Bundesministerium
für Bildung
und Forschung

Werte-orientierte Gestaltung — Instrument für eine zukunftsgerechte Gewährleistung von individueller und kollektiver Selbstbestimmung

Claudia Müller-Birn | Peter Sörries | David Leimstädtner, Freie Universität Berlin
Sandra Hofhues, Fernuniversität in Hagen
Marian Margraf, Fraunhofer AISEC
Matthias Rose, Charité - Universitätsmedizin Berlin

JahreskonferenzForum Privatheit 2022: Daten-Fairness in einer globalisierten Welt
14.Oktober 2022

Stärkung der individualisierten Medizin

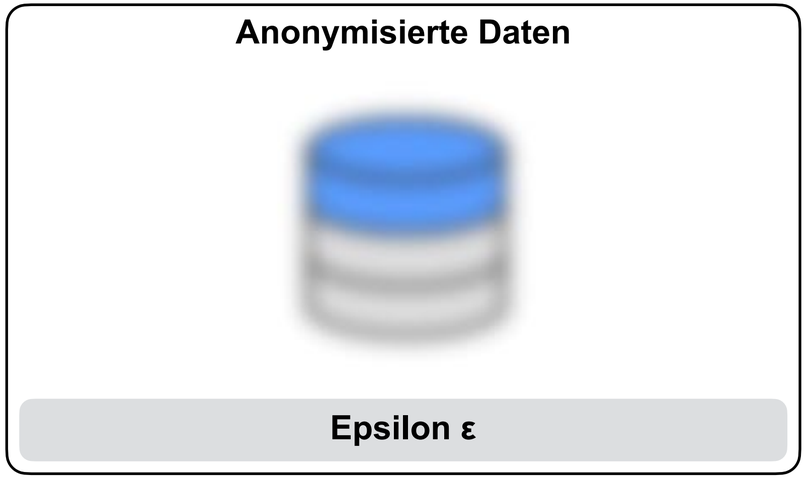
Schutz personenbe-zogener Daten

Stärkung der Akzeptanz durch

Partizipation in der Gestaltung

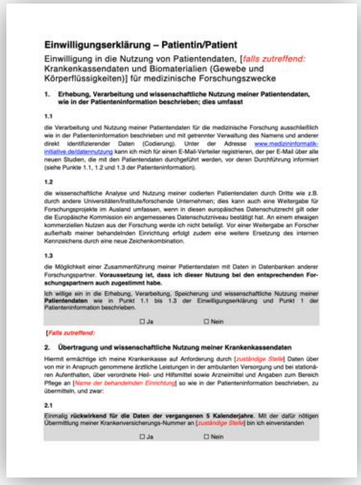
Kommunikation der Privacy-Enhancing-Technology

Anonymisierung der Daten mit Differential Privacy (DP)



Einsatz von DP bei hohem Schutzbedarf

Datengebende
Anton B., Patient



Einwilligungs-erklärung

Einwilligungserklärung – Patientin/Patient

Einwilligung in die Nutzung von Patientendaten, [*falls zutreffend:* Krankenkassendaten und Biomaterialien (Gewebe und Körperflüssigkeiten)] für medizinische Forschungszwecke

1. Erhebung, Verarbeitung und wissenschaftliche Nutzung meiner Patientendaten, wie in der Patienteninformation beschrieben; dies umfasst

1.1
die Verarbeitung und Nutzung meiner Patientendaten für die medizinische Forschung ausschließlich wie in der Patienteninformation beschrieben und mit getrennter Verwaltung des Namens und anderer direkt identifizierender Daten (Codierung). Unter der Adresse www.medizininformatik-initiative.de/datennutzung kann ich mich für einen E-Mail-Verteiler registrieren, der per E-Mail über alle neuen Studien, die mit den Patientendaten durchgeführt werden, vor deren Durchführung informiert (siehe Punkte 1.1, 1.2 und 1.3 der Patienteninformation).

