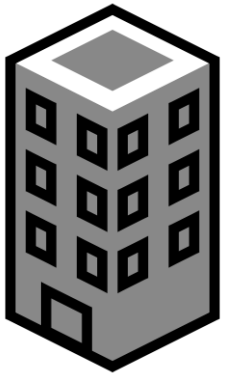
Adieu Einwilligung

Neue Herausforderungen für die informationelle Selbstbestimmung im Angesicht von Big Data Technologien

Szenario

Szenario

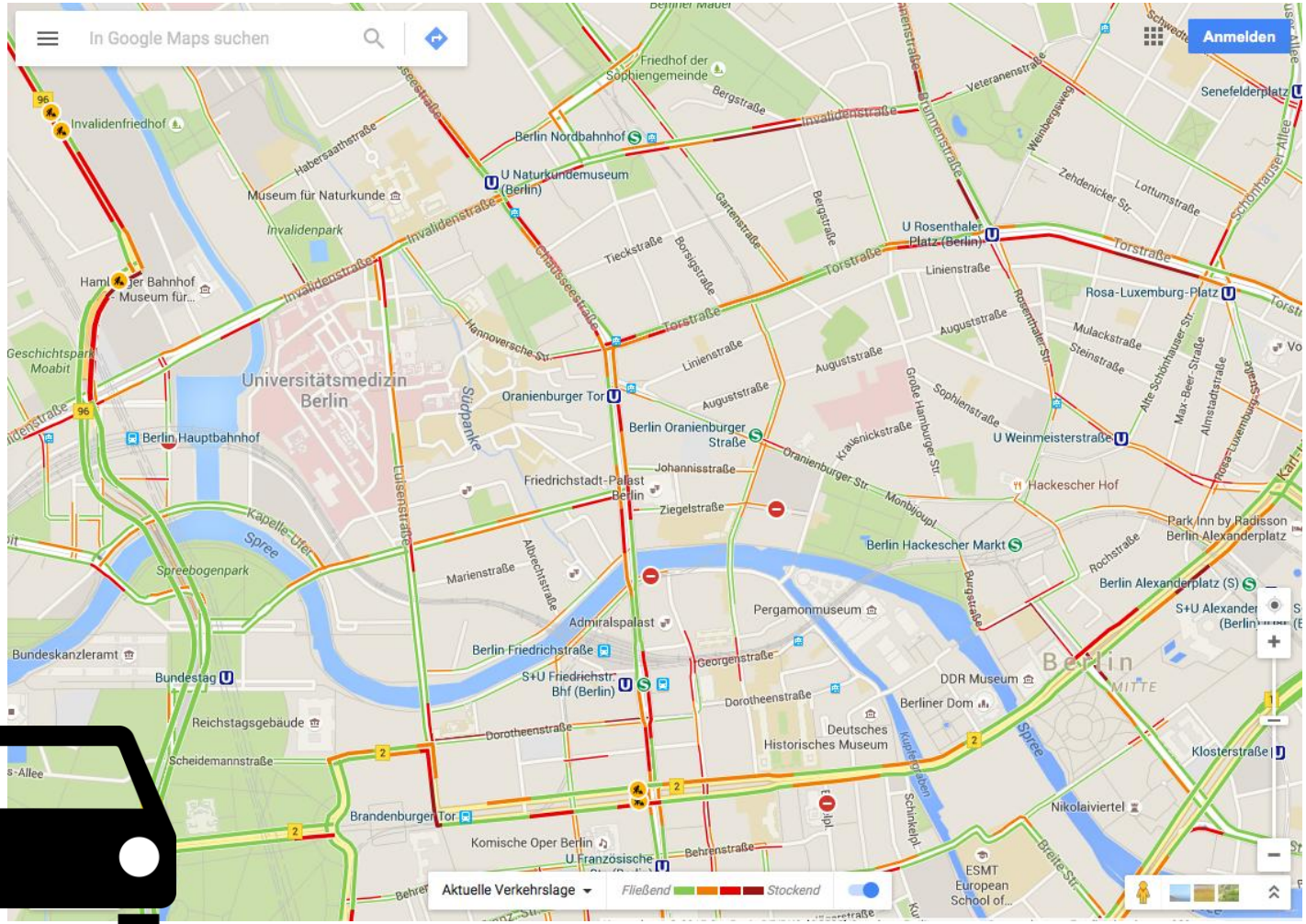


Institut für
Verkehrsforschung

Forschungsprojekt:

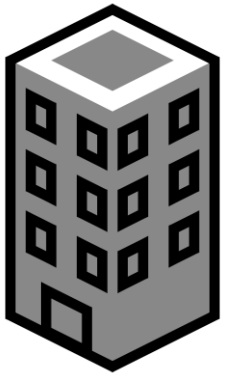
- Lassen sich Zusammenhänge zwischen Verkehrsflüssen und dem Stresslevel beteiligter Verkehrsteilnehmer finden?
- Sind diese durch städtebauliche Faktoren beeinflussbar?

Szenario

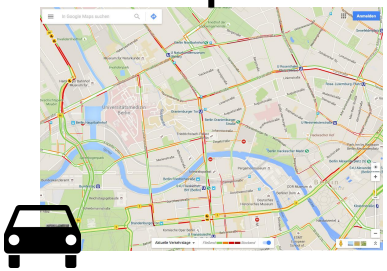

In Google Maps suchen
Anmelden
Invalidenfriedhof
Berlin Nordbahnhof
U Naturkundemuseum (Berlin)
Museum für Naturkunde
Invalidenpark
Hamburger Bahnhof – Museum für...
Universitätsmedizin Berlin
Berlin Hauptbahnhof
Oranienburger Tor
Berlin Oranienburger Straße
Friedrichstadt-Palast Berlin
Berlin Hackescher Markt
Hackescher Hof
U Weinmeisterstraße
U Rosenthaler Platz (Berlin)
Rosa-Luxemburg-Platz
Senefelderplatz
Friedhof der Sophiengemeinde
Spree
Spreebogenpark
Pergamonmuseum
Admiralspalast
Berlin Friedrichstraße
S+U Friedrichstr. Bhf (Berlin)
Bundeskanzleramt
Bundestag
Reichstagsgebäude
Brandenburger Tor
Komische Oper Berlin
Deutsches Historisches Museum
DDR Museum
Berliner Dom
Nikolaiviertel
Klosterstraße
Berlin Alexanderplatz (S)
Park Inn by Radisson Berlin Alexanderplatz
ESMT European School of...
Aktuelle Verkehrslage
Fließend
Stockend

