

LISA Vienna 2024

Regulatory Affairs Konferenz für Medizinprodukte und In-vitro Diagnostika

Ing. Dr. iur. Christof Tschohl

Lebendiger European Health Data Space (EHDS) – „Design Thinking“ als Lösungsmodell

Vortrag am 17. Oktober 2024

Research Institute AG & Co KG
Digital Human Rights Center

Florianigasse 55/10
1080 Wien

www.researchinstitute.at



Research Institute

Digital Human Rights Center

Research Institute AG & Co KG— Digital Human Rights Center

Florianigasse 55/10
1080 Wien

www.researchinstitute.at

Research Institute: Team



**Christof
Tschohl**



**Walter
Hötendorfer**



**Markus
Kastelitz**



**Jan
Hospes**



**Heidi
Scheichenbauer**



**Robert
Rothmann**



**Philipp
Poindl**



**Elisabeth
Mayer**



**Andreas
Czák**



**Michael
Löffler**



**David M.
Schneeberger**



**Madeleine
Müller**



**Georg
Fröwis**



**Michael
Schally**



**Mirjam
Tercero**

* Sortierung nach Dienstalter

Research Institute



Forschung

Wissenschaftliche Projekte an der Schnittstelle von Technik, Recht, Gesellschaft. Grund- und datenschutzrechtliche Fragen sowie gesellschaftliche Folgen und ethische Aspekte neuer Technologien.



Consulting

Fachlich kompetente sowie effiziente und lösungsorientierte Beratung im Bereich Datenschutz, Informationssicherheit und IT-Compliance.



Lehre

Seminare, Vorträge und Tagungen, akademische Lehre und Kurse in Kooperation mit führenden Expert*innen der Branche sowie wissenschaftliche Publikationen



Academy

Die Research Institute-Academy (RIAC) als interdisziplinäre Plattform für Wissenstransfer und berufliche Weiterbildung in den Bereichen Technik, Recht, Verwaltung und Ethik.



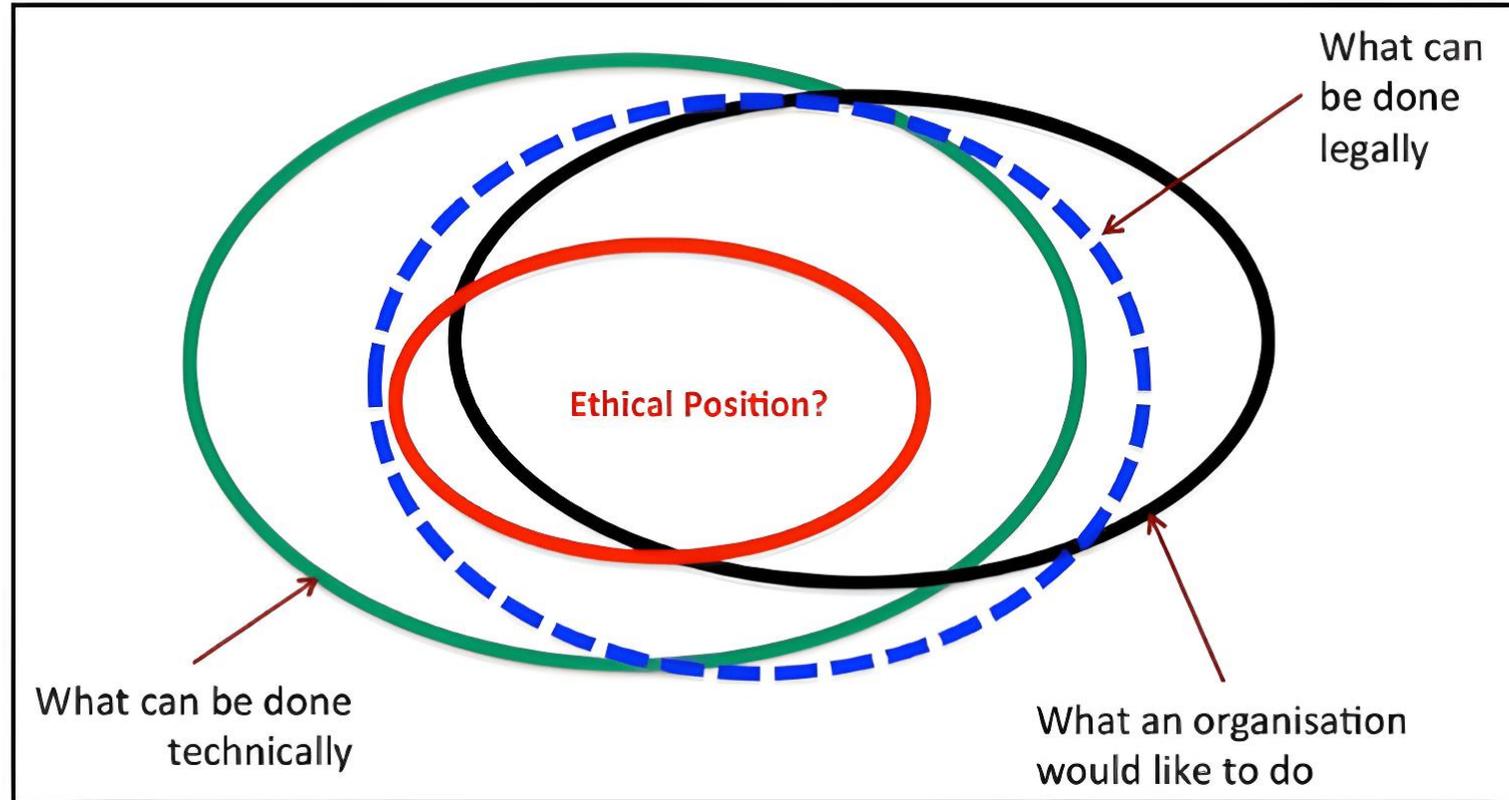
network.fair.data

network.fair.data ein Netzwerk von gemeinnützigen Organisationen und social Entrepreneurs, das es ermöglicht, niederschwellig und preiswert Zugang zu praxisrelevanten Informationen zum Datenschutz mit Blick auf NPOs zu bekommen.

Datenschutz und der Menschenrechtsbasierte Ansatz in der Digitalisierung



The art to find the perfect middle...



Source: IBM, <http://www.informatica.uniroma2.it/upload/2017/IA2/IBM-%20Ethics%20for%20BD&A.pdf>

Grund- und Menschenrechte in der digitalen Gesellschaft

- Datenschutz ist zwar das prominenteste, aber nicht das einzige Grundrecht für die „digitalisierte Gesellschaft“

für

- **Datenschutz ist nicht Selbstzweck**, sondern Voraussetzung für
 - das Funktionieren einer freien demokratischen Gesellschaft und
 - die Ausübung zahlreicher anderer Grundrechte

