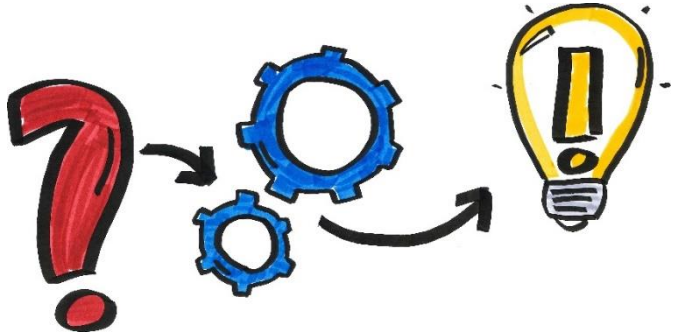
Umgang mit personenbezogenen Forschungsdaten

Rechtliche Grundlagen, Methoden und Hilfsmittel



Frauke Ziedorn, TIB Publikationsdienste

Volker Soßna, LUH Forschungsservice

Stand: 7. September 2020

Titel-/Hintergrundgrafik: Maria Leuteritz

Diese Präsentation steht unter der Lizenz CC-BY 3.0 DE. Sie darf frei genutzt, vervielfältigt, verbreitet und geändert werden, sofern in angemessener Form auf die Urheber hingewiesen wird.

Kapitel

- Einführung
- Rechtliche Grundlagen
- Die informierte Einwilligung
- Schutz vor Datenmissbrauch
- Daten anonymisieren
- Personenbezogene Forschungsdaten publizieren

Herzlich willkommen!

Frauke Ziedorn

TIB - Leibniz-Informations-zentrum Technik und Naturwissenschaften und Universitätsbibliothek

Publikationsdienste

Volker Soßna

Gottfried Wilhelm Leibniz Universität Hannover

Dezernat Forschung und EU-Hochschulbüro, Technologietransfer

Kapitel

Einführung
Rechtliche Grundlagen
Die informierte Einwilligung
Schutz vor Datenmissbrauch
Daten anonymisieren
Personenbezogene Forschungsdaten publizieren

Wie funktioniert die GUI?

zurück zur Folie „Wie funktioniert die GUI?“

Audio-Kommentare, Animationen und automatische Übergängen ein/ausschalten

zurück zur zuletzt angesehenen Folie

direkt zur nächsten Folie (Animationen und Audio-Kommentar abbrechen)

Das aktuelle Hauptkapitel ist immer grün hervorgehoben (funktioniert nur, wenn Makros zugelassen werden!)

Über diese Schaltflächen können Sie direkt zum jeweiligen Kapitel springen

zur Webseite

Auf vielen Folien finden Sie Schaltflächen. Mit einem Klick darauf gelangen Sie zu weiterführender Information auf externen Seiten, z.B. zu Video-Tutorials, Gesetzestexten, Checklisten und vielem mehr.

Kapitel

Einführung
Rechtliche Grundlagen
Die informierte Einwilligung
Schutz vor Datenmissbrauch
Daten anonymisieren
Personenbezogene Forschungsdaten publizieren

Einführung

- Anspruch und Inhalte dieses Kurses
- Was sind Forschungsdaten?
- Forschungsdaten im Projektverlauf managen
- Personenbezogene Daten: Wichtige Begrifflichkeiten

Kapitel

Einführung
Rechtliche Grundlagen
Die informierte Einwilligung
Schutz vor Datenmissbrauch
Daten anonymisieren
Personenbezogene Forschungsdaten publizieren

Anspruch und Inhalte dieses Kurses

Die Inhalte dieses Kurses

- **Einführung**
- **Rechtliche Grundlagen**
- **Die informierte Einwilligung**
- **Schutz vor Datenmissbrauch**
- **Daten anonymisieren**
- **Personenbezogene Forschungsdaten publizieren**

i

Anspruch dieses Kurses: Vertiefender Überblick über den Umgang mit personenbezogenen Forschungsdaten. Andere Arten pers.-bez. Daten unterliegen teils anderen/zusätzlichen Anforderungen und Bestimmungen und werden hier nicht berücksichtigt.

i

Die Inhalte zu den Kapiteln „Rechtliche Grundlagen“ und „Die informierte Einwilligung“ sind inhaltlich mit dem juristischen Fachpersonal der Stabstelle Datenschutz der LUH abgestimmt.

Die Stabstelle bietet allen LUH-Angehörigen Beratung und Unterstützung zu allen datenschutzrechtlichen Fragen.

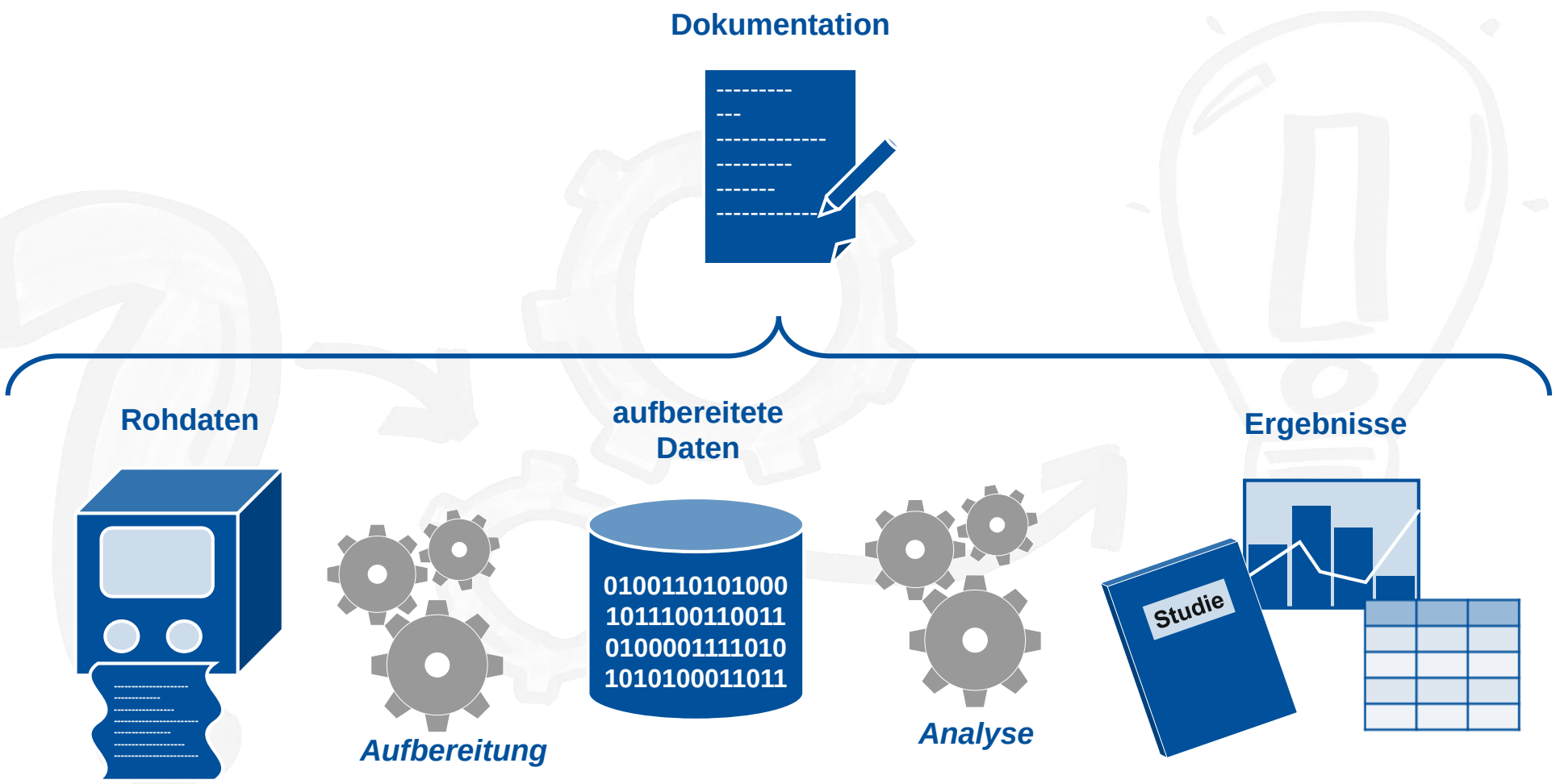
zur Webseite der Stabstelle Datenschutz

CC BY

Kapitel

- Einführung
- Rechtliche Grundlagen
- Die informierte Einwilligung
- Schutz vor Datenmissbrauch
- Daten anonymisieren
- Personenbezogene Forschungsdaten publizieren

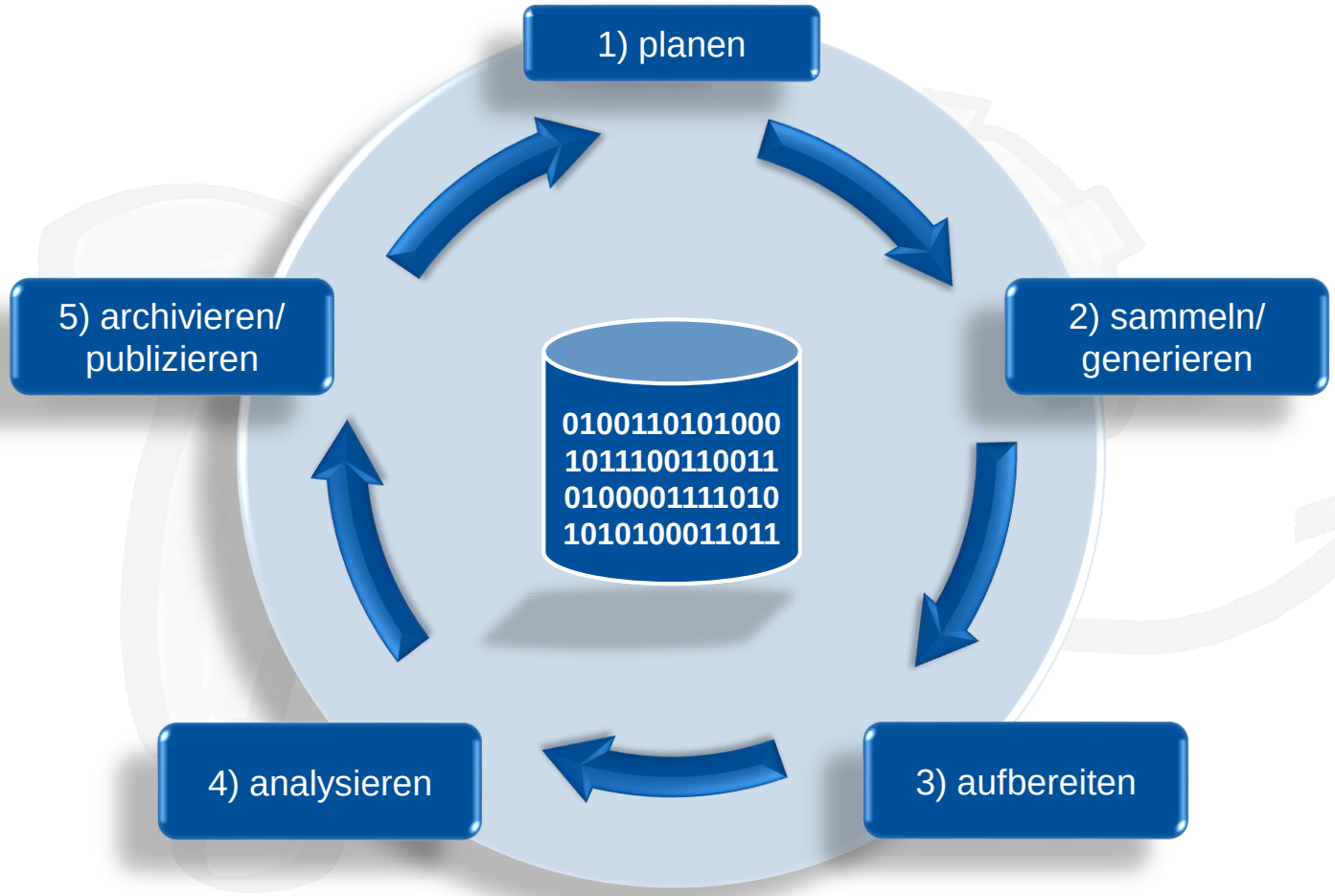
Was sind Forschungsdaten?



Kapitel

Einführung
Rechtliche Grundlagen
Die informierte Einwilligung
Schutz vor Datenmissbrauch
Daten anonymisieren
Personenbezogene Forschungsdaten publizieren

Forschungsdaten im Projektverlauf managen



Dokumentation?