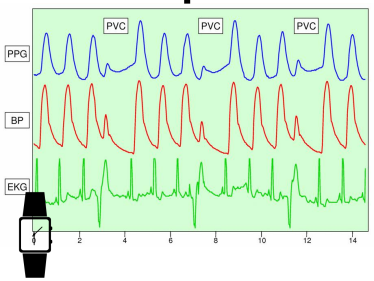
Szenario

Szenario

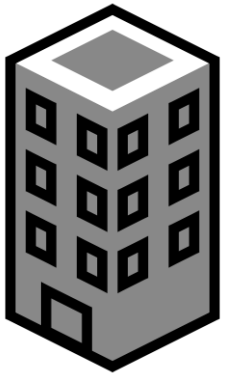


Institut für Verkehrsforschung





Szenario

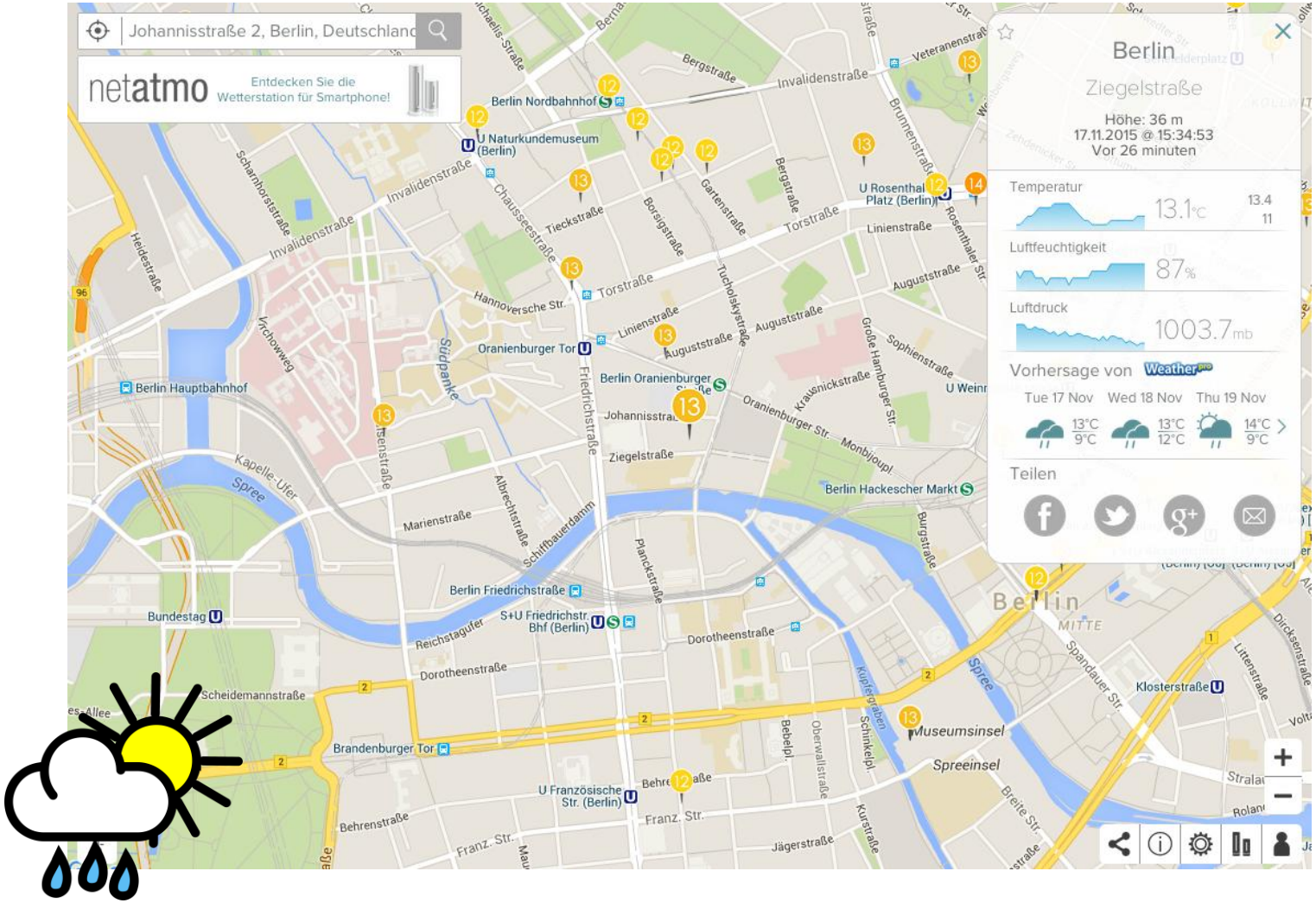


Institut für Verkehrsforschung

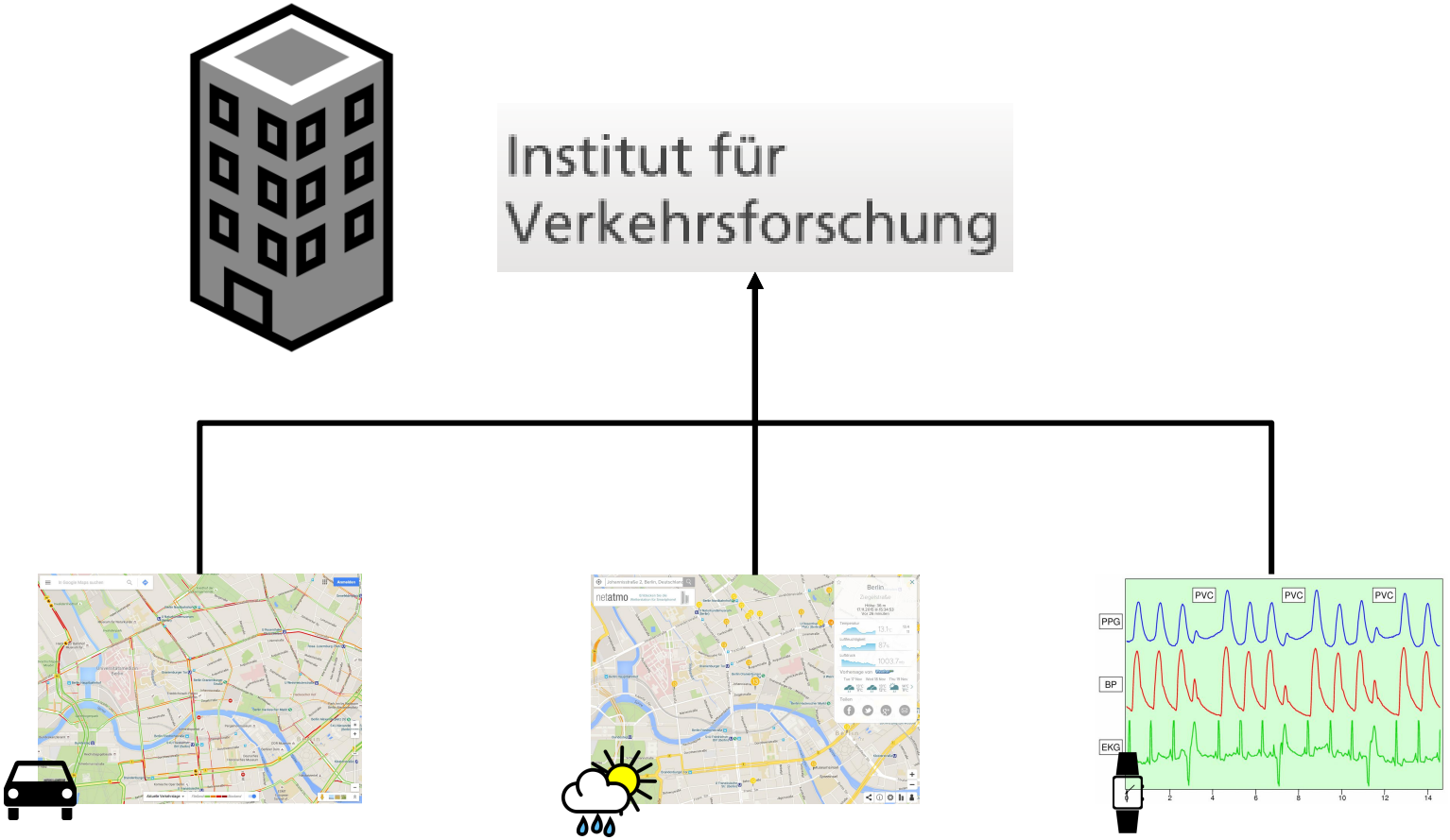
Forschungsprojekt:

- Lassen sich Zusammenhänge zwischen Verkehrsflüssen und dem Stresslevel beteiligter Verkehrsteilnehmer finden?
- Sind diese durch städtebauliche Faktoren beeinflussbar?
- Erweiterung: Welchen Einfluss hat das Wetter?

Szenario


Johannisstraße 2, Berlin, Deutschland
netatmo
Entdecken Sie die Wetterstation für Smartphone!
Berlin
Ziegelstraße
Höhe: 36 m
17.11.2015 @ 15:34:53
Vor 26 minuten
Temperatur
13.1°C
13.4
11
Luftfeuchtigkeit
87%
Luftdruck
1003.7mb
Vorhersage von Weather pro
Tue 17 Nov
13°C
9°C
Wed 18 Nov
13°C
12°C
Thu 19 Nov
14°C
9°C
Teilen
Berlin Nordbahnhof
U Naturkundemuseum (Berlin)
U Rosenthaler Platz (Berlin)
Oranienburger Tor
Berlin Oranienburger
Berlin Hauptbahnhof
Berlin Hackescher Markt
Berlin Friedrichstraße
S+U Friedrichstr. Bhf (Berlin)
Bundestag
Brandenburger Tor
U Französische Str. (Berlin)
Museumsinsel
Spreeinsel
Klosterstraße
Berlin
MITTE
Invalidenstraße
Torstraße
Linienstraße
Ziegelstraße
Dorotheenstraße
Behrenstraße
Franz. Str.
Jägerstraße
Scheidemannstraße
Spree

Szenario



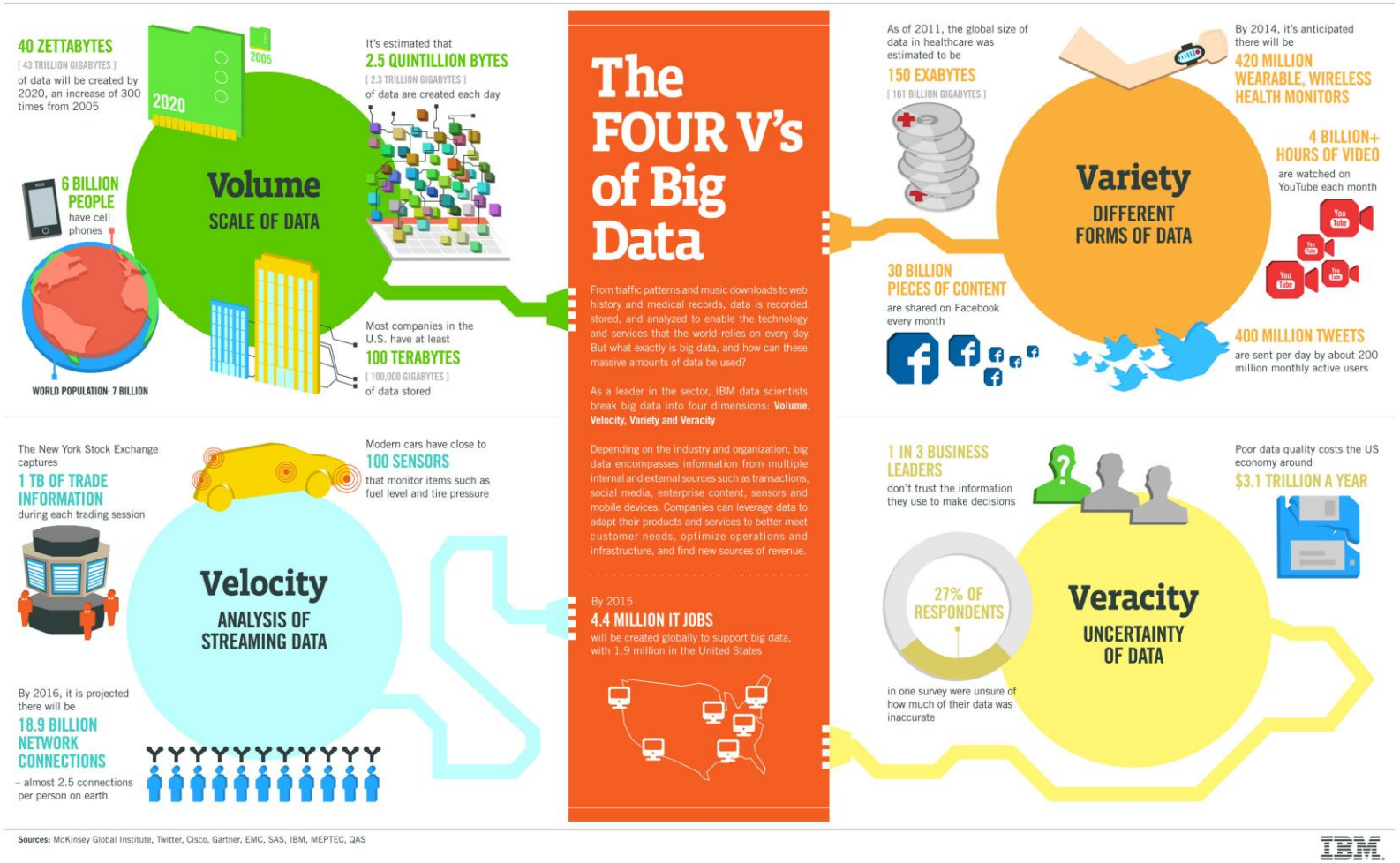
Problem:

Eigentlich schon vorliegende Daten lassen sich nicht für neue Nutzungsformen kombinieren, da Einwilligung und Zweckbindung nicht gegeben sind.

Einwilligung & Zweckbindung als Kernprobleme im Kontext von Big Data

Big Data?

Big Data: „Daten"-Perspektive



Big Data: „Technologie“-Perspektive

HACE Theorem:

Big Data starts with large volume, **H**eterogeneous, **A**utonomous sources with distributed and decentralized control, and seeks to explore **C**omplex and **E**volving relationships among data.

Informationelle Selbstbestimmung?