Datenschutz ist ein Katalysator für alle Grund- und Menschenrechte

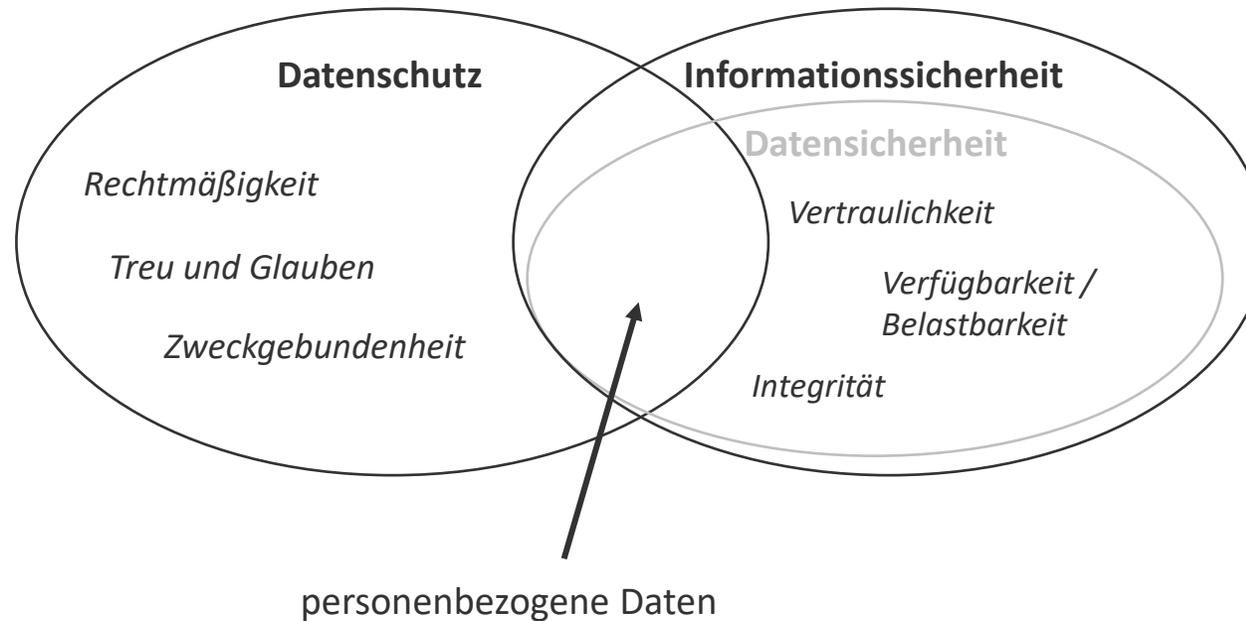
- **Und wie die meisten Grundrechte nicht absolut garantiert – sondern einer Abwägung zugänglich**

- Weitere relevante Grund- und Menschenrechte im digitalen Bereich:
 - Würde des Menschen (Art 1 EU Grundrechte-Charta)
 - Recht auf Achtung des Privat- und Familienlebens
 - Gedanken-, Gewissens- und Religionsfreiheit
 - Freiheit der Meinungsäußerung und Informationsfreiheit
 - Freiheit von Kunst und Wissenschaft
 - Recht auf Bildung
 - Recht auf Zugang zu sozialen Leistungen
 - Recht auf Nichtdiskriminierung
 - Verbraucherschutz
 - Rechte schutzbedürftiger Personen (Kinder, ältere Menschen, Menschen mit Behinderung, etc.)
 - ...

Datenschutz und Informationssicherheit: eine Ehe auf Lebenszeit

strenge Zweckbindung
Rechtfertigungszwang

„need to know“ Prinzip
Berechtigungskonzept



Menschenrechtsbasierter Ansatz

- ✓ Technologie muss menschenzentriert sein („Human Dignity by Design“)
- ✓ Gesellschaftlicher Dialog als Prämisse für ein Gleichgewicht zwischen Sicherheit und Freiheit
- ✓ Rechtliche Rahmenwerke müssen technologische Aspekte miteinbeziehen
- ✓ Technologie muss die Grenzen der Grund- und Menschenrechte respektieren („Human Dignity by Design“ und „Rule of Law by Design“)
- ✓ Compliance mit ethischen Standards
- ✓ Impact Assessments (Folgenabschätzungen) sind das wichtigste Instrument im Zeitalter dieser Entwicklungen



Privilegierung der wissenschaftlichen Forschung im Datenschutz

im Rahmen rechtlicher
und ethischer Regeln



EU-WEITE HARMONISIERUNG DES DATENSCHUTZRECHTS FÜR DIE FORSCHUNG?

- DSGVO enthält **Öffnungsklauseln** → keine EU-weite Harmonisierung
 - in Deutschland wird nach der Kompetenzlage dort die Öffnungsklausel im Recht der Länder (unterschiedlich) umgesetzt → u.a. Motivation für die deutsche „Medizininformatik Initiative“ (MII)
<https://www.medizininformatik-initiative.de/de/start>
- DSGVO **privilegiert** die wissenschaftliche Forschung, z.B.:
 - **Art 5 Abs 1 lit b, e**: Zweckbindung (ErwGr 50: Weiterverwendung) u. Speicherbegrenzung
 - **Art 9 Abs 2 lit j**: Gesetzgeber kann Verarbeitung „sensibler“ Daten für Forschung vorsehen → zB in § 7 DSG oder im FOG
 - **Art 9 Abs 4**: Die Mitgliedstaaten können zusätzliche Bedingungen, einschließlich Beschränkungen, einführen oder aufrechterhalten, soweit die Verarbeitung von **genetischen, biometrischen oder Gesundheitsdaten** betroffen ist.
 - **Art 89 Abs 1 DSGVO**: Verarbeitung zu Forschungszwecken unterliegt geeigneten Garantien für die Rechte und Freiheiten der betroffenen Person → technische und organisatorische Maßnahmen
 - **Art 89 Abs 2**: Gesetzgeber kann **Ausnahmen von Betroffenenrechten** bei der Datennutzung zu Forschungszwecken vorsehen

Aber Achtung: Art 89 Abs 4 DSGVO („Zweckbindung“ der Privilegierungen)

EXKURS: WAS IST WISSENSCHAFTLICHE FORSCHUNG?

https://www.datenschutzkonferenz-online.de/media/dskb/2024-09-11_DSK_Positionspapier%20Wissenschaftliche_Forschungszwecke.pdf



Beschluss

**der Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes
und der Länder vom 11. September 2024**

DS-GVO privilegiert wissenschaftliche Forschung
Positionspapier zum Begriff „wissenschaftliche Forschungszwecke“

- Verdrängung durch ForschungsorganisationsG? (DSB wendet § 7 DSGVO aber weiterhin an!)
- Art 89 Abs 1 DSGVO fordert „**angemessene Garantien**“ → ausreichende Umsetzung in § 7 DSGVO durchaus fraglich
- Genehmigung von DSB jedoch an Bedingungen und Auflagen zu knüpfen
- **Immer: ehestmögliche Anonymisierung bzw Pseudonymisierung** (§ 7 Abs 5 DSGVO; Art 89 Abs 1 DSGVO)
- **ForschungsorganisationsG (FOG)**
 - zentrale Bestimmung: **§ 2d Abs 2 Z 1 FOG** (Datensicherheitsmaßnahmen: § 2d Abs 2)
 - Darunter dürfen (verkürzt gesprochen) von wissenschaftlichen Einrichtungen alle personenbezogenen Daten verarbeitet werden, wenn entweder keine Offenlegung oder die Offenlegung dieser Daten so erfolgt, dass eine Rückführbarkeit auf die betroffenen Personen „praktisch ausgeschlossen“ ist.
 - in Deutschland sog. „Eigenforschungsprivileg“ auf Länderebene → deutsche MII daher Vorbild für EHDS va bzgl. Governance!