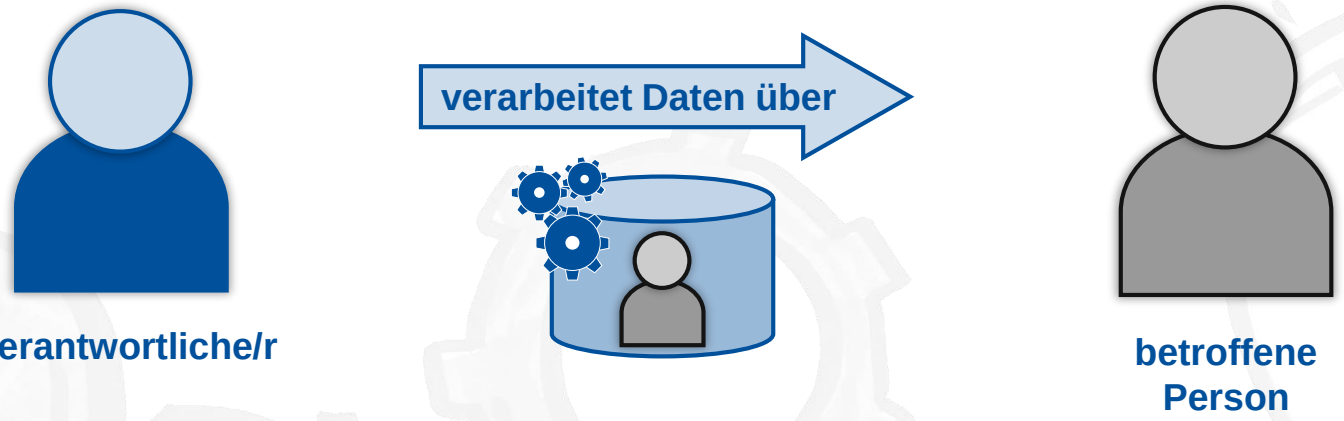
IT-Infrastruktur?

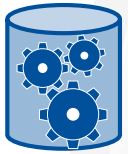
Prozesse und Verantwortlichkeiten?

Kapitel

Einführung
Rechtliche Grundlagen
Die informierte Einwilligung
Schutz vor Datenmissbrauch
Daten anonymisieren
Personenbezogene Forschungsdaten publizieren

Personenbezogene Daten: Wichtige Begrifflichkeiten





Datenverarbeitung: jeglicher Umgang mit Daten, z.B.: erheben, zusammenstellen, speichern, übertragen, analysieren, weitergeben (vgl. Art. 4, Abs. 2 DSGVO)

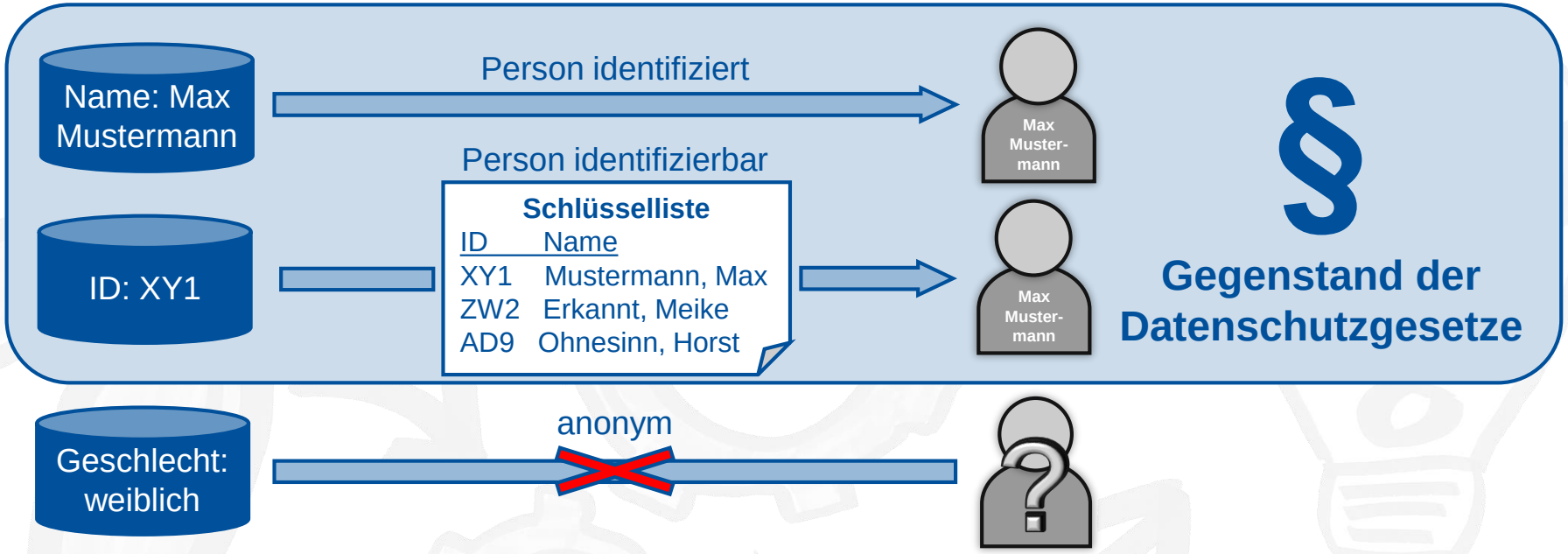
Betroffene/r: eine natürliche Person, also ein physisch existierender Mensch (vgl. Art. 4, Abs. 1 DSGVO)

Verantwortliche/r: eine natürliche *oder* juristische Person (z.B. ein Verein, eine Gesellschaft, eine Firma, eine Stiftungen, eine Behörde usw.) (vgl. Art. 4, Abs. 7 DSGVO)

Kapitel

Einführung
Rechtliche Grundlagen
Die informierte Einwilligung
Schutz vor Datenmissbrauch
Daten anonymisieren
Personenbezogene Forschungsdaten publizieren

Personenbezogene Daten: Wichtige Begrifflichkeiten



- identifiziert: Die natürliche Person, von der die Daten stammen, ist eindeutig bestimmt
- identifizierbar: Die natürliche Person, von der die Daten stammen, ist indirekt, z.B. durch Kombination mehrerer Merkmale oder unter Zuhilfenahme einfacher Hilfsmittel (z.B. „googeln“), bestimmbar
- pseudonym: Daten, bei denen Merkmale 1:1 ersetzt wurden, z.B. durch einen Alias oder einen Code (das Pseudonym). Es existiert jedoch eine Schlüsselliste (unter Verschluss), mit der sich die Pseudonyme wieder den echten Daten zuordnen lassen. Pseudonyme Daten sind daher nach wie vor personenbezogene Daten.
- anonym: nicht (mehr) einer bestimmten natürlichen Person zuzuordnen

CC BY

Kapitel

Einführung
Rechtliche Grundlagen
Die informierte Einwilligung
Schutz vor Datenmissbrauch
Daten anonymisieren
Personenbezogene Forschungsdaten publizieren

Rechtliche Grundlagen

- Das Grundrecht auf „informationelle Selbstbestimmung“
- Die Evolution der Datenschutzgesetze
- Datenschutz versus Forschungsfreiheit
- Die Europäische Datenschutz-Grundverordnung (DSGVO)
- Rechtmäßigkeit der Datenverarbeitung nach Art. 6 DSGVO
- Grundsätze nach Art. 5 Abs. 1 DSGVO
- „Besondere Kategorien“ personenbezogener Daten (Art. 9 DSGVO)
- Das Bundesdatenschutzgesetz (BDSG)
- Das Niedersächsische Datenschutzgesetz (NDSG)
- Datenverarbeitung zu wissenschaftlichen Zwecken nach § 13 NDSG

Kapitel

Einführung
Rechtliche Grundlagen
Die informierte Einwilligung
Schutz vor Datenmissbrauch
Daten anonymisieren
Personenbezogene Forschungsdaten publizieren

Das Grundrecht auf „informationelle Selbstbestimmung“

Bundesverfassungsgericht

1983

Volkszählungs-Urteil

bestehende Datenschutz-gesetze nicht GG-konform

Grundgesetz

§ **Art. 1 Abs. 1**
→ Menschenwürde

§ **Art. 2 Abs. 1**
→ freie Entfaltung der Persönlichkeit

Grundrecht auf **informationelle Selbstbestimmung**

Lese-Tipp

Informationen des Bundesdatenschutzbeauftragten zum Hintergrund des Volkszählungsurteils

zur Webseite des Bundesdatenschutzbeauftragten

CC BY

Kapitel

Einführung

Rechtliche Grundlagen

Die informierte Einwilligung

Schutz vor Datenmissbrauch

Daten anonymisieren

Personenbezogene Forschungsdaten publizieren

Die Evolution der Datenschutzgesetze

- 1970: Weltweit erstes Datenschutzgesetz in Hessen
- 1977: Erstes Bundesdatenschutzgesetz
- 1983: Volkszählungsurteil des Bundesverfassungsgerichts → Datenschutz als Grundrecht. Anpassung der bestehenden Datenschutzgesetze gefordert
- 1986-1990: Novellierung der Datenschutzgesetze von Bund und Ländern
- 1995-2018: Europäische Datenschutzrichtlinie 95/46/EG (2018 abgelöst durch DSGVO)
- seit 2009: Verankerung des Datenschutzes in der Europäischen Grundrechtecharta (GrCh) in Art. 7 (Achtung des Privat- und Familienlebens) und Art. 8 (Recht auf Schutz personenbezogener Daten)
- Seit 2018: Europäische Datenschutzgrundverordnung (DSGVO) als unmittelbar geltendes Recht. Anpassung der Datenschutzgesetze von Bund und Ländern an die DSGVO

CC BY

Kapitel

Einführung
Rechtliche Grundlagen
Die informierte Einwilligung
Schutz vor Datenmissbrauch
Daten anonymisieren
Personenbezogene Forschungsdaten publizieren

Datenschutz versus Forschungsfreiheit

Grundrecht auf **informationelle Selbstbestimmung**

Konkurrenz

Grundgesetz

§ **Art. 5 Abs. 3** Forschungs-freiheit

Gesetze schaffen Ausgleich

wenn nicht hinreichend konkret

„Praktische Konkordanz“ (Abwägung im Einzelfall)

Lese-Tipp

Dieser Artikel berücksichtigt speziell die Perspektive der Forschenden:

Eva Barlösius, Friederike Knocke (2019): Regeln zum Umgang mit Forschungsdaten und die Wissenschaftsfreiheit. Eine Analyse auf der Grundlage empirischer Ergebnisse. Rechtstheorie, Bd. 50, Heft 2: S. 203–224. DOI: 10.3790/rth.50.2.203.

zum Artikel

CC BY

Kapitel

Einführung
Rechtliche Grundlagen
Die informierte Einwilligung
Schutz vor Datenmissbrauch
Daten anonymisieren
Personenbezogene Forschungsdaten publizieren

Die Europäische Datenschutz-Grundverordnung (DSGVO)

Europäische Datenschutz-grundverordnung (DSGVO)

- EU-weit unmittelbar geltendes Recht
- gilt für Datenverarbeitung in der EU (auch wenn Nicht-EU-Bürger betroffen sind)
- gilt für Datenverarbeitung durch Stellen, die ihren Sitz in der EU haben
- einige Details werden in untergeordnete nationalen Gesetzen geregelt

Nationale Gesetze in Deutschland

- Bundesdatenschutzgesetz (BDSG)
- Landesdatenschutzgesetze, z.B. das Niedersächsische Datenschutzgesetzt (NDSG)

→ konkretisieren, ergänzen oder modifizieren einige Bestimmungen der DSGVO in ihrem jeweiligen Geltungsbereich