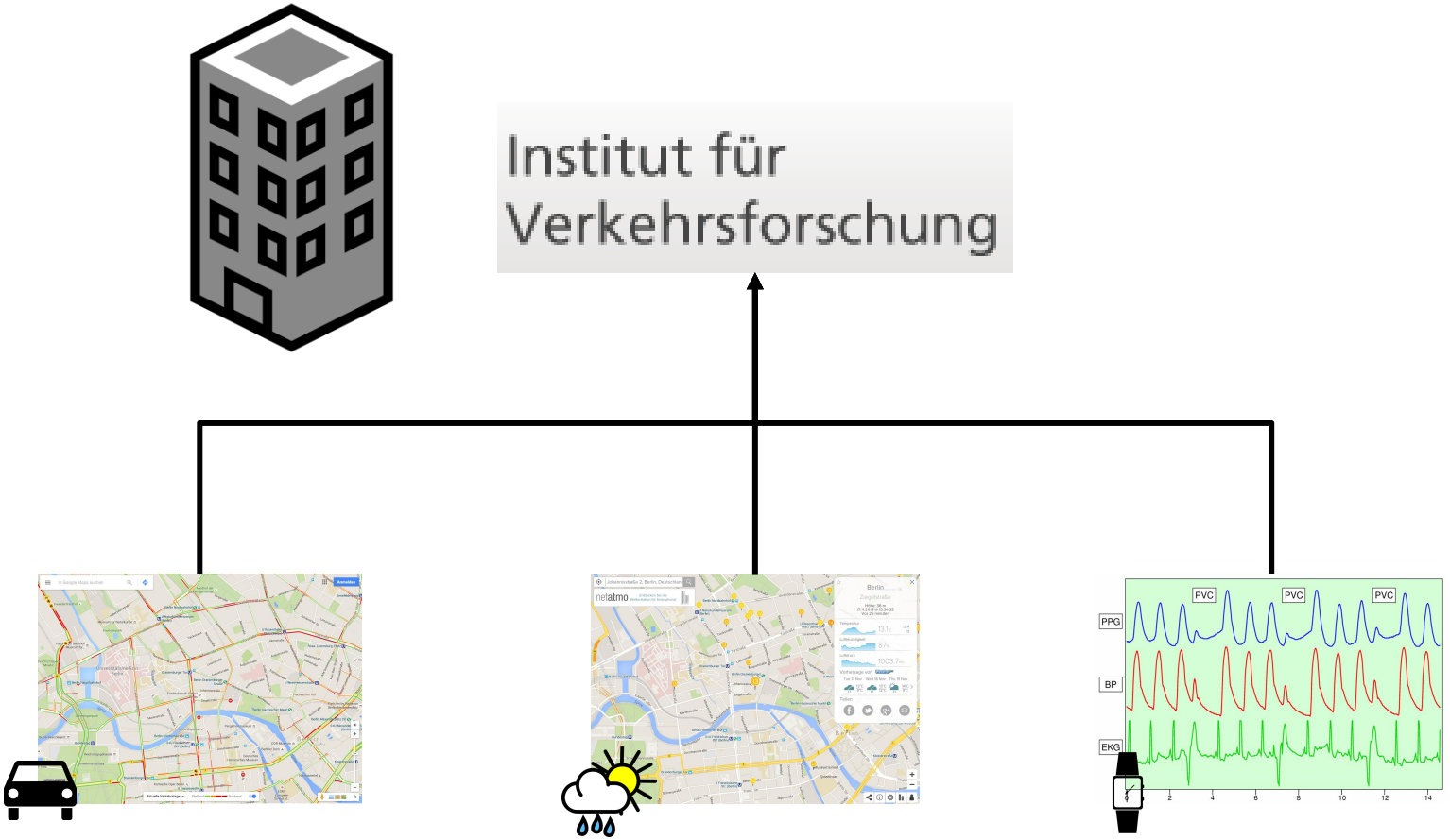
„Informationelle Selbstbestimmung“

„Privacy is the claim of **individuals**, groups, or institutions to **determine** for themselves when , and how, and to **what** extent **information** about them **is communicated to others**.“

(Westin 1967, S. 7)

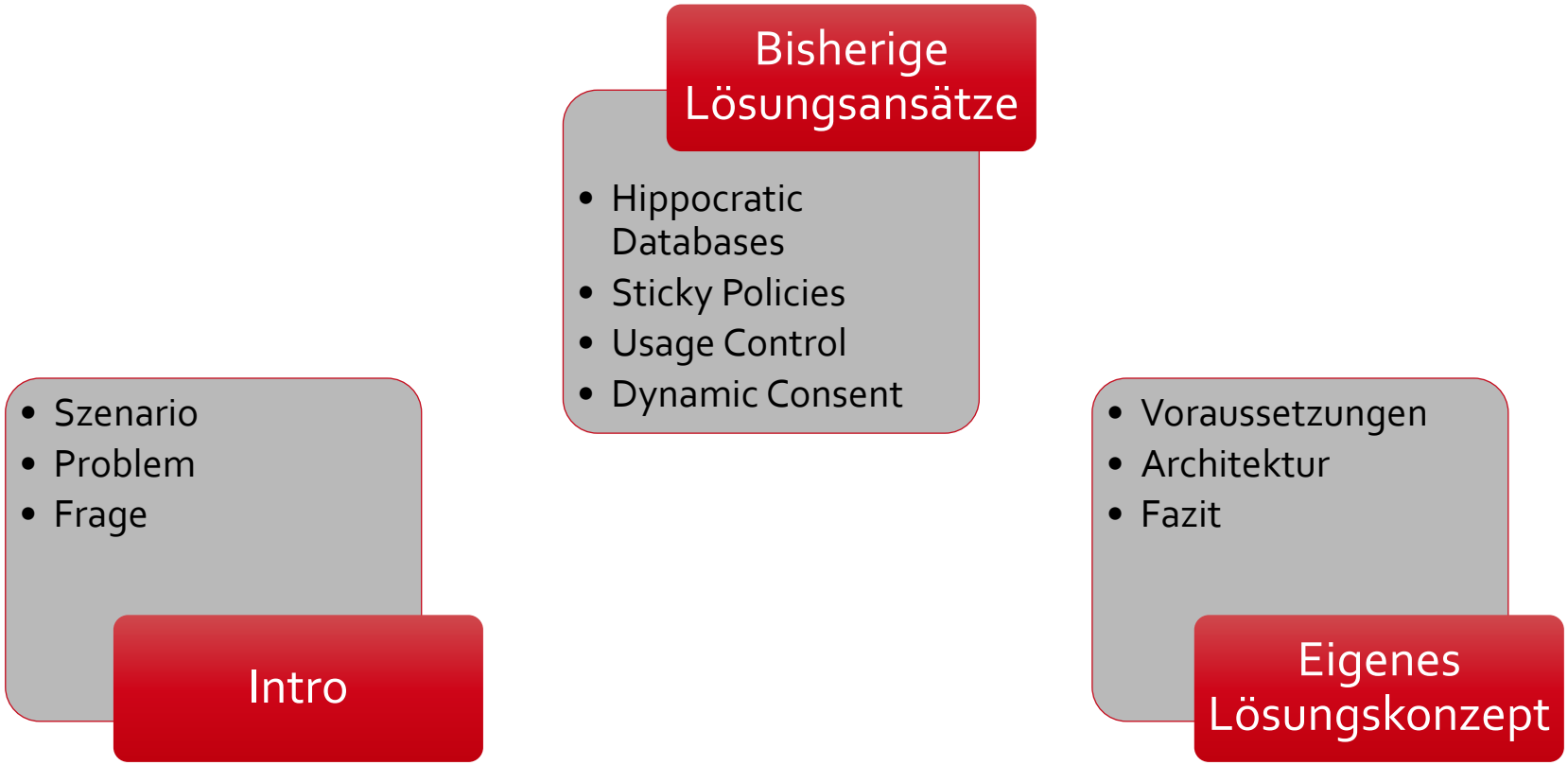
- Einwilligung zur Informationsweitergabe zu festgelegten Bedingungen (Adressat, Zweck)

Szenario


Institut für
Verkehrsforschung
netatmo
PVC
PVC
PVC
PPG
BP
EKG

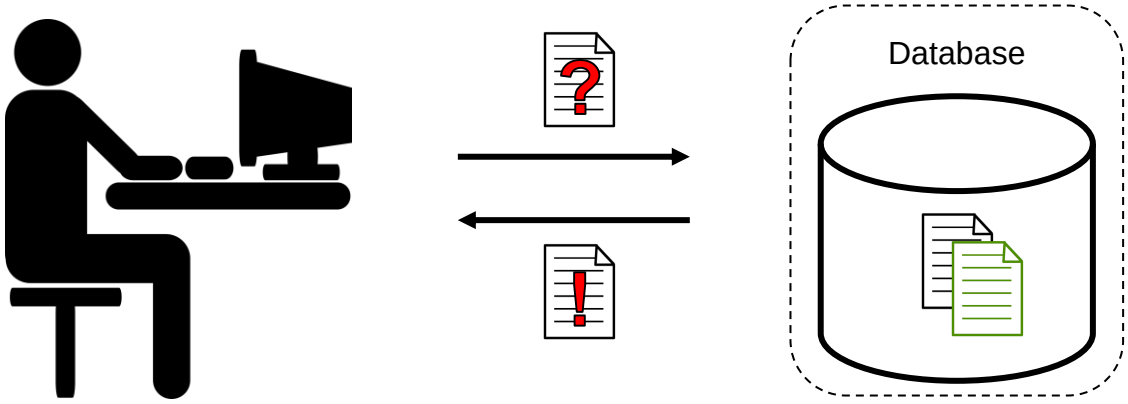
Frage:

Müssen wir uns von der bisherigen (juristischen) Handhabung der (informierten) Einwilligung verabschieden?