Europäischer Raum für Gesundheitsdaten (EHDS)

Europäischer Raum für Gesundheitsdaten (EHDS)

„Binnenmarkt für digitale Gesundheit“

Bessere Diagnose
und Behandlung:

- verbesserte Patientensicherheit
- kontinuierliche medizinische Versorgung
- größere Effizienz des Gesundheitswesens

Befähigung der **Menschen** zur Kontrolle über die eigenen Gesundheitsdaten

Eröffnung des Zugangs zu relevanten Gesundheitsdaten für **Angehörige der Gesundheitsberufe**



Unterstützung der **politischen Entscheidungsträger und Regulierungsbehörden** beim Zugang zu relevanten Gesundheitsdaten

Erleichterung des Zugangs zu Gesundheitsdaten für **Forschende und Innovatoren**

Bessere Gesundheitspolitik,
größere Chancen für Forschung und Innovation

Datenräume (Data Spaces)

2020: Europäische Datenstrategie der Europäischen Kommission

→ Ankündigung von (ursprünglich nur 9) gemeinsamen europäischen Datenräumen:

1. Industriedatenraum (Fertigung)
2. Datenraum für den europäischen Grünen Deal
3. Mobilitätsdatenraum
4. **Gesundheitsdatenraum (EHDS)**
5. Finanzdatenraum
6. Energiedatenraum
7. Agrardatenraum
8. **Datenräume für die öffentliche Verwaltung**
9. Kompetenzdatenraum (Bildung/Skills)
10. Kulturelles Erbe
11. Medien
12. Common European research & innovation data space
13. Tourismus
14. Europäische Sprache(n) - European Language Data Space

Einheitliches Ziel:

- Schaffung großer **Datenpools** in diesen Sektoren
- Verbesserter **Datenzugang** für **Entwicklung** neuer datengestützter Dienste und Anwendungen
- KOM: Common European data spaces play a critical role in providing a steady supply of data for **training of foundation models (GenAI)**

EHDS: Inkrafttreten

COM(2022) 197 final; 2022/0140(COD)

- 14. März 2024: Rat, Europäische Parlament und EU-Kommission im Trilog: Einigung gemeinsamer Kompromisstext
- **24. April 2024: Europäische Parlament beschließt Text in erster Lesung**
 - Text wird noch redaktionell bereinigt, sprachjuristisch geprüft und übersetzt
 - **Der finalisierte Text wird voraussichtlich im Herbst 2024 dem neuen Europäischen Parlament zur erneuten Abstimmung vorgelegt, bevor er dann dem Rat zur förmlichen Annahme übermittelt wird**
- EHDS-VO tritt 20 Tage nach ihrer Veröffentlichung im Amtsblatt der EU in Kraft, **voraussichtlich im Herbst/Winter 2024**
- Anwendung tlw. nach 2 Jahren, teilweise nach 4, 6 oder 10 Jahren nach Inkrafttreten

Quellen:

<https://data.consilium.europa.eu/doc/document/ST-10078-2024-INIT/de/pdf> (18.6.2024)

<https://www.bundesgesundheitsministerium.de/themen/internationale-gesundheitspolitik/europa/europaeische-gesundheitspolitik/ehds>

Kapitel I – Artikel 2 (2)

(y) „**Gesundheitsdateninhaber**“ bezeichnet natürliche oder juristische Personen, Behörden, Einrichtungen oder sonstige Stellen im **Gesundheits- oder im Pflegesektor**, darunter soweit erforderlich **Erstattungsdienste** sowie natürliche oder juristische Personen, die **Produkte oder Dienstleistungen für die Gesundheitsversorgung**, den **Gesundheits- oder den Pflegesektor entwickeln**, die **Wellness-Anwendungen entwickeln oder herstellen**, die **Forschungstätigkeiten im Bereich des Gesundheits- oder Pflegesektors** durchführen, oder als Sterblichkeitsregister fungieren, sowie Organe, Einrichtungen oder sonstige Stellen der Union, die entweder

a) nach dem geltenden Unionsrecht oder den geltenden nationalen Rechtsvorschriften dazu berechtigt oder verpflichtet sind, in ihrer **Eigenschaft als Verantwortlicher** oder **gemeinsam Verantwortlicher** **personenbezogene elektronische Gesundheitsdaten** für die **Erbringung von Gesundheits- oder Pflegeleistungen** oder für **Zwecke der öffentlichen Gesundheit, der Kostenerstattung, der Forschung, der Innovation, der Politikgestaltung, der amtlichen Statistik, der Patientensicherheit oder der Regulierung zu verarbeiten**; oder

b) dazu befähigt sind, **nicht personenbezogene elektronische Gesundheitsdaten** durch die **Kontrolle der technischen Konzeption eines Produkts und der damit zusammenhängenden Dienste zur Verfügung zu stellen** und sie auch zu registrieren, bereitzustellen, den Zugang zu ihnen einzuschränken oder sie auszutauschen.

Europäischer Raum für Gesundheitsdaten (EHDS)



Gegenstand und Ziele:

1. Primärnutzung,
2. Sekundärnutzung elektronischer Gesundheitsdaten
3. Rechtlicher und technischer Rahmen für elektronische Patientenaktensysteme (EHR-Systeme) und Wellness-Anwendungen



Anwendungsbereich:

Sachlich:

- **Elektronische Gesundheitsdaten**

Räumlich:

- **Europäische Union**

Elektronische Gesundheitsdaten sollen in Versorgung, in Forschung und Entwicklung sowie für die Weiterentwicklung des Gesundheitswesens besser genutzt werden können.