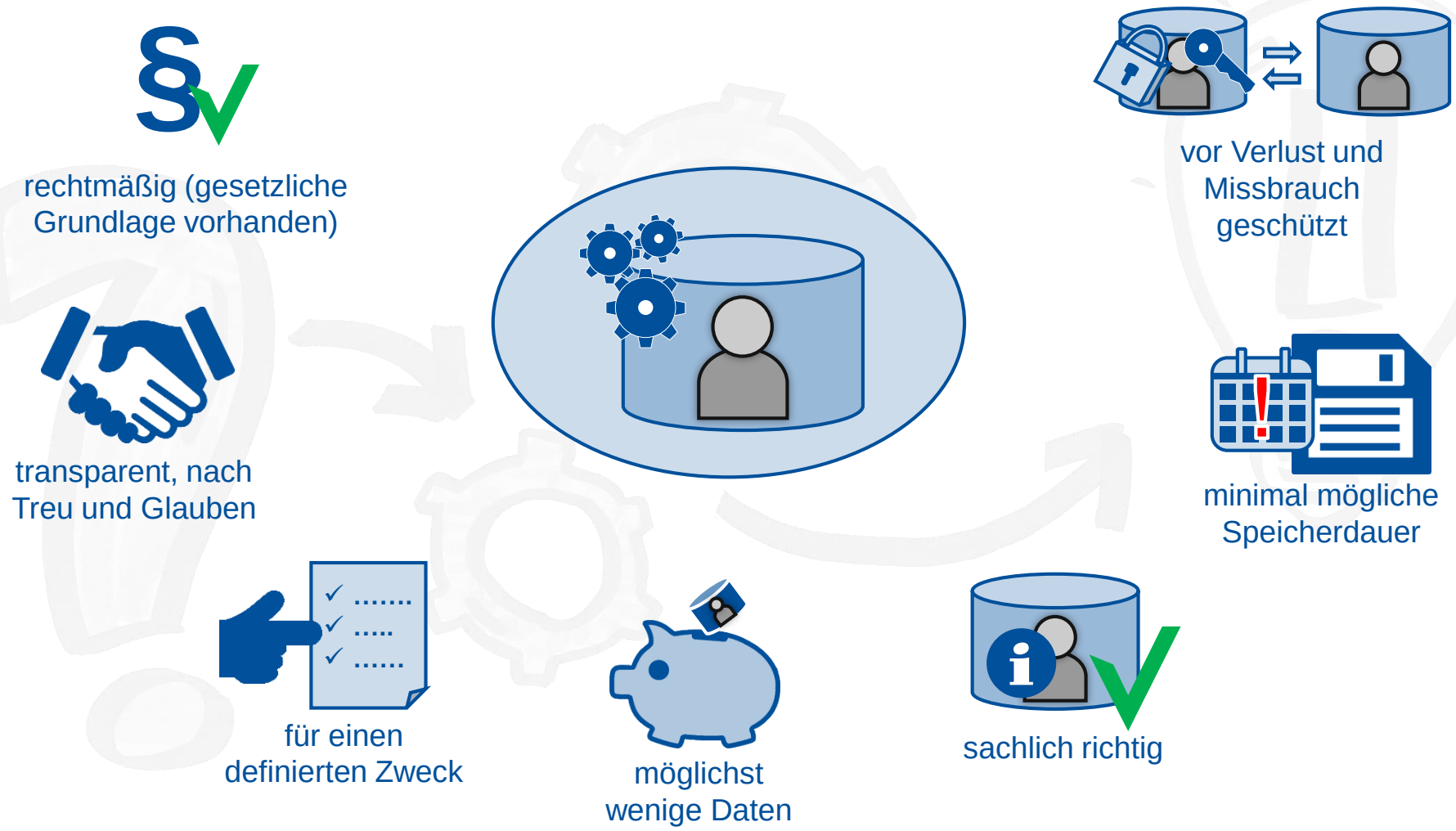
§ zur offiziellen deutschen Fassung der DSGVO (Amtsblatt der EU)

CC BY

Kapitel

- Einführung
- Rechtliche Grundlagen
- Die informierte Einwilligung
- Schutz vor Datenmissbrauch
- Daten anonymisieren
- Personenbezogene Forschungsdaten publizieren

Grundsätze der Datenverarbeitung nach Art. 5, Abs. 1 DSGVO

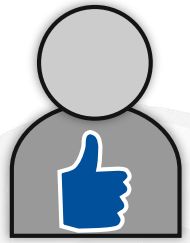


Kapitel

Einführung
Rechtliche Grundlagen
Die informierte Einwilligung
Schutz vor Datenmissbrauch
Daten anonymisieren
Personenbezogene Forschungsdaten publizieren

Rechtmäßigkeit der Datenverarbeitung nach Art. 6 DSGVO

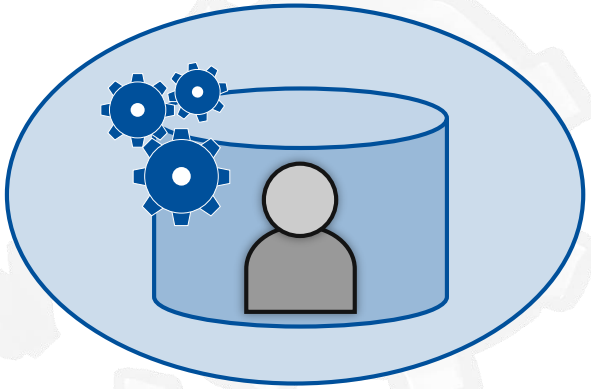
! Die Verarbeitung ist nur rechtmäßig, wenn mindestens eine dieser Bedingungen erfüllt ist

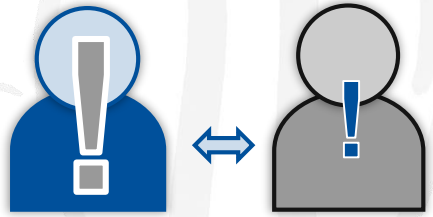


Betroffene willigen ein

relevant für die Forschung

schutzwürdiges öffentliches Interesse



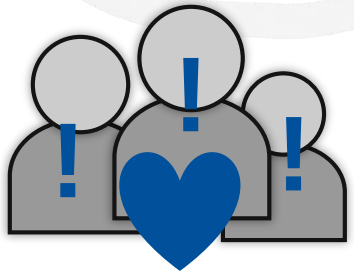


Interesse des Verantwortliche überwiegt Interesse des Betroffenen (gilt nicht für staatliche Stellen!)

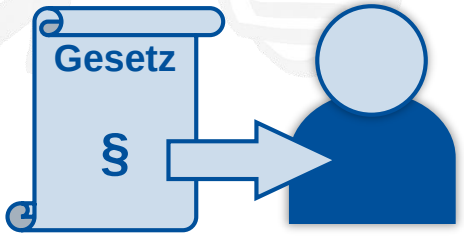
Vertrag

§ …..
§ ….
§ ….

zur Vertragserfüllung erforderlich



zur Wahrung lebens-wichtiger Interessen

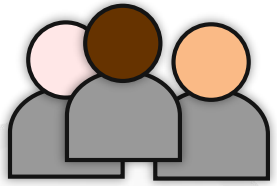


Verantwortlicher ist gesetzlich verpflichtet

Kapitel

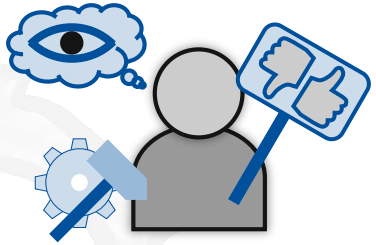
Einführung
Rechtliche Grundlagen
Die informierte Einwilligung
Schutz vor Datenmissbrauch
Daten anonymisieren
Personenbezogene Forschungsdaten publizieren

„Besondere Kategorien“ personenbezogener Daten (Art. 9 DSGVO)

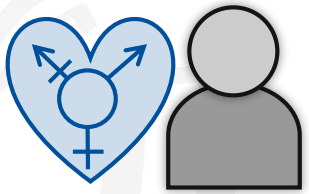


rassische und ethnische Herkunft

genetische, biometrische und Gesundheitsdaten



politische Meinungen, religiöse oder weltanschauliche Überzeugungen, Gewerkschafts-zugehörigkeit



Daten zum Sexualleben / zur sexuellen Orientierung

!

Da Daten dieser Kategorien sehr sensibel sind, ist ihre Verarbeitung grundsätzlich untersagt. Ausnahmen regelt Art. 9, Abs. 2 DSGVO.

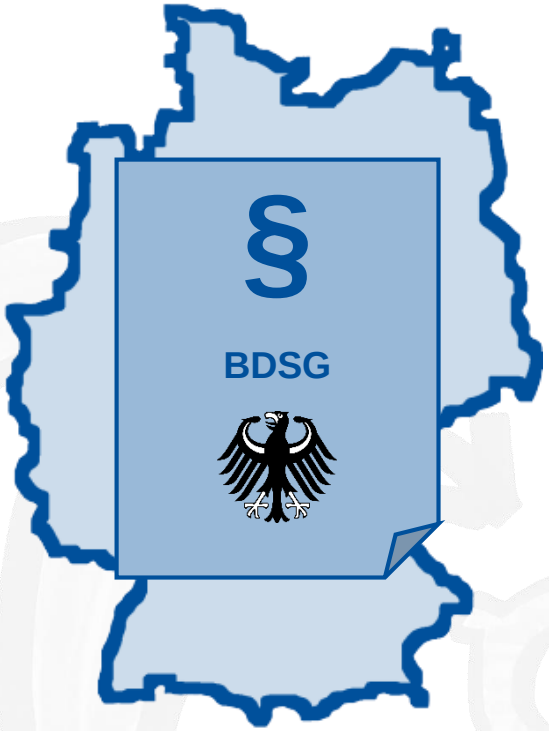
Für Forschungszwecke dürfen solche Daten i.d.R. nur mit ausdrücklicher Einwilligung der Betroffenen verarbeitet werden und sind dann besonders sorgfältig zu schützen!

CC BY

Kapitel

Einführung
Rechtliche Grundlagen
Die informierte Einwilligung
Schutz vor Datenmissbrauch
Daten anonymisieren
Personenbezogene Forschungsdaten publizieren

Das Bundesdatenschutzgesetz (BDSG)



gilt für

öffentliche Stellen des Bundes (und der Länder, wenn kein Landesgesetz greift)

gilt für

nicht-öffentliche Stellen (z.B. Unternehmen) bei (teil-)automatisierte Datenverarbeitung

gilt innerhalb Deutschlands, sofern nicht direkt die DSGVO greift

§ zum Text des BDSG (Bundesamt für Justiz)

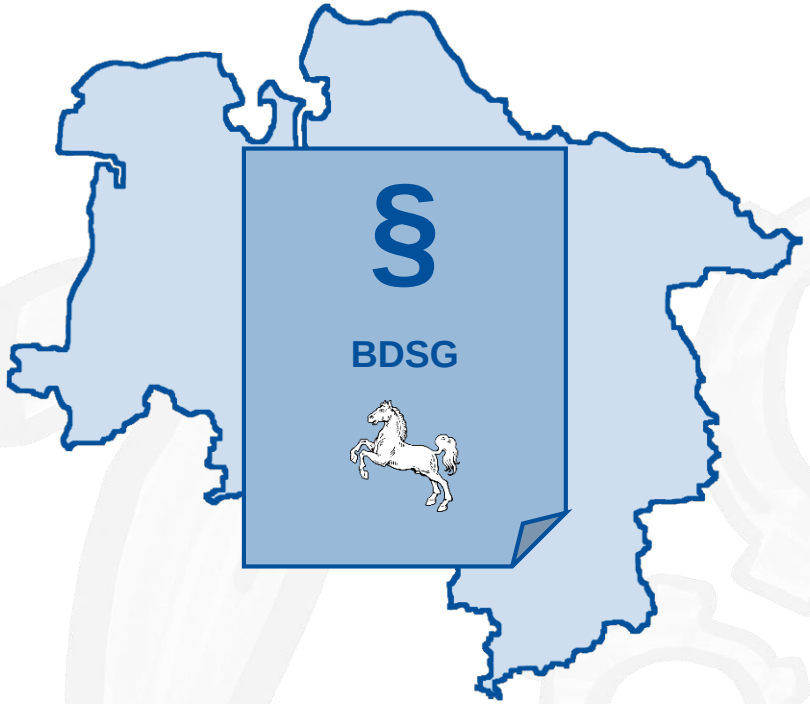
! Für die Forschung an (staatlichen) Hochschulen gilt nicht das BDSG, sondern das jeweilige Landesdatenschutzgesetz!

CC BY

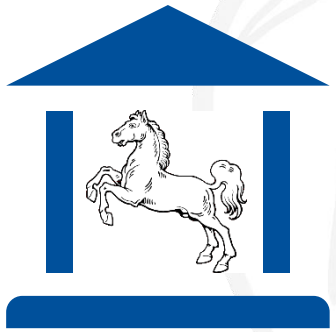
Kapitel

- Einführung
- Rechtliche Grundlagen
- Die informierte Einwilligung
- Schutz vor Datenmissbrauch
- Daten anonymisieren
- Personenbezogene Forschungsdaten publizieren

Das Niedersächsische Datenschutzgesetz (NDSG)



gilt für



öffentliche Stellen des Landes und der Kommunen (einschließlich der staatlichen Hochschulen)

gilt innerhalb Niedersachsens, sofern nicht direkt die DSGVO greift

§

zum Text des NDSG (niedersächsisches Vorschrifteninformationssystem)

!