1.2
die wissenschaftliche Analyse und Nutzung meiner codierten Patientendaten durch Dritte wie z.B. durch andere Universitäten/Institute/forschende Unternehmen; dies kann auch eine Weitergabe für Forschungsprojekte im Ausland umfassen, wenn in diesen europäisches Datenschutzrecht gilt oder die Europäische Kommission ein angemessenes Datenschutzniveau bestätigt hat. An einem etwaigen kommerziellen Nutzen aus der Forschung werde ich nicht beteiligt. Vor einer Weitergabe an Forscher außerhalb meiner behandelnden Einrichtung erfolgt zudem eine weitere Ersetzung des internen Kennzeichens durch eine neue Zeichenkombination.

1.3
die Möglichkeit einer Zusammenführung meiner Patientendaten mit Daten in Datenbanken anderer Forschungspartner. **Voraussetzung ist, dass ich dieser Nutzung bei den entsprechenden Forschungspartnern auch zugestimmt habe.**

Ich willige ein in die Erhebung, Verarbeitung, Speicherung und wissenschaftliche Nutzung meiner **Patientendaten** wie in Punkt 1.1 bis 1.3 der Einwilligungserklärung und Punkt 1 der Patienteninformation beschrieben.

☐ Ja ☐ Nein

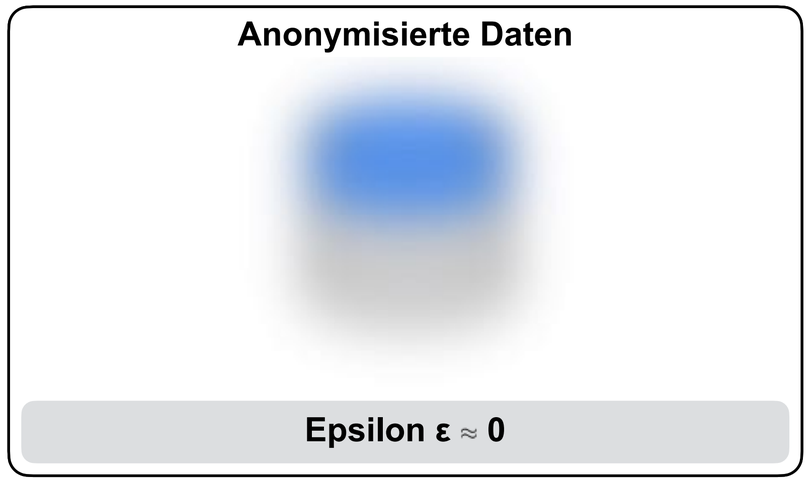
[*Falls zutreffend:*

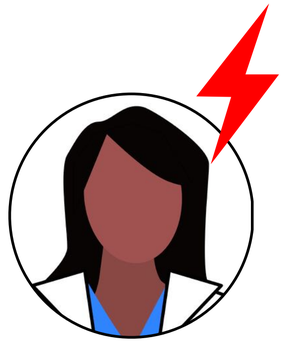
2. Übertragung und wissenschaftliche Nutzung meiner Krankenkassendaten

Hiermit ermächtige ich meine Krankenkasse auf Anforderung durch [*zuständige Stelle*] Daten über von mir in Anspruch genommene ärztliche Leistungen in der ambulanten Versorgung und bei stationären Aufenthalten, über verordnete Heil- und Hilfsmittel sowie Arzneimittel und Angaben zum Bereich Pflege an [*Name der behandelnden Einrichtung*] so wie in der Patienteninformation beschrieben, zu übermitteln, und zwar:

2.1
Einmalig **rückwirkend für die Daten der vergangenen 5 Kalenderjahre**. Mit der dafür nötigen Übermittlung meiner Krankenversicherungs-Nummer an [*zuständige Stelle*] bin ich einverstanden