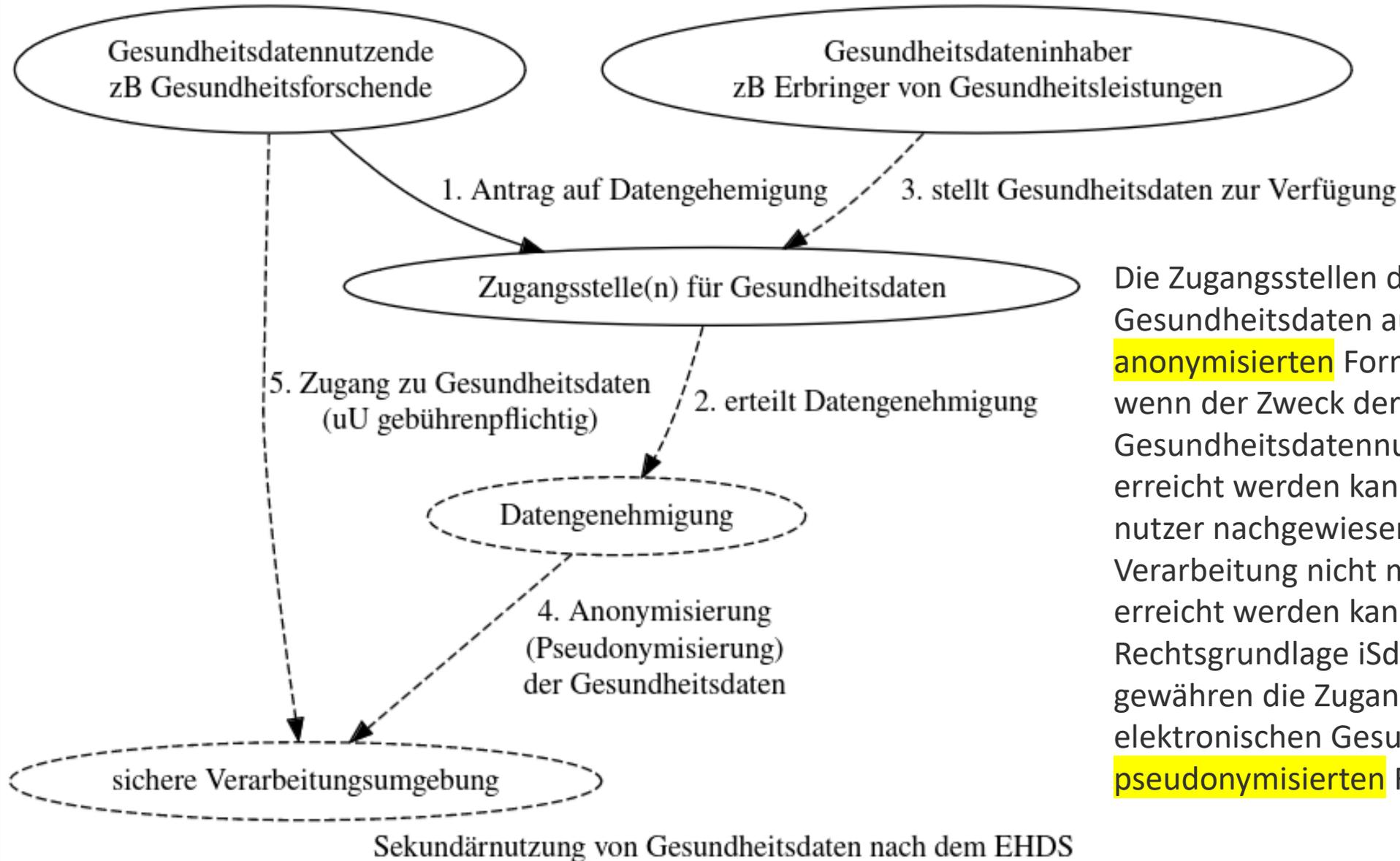


Betroffene Institutionen / Sektoren:

Generell: Gesundheits- u- Pflegesektor, insb.

- **Mitgliedsstaaten**
- **„Patienten“**
- **„Gesundheitsdateninhaber“**
- **„Gesundheitsdatennutzer“**
- **Anbieter von EHR-Systemen und Wellness-Anwendungen**
- ...

EHDS Ablauf Sekundärnutzungszugang



Die Zugangsstellen dürfen elektronische Gesundheitsdaten ausschließlich in einem **anonymisierten** Format zur Verfügung stellen, wenn der Zweck der Verarbeitung durch den Gesundheitsdatennutzer mit diesen Zwecken erreicht werden kann. Hat der Gesundheitsdatennutzer nachgewiesen, dass der Zweck der Verarbeitung nicht mit anonymisierten Daten erreicht werden kann und hat er eine Rechtsgrundlage iSd Art 6 Abs 1 DSGVO benannt, gewähren die Zugangsstellen Zugang zu elektronischen Gesundheitsdaten in einem **pseudonymisierten** Format.

Datenräume (Data Spaces)

Overview of the **legislative framework** for the implementation of the European strategy for data

→ Data Spaces werden durch horizontale Rechtsakte „unterstützt“, insb.

DGA: Weiterverwendung von Daten öffentlicher Stellen; Daten-Altruismus etc.

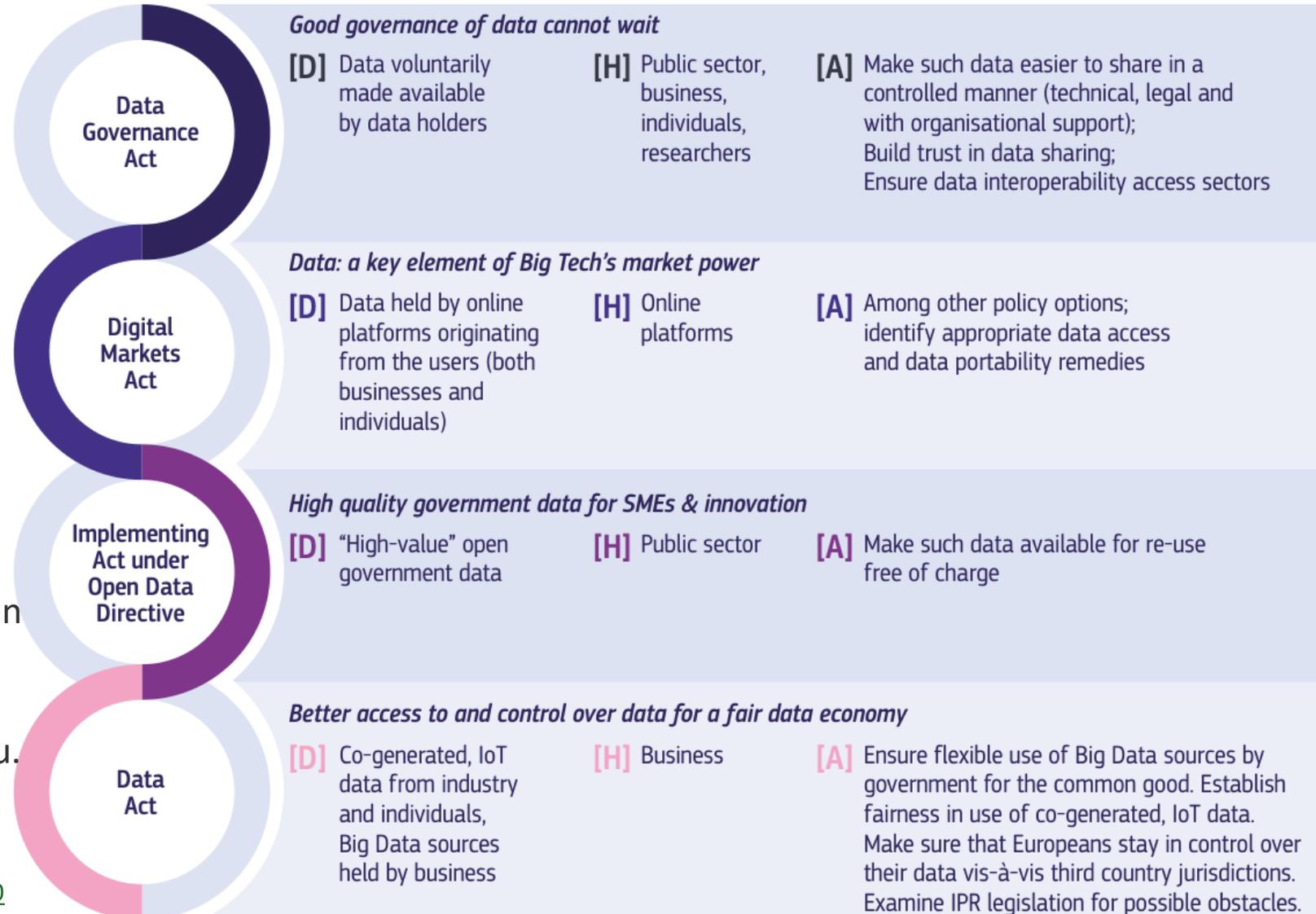
DA: Datenzugang f. Nutzer eines vernetzten Produkts („IoT“) u. verbundene Dienste; B2C/B2B; u.a. Anforderungen an Interoperabilität v. Datenräumen (Art 33) u. Datenweitergabevereinbarungen

Overview of data actions

[D] What data are we talking about?

[H] Who holds such data?

[A] What policy intervention?





Datenräume (Data Spaces) und Governance

Voraussetzung für einen funktionierenden Datenraum ist vor allem ein klare definierter **Governance-Rahmen** der

- die **Grundsätze, Prozesse und Praktiken** enthält, die die **Führung, das Management und den Betrieb innerhalb eines Datenraums leiten und regeln**, um eine effektive und verantwortungsvolle Führung, Kontrolle und Aufsicht zu gewährleisten.
- die **Funktionalitäten definiert**, die **innerhalb des Datenraums verfügbar** sein müssen, d.h. die Beiträge, die seine Komponenten oder Elemente zur Effektivität, Effizienz und Anpassungsfähigkeit des Datenraums leisten müssen.
- die **Datenraumrollen** definiert, d. h. die **Rechte und Pflichten (Verantwortlichkeiten)**, die es den Parteien, die diese **Rollen ausüben**, ermöglichen, **Aufgaben zu erfüllen**, die diese Funktionalitäten bereitstellen.