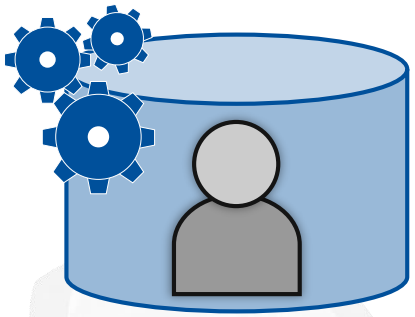
Die Landesdatenschutzbeauftrage findet viele Regelungen des NDSG rechtlich problematisch und lückenhaft. Es könnte also bald zu einer Überarbeitung oder zu Grundsatzurteilen kommen.

zur Webseite der Landesbeauftragten für den Datenschutz Niedersachsen

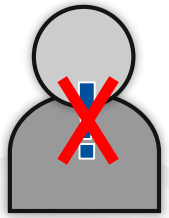
Kapitel

Einführung
Rechtliche Grundlagen
Die informierte Einwilligung
Schutz vor Datenmissbrauch
Daten anonymisieren
Personenbezogene Forschungsdaten publizieren

Datenverarbeitung zu wissenschaftlichen Zwecken nach § 13 NDSG

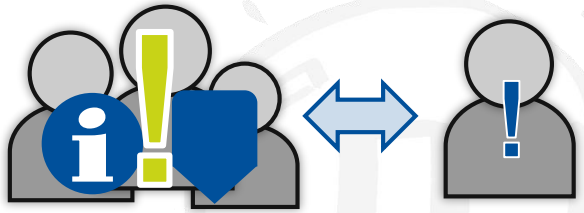


zulässig, wenn



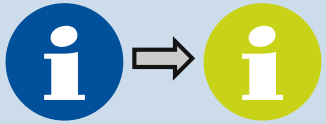
keine schutzwürdigen Interessen der Betroffenen

ODER

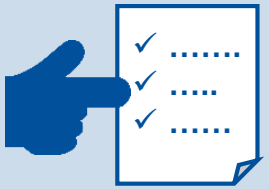


öffentliches Interesse überwiegt schutzwürdige Interesse der Betroffenen

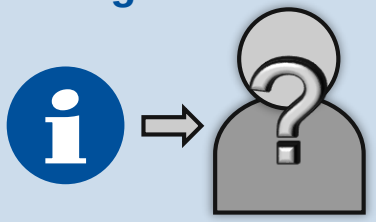
Voraussetzungen



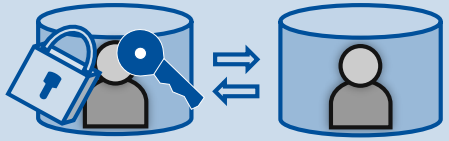
sofortige Pseudonymisierung



ausschließlich zum Zweck des Forschungsvorhabens



Anonymisierung, sobald der Forschungszweck dies zulässt



angemessene Schutzmaßnahmen nach § 17

!

Die Publikation von personenbezogenen Forschungsdaten ist nur zulässig, wenn entweder

- die Betroffenen eingewilligt haben oder
- dies für die Darstellung von Forschungsergebnissen über Ereignisse der Zeitgeschichte unerlässlich ist

CC BY

Kapitel

- Einführung
- Rechtliche Grundlagen
- Die informierte Einwilligung
- Schutz vor Datenmissbrauch
- Daten anonymisieren
- Personenbezogene Forschungsdaten publizieren

Die informierte Einwilligung

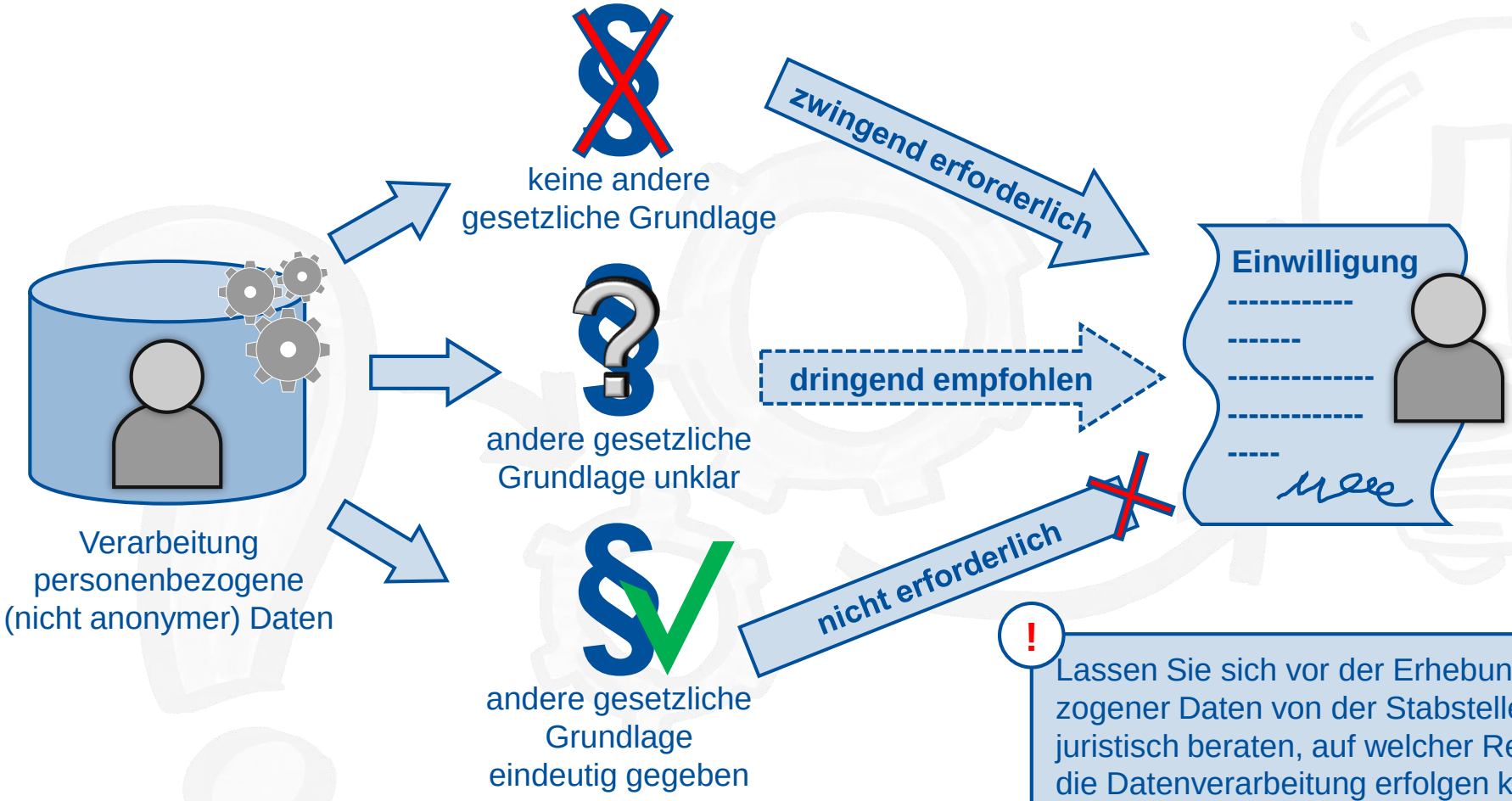
- Wann wird eine Einwilligung der Betroffenen benötigt?
- Unterschiede zwischen Direkterhebung und Dritterhebung
- Formale Anforderungen für eine wirksame Einwilligung
- Verpflichtend mitzuteilende Informationen
- Weitere Betroffenenrechte nach der DSGVO
- Zusätzlich mitzuteilende Informationen in bestimmten Fällen
- Abläufe in der Forschungspraxis
- Abstimmung mit der Stabstelle Datenschutz
- Weitere Infos, Handreichungen, Vorlagen und Muster

CC BY

Kapitel

Einführung
Rechtliche Grundlagen
Die informierte Einwilligung
Schutz vor Datenmissbrauch
Daten anonymisieren
Personenbezogene Forschungsdaten publizieren

Wann wird eine Einwilligung der Betroffenen benötigt?



! Lassen Sie sich vor der Erhebung personenbezogener Daten von der Stabstelle Datenschutz juristisch beraten, auf welcher Rechtsgrundlage die Datenverarbeitung erfolgen kann!

zum Webseite der Stabsstelle

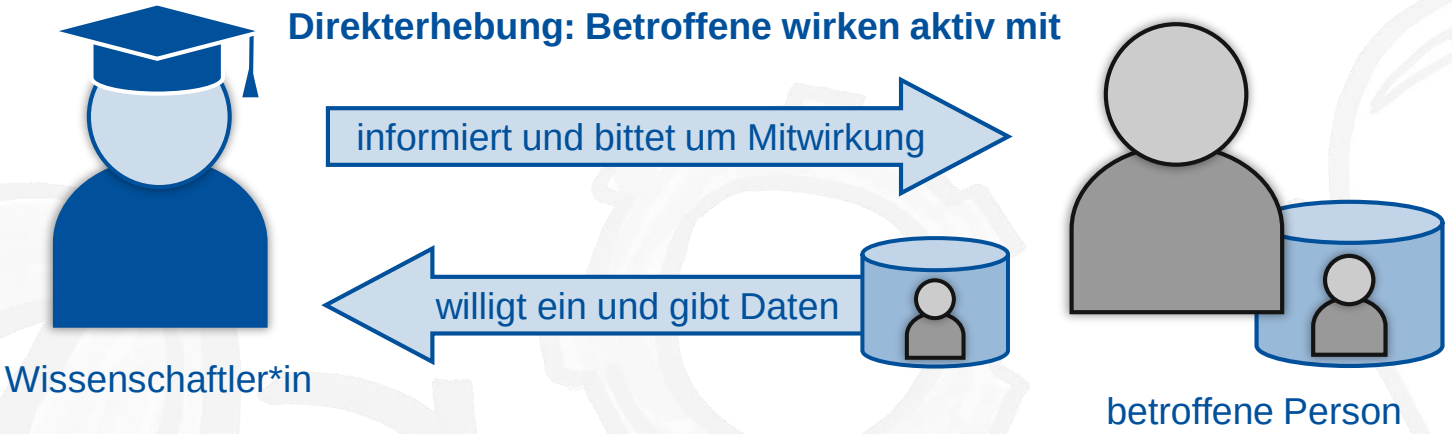
CC BY

Kapitel

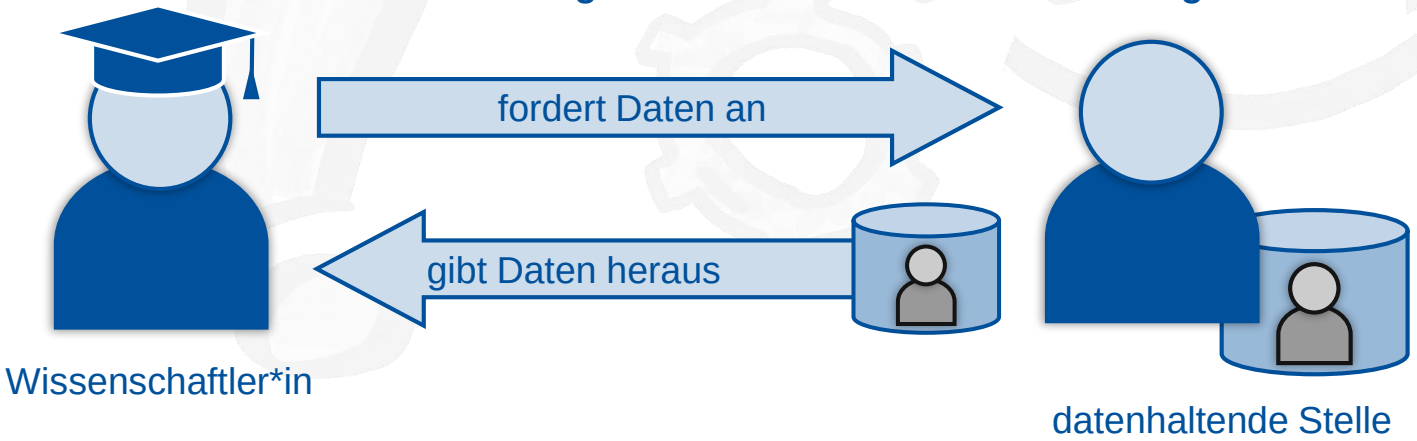
Einführung
Rechtliche Grundlagen
Die informierte Einwilligung
Schutz vor Datenmissbrauch
Daten anonymisieren
Personenbezogene Forschungsdaten publizieren

Unterschiede zwischen Direkterhebung und Dritterhebung

Direkterhebung: Betroffene wirken aktiv mit



Dritterhebung: vorhandene Daten werden nachgenutzt



!

Nur zulässig, wenn

- es von der ursprünglichen Einwilligung gedeckt ist
- Betroffene erneut informiert wurden und einwilligen
- ein Gesetz die Verarbeitung ohne Einwilligung gestattet

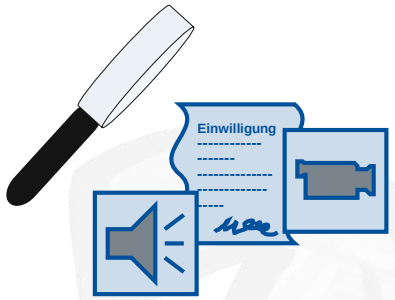
CC BY

Kapitel

- Einführung
- Rechtliche Grundlagen
- Die informierte Einwilligung
- Schutz vor Datenmissbrauch
- Daten anonymisieren
- Personenbezogene Forschungsdaten publizieren

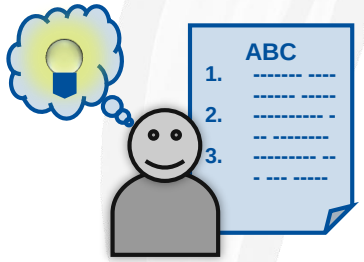
Formale Anforderungen für eine wirksame Einwilligung

! Sind die formalen Anforderungen nicht vollständig erfüllt, kann die Einwilligung unwirksam sein!