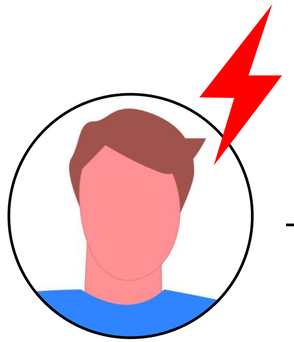
☐ Ja ☐ Nein



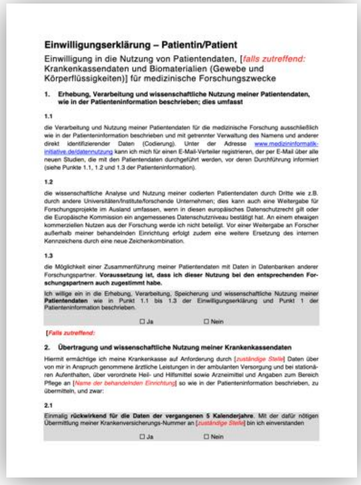


Datenkonsument
Cecilia D., Forscherin

Einsatz von DP bei niedrigen Schutzbedarf



Datengebende
Anton B., Patient



Einwilligungserklärung – Patientin/Patient

Einwilligung in die Nutzung von Patientendaten, [*falls zutreffend:* Krankenkassendaten und Biomaterialien (Gewebe und Körperflüssigkeiten)] für medizinische Forschungszwecke

1. **Erhebung, Verarbeitung und wissenschaftliche Nutzung meiner Patientendaten, wie in der Patienteninformation beschrieben; dies umfasst**

1.1

die Verarbeitung und Nutzung meiner Patientendaten für die medizinische Forschung ausschließlich wie in der Patienteninformation beschrieben und mit getrennter Verwaltung des Namens und anderer direkt identifizierender Daten (Codierung). Unter der Adresse www.medizininformatik-initiative.de/datennutzung kann ich mich für einen E-Mail-Verteiler registrieren, der per E-Mail über alle neuen Studien, die mit den Patientendaten durchgeführt werden, vor deren Durchführung informiert (siehe Punkte 1.1, 1.2 und 1.3 der Patienteninformation).

1.2

die wissenschaftliche Analyse und Nutzung meiner codierten Patientendaten durch Dritte wie z.B. durch andere Universitäten/Institute/forschende Unternehmen; dies kann auch eine Weitergabe für Forschungsprojekte im Ausland umfassen, wenn in diesen europäisches Datenschutzrecht gilt oder die Europäische Kommission ein angemessenes Datenschutzniveau bestätigt hat. An einem etwaigen kommerziellen Nutzen aus der Forschung werde ich nicht beteiligt. Vor einer Weitergabe an Forscher außerhalb meiner behandelnden Einrichtung erfolgt zudem eine weitere Ersetzung des internen Kennzeichens durch eine neue Zeichenkombination.

1.3

die Möglichkeit einer Zusammenführung meiner Patientendaten mit Daten in Datenbanken anderer Forschungspartner. **Voraussetzung ist, dass ich dieser Nutzung bei den entsprechenden Forschungspartnern auch zugestimmt habe.**

Ich willige ein in die Erhebung, Verarbeitung, Speicherung und wissenschaftliche Nutzung meiner **Patientendaten** wie in Punkt 1.1 bis 1.3 der Einwilligungserklärung und Punkt 1 der Patienteninformation beschrieben.