Daten-Governance-Rechtsakt/ Data Governance Act (DGA)



Gegenstand und Ziele:

Zugang zu geschützten **Daten öffentlicher Stellen**;
Etablierung von **Datenvermittlungsdiensten + Datenaltruismus**;



Anwendungsbereich:

Sachlich:

- **Öffentliche Stellen**
- **Datenvermittlungsdienste**
- **datenaltruistische Organisationen**

Räumlich:

- in der **Union**



Betroffene Institutionen / Sektoren:

Öffentlicher Sektor:

Staat, Gebietskörperschaften, Einrichtungen des öffentlichen Rechts oder Verbände, die aus einer oder mehreren dieser Körperschaften oder einer oder mehreren dieser Einrichtungen des öffentlichen Rechts bestehen;

datenaltruistische Organisationen

Datenvermittlungsdienste

Inkrafttreten: 23. Juni 2022 (anwendbar seit 24. September 2023)

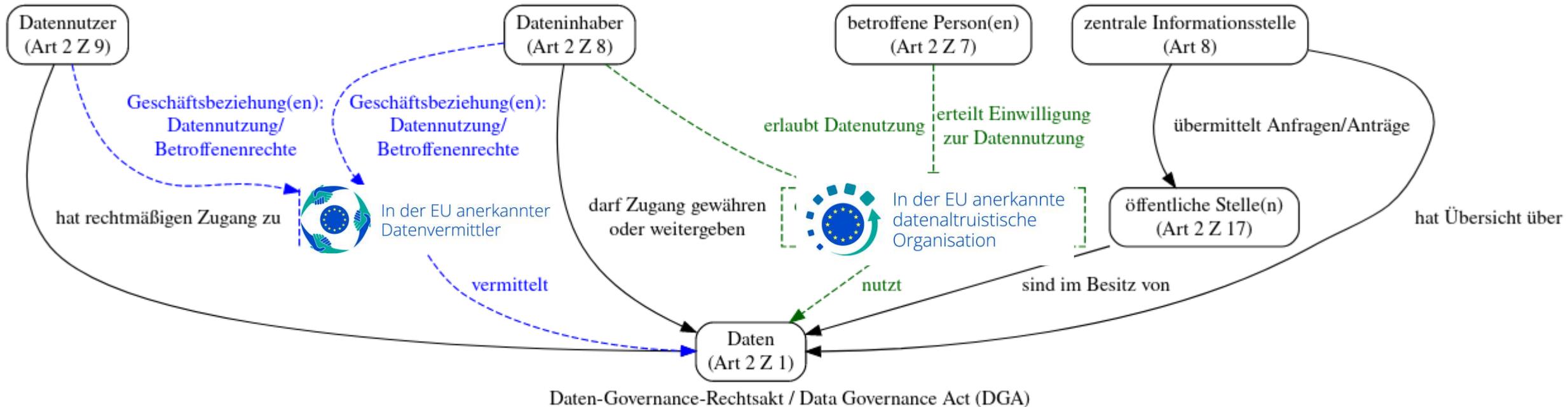


Daten-Governance-Rechtsakt/ Data Governance Act (DGA)

Leitsatz/Leitmotiv:

Weiterverwendung von Daten öffentlicher Stellen;
Etablierung von **Datenvermittlungsdiensten** +
Datenaltruismus (freiwillige gemeinsame, kostenlose
Nutzung von Daten)

- Begriffsbestimmungen:**



Daten-Governance-Rechtsakt/ Data Governance Act (DGA)

- **Kernregelungen:**
 - **keine Verpflichtung für öffentliche Stellen**, die Weiterverwendung von Daten zu erlauben;
 - **keine Befreiung** öffentlicher Stellen **von Geheimhaltungspflichten**;
 - **Verpflichtung** öffentlicher Stellen **zum Schutz von Daten** (etwa Anonymisierung/Aggregation/etc.);
- **Konsequenzen bei Nichteinhaltung :**
 - Sanktionsregime ist Mitgliedstaaten überlassen (Art 34);
 - Beschwerderecht (Art 27);
 - Gerichtlicher Rechtsbehelf (Art 28);

Weitere Informationen: *Europäische Kommission (EK)*, Data Governance Act explained <https://digital-strategy.ec.europa.eu/en/policies/data-governance-act-explained> (aufgerufen am 02.10.2024).

DSGVO Bezug:

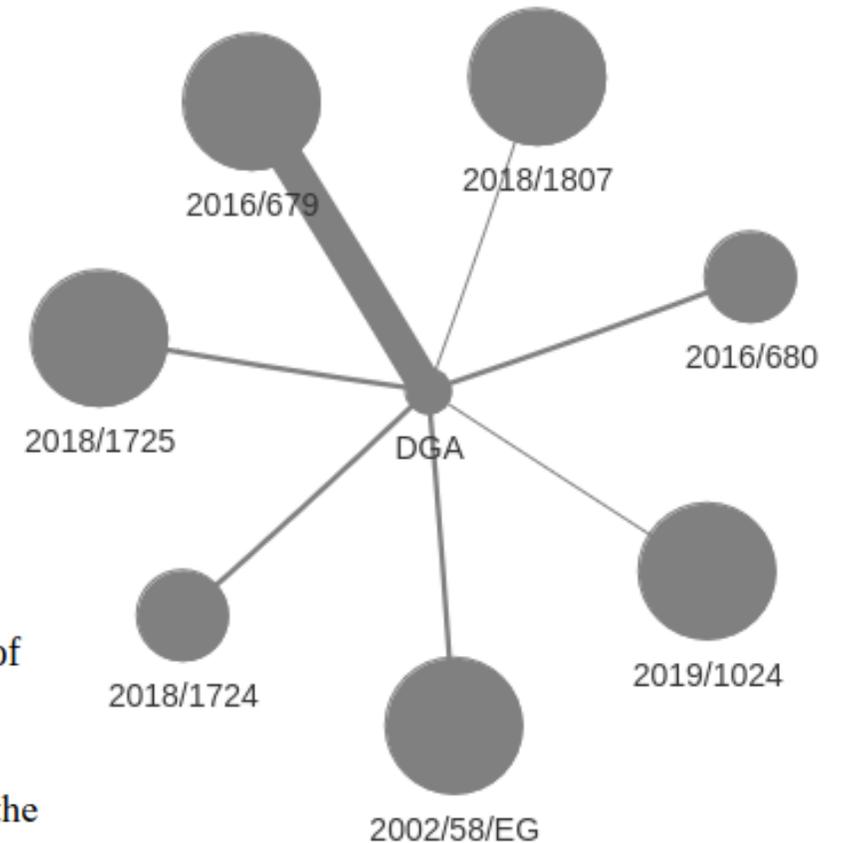
- **DSGVO bleibt unberührt** bzw. genießt Vorrang;
- **DGA schafft keine Rechtsgrundlage** iSv Art 6 DSGVO;
- EK soll **Einwilligungsformular** für Datenaltruismus erlassen (Art 25 DGA)
 - Problem „broad consent“