Bisherige Lösungsansätze
• Hippocratic Databases
• Sticky Policies
• Usage Control
• Dynamic Consent
• Szenario
• Problem
• Frage
Intro
• Voraussetzungen
• Architektur
• Fazit
Eigenes Lösungskonzept

Hippocratic Databases

Classical Database



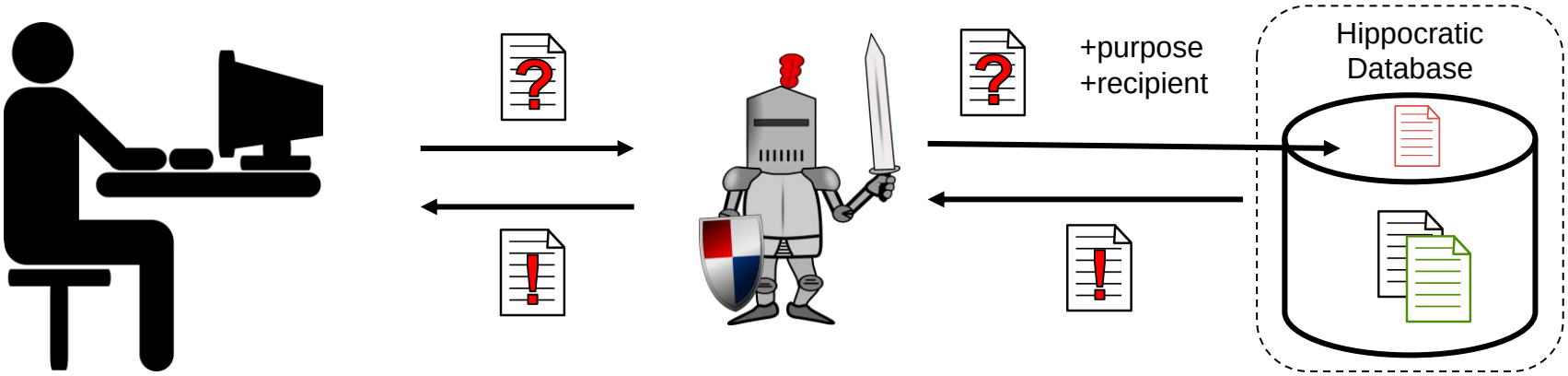
customer

customer ID	name	address	email	credit card

order

customer ID	transaction ID	book info	status

Hippocratic Database



privacy-policies

purpose	table	attribute	recipient	retention
purchase	customer	address	delivery-company	1 month

customer

purpose	customer ID	name	address	email	credit card

order

purpose	customer ID	transaction ID	book info	status

Hippocratic Databases

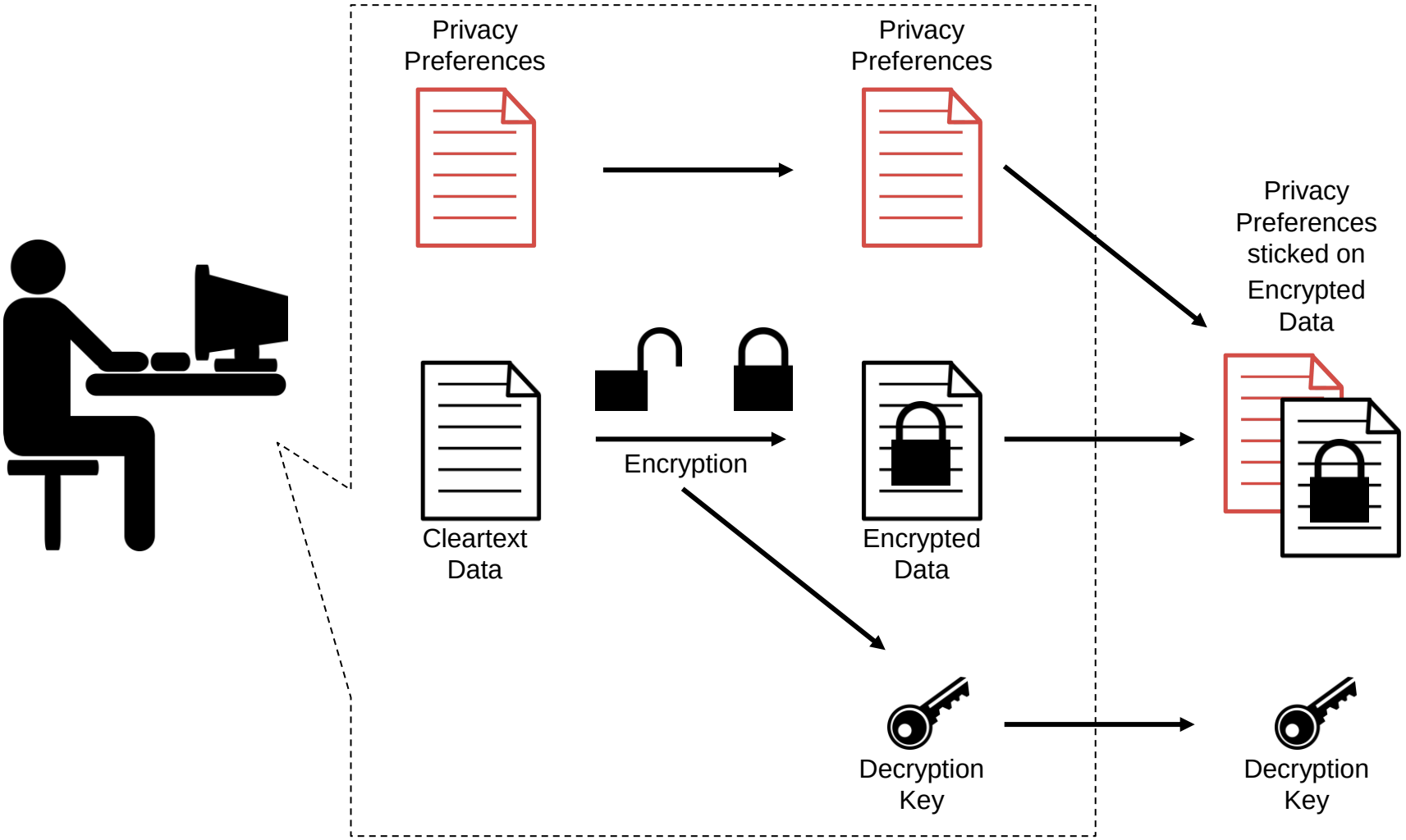
Vorteile:

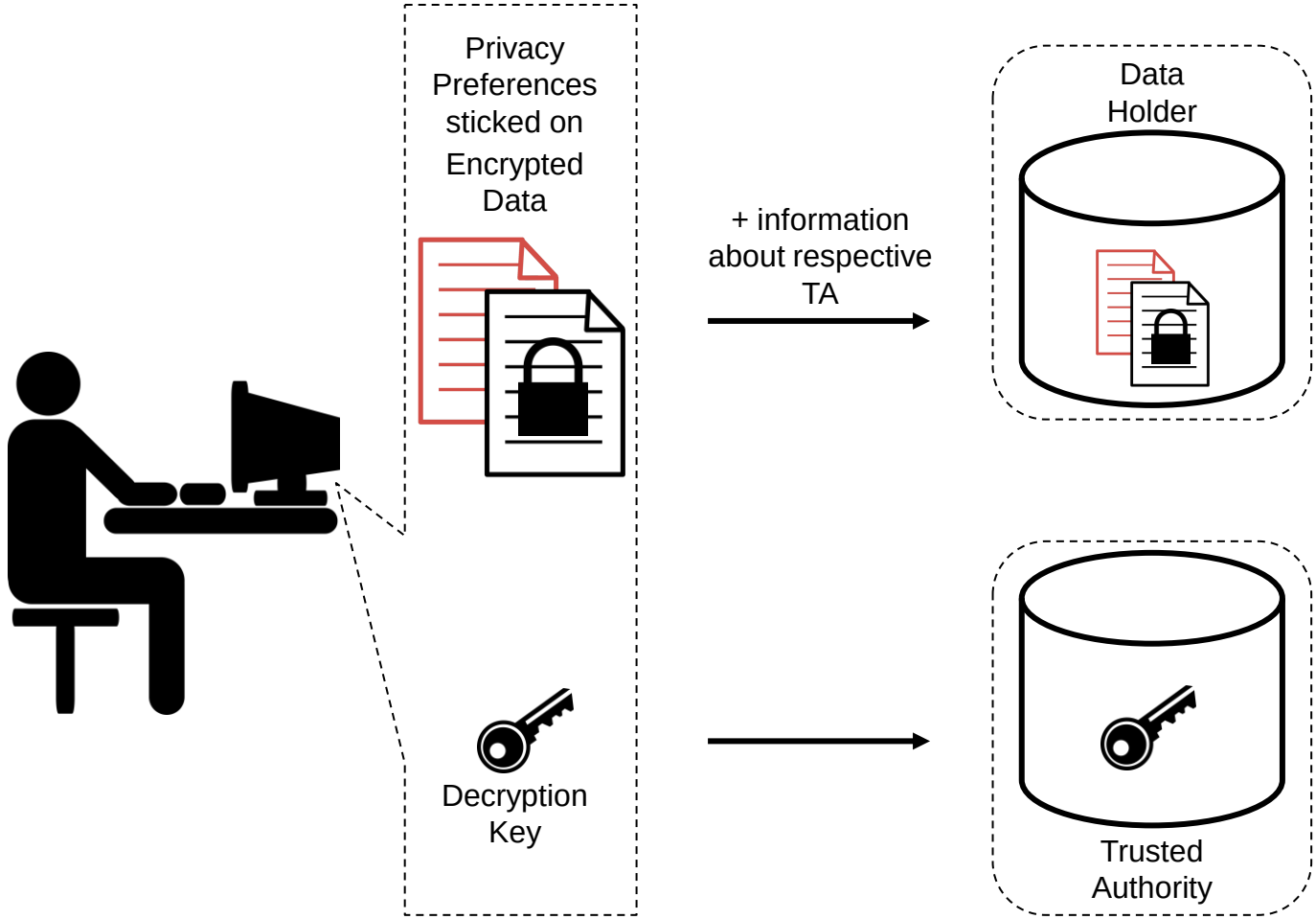
- Technische Umsetzung von Einwilligung und Zweckbindung
- Bei korrekter Implementierung keinerlei Zugriff von Unbefugten möglich