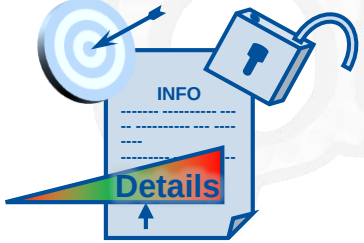


in nachweisbarer Form

Recht auf Widerruf grafisch hervorgehoben



verfasst in einfacher, Zielgruppen-gerechter Sprache



Begleitinformationen ausreichend detailliert, präzise, transparent und leicht zugänglich

Einwilligungsteil vom Infoteil getrennt oder grafisch abgesetzt

Lese-Tipp

Verbund Forschungsdaten Bildung (2019): Checkliste zur Erstellung rechtskonformer Einwilligungserklärungen mit besonderer Berücksichtigung von Erhebungen an Schulen. Version 2.0, fdbinfo Nr. 1

zum Artikel

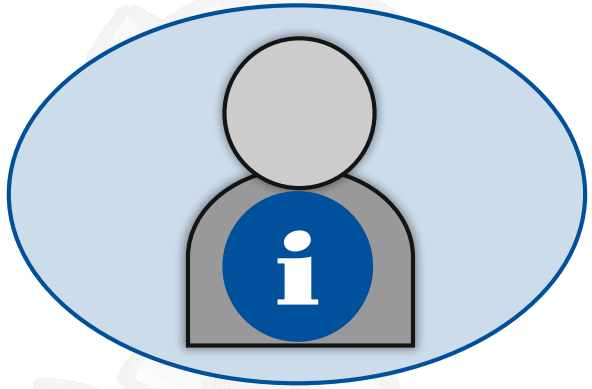
CC BY

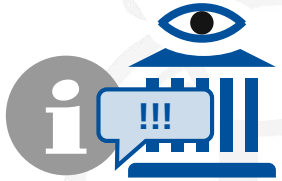
Kapitel

Einführung
Rechtliche Grundlagen
Die informierte Einwilligung
Schutz vor Datenmissbrauch
Daten anonymisieren
Personenbezogene Forschungsdaten publizieren

Verpflichtend mitzuteilende Informationen

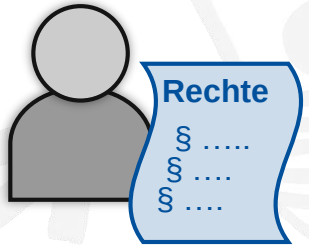
Name und Kontaktdaten des Verantwortlichen und ggf. seines Vertreters



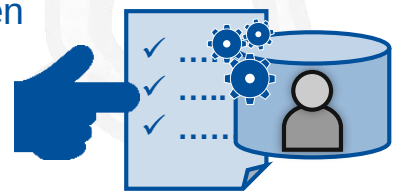


Hinweis auf Beschwerderecht bei der Aufsichtsbehörde

Kontaktdaten des Datenschutzbeauftragten



Rechte des Betroffenen ggü. dem Verantwortlichen



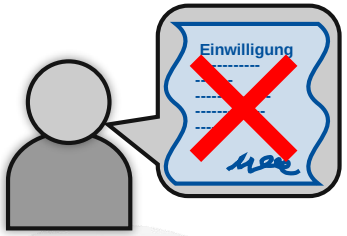
Zweck(e) und Art der Verarbeitung (insb. Speicherdauer)

rechtliche Grundlage der Verarbeitung

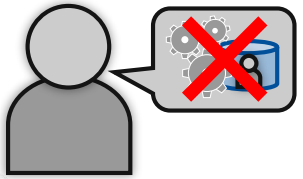
Kapitel

- Einführung
- Rechtliche Grundlagen
- Die informierte Einwilligung
- Schutz vor Datenmissbrauch
- Daten anonymisieren
- Personenbezogene Forschungsdaten publizieren

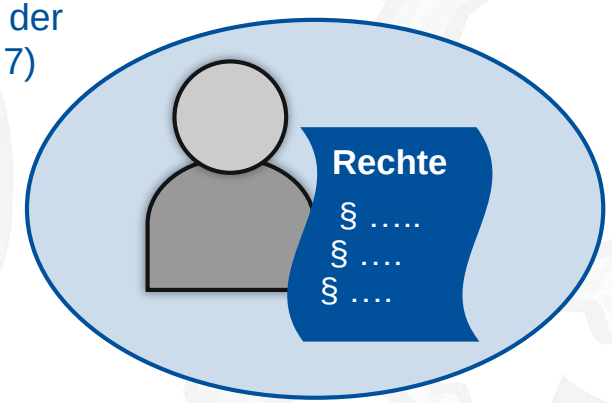
Weitere Betroffenenrechte nach der DSGVO



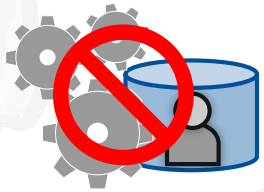
Recht auf Widerruf der Einwilligung (Art. 7)



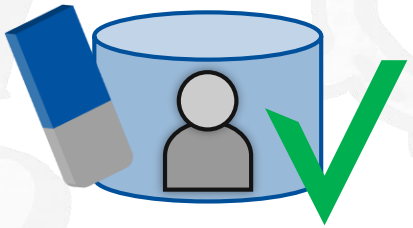
Widerspruchsrecht gegen die Verarbeitung (Art. 21)



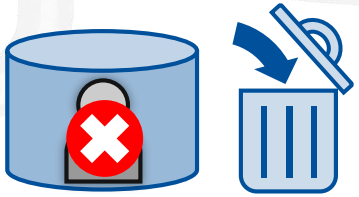
Recht auf Auskunft (Art. 15)



Recht auf Einschränkung der Verarbeitung (Art. 18)



Recht auf Berichtigung (Art. 16)



Recht auf Löschung (Art. 17)

Lese-Tipp

Verbund Forschungsdaten Bildung (2018): Formulierungsbeispiele für „informierte Einwilligungen“. Version 2.1, fdbinfo Nr. 4

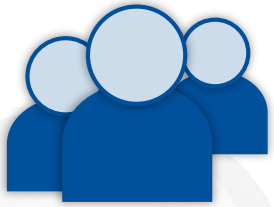
zu den Beispielen

Kapitel

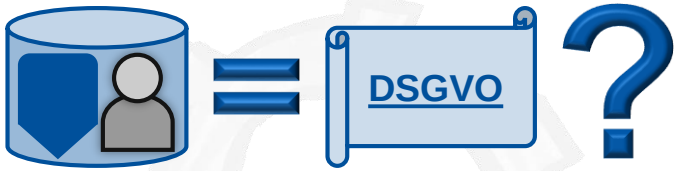
Einführung
Rechtliche Grundlagen
Die informierte Einwilligung
Schutz vor Datenmissbrauch
Daten anonymisieren
Personenbezogene Forschungsdaten publizieren

Zusätzlich mitzuteilende Informationen in bestimmten Fällen

Wenn Daten an weitere Stellen übermittelt werden sollen



Empfänger der Daten
(oder Empfängerkategorien)



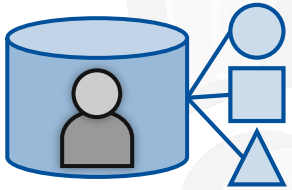
Bei Übermittlung ins Nicht-EU-Ausland:
Kann DSGVO-vergleichbarer
Datenschutz garantiert werden?

Lese-Tipp

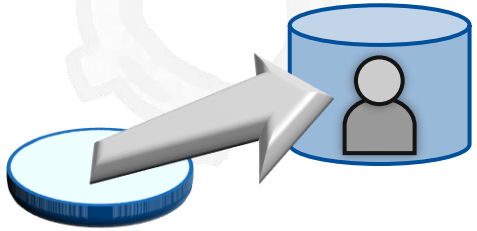
Hier finden Sie eine Liste der Länder, zu denen es einen Angemessenheitsbeschluss der EU-Kommission gibt:

zur Webseite der EU-Kommission

Wenn existierende Daten verarbeitet werden sollen (Dritterhebung):



Kategorien der zu
verarbeitenden Daten



Datenquelle(n)

Sind die Datenquellen
öffentlich zugänglich?

Kapitel

Einführung
Rechtliche Grundlagen
Die informierte Einwilligung
Schutz vor Datenmissbrauch
Daten anonymisieren
Personenbezogene Forschungsdaten publizieren

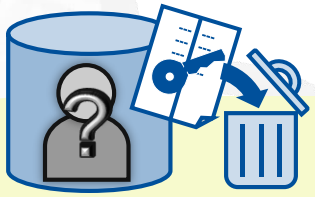
Abläufe in der Forschungspraxis

Datenmanagement durchplanen

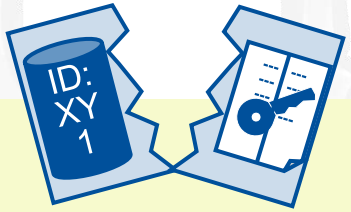
Einwilligung und Infoblatt entwerfen

Entwürfe mit der Stabsstelle Datenschutz abstimmen

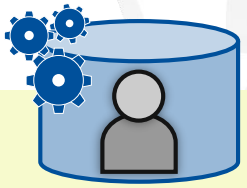
Betroffene informieren und Einwilligungen einholen



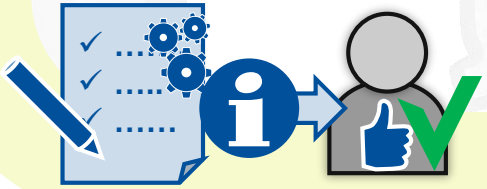
Daten anonymisieren. Schlüsselliste vernichten



Daten pseudonymisieren. Schlüsselliste und Daten trennen

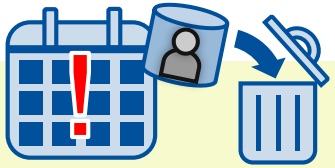


Daten erheben und verarbeiten



Ändert sich der Zweck der Verarbeitung, erneute Info & Einwilligung

Bei Widerruf, Daten sofort löschen



Daten fristgerecht löschen

CC BY

Kapitel

Einführung

Rechtliche Grundlagen

Die informierte Einwilligung

Schutz vor Datenmissbrauch

Daten anonymisieren

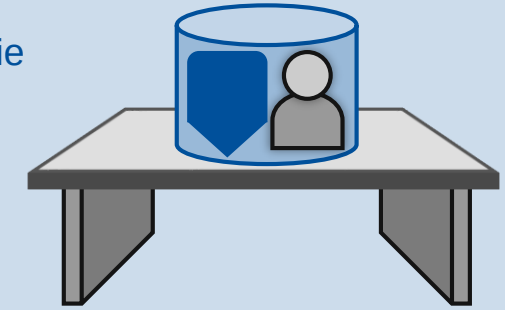
Personenbezogene Forschungsdaten publizieren

Abstimmung mit der Stabsstelle Datenschutz

Die Stabsstelle Datenschutz der LUH

Wenden Sie sich an die Stabsstelle Datenschutz, wenn…

- … Sie beabsichtigen, personenbezogene Daten zu verarbeiten (Aufnahme ins „Verzeichnis der Verarbeitungstätigkeiten“)
- … Sie Entwürfe für Einwilligungserklärungen und andere Dokumenten mit Datenschutzbezug prüfen lassen möchten
- … personenbezogene Daten von Unbefugten eingesehen wurden oder sie die Möglichkeit dazu gehabt hätten (meldepflichtiger Datenschutzvorfall)
- … Sie sonstige, insbesondere rechtliche Fragen rund um das Thema Datenschutz haben



zum Webauftritt und den Kontaktinformationen

CC BY

Kapitel

Einführung
Rechtliche Grundlagen
Die informierte Einwilligung
Schutz vor Datenmissbrauch
Daten anonymisieren
Personenbezogene Forschungsdaten publizieren

Weitere Infos, Handreichungen, Vorlagen und Muster

Lese-Tipps

- Beschäftigtenportal der LUH (diverse Handreichungen und Vorlagen, nur aus dem LUH-Netz erreichbar)
- Zentrale Datenschutzstelle der baden-württembergischen Universitäten (Infos, Checklisten, Vorlagen rund um die DSGVO)
- Rat für Sozial- und Wirtschaftsdaten (Datenschutz allgemein)
- forschungsdaten.info (Datenschutz allgemein)
- Verbund Forschungsdaten Bildung (Einwilligungserklärung)

Kapitel

Einführung
Rechtliche Grundlagen
Die informierte Einwilligung
Schutz vor Datenmissbrauch
Daten anonymisieren
Personenbezogene Forschungsdaten publizieren

Schutz vor Datenmissbrauch

- Durchgehende Verschlüsselung von Datenträgern
- Wie Sie Datenträger verschlüsseln können
- Sicherheitsabstufungen bei der Verschlüsselung
- Verschlüsselt kommunizieren
- Rechtemanagement
- Rechtemanagement (Beispielschema)
- Umgang mit Passwörtern: so bitte NICHT!
- Sichere Passwörter erstellen
- Physische Zugangsbeschränkungen
- Weitere organisatorische Maßnahmen