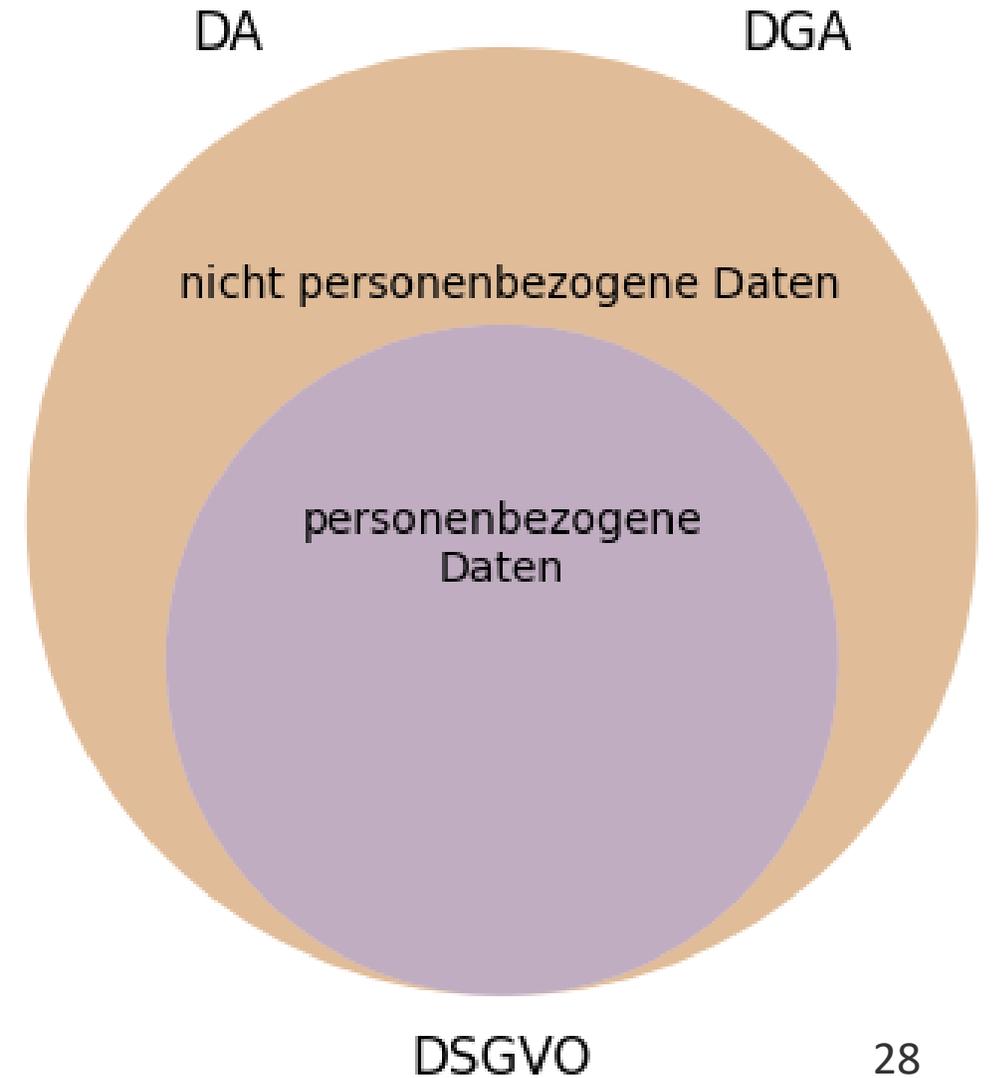
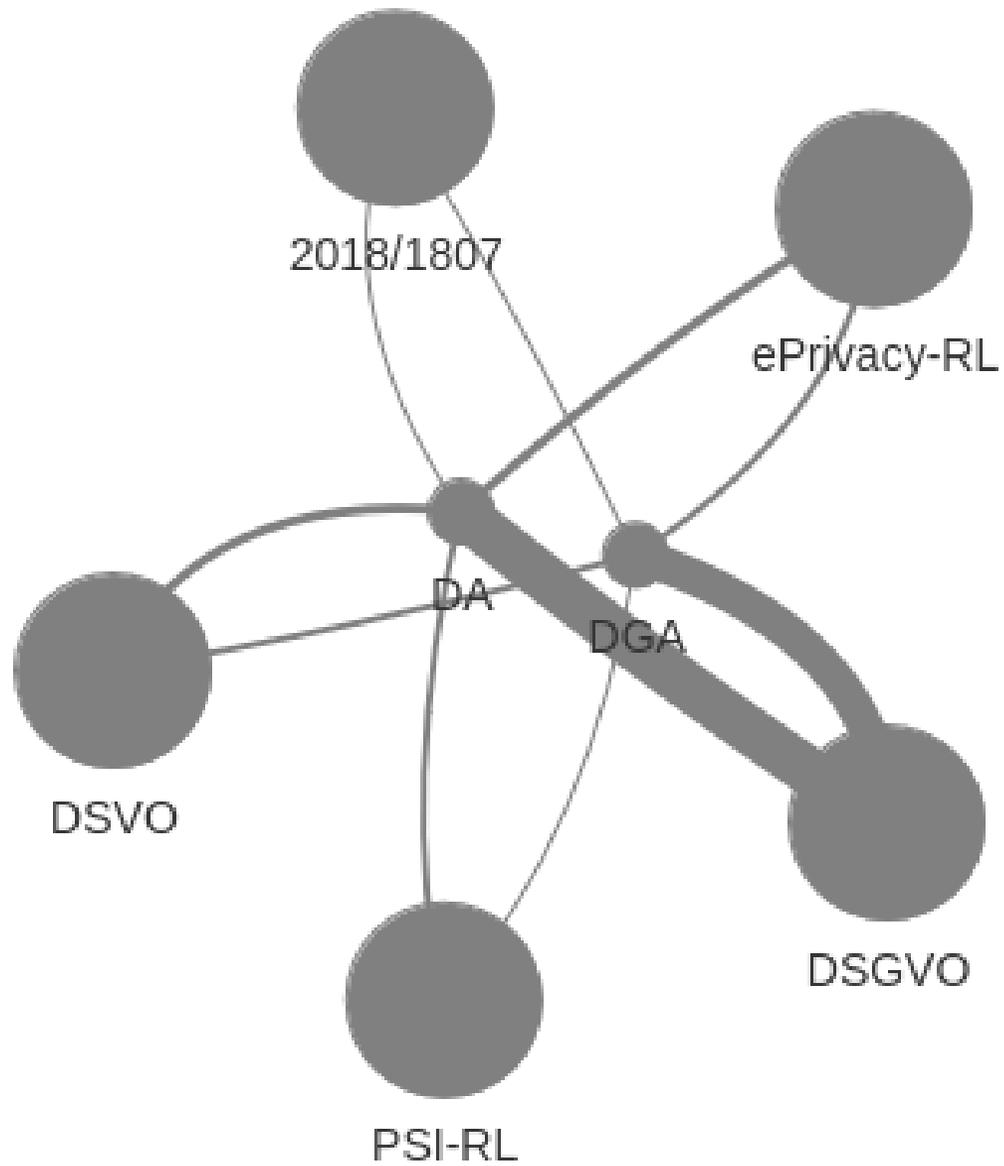
8. Data Altruism

- In its introductory presentation (see also slide deck), the Commission explained the potential of data altruism, both by individuals and by companies (data philanthropy). The Commission specified that data altruism is – in compliance with the GDPR – a revocable act of making available data. It reserves the term “consent” to situations of use of personal data, whereas in the context of sharing of non-personal data, the term “**permission**” would be used.

