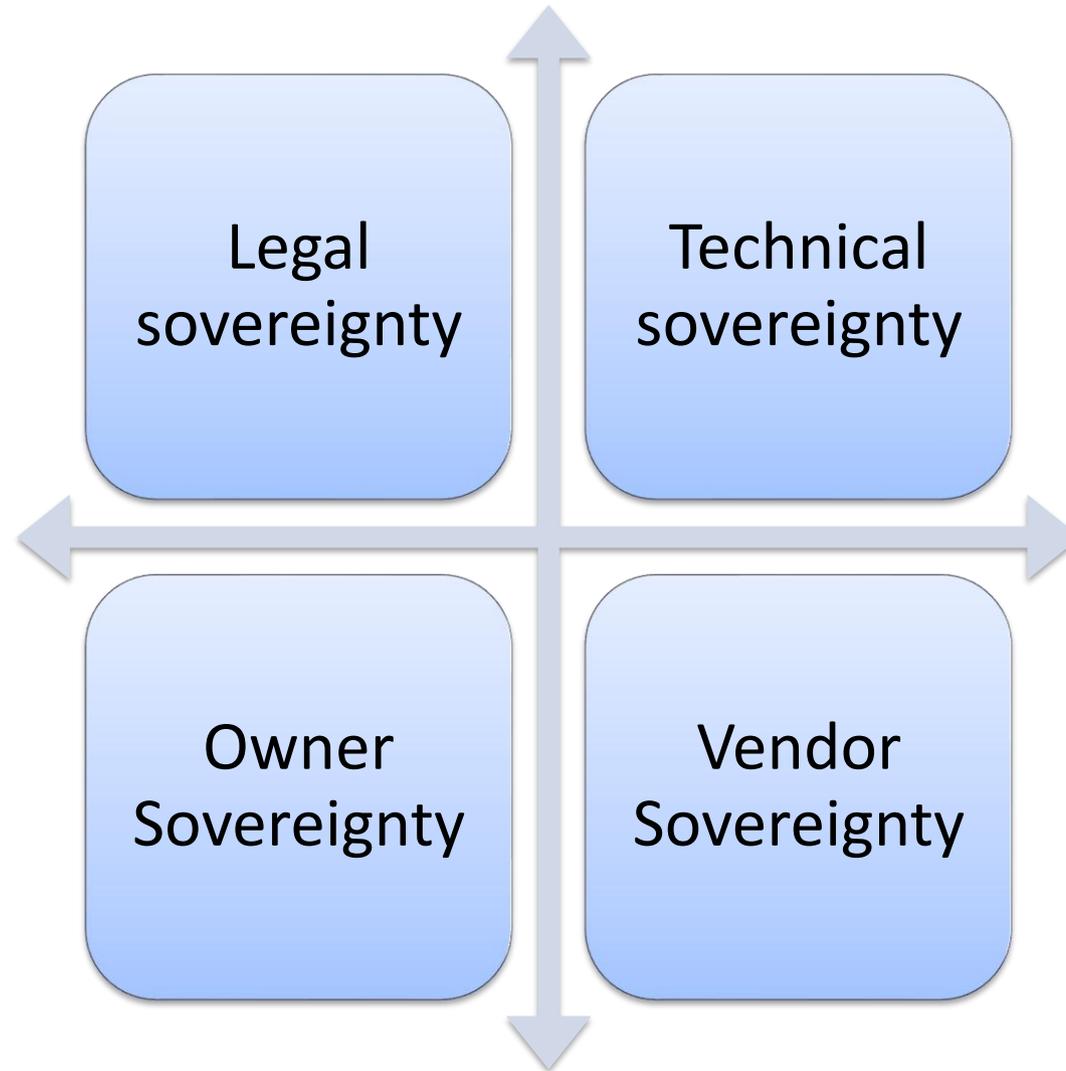


Figure: The key dimensions of Sovereignty



## Cross-Border Cloud Complexities

Your hosted data (Meta, Google, Alibaba, Microsoft, Huawei, Apple, AWS, ..) may not only be governed by the data laws of your country **but also** by the data laws of the country where your cloud operator has its legal HQ, i.e.