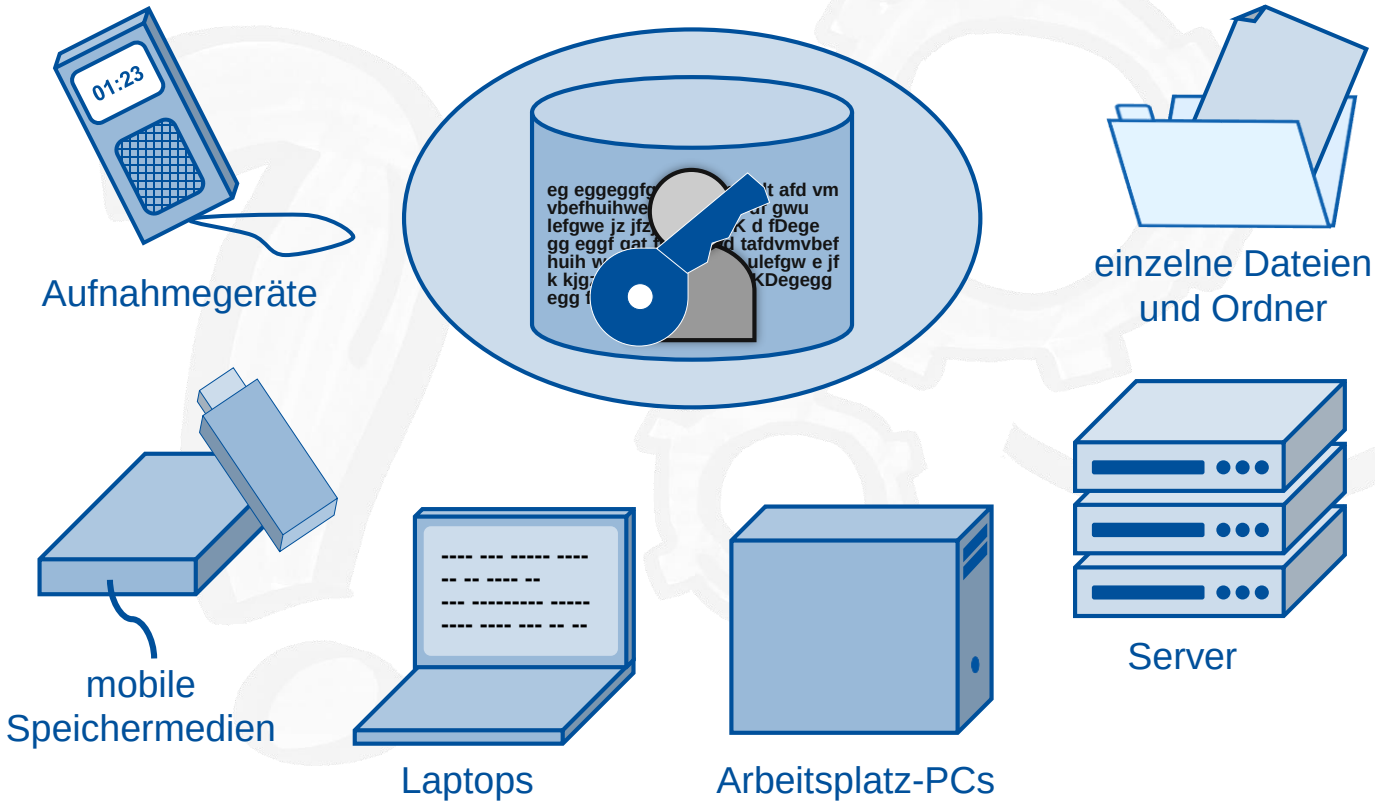
CC BY

Kapitel

Einführung
Rechtliche Grundlagen
Die informierte Einwilligung
Schutz vor Datenmissbrauch
Daten anonymisieren
Personenbezogene Forschungsdaten publizieren

Durchgehende Verschlüsselung von Datenträgern

! Je sensibler die Daten, desto wichtiger ist eine *durchgehende* Verschlüsselung!



Lese-Tipps

Cornelia Möhring (4.12.2017): ZIP-Archiv mit einem Passwort schützen? So geht's! Internet-Artikel bei heise online.

zum Internet-Artikel

Tim Aschermann (18.6.2016): Dateien mit WinRAR verschlüsseln - so geht's. Internet-Artikel bei CHIP.

zum Internet-Artikel

Privacy Handbuch: Daten verschlüsseln. Undatierter Internet-Artikel.

zum Internet-Artikel

CC BY

Kapitel

- Einführung
- Rechtliche Grundlagen
- Die informierte Einwilligung
- Schutz vor Datenmissbrauch
- Daten anonymisieren
- Personenbezogene Forschungsdaten publizieren

Wie Sie Datenträger verschlüsseln können

! Softwareseitige Verschlüsselung ist tendenziell sicherer als hardwareseitige!

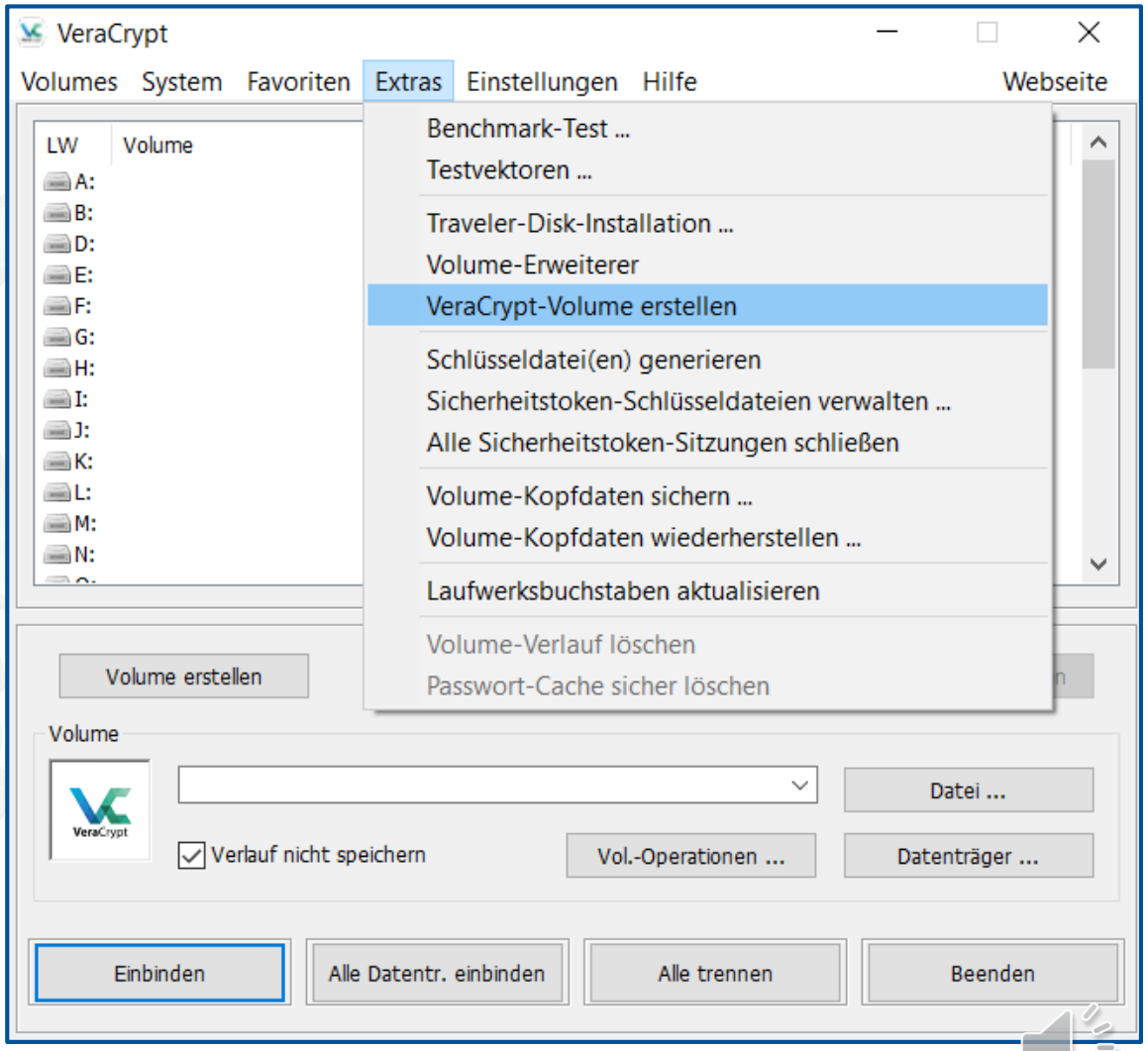
Tool-Tipp

VeraCrypt ist ein leistungsfähiges, benutzerfreundliches OpenSource-Programm, mit dem sich einzelne Ordner, Partitionen und ganze Festplatten sicher verschlüsseln lassen. Es ist für alle gängigen Betriebssysteme verfügbar.

zum Download

Die folgenden YouTube-Videos von TDUCity erläutern anschaulich die Installation und die verschiedenen Funktionen und Einstellmöglichkeiten von TrueCrypt (dem VeraCrypt-Vorläufer) und VeraCrypt:

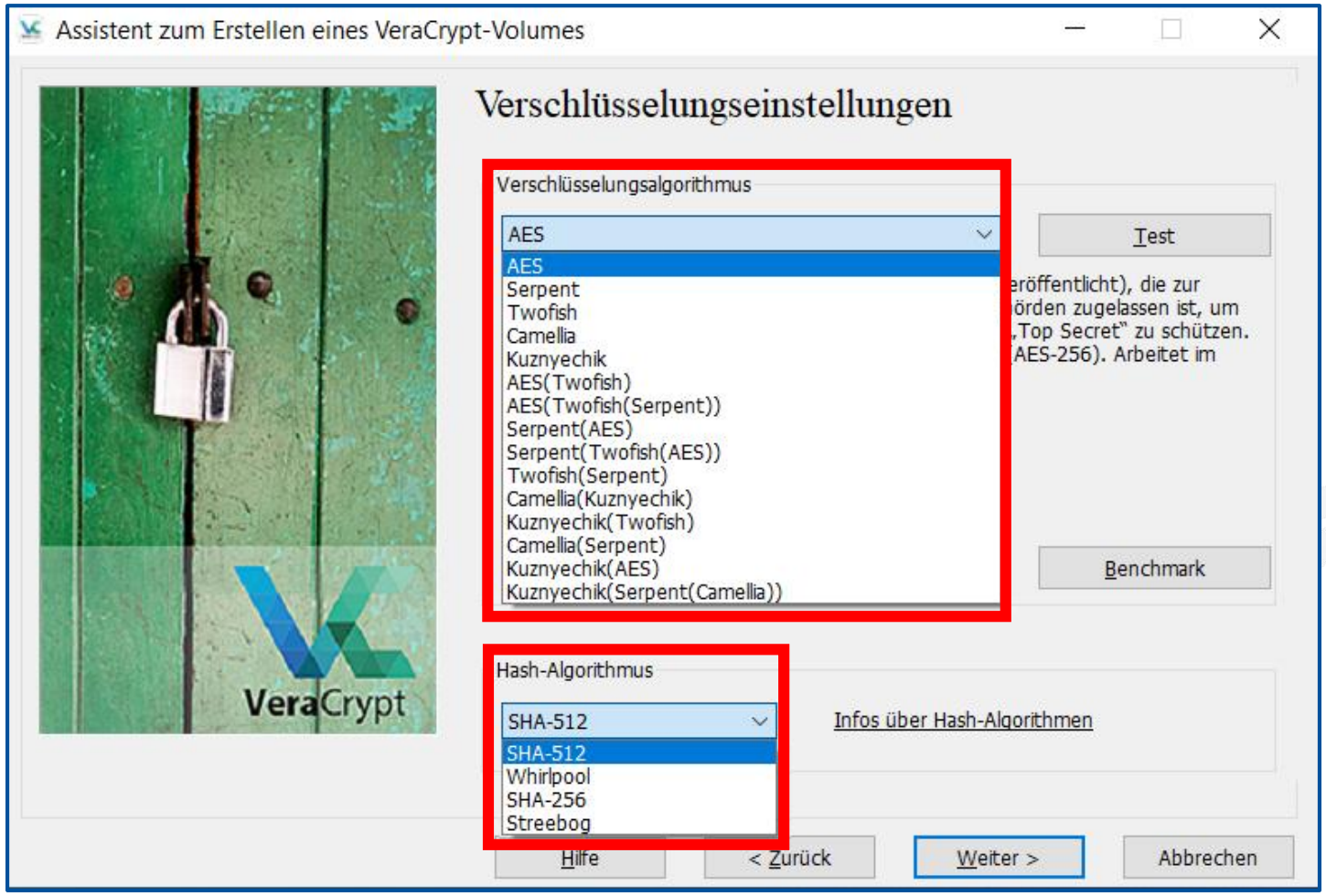
zu den Videos



Kapitel

- Einführung
- Rechtliche Grundlagen
- Die informierte Einwilligung
- Schutz vor Datenmissbrauch
- Daten anonymisieren
- Personenbezogene Forschungsdaten publizieren

Sicherheitsabstufungen bei der Verschlüsselung



Empfohlene Einstellungen:

Sicherheitsstandard: AES-256-bit oder gleichwertig ist i.d.R. ausreichend.