Daten-Governance-Rechtsakt/ Data Governance Act (DGA)

Sonstige Querverbindungen:





Kombinierte (integrierte) Folgenabschätzungs- Methodologie



Datenschutz-Folgenabschätzung
(DSFA) – Artikel 35 DSGVO



Grundrechte-Folgenabschätzung
(GRFA) – Artikel 27 AI Act



Ethik-Folgenabschätzung (EFA)



Beispiele aus laufenden Forschungsprojekten mit Beteiligung des RI

Gemeinsamkeit: federated machine learning

- Projekt FeatureCloud (Horizon Europe, 1.1.2019 – 31.12.2023)
- Projekt SCREEN4CARE (IMI, 1.9.2021 – 31.8.2026)

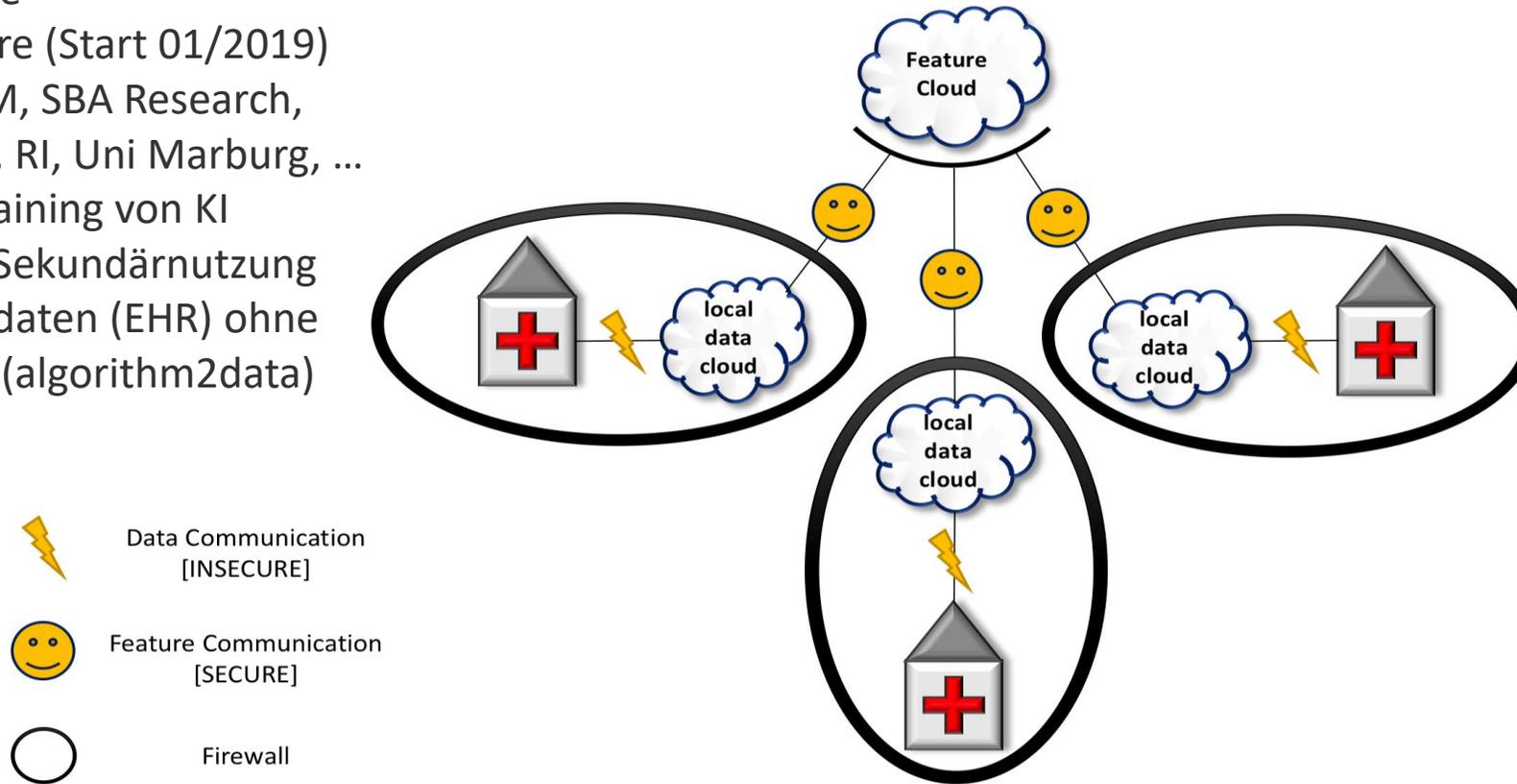


„Privacy by Architecture“ – EU Projekt „FeatureCloud“

<https://featurecloud.eu/>

Projektstatus: abgeschlossen

- Horizon Europe
- Laufzeit: 5 Jahre (Start 01/2019)
- Partner: UHAM, SBA Research, Med-Uni Graz, RI, Uni Marburg, ...
- Föderiertes Training von KI Modellen zur Sekundärnutzung von Patientendaten (EHR) ohne Datentransfer (algorithm2data)



REVOLUTIONISING CLOUD COMMUNICATION

Privacy preserving federated
machine learning and block chaining
for reduced cyber risks in a world
of distributed healthcare



<https://featurecloud.eu/>



FeatureCloud on Twitter:
[@Feature_Cloud](https://twitter.com/Feature_Cloud)

featurecloud appstore (free)
<https://featurecloud.ai/>

Proof of Concept
für praktisch gleichwertigen
machine learning Erfolg mit
federated learning (statt „data lake“)
In der medizinischen Forschung
Inklusive XAI (explainable AI)

FEDERATED MACHINE LEARNING ALS MITTEL ZUR ÜBERWINDUNG RECHTLICHER HÜRDEN DER FORSCHUNG MIT GESUNDHEITSDATEN

Jan Hospes / Walter Hötendorfer / Philipp Poindl / Christof Tschohl

Researcher, Research Institute AG & Co KG
Amundsenstraße 9, 1170 Wien, AT
jan.hospes@researchinstitute.at; <https://researchinstitute.at>

Senior Researcher, Research Institute AG & Co KG
Amundsenstraße 9, 1170 Wien, AT
walter.hoetendorfer@researchinstitute.at; <https://researchinstitute.at>

Researcher, Research Institute AG & Co KG
Amundsenstraße 9, 1170 Wien, AT
phillipp.poindl@researchinstitute.at; <https://researchinstitute.at>

Wissenschaftlicher Leiter, Research Institute AG & Co KG
Amundsenstraße 9, 1170 Wien, AT
christof.tschohl@researchinstitute.at; <https://researchinstitute.at>

Schlagworte: *Federated Machine Learning, KI, Gesundheitsdaten, Datenschutz, Privacy by Architecture, FeatureCloud*

Abstract: *Machine Learning in der medizinischen Forschung erfordert große Datenmengen und somit häufig die Einbeziehung von Daten aus mehreren medizinischen Einrichtungen. Federated Machine Learning ermöglicht dies, ohne dass die Daten die jeweilige Einrichtung verlassen, in der sie erhoben wurden. Dadurch steigert Federated Machine Learning nicht nur die Zugänglichkeit vorhandener Gesundheitsdaten für die Forschung, sondern eröffnet auch neue Möglichkeiten betreffend die Rechtsgrundlagen für diese Forschung, die im Beitrag analysiert werden.*

Zitiervorschlag: Jan Hospes / Walter Hötendorfer / Philipp Poindl / Christof Tschohl, Federated Machine Learning als Mittel zur Überwindung rechtlicher Hürden der Forschung mit Gesundheitsdaten, in: Jusletter IT 24. April 2024

Sammlung: Tagungsband IRIS 2024

https://jusletter-it.weblaw.ch/issues/2024/24-April-2024/federated-machine-le_c3d3ce3234.html

Das Projekt SCREEN4CARE



Shortening the path to rare disease diagnosis by using newborn genetic screening and digital technologies