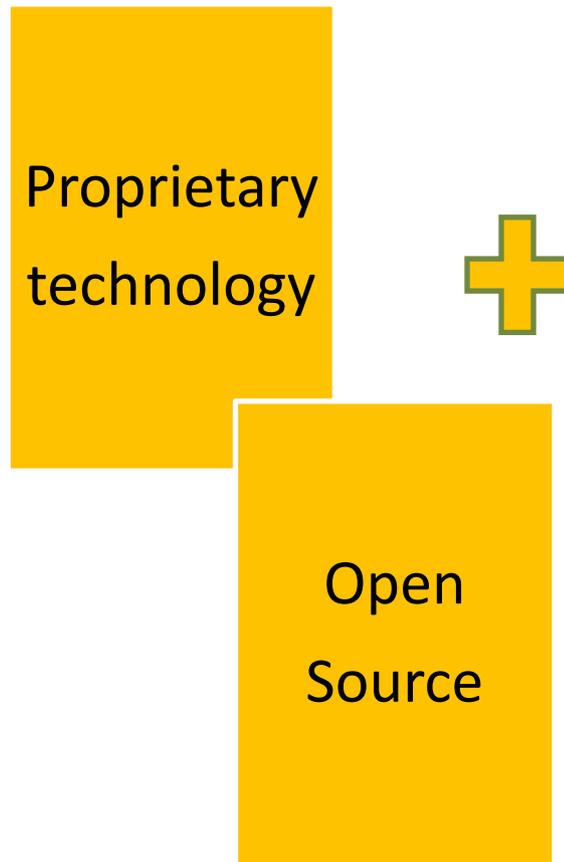
- US Cloud Act ... or
- China Data Laws
- ...



**Data Sovereignty may be at risk**, e.g. discussed at [ISACA](#).



## Check your Tech Solution Stack !



### Proprietary Technology

- Single vendor
- Multi-vendor
- Interdependencies
- Vendor support

### Open Source

- Infrastructural layer:  
OS Linux, DB ..
- Flexibility
- Independence
- Own skillset required



## Avoid Vendor-Lockin

- Stay Cloud agnostic
  - Software has to work on any Cloud, any Cloud OS (e.g. MS Azure)
- Stay Data Center agnostic
  - Minimal Data Center requirements (e.g. Virtual Machine as foundation)
- Maximize Data Transfer Options
  - APIs for Cloud Migration
  - Multi-carrier connectivity
- Minimize commercial risks
  - Guarantees, Software Escrow

**For highly sensitive health data ecosystems :**  
Control the source code, source code license agreements will guarantee quasi-ownership.



pic.: Midjourney



## Personal ownership

- Personal health data
- Full individual ownership rights
- Custodian role for health operators
- T&Cs of operators do apply



## Stakeholder ownership

- De-identified health data
- Quasi-ownership rights
- Global Efforts to regulate access
- Key driver AI: „no good data, no AI“



# PPP to ensure Sovereignty in Health Data Ecosystems



## GOVERNANCE LAYER

### DATA CLEARING AND INTERCONNECTION SERVICES

- Transaction registry, full audit trail
- Metering capabilities
- Non-repudiation qualities
- Access control and validation services (certify integrity, authenticity, etc.)
- Operated by a trusted third party (GOV)

## BUSINESS LAYER

SERVICE PROVIDER 1

SERVICE PROVIDER 2

SERVICE PROVIDER ...N

- Providing regional & business - related services for data sharing
- User management & user authentication
- Software distribution
- Commercial agreements

Hospitals

Pharma

Science

Universities

- End users or machines producing or consuming data
- Machine to machine communication
- Integration by using software development kits (SDK)

## TRANSPORT LAYER

email

(s)ftp

www

usb

- Any electronic transport channel
- Machine - machine, machine - human, human - human

Public-Private-Partnerships (PPP) to balance governance and business needs.



[Access whitepaper](#)



DataVaccinator (DV) software powers Data Ecosystems. By “vaccinating data against abuse”, DV solutions protect sensitive data, enable secure collaboration and ensure Data Sovereignty in and across Ecosystems. DV solutions are based on DV’s unique technologies (60 patents).

As strategic partner in major initiatives, DV also gives guidance on cyber security, governance, compliance, setup and operation of Data Network business, in healthcare and beyond.

## Background and Expertise:

- Technical Expertise in secure Collaboration and Ecosystems
- Intellectual Property Rights (IPR): Assessment and Management
- Data Ecosystems: Healthcare in EU/MENA, Secure Supply Chains (WEF), Belt&Road (Asia), Logistics (Air, Sea, Road), Cyber Security (ASEAN)
- Belfer Security Center (Harvard, JFK), WEF Security Group



# Thank you.

Kurt Kammerer, CEO [kurt@datavaccinator.com](mailto:kurt@datavaccinator.com)  
(slides: <https://datavaccinator.com/news.html>)

**DataVaccinator SARL**  
7, route d'Esch  
L-1470 Luxembourg  
Luxembourg

**DataVaccinator Limited**  
VD, 1st floor  
Masdar City, Abu Dhabi  
United Arab Emirates