Mögliche zusätzliche Maßnahmen für besonders sensible Daten:

- verschlüsselte Partition verstecken (mobile Datenträger in unsicheren Gegenden)
- mehrere Verschlüsselungs-algorithmen verschachteln
- nicht den Standard-Hash-Algorithmus (SHA-512) auswählen

Kapitel

- Einführung
- Rechtliche Grundlagen
- Die informierte Einwilligung
- Schutz vor Datenmissbrauch
- Daten anonymisieren
- Personenbezogene Forschungsdaten publizieren

Verschlüsselt kommunizieren

Bei browserbasierten Diensten darauf achten, dass diese das „Hypertext Transfer Protocol Secure“ (https) verwenden

In E-Mails keine sensiblen Informationen im Klartext schreiben! Ganze Mail per OpenPGP oder S/MIME verschlüsseln oder verschlüsselte Datei anhängen.

Dienste und Apps verwenden, die eine echte Ende-zu-Ende-Verschlüsselung unterstützen

i

Nutzerzertifikate zum Verschlüsseln und signieren von E-Mails nach dem S/MIME-Verfahren können Sie bei den Leibniz Universität IT Services beantragen.

zur LUIS-Webseite

Lese-Tipp

Torge Schmidt (2020): Ende-zu-Ende Verschlüsselung von Videokonferenzen. Online-Artikel auf der Webseite der „Datenschutzgruppe Nord“

zum Internet-Artikel

Tool-Tipp

Für gängige E-Mail Clients gibt es OpenPGP-Plug-Ins. Eine Übersicht finden Sie auf der OpenPGP-Webseite

zur Liste der PlugIns

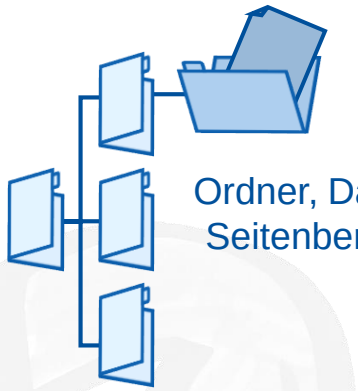
Ein beliebtes OpnePGP-Plug-In für Mozilla Thunderbird ist z.B. Enigmail. Das folgenden YouTube-Videos von Wolfgang Wagner erläutert einfach verständlich die Funktionsweise und die Einrichtung des Plug-Ins.

zum Video

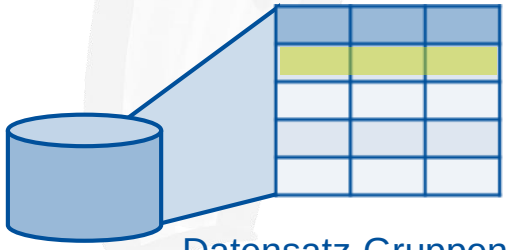
Kapitel

Einführung
Rechtliche Grundlagen
Die informierte Einwilligung
Schutz vor Datenmissbrauch
Daten anonymisieren
Personenbezogene Forschungsdaten publizieren

Rechtemanagement



Ordner, Dateien, Seitenbereiche



Datensatz-Gruppen in Datenbanken

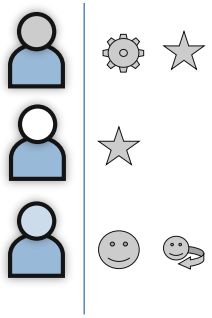
Rechte (Beispiele)

- lesen (angucken)
- schreiben (verändern)
- erstellen (neu anlegen)
- verschieben
- löschen
- herunterladen

Nutzergruppen (Beispiele)

- IT-Admins
- Projektleitung
- Mitarbeitende
- Externe Partner

Gruppen-zuordnung



! Das zuverlässige Einrichten und Verwalten von Berechtigungen erfordert IT-Fachkenntnisse und ggf. spezielle Software. Berücksichtigen Sie dies in Ihrer Projekt- und Ressourcenplanung!

LOG

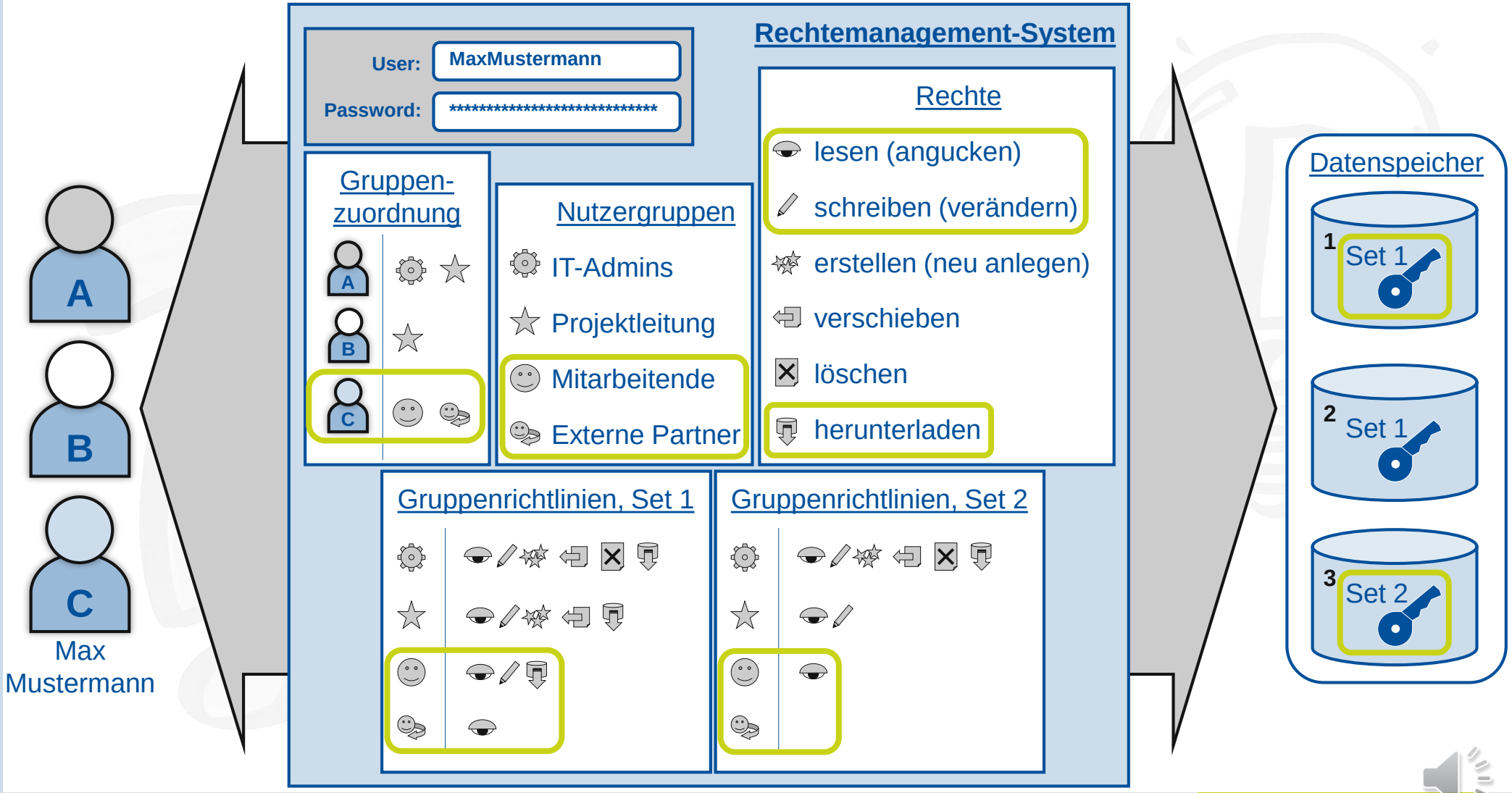
Datum	Uhrzeit	Nutzer	Aktion
.....	....	.....	.....
.....	.....	....	.....
.....	....	.....	.....
.....	.....	....	.....

CC BY

Kapitel

- Einführung
- Rechtliche Grundlagen
- Die informierte Einwilligung
- Schutz vor Datenmissbrauch
- Daten anonymisieren
- Personenbezogene Forschungsdaten publizieren

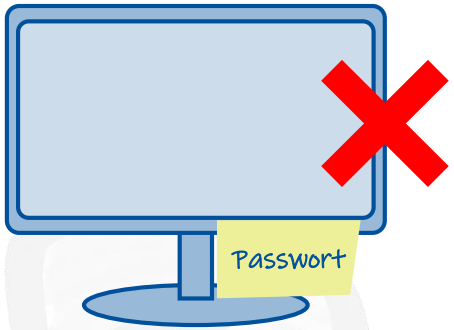
Rechtemanagement (Beispielschema)



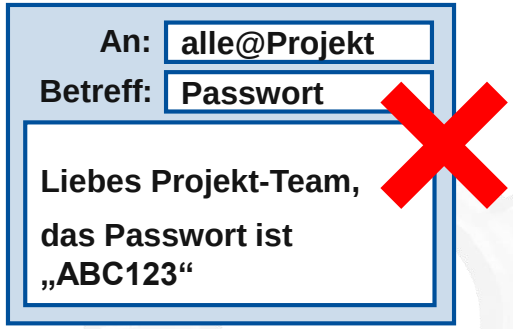
Kapitel

- Einführung
- Rechtliche Grundlagen
- Die informierte Einwilligung
- Schutz vor Datenmissbrauch
- Daten anonymisieren
- Personenbezogene Forschungsdaten publizieren

Umgang mit Passwörtern: so bitte NICHT!



Passwort nicht an den Bildschirm kleben!



Passwort niemals im Klartext per E-Mail senden!

Nicht dasselbe Passwort für verschiedene Accounts verwenden!

Tool-Tipp

Mit dem Passwort-Manager KeePass lassen sich Passwörter einigermaßen sicher verwalten (für hochsensible Passwörter besser nicht verwenden). Sie müssen sich dann nur Ihr Masterpasswort merken.

Tipp: speichern Sie die Passwort-Datenbank in Ihrem persönlichen LUH-Cloudspeicher, um von verschiedenen Geräten darauf zugreifen zu können.

zum Download

Kapitel

Einführung
Rechtliche Grundlagen
Die informierte Einwilligung
Schutz vor Datenmissbrauch
Daten anonymisieren
Personenbezogene Forschungsdaten publizieren

Sichere Passwörter erstellen

User: MaxMustermann

Password: **********

Lese-Tipp

Empfehlungen des Bundesamtes für Sicherheit in der Informationstechnik (BSI)

zur Webseite des BSI

Tipps für sichere Passwörter:

- mindestens 20 Zeichen
- schwer zu erraten (keine Geburtstage etc. verwenden)
- Passphrase statt einzelnem Wort
- ohne erkennbaren Sinn, also keine Sprichwörter usw.
- Schreibweisen verfremden (z.B. „Tr!ck“ statt „Trick“)
- mehrere Sprachen kombinieren

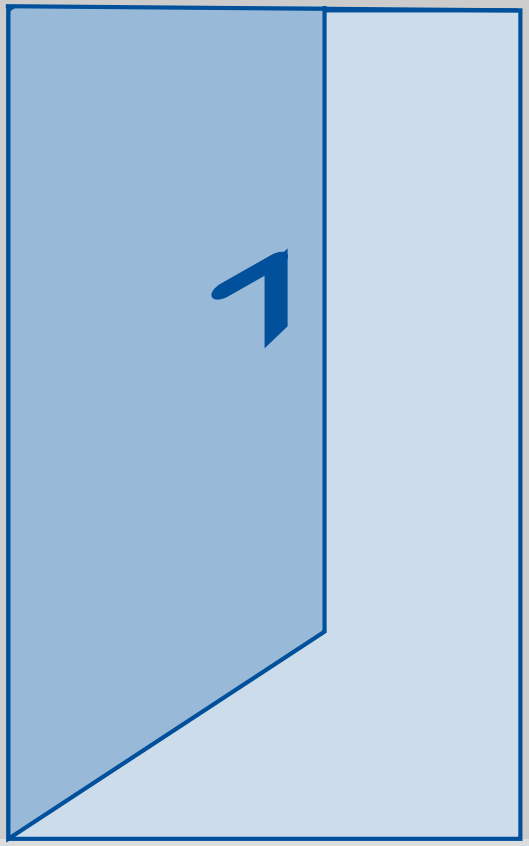
Vermeiden Sie in Passwörtern länderspezifische Sonderzeichen wie ö,ä,ü,ß usw. Diese stehen Ihnen auf Geräten mit dem Tastaturlayout eines anderen Landes nicht zur Verfügung, so dass Sie dann Ihr Passwort nicht eingeben können!