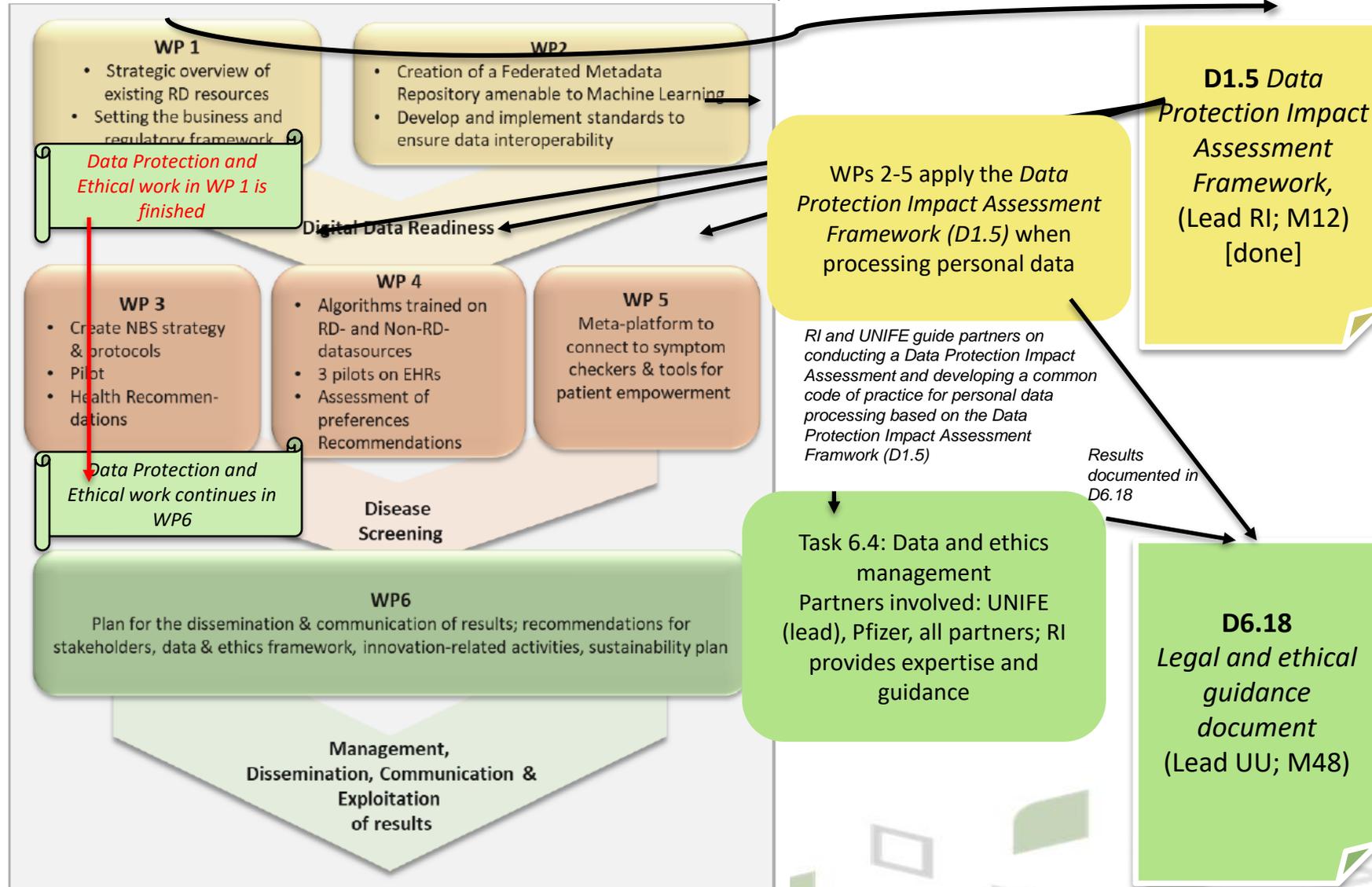
<https://screen4care.eu/de>

- Gefördert durch die „Innovative Medicines Initiative“ (IMI)
- Betrieben durch Partner aus Forschung und Industrie
- Laufzeit: 09/2021 bis 08/2026
- innovative Forschung zur Beschleunigung der Diagnose seltener Erkrankungen, basierend auf genetischem Screening für Neugeborene und digitale Technologien.

Durch die deutschen Partner Charité, Uni Göttingen, Uni Freiburg, enge Verbindung zur „Medizininformatik Initiative“ (MII)
<https://www.medizininformatik-initiative.de/de/start>

S4C DATA PROTECTION MANAGEMENT

In WP1, D1.5 was created as a framework for further data protection work in S4C



FAIR AI –

Fostering Austria's Innovative Strength and Research excellence in AI



Fostering
Austria's
Innovative strength and
Research excellence
in
Artificial
Intelligence

- FFG-Förderung
- Laufzeit: 3 Jahre (Start 11/2023)
- Partner: AIT, TU Wien, FHs, ÖAW, Industriepartner, etc.
- Ziel: Mittels Bottom-up-Strategie sollen typische Fallstricke in der Entwicklung und Anwendung von KI ausgewählt und analysiert werden, um eine Sammlung von Use Cases und darauf aufbauenden KI-Leitlinien für rechtliche und ethische Compliance zu erstellen.

Aktuelle Forschung des RI – weitere laufende Projekte im Überblick

- **dAlbetes (Horizon Europe) – seit 01/2024, 5 Jahre**
- **Microb-AI-ome (Horizon Europe) – seit 04/2023, 5 Jahre**
- **REPO4EU (Horizon Europe) – seit 09/2022, 5 Jahre**
- **RoleModel Justiz 3.0 (FFG KIRAS) – seit 10/2024, 2 Jahre**
- **Aufklärung 4.0 Art 86 AI Act (BMSGPK) – seit 06/2024, 6 Monate**
- **CERTIFIER (FFG KIRAS) – seit 11/2023, 2 Jahre**
- **HYBRIS (FFG KIRAS) – seit 01/2023, 2 Jahre**
- **GEOCROW (FFG FORTE) – seit 02/2023, 2 Jahre**



Fragen und Diskussion



Vielen Dank!



Abonnieren Sie unseren Newsletter und
besuchen Sie uns unter: www.researchinstitute.at

Dieses Dokument dient als Präsentationsunterlage, erstellt von den auf der Titelseite genannten AutorInnen.

Copyright:

Die vorliegenden (elektronischen) Unterlagen wurden von Markus Kastelitz sowie Christof Tschohl bzw. vom Team des Research Institute entwickelt. Wir dürfen Sie daher bitten, das geistige Eigentum im Sinne des Urheberrechts zu respektieren. Auch die Vervielfältigung der Unterlagen und Dateien, die kein veröffentlichtes Werk darstellt, ist nicht gestattet. Ohne schriftliche Genehmigung durch die AutorInnen dürfen weder die Unterlagen selbst noch einzelne Informationen daraus reproduziert oder an Dritte weitergegeben werden.

Disclaimer:

Dieses Dokument wurde auf Basis jener Informationen erstellt, die den Autor*innen als für den Zweck des Dokuments relevant erschienen. Die Autor*innen übernehmen jedoch keine Haftung/Gewähr für Vollständigkeit und Richtigkeit der in diesem Dokument zur Verfügung gestellten Informationen. Die Angaben in diesem Dokument können von dem Empfänger nicht als Zusicherung oder Garantie verstanden werden. Die in diesem Dokument enthaltenen Informationen können sich im Laufe der Zeit verändern oder zum Übergabezeitpunkt bereits verändert haben. Technische Änderungen vorbehalten.