☐ Ja ☐ Nein

[*Falls zutreffend:*

2. **Übertragung und wissenschaftliche Nutzung meiner Krankenkassendaten**

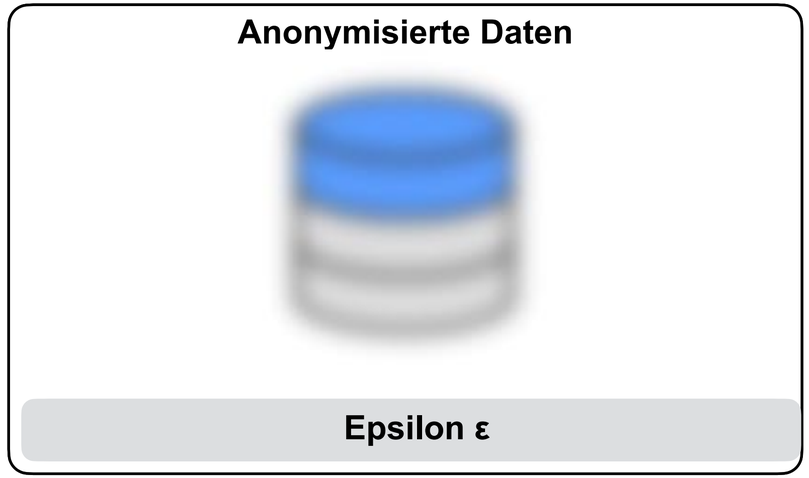
Hiermit ermächtige ich meine Krankenkasse auf Anforderung durch [*zuständige Stelle*] Daten über von mir in Anspruch genommene ärztliche Leistungen in der ambulanten Versorgung und bei stationären Aufenthalten, über verordnete Heil- und Hilfsmittel sowie Arzneimittel und Angaben zum Bereich Pflege an [*Name der behandelnden Einrichtung*] so wie in der Patienteninformation beschrieben, zu übermitteln, und zwar:

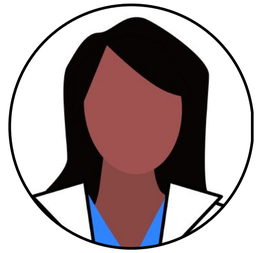
2.1

Einmalig **rückwirkend für die Daten der vergangenen 5 Kalenderjahre.** Mit der dafür nötigen Übermittlung meiner Krankenversicherungs-Nummer an [*zuständige Stelle*] bin ich einverstanden

☐ Ja ☐ Nein

Einwilligungs-erklärung





Datenkonsument
Cecilia D., Forscherin

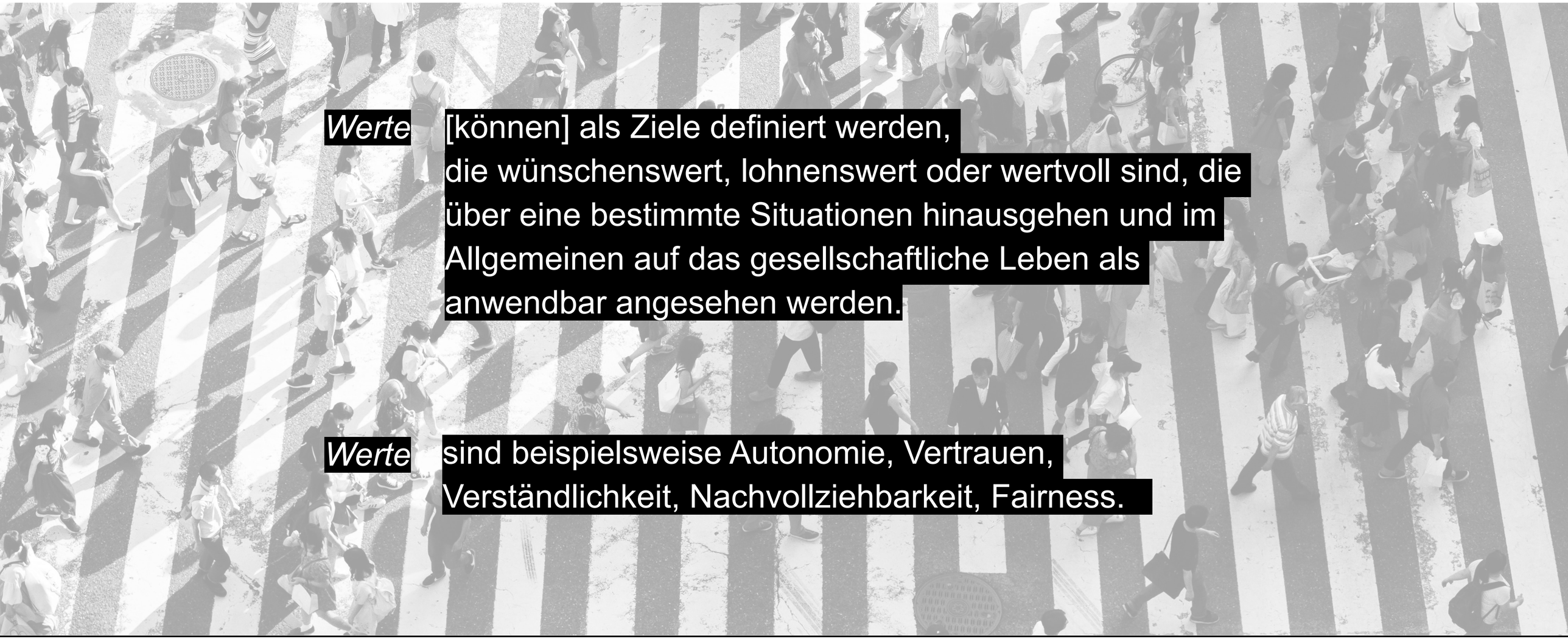
Verantwortungsvolle Technologieentwicklung durch Partizipation in der Gestaltung