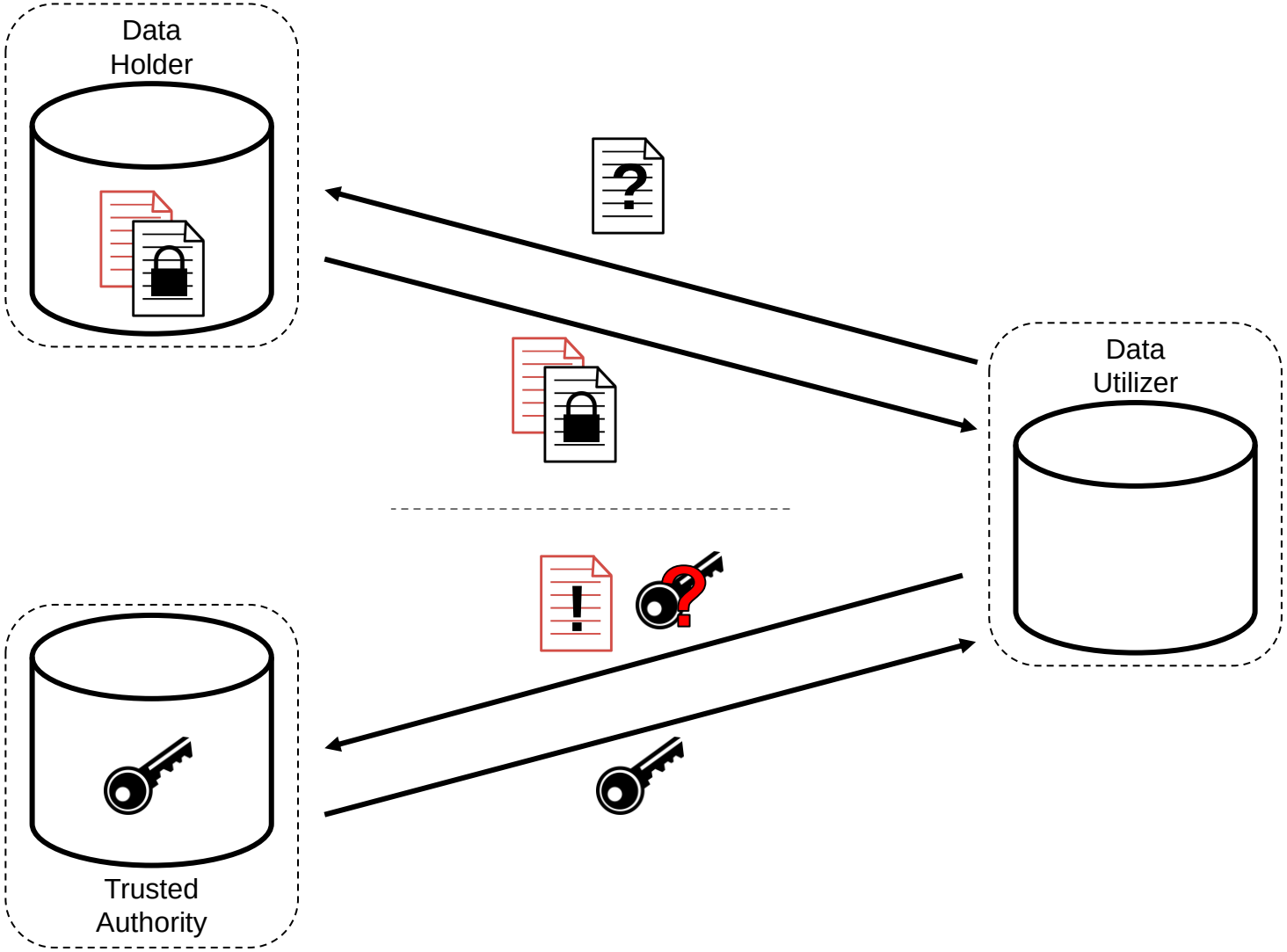
Nachteile:

- In der Praxis recht selten genutzt (eher akademisches Konzept)
- Bei förderierten Datenquellen müsste jede einzelne hippokratisch organisiert sein
- Nachträgliche Umstrukturierung erzeugt Aufwand

Sticky Policies


Privacy Preferences
Privacy Preferences
Privacy Preferences sticked on Encrypted Data
Cleartext Data
Encryption
Encrypted Data
Decryption Key
Decryption Key


Privacy Preferences sticked on Encrypted Data
+ information about respective TA
Data Holder
Decryption Key
Trusted Authority


Data
Holder
Data
Utilizer
Trusted
Authority

Sticky Policies

Vorteile:

- Kein Zugriff ohne Zustimmung der Trusted Authority (TA) möglich
- Alle Zugriffe können bei TA protokolliert werden

Nachteile:

- Verfahren abhängig von dritter Instanz (→ TA)
- Neben Richtlinienerstellung weitere Vorarbeiten (Verschlüsselung, Transfer der Schlüssel zu den TAs, …) nötig
- Keine Verhinderung/Kontrolle von Regelübertritten nach Zugriff möglich

Distributed Usage Control

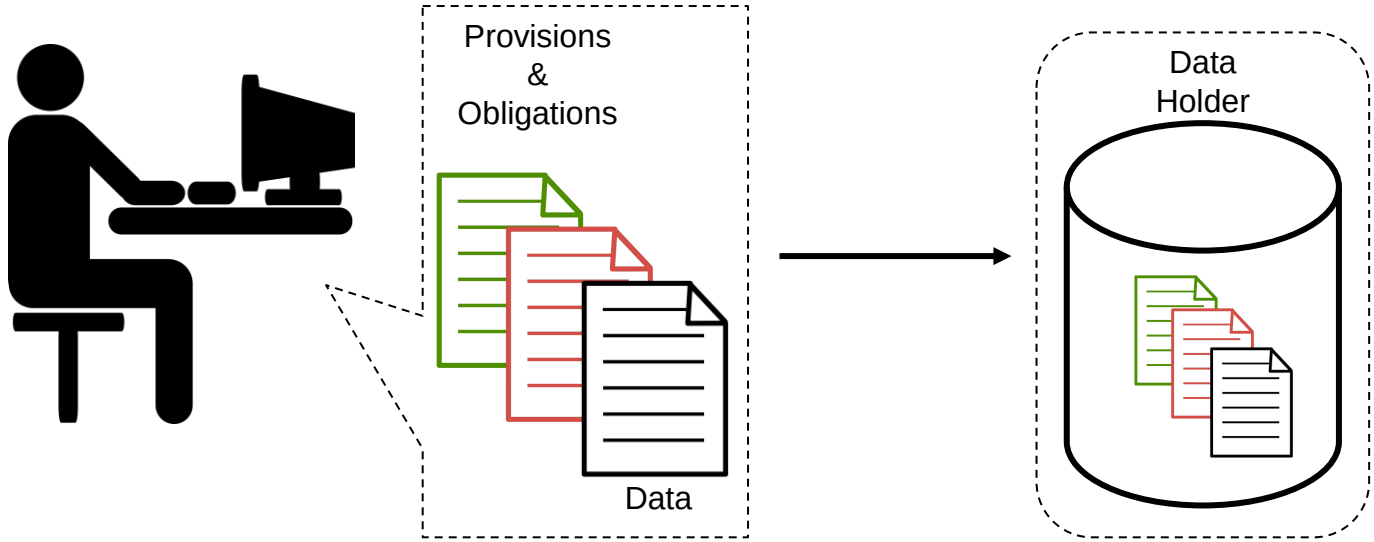
Provisions:

- Realisieren Zugriffskontrolle (ähnlich Sticky Policies)
- Sind bei diesem Konzept Voraussetzung für weitere Aushandlungen

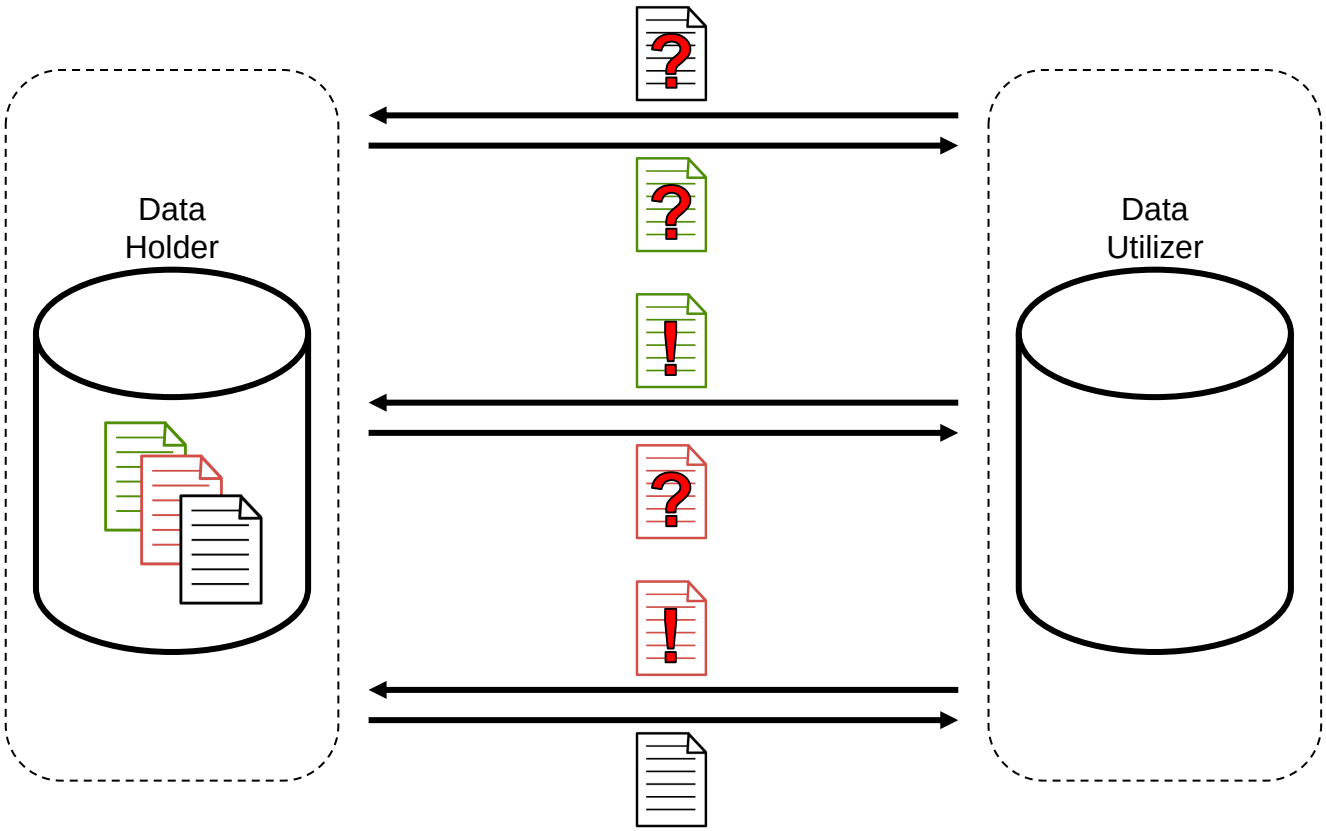
Obligations:

- „*Verträge*" über die Bedingungen der Nutzung angeforderter Daten (Löschfristen, Begrenzung von Kopiervorgängen u.ä.)
- Enthalten auch mögliche Kompensationen bei Zuwiderhandlungen

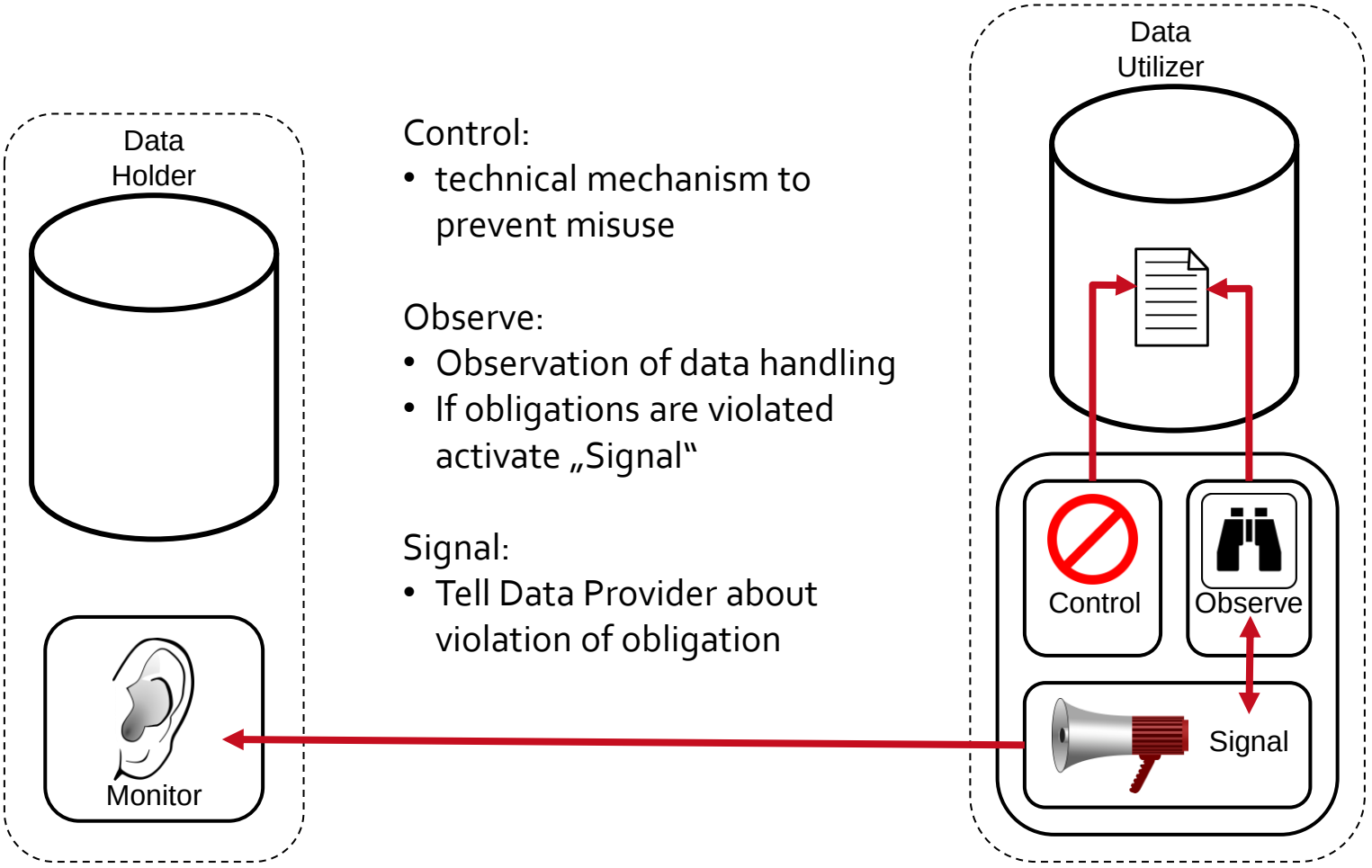
Initialisierung



Aushandlung



Kontrolle



Control:
- technical mechanism to prevent misuse

Observe:
- Observation of data handling
- If obligations are violated activate „Signal“

Signal:
- Tell Data Provider about violation of obligation

Distributed Usage Control

Vorteile:

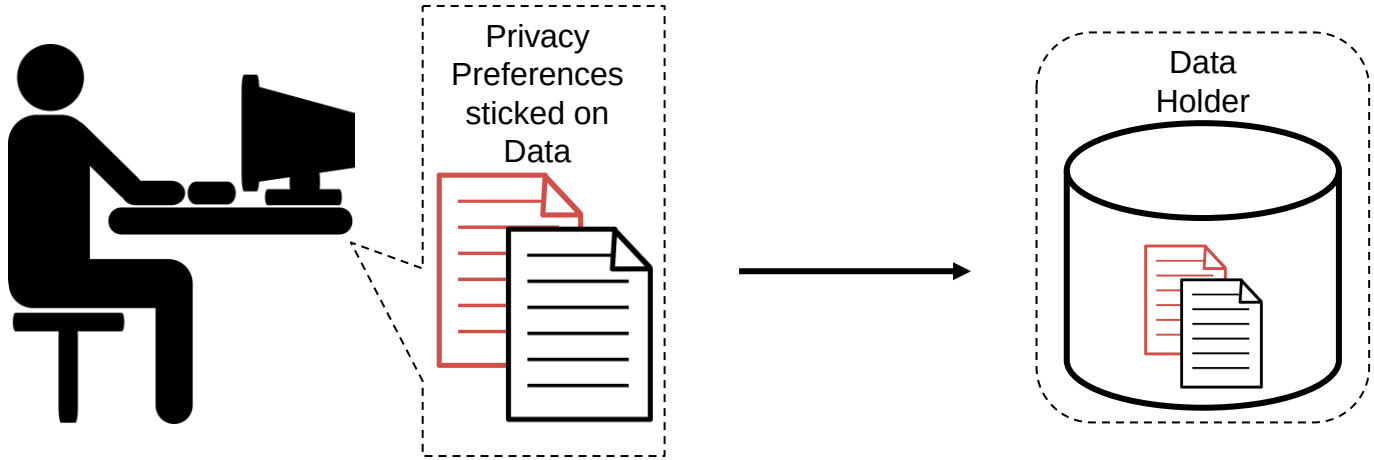
- Zugriffs- sowie Nutzungskontrolle
- Teilweise technische Verhinderung von Fehlverhalten
- Signalisierung von Regelübertritten löst vorher festgelegte Kompensationen aus

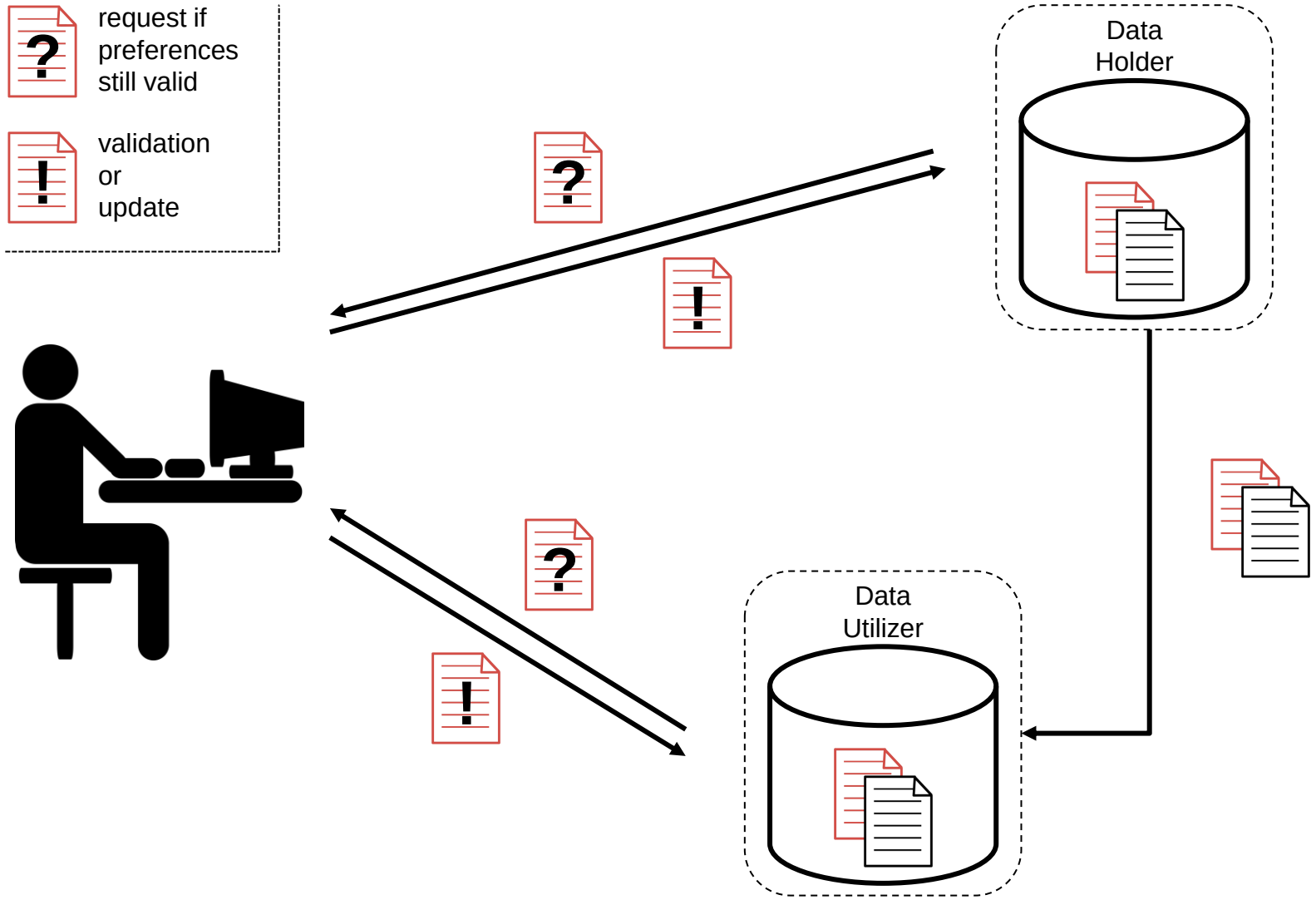
➢ ex-ante **&** ex-post Regulierung

Nachteile:

- Implementierungsaufwand (Kontrollmechanismen müssen auf allen beteiligten Systemen vorhanden sein)
- Für autonome Systeme weniger geeignet, da hohes Maß an Kooperation nötig

Dynamic Consent


Privacy
Preferences
sticked on
Data
Data
Holder


request if preferences still valid
validation or update
Data Holder
Data Utilizer