Werte-orientierte Gestaltung

Batya Friedman
University of Washington

… ist ein theoretisch fundierter Ansatz bei dem Werte, Bedürfnisse und Bedenken von Interessengruppen systematisch in der Technologiegestaltung berücksichtigt werden.

… bildet die Grundlage für die Methode “Value-based Engineering” zertifiziert in der ISO/IEC/IEEE 24748-7000.



Werte [können] als Ziele definiert werden, die wünschenswert, lohnenswert oder wertvoll sind, die über eine bestimmte Situationen hinausgehen und im Allgemeinen auf das gesellschaftliche Leben als anwendbar angesehen werden.

Werte sind beispielsweise Autonomie, Vertrauen, Verständlichkeit, Nachvollziehbarkeit, Fairness.

Zentrale Prämissen der Werte-orientierten Gestaltung

Pro-aktive Haltung für die Notwendigkeit, dass “Werte” in den Prozess der Technologiegestaltung von Beginn an und während des gesamten Gestaltungsprozesses einfließen zu lassen.

Verständnis darüber, dass Werte ko-konstitutiv sind, d.h. die in der Gestaltung verwendeten Werte bedingen die Möglichkeiten der Technologienutzung.

Berücksichtigung der Werte sowohl von direkten als auch indirekten Interessengruppen bei der Technologiegestaltung.

Gestaltung basiert auf einer dreiteiligen Methodik, in Rahmen derer konzeptionelle, empirische und technische Untersuchungen erfolgen.

Anwendungskontext: Partizipation in der Gestaltung von Einwilligungsdokumenten

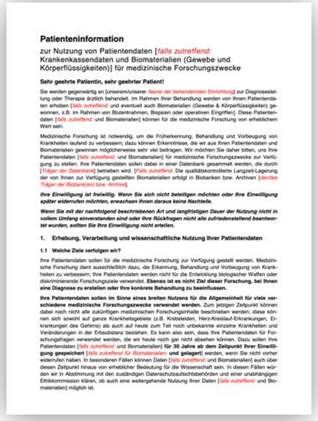
Forschungskontext Broad Consent

Der Broad Consent (sog. breite Einwilligung) erlaubt die DSGVO-konforme, pseudonymisierte und standortübergreifende Nutzung von klinische Daten von Patient:innen für medizinische Forschungszwecke.

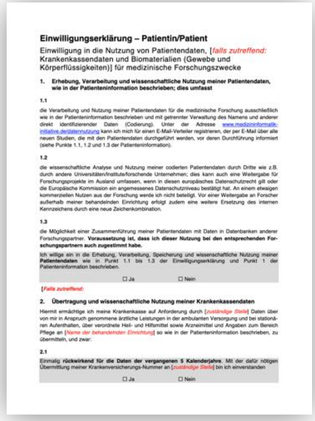
Iterativer Konsultationsprozess

- **Ethikkommissionen für medizinische Forschung**
- **Datenschutzbehörden auf Bundes- und Länderebene**
- **Konsultationsgruppe mit Patientenvertretern des Gemeinsamen Bundesausschusses**

Erstellte Kerndokumente



Patienten-information



Patienten-einwilligung

Handreichung zur Umsetzung

Forschungsansatz

Theoretische Konzeption eines partizipativen werte-orientierten Konzepts zur Datenspende

Data protection-compliant broad consent for secondary use of health care data and human biosamples for (bio)medical research: Towards a new German national standard

Sven Zenker [a,1,*], Daniel Strech [b,1], Kristina Ihrig [c,d], Roland Jahns [e], Gabriele Müller [f], Christoph Schickhardt [g], Georg Schmidt [h], Ronald Speer [i], Eva Winkler [j], Sebastian Graf von Kielmansegg [k], Johannes Drepper [l]

Facilitating Democracy:
Concerns from Participatory Design with Asymmetric Stakeholder Relations in Health Care

Yngve Dahl[1] and Dag Svanæs[1,2]
[1]Department of Computer Science, Norwegian University of Science and Technology Trondheim, Norway
[2]Digital Design Department, The IT University of Copenhagen, Denmark
{yngveda; dag.svanes}@ntnu.no

Durchführung von Workshop zur Offenlegung von Werten aus der Sicht von Patient:innen und Ableitung von Gestaltungsanforderungen

Umsetzung innerhalb eines interaktiven Demonstrators zur Patienteneinwilligung unter Berücksichtigung des Datenschutzkonzepts und Verprobung

Ablauf der partizipativen werte-orientierten Workshops

Exploration

Die Teilnehmer:innen explorieren ihre Werte im Hinblick auf den Workshop-Kontext.

Ergebnis: Eine individuelle Werteliste, wovon ausgehend die drei wichtigsten Werte gewählt und durch den Werte-Fragebogen ausformuliert werden.

Systematisierung

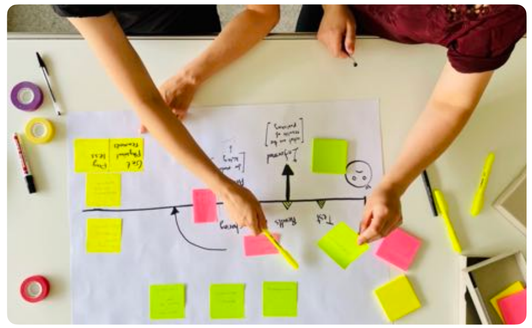
Alle Teilnehmer:innen identifizieren Interessengruppen unter Berücksichtigung ihrer Werte aus Phase 1.

Ergebnis: Eine systematisierte Werte-Karte mit Werten, Interessengruppen und Beziehungen, um Konflikte oder Gemeinsamkeiten dieser zu identifizieren.

Übersetzung

In Kleingruppen illustrieren die Teilnehmer:innen ein Werte-Szenario, das drei Werte aus Phase 2 beinhaltet.

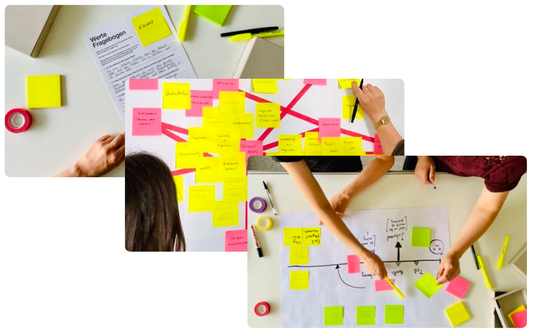
Ergebnis: Ein Werte-Szenario, das einen “ideale” Datenspende-Prozess für Patient:innen darstellt.



Reflexion

Moderierte Gruppendiskussion, um die Teilnehmer:innen bei der Reflexion ihrer Erfahrungen aus dem Workshop zu unterstützen.

Ergebnis: Kritische Reflexion über die Werte der Teilnehmer in Bezug auf die einzelnen Phasen des Workshops und dessen Kontexts.



Ablauf der partizipativen werte-orientierten Workshops

Exploration

Die Teilnehmer:innen explorieren ihre Werte im Hinblick auf den Workshop-Kontext.