Dynamic Consent

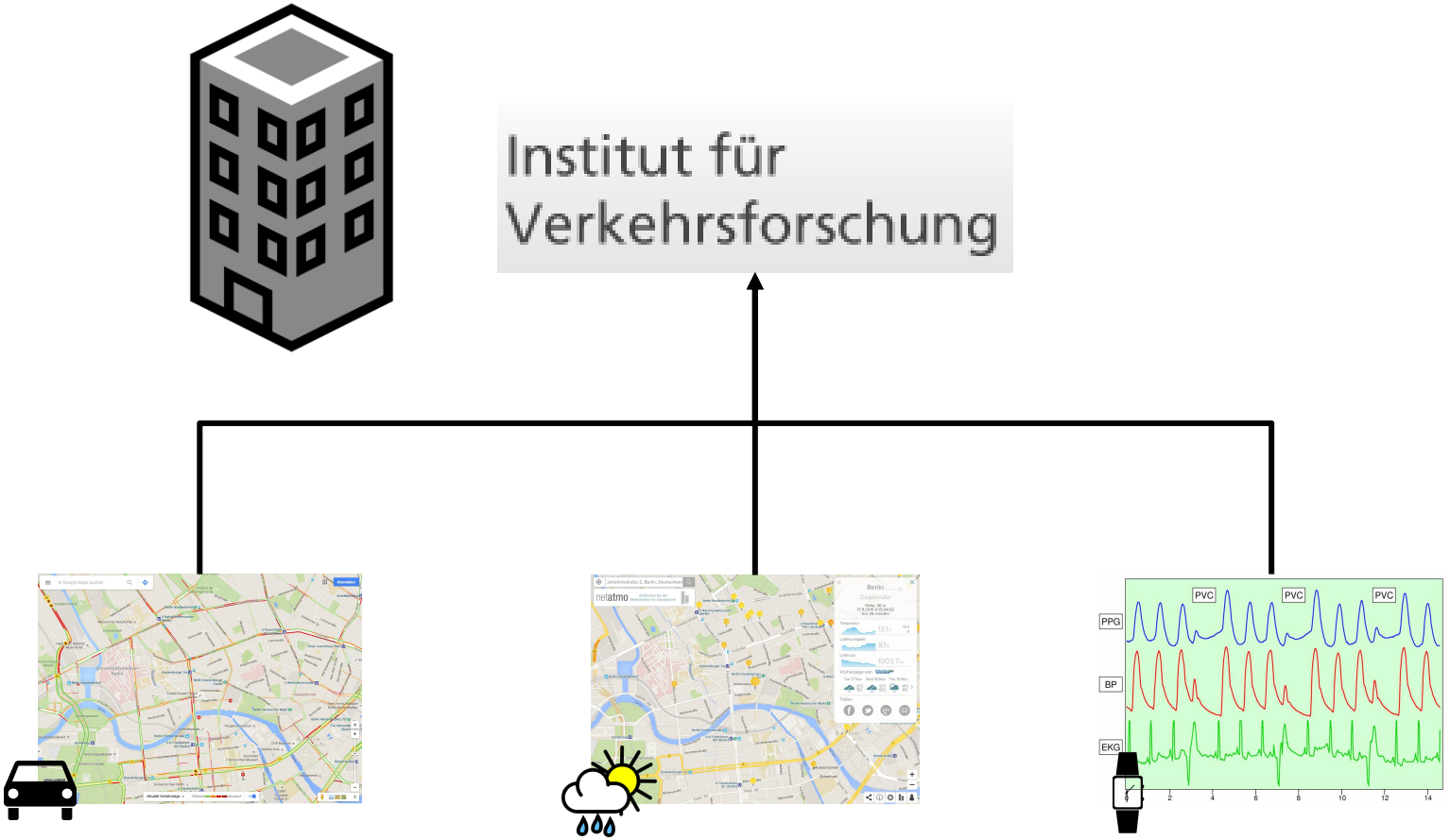
Vorteile:

- Ermöglicht dynamische Anpassung von Nutzer-präferenzen (auch bezgl. neuer Verarbeitungszwecke)
- Verhinderung von „broad consent"

Nachteile:

- Implementierungsaufwand
- Anpassungen erzeugen Zeit-Aufwand durch Kommunikation (→ nur bedingt „echtzeit"-tauglich)

Szenario


Institut für
Verkehrsforschung
netatmo
PVC
PVC
PVC
PPG
BP
EKG

Lösungsansatz

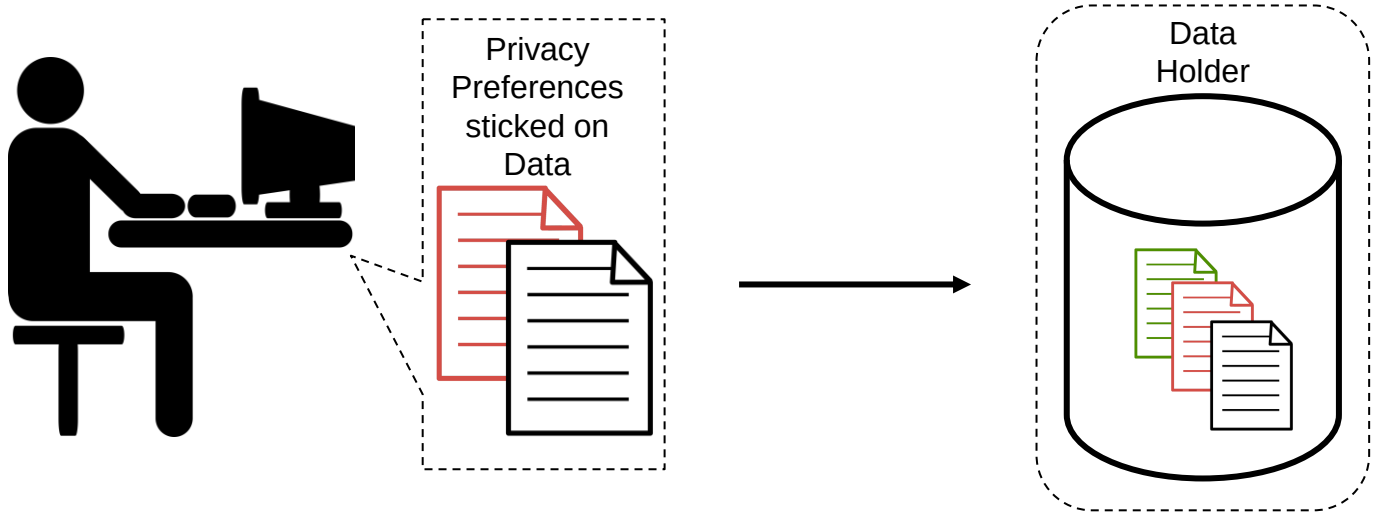
Hippocratic Data Integration

Privatsphäre - Präferenzen

„Vorab"-Einwilligungen zu Kategorien von Zwecken und potenziellen Verwendern

Auf dieses Datum darf zu folgenden Zwecken zugegriffen werden:

- Forschung
  - Generell
  - Spezifisch
    - Stadtentwicklung
    - Pharmaforschung
    - ...
- Demographische Erhebungen
  - Generell
  - Spezifisch
    - ...

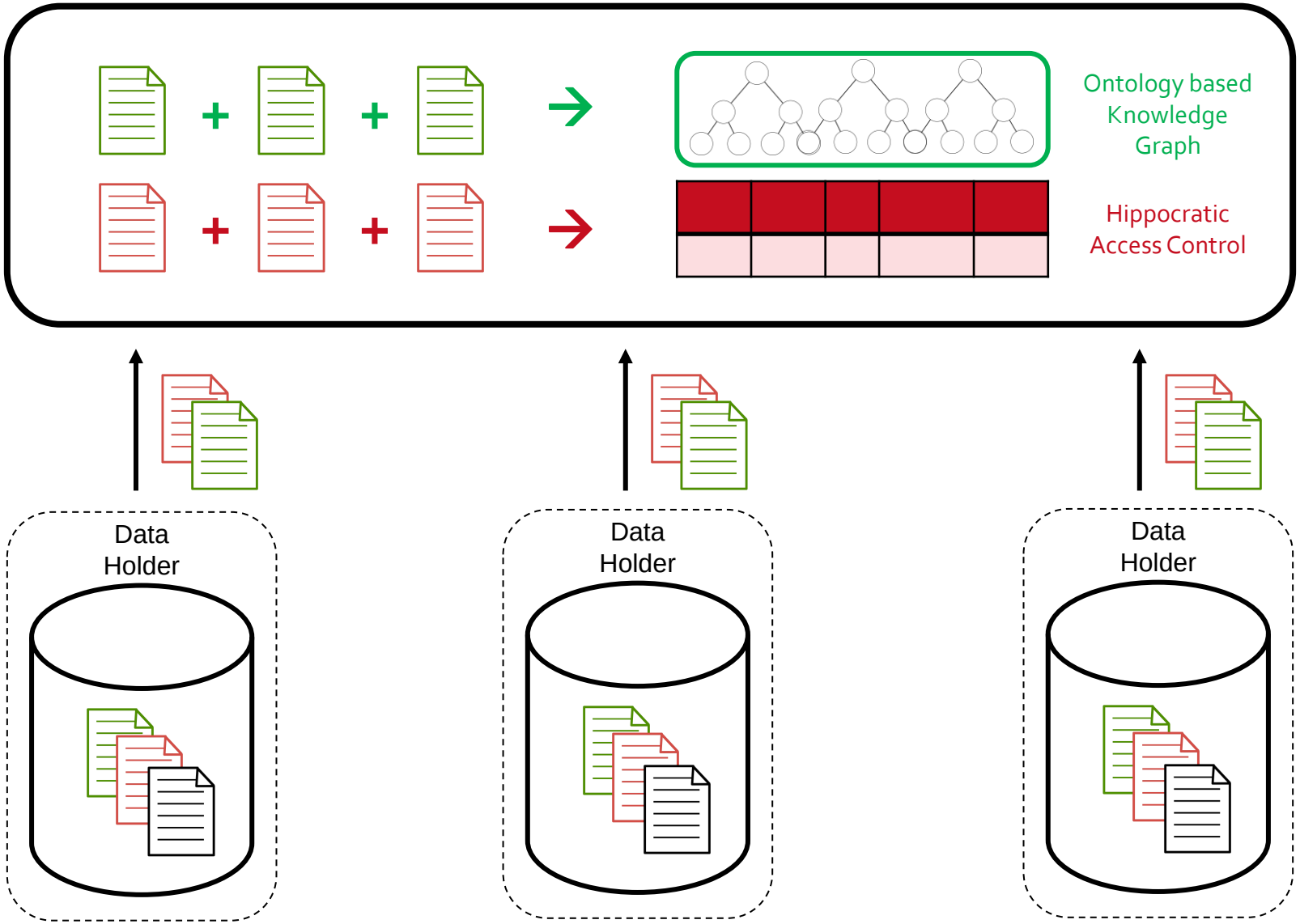


Data

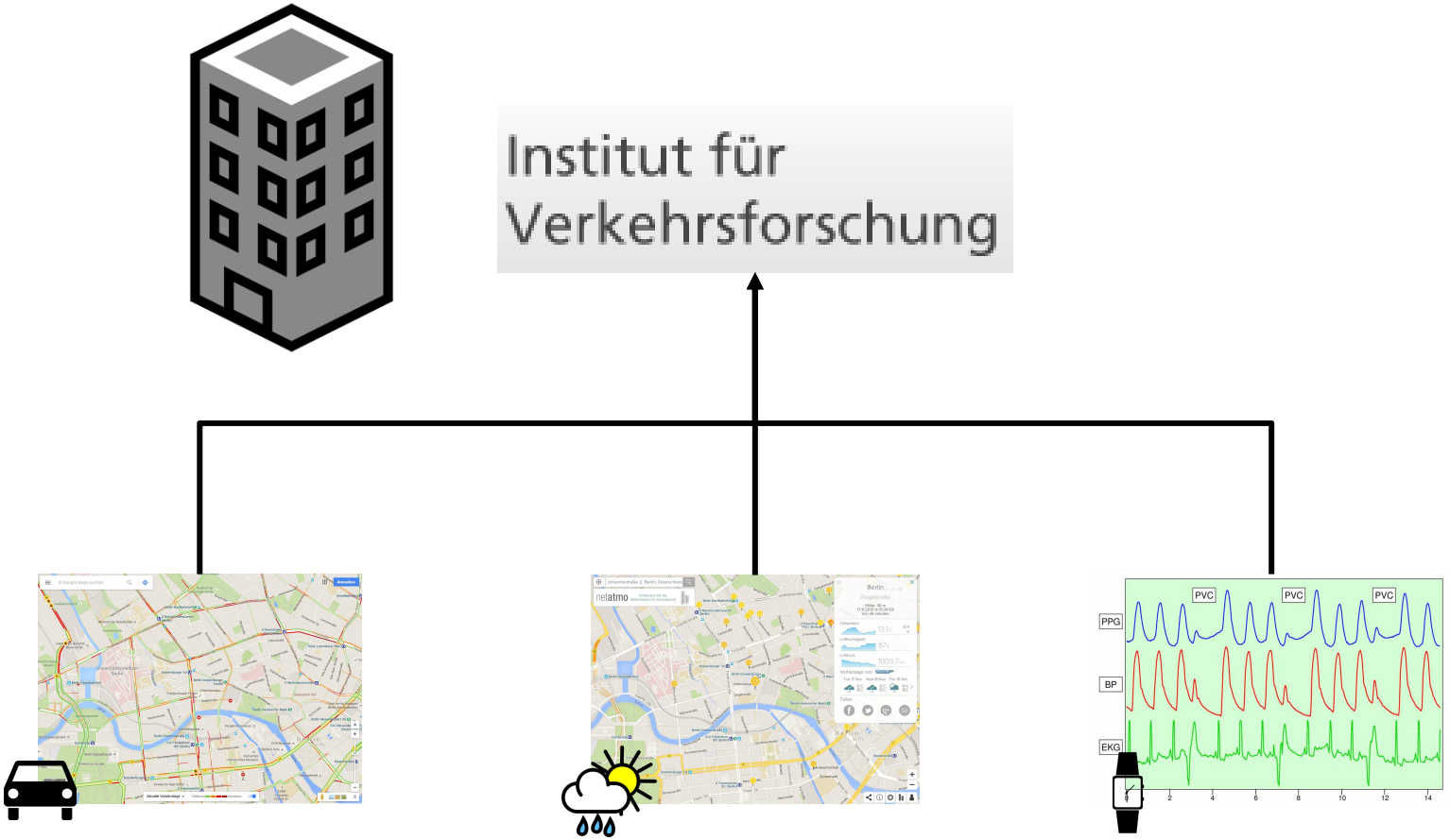
Privacy
Preferences

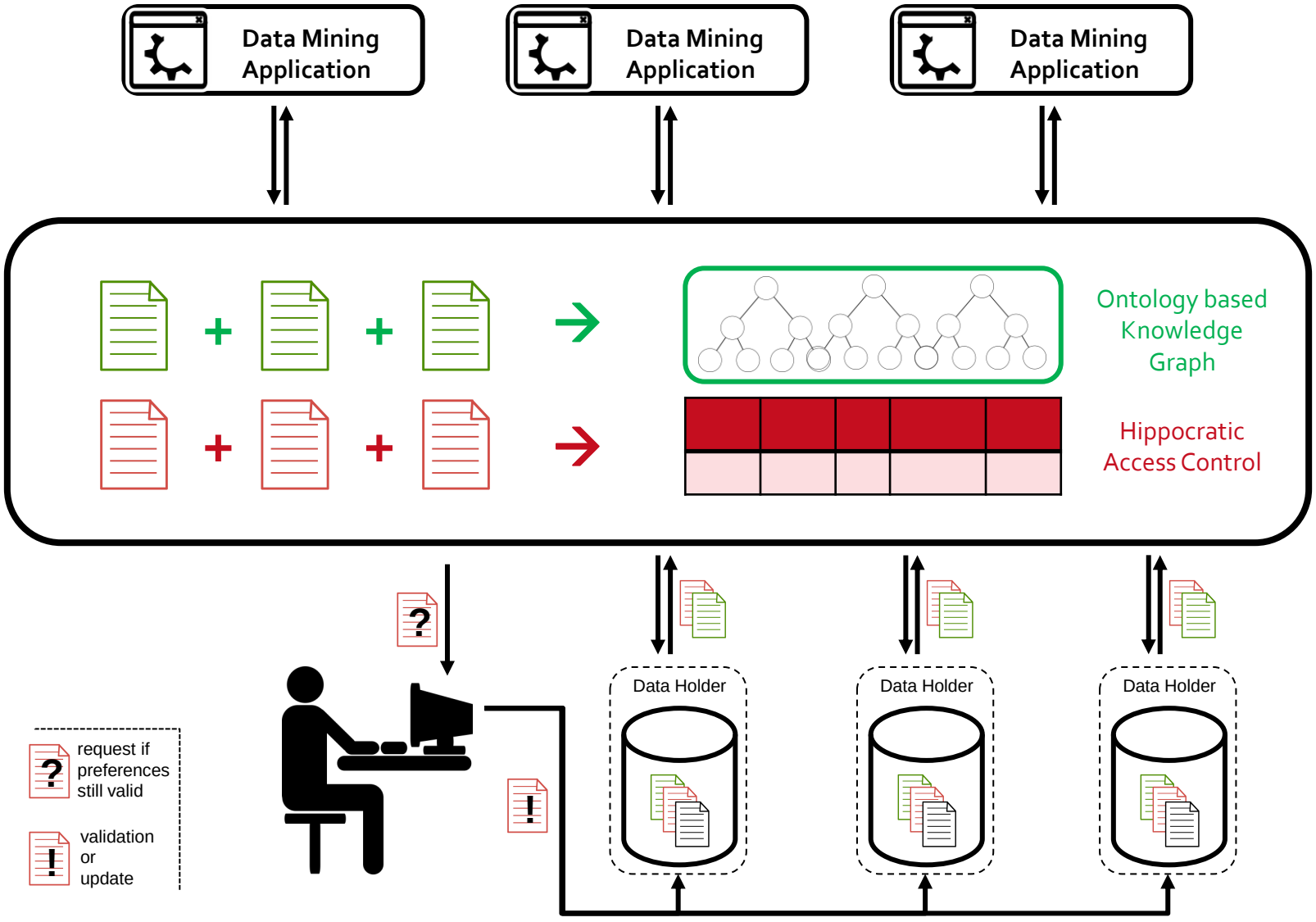
Specification/Description
of the Dataset

Hippocratic Data Integration Platform



Szenario


Institut für
Verkehrsforschung
netatmo
PVC
PVC
PVC
PPG
BP
EKG


Data Mining Application
Data Mining Application
Data Mining Application
Ontology based Knowledge Graph
Hippocratic Access Control
Data Holder
Data Holder
Data Holder
request if preferences still valid
validation or update

Hippocratic Data Integration

Vorteile:

- Autonomie der Datenquellen bleibt erhalten
- Keine Änderungen bestehender Systeme nötig
- Technische Umsetzung von Einwilligung und Zweckbindung (Kontrolle & Protokolle durch Plattform)

Nachteile:

- Evtl. neuer einheitlicher Standard für Datenschutz-Präferenzen (evtl. Meta-Daten-Format) nötig
- Juristische Ausgestaltung von Einwilligung und Zweckbindung müsste reformiert werden

Fazit

Einwilligung und **Zweckbindung** funktionieren in der momentan angewandten Form für viele Big Data Szenarien nicht.

Problem

Bisherige Lösungsansätze

sind für **Echtzeit**-anwendungen mit **heterogenen**, **autonomen** und **verteilten** Datenquellen **nicht praktikabel**

Mit **„Vorab-zustimmung“**, **Kategorisierung** von Zwecken und Verwendern sowie Möglichkeiten zur **dynamischen Anpassung** könnte informationelle Selbstbestimmung auch in Big Data Kontexten realisiert werden.

Einwilligung & Zweckbindung „neu“ denken


Adieu Einwilligung.
Bitte komm bald,
gut erholt und neu
aufgestellt, wieder.

Kontakt

Max-R. Ulbricht

Technische Universität Berlin
Information Systems Engineering

mu@ise.tu-berlin.de

@maroulb

References

Informationelle Selbstbestimmung:

Westin, A. (1967). *Privacy and Freedom.* New York: Atheneum.

HACE Theorem:

Wu, X. et al. 2014. Data mining with big data. *IEEE Transactions on Knowledge and Data Engineering*. 26, 1 , 97–107.

Hippocratic Databases:

Agrawal, R. et al. 2002. Hippocratic Databases. *Proceedings of the 28th International Conference on Very Large Data Bases* (Hong Kong, China, 2002), 143–154.

Sticky Policies:

Pearson, S. and Mont, M.C. 2011. Sticky policies: an approach for managing privacy across multiple parties. *Computer*. 44, 9 (2011), 60–68.

Distributed Usage Control:

Pretschner, A. et al. 2006. Distributed Usage Control. *Commun. ACM*. 49, 9 (Sep. 2006), 39–44.

Dynamic Consent:

Kaye, J. et al. 2015. Dynamic consent: a patient interface for twenty-first century research networks. *European Journal of Human Genetics*. 23, 2 (Feb. 2015), 141–146.

Pictures

Frogs: https://pixabay.com/en/frog-farewell-travel-luggage-897419/ & https://pixabay.com/en/time-to-go-frog-farewell-travel-937265/ (Alexas_Fotos) CCo; Public Domain

4V's: http://www.ibmbigdatahub.com/infographic/four-vs-big-data (IBM, McKinsey, Gartner et al.) Lizenz unbekannt

EKG:https://en.wikipedia.org/wiki/File:PVC_detectionUsing_PGG.png#/media/File:PVC_detectionUsing_PGG.png (Wikipedia-Nutzer: Spl4) CC BY-SA 3.0

Shiny Metal Smart Watches: https://www.flickr.com/photos/mstable/17332357558 (C_osett) Public Domain

All Cliparts: openclipart.org (diverse artists) Public Domain