Systematisierung

Alle Teilnehmer:innen identifizieren Interessengruppen unter Berücksichtigung ihrer Werte aus Phase 1.

Übersetzung

In Kleingruppen illustrieren die Teilnehmer:innen ein Werte-Szenario, das drei Werte aus Phase 2 beinhaltet.

Reflexion

Moderierte Gruppendiskussion, um die Teilnehmer:innen bei der Reflexion ihrer Erfahrungen aus dem Workshop zu unterstützen.

David Leimstädtner, Peter Sörries, and Claudia Müller-Birn. 2022. **Unfolding Values through Systematic Guidance: Conducting a Value-Centered Participatory Workshop for a Patient-Oriented Data Donation.** In Proceedings of Mensch und Computer 2022 (MuC '22). Association for Computing Machinery, New York, NY, USA, 477–482. https://doi.org/10.1145/3543758.3547560

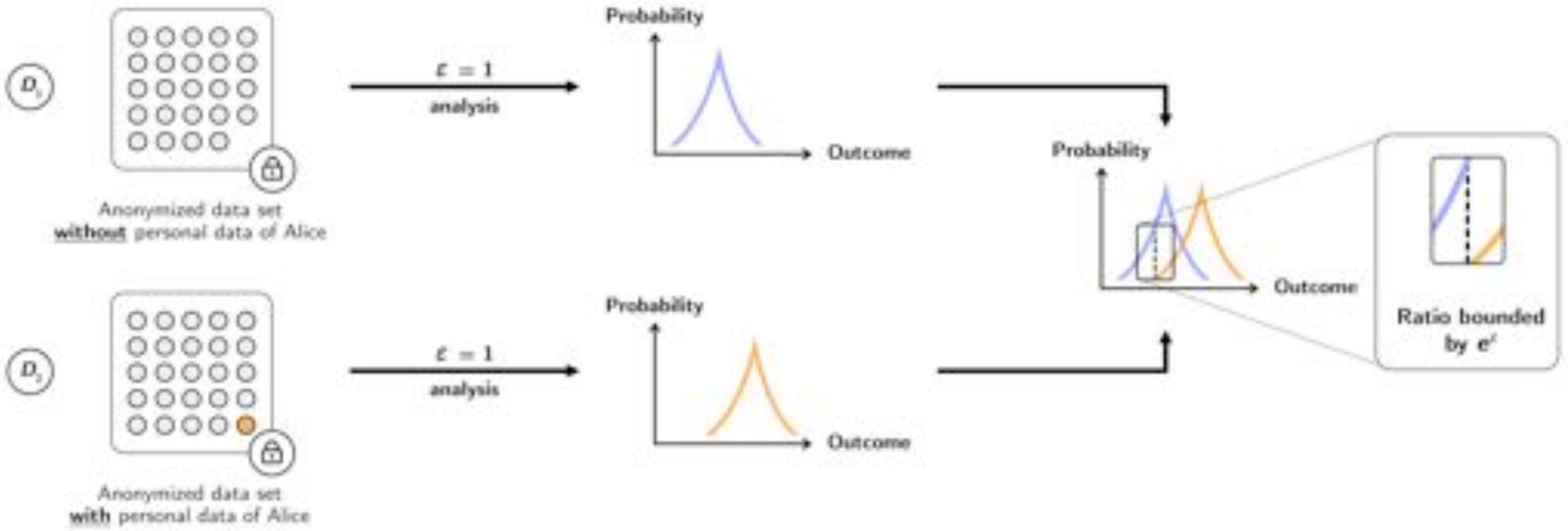
Zusammenfassung

- Die Akzeptanz für eine datengetriebene Gesundheitsforschung kann durch eine partizipative Technologiegestaltung sowie einen transparenten und verständlichen PET-Einsatz sichergestellt werden.
- Differential Privacy kann es der Gesellschaft ermöglichen, von Big Data zu profitieren und gleichzeitig die individuelle und kollektive Privatsphäre zu schützen.
- Partizipative und werte-orientierte Gestaltungsansätze helfen dabei, die sozialen Folgen von technologischen Innovationen offenzulegen.

> **“[…] we recognize that in designing tools we are designing ways of being”**
> **Winograd and Flores, 1986**

Appendix

Visualisierung des DP-Mechanismus durch Hinzufügen von Rauschen zu Datensätzen



Franzen, D., von Voigt, S. N., Sörries, P., Tschorsch, F., & Müller-Birn, C. (2022). **"Am I Private and If So, how Many?"- Communicating Privacy Guarantees of Differential Privacy with Risk Communication Formats**. Accepted at the ACM Conference on Computer and Communications Security (CCS).

"Am I Private and If So, how Many?" — Communicating Privacy Guarantees of Differential Privacy with Risk Communication Formats

Daniel Franzen
daniel.franzen@fu-berlin.de
Freie Universität Berlin
Germany

Saskia Nuñez von Voigt
saskia.nunezvonvoigt@tu-berlin.de
Technische Universität Berlin
Germany

Peter Sörries
peter.soerries@fu-berlin.de
Freie Universität Berlin
Germany

Florian Tschorsch
florian.tschorsch@tu-berlin.de
Technische Universität Berlin
Germany

Claudia Müller-Birn
clmb@inf.fu-berlin.de
Freie Universität Berlin
Germany

ABSTRACT

Every day, we have to decide multiple times, whether and how much personal data we allow to be collected. This decision is not trivial, since there are many legitimate and important purposes for data collection, for examples, the analysis of mobility data to improve urban traffic and transportation. However, often the collected data can reveal sensitive information about individuals. Recently visited locations can, for example, reveal information about political or religious views or even about an individual's health. Privacy-preserving technologies, such as differential privacy (DP), can be employed to protect the privacy of individuals and, furthermore, provide mathematically sound guarantees on the maximum privacy risk. However, they can only support informed privacy decisions, if individuals understand the provided privacy guarantees. This article proposes a novel approach for communicating privacy guarantees to support individuals in their privacy decisions when sharing data. For this, we adopt risk communication formats from the medical domain in conjunction with a model for privacy guarantees of DP to create quantitative privacy risk notifications.

We conducted a crowd-sourced study with 343 participants to evaluate how well our notifications conveyed the privacy risk information and how confident participants were about their own understanding of the privacy risk.

Our findings suggest that these new notifications can communicate the objective information similarly well to currently used qualitative notifications, but left individuals less confident in their understanding. We also discovered that several of our notifications and the currently used qualitative notification disadvantage indi-

CCS CONCEPTS

• **Security and privacy → Usability in security and privacy**; **Data anonymization and sanitization**; • **General and reference → Surveys and overviews**; • **Human-centered computing → Empirical studies in visualization**.

KEYWORDS

communication, privacy, privacy risk, differential privacy

1 INTRODUCTION

We generate a large amount of mobility data daily, for example, when using online map services for navigation or when purchasing public transport tickets. Due to the ubiquitousness of smartphones, collecting location and mobility data has become a quasi-standard also for many other applications, and prediction algorithms use the data collected for various purposes (e.g., [7, 31, 50]). Mobility data is also essential for the development of urban areas [62, 80], for example, to identify where public transport can be improved, bicycle lanes can be added or how new pedestrian zones might influence a neighborhood. These tasks are vital also to meet current environmental challenges [49, 80]. To obtain the necessary data for such legitimate tasks we have to rely on either data donations by individuals [35] or on existing data collections by third parties. However, laypeople are often unaware [8, 10, 56], but location data can reveal sensitive information [39]. They can be used to identify locations of interest (e.g., home address, religious or political organizations), reveal daily routines (e.g., doing exercises), show social relationships (e.g., collecting a child from daycare, dating)

Franzen, D., von Voigt, S. N., Sörries, P., Tschorsch, F., & Müller-Birn, C. (2022). **"Am I Private and If So, how Many?"- Communicating Privacy Guarantees of Differential Privacy with Risk Communication Formats.** Accepted at the ACM Conference on Computer and Communications Security (CCS).