CC BY

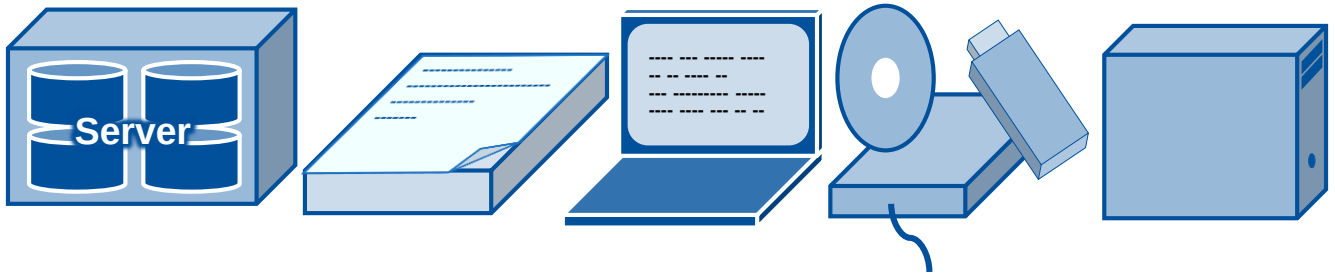
Kapitel

- Einführung
- Rechtliche Grundlagen
- Die informierte Einwilligung
- Schutz vor Datenmissbrauch
- Daten anonymisieren
- Personenbezogene Forschungsdaten publizieren

Physische Zugangsbeschränkungen



- Auf welchen Datenträger existieren Originale oder Kopien der Daten?
- Wo befinden sich die Datenträger?
- Wer hat legal physischen Zugang (auch Hausmeister, Putzdienst etc.)?
- Wie einfach könnte man sich illegal Zugang verschaffen (Einbruch)?



Wählen Sie Aufbewahrungsorte, deren Sicherheit und Zugangsbeschränkung der Sensibilität Ihrer Daten angemessen sind!

Lese-Tipp

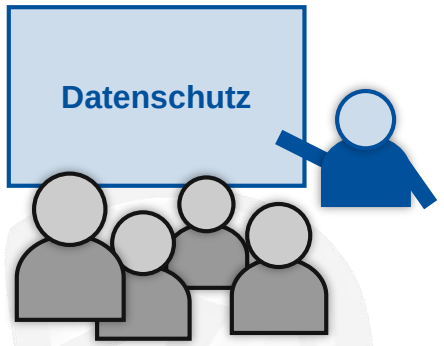
Ein aktuelles Beispiel:
Michael Schneider (2020): EU-Parlament - Einbruchsserie beunruhigt Abgeordnete. (online-Artikel vom 4.7.2020 aufauf tagesschau.de)

zum Internet-Artikel

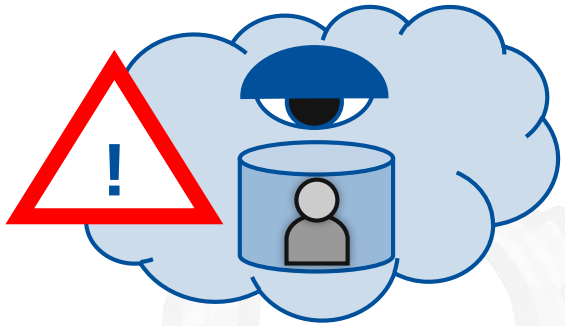
Kapitel

Einführung
Rechtliche Grundlagen
Die informierte Einwilligung
Schutz vor Datenmissbrauch
Daten anonymisieren
Personenbezogene Forschungsdaten publizieren

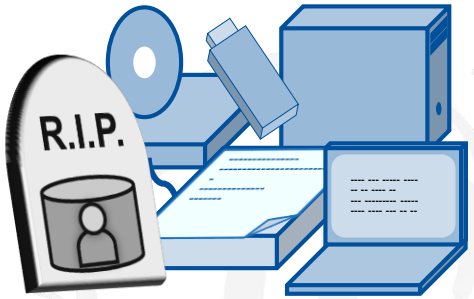
Weitere organisatorische Maßnahmen



Schulung und Sensibilisierung der datenverarbeitenden Personen



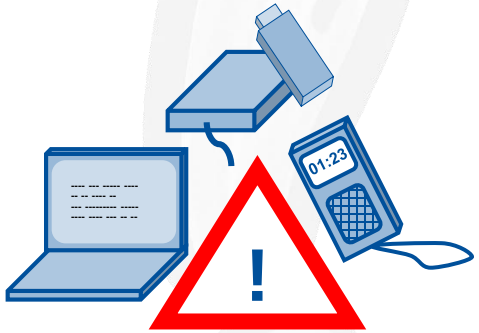
Möglichst keine kostenfreien kommerziellen Cloudspeicher, Filehoster etc. nutzen.



Nicht mehr benötigte oder defekte Datenträger professionell (!) physisch vernichten (lassen)

i

Zur Vernichtung bestimmte elektronische Datenträger können Sie im Sachgebiet 12 (IuK) im Welfenschloss (R318A) abgeben.



Daten möglichst nicht auf mobilen Datenträgern speichern und wenn, dann nur kurzfristig!

Regelmäßige Kontrollen, ob Regeln eingehalten werden. Workflows und Verantwortlichkeiten festlegen!

Lese-Tipp

Surveillance Self-Defence (2019): Your Security Plan. Online-Artikel vom 1.10.2019

zum Internet-Artikel

CC BY

Kapitel

Einführung
Rechtliche Grundlagen
Die informierte Einwilligung
Schutz vor Datenmissbrauch
Daten anonymisieren
Personenbezogene Forschungsdaten publizieren

Daten anonymisieren

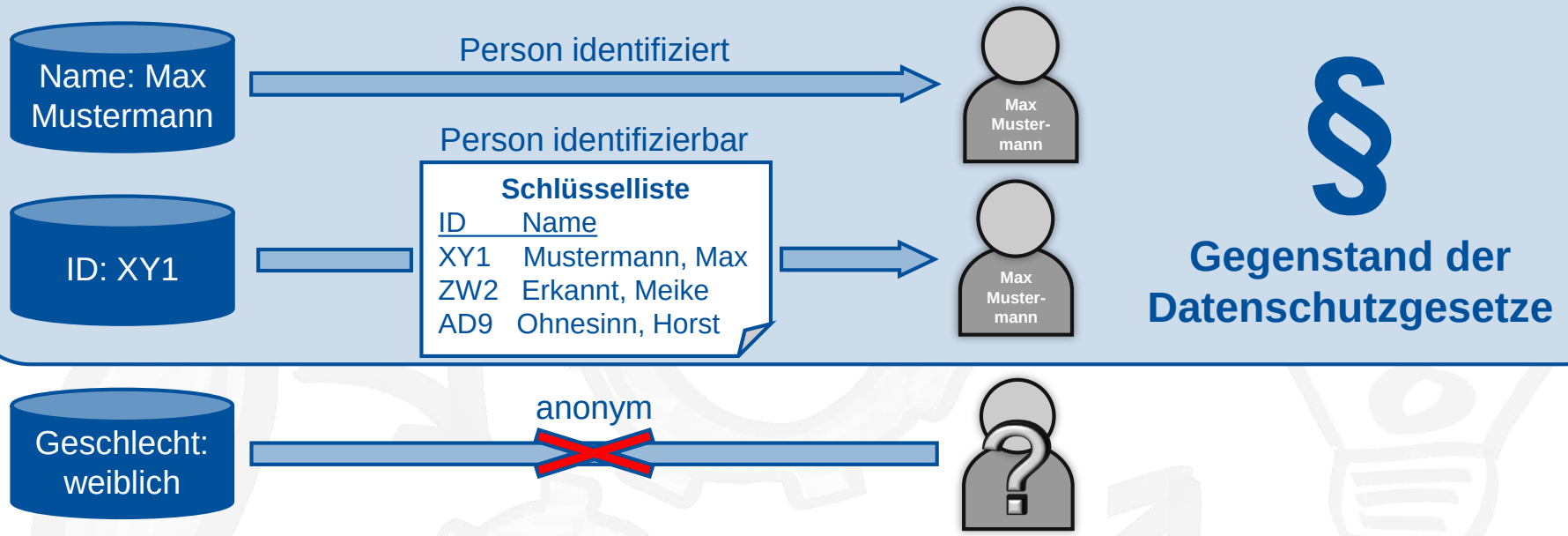
- Wann sind Daten anonym?
- Risikoabschätzung für eine De-Anonymisierung
- Anonymisierungsverfahren
- Pseudonymisierungsverfahren
- Einsatz von Datentreuhändern bei pseudonymisierten Daten
- Verfremden von Ton und Bild
- Vergröbern personenbezogener Merkmale in strukturierten Daten
- Anonymisieren eines Transkripts
- Löschen personenbezogener Merkmale

CC BY

Kapitel

Einführung
Rechtliche Grundlagen
Die informierte Einwilligung
Schutz vor Datenmissbrauch
Daten anonymisieren
Personenbezogene Forschungsdaten publizieren

Wann sind Daten anonym?



- Daten sind anonym, wenn sie sich nicht (mehr) einer natürlichen Person zuordnen lassen und ein solcher Bezug auch nicht (wieder)hergestellt werden kann.
- Absolute Anonymität kann selten garantiert werden, da es mit aktuellen (oder zukünftigen!) elektronischen Hilfsmitteln und Datensammlungen oft möglich ist, ein Person zu identifizieren.
- Daten sind „faktisch“ anonym, solange der Aufwand für die Identifizierung einer Person so groß wäre, dass eine De-Anonymisierung extrem unwahrscheinlich ist.

CC BY

Kapitel

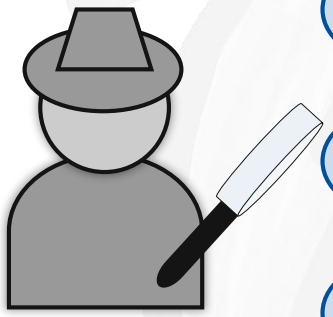
- Einführung
- Rechtliche Grundlagen
- Die informierte Einwilligung
- Schutz vor Datenmissbrauch
- Daten anonymisieren
- Personenbezogene Forschungsdaten publizieren

Risikoabschätzung für eine De-Anonymisierung

Wer könnte ein Interesse an einer De-Anonymisierung haben?

gering — **Kompetenz und Ressourcen des Angreifers** — erheblich

gering — **Folgen einer De-Anonymisierung** — gravierend



- neugieriger Durchschnittsbürger?
- Journalisten?
- Polizei und Justiz?
- Hacker/Internet-Troll?
- staatlicher Geheimdienst?
- Internet-Konzern?

! Anonymisieren Sie umso sorgfältiger, je größer die Fähigkeiten potentieller Angreifer sind und je gravierender die Folgen einer De-Anonymisierung wären!

Lese-Tipp

Rolf Schwartmann, Steve Ritter (2020): Wer haftet beim Verlust von Forschungsdaten? Online-Artikel vom 2.8.2020 auf der Webseite von Forschung & Lehre

zum Internet-Artikel

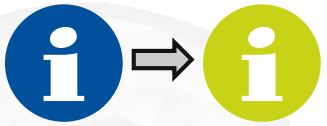
CC BY

Kapitel

- Einführung
- Rechtliche Grundlagen
- Die informierte Einwilligung
- Schutz vor Datenmissbrauch
- Daten anonymisieren
- Personenbezogene Forschungsdaten publizieren

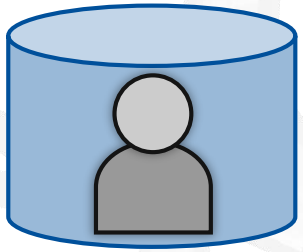
Anonymisierungsverfahren

! Bedenken Sie, dass auch seltene Kombination an sich häufiger Merkmale eine Person identifizierbar machen kann!



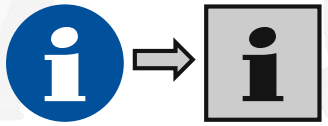
Merkmale durch ähnliche Angabe mit vergleichbaren Eigenschaften 1:1 ersetzen

(Beruf: Maler → Beruf: Lackierer)



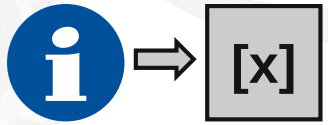
Merkmale ersatzlos löschen / schwärzen

(Beruf: Maler → xxxx)



Merkmale durch eine breitere Kategorie ersetzen

(Beruf: Maler → Beruf: Handwerker)



Merkmale durch Merkmals-bezeichnung ersetzen

(Beruf: Maler → [Beruf])

Lese-Tipp

Alexia Meyermann, Maike Porzelt (2014): Hinweise zur Anonymisierung von qualitativen Daten

Thomas Ebel, Alexia Meyermann (2015): Hinweise zur Anonymisierung von quantitativen Daten

zu den Artikeln

CC BY

Kapitel

- Einführung
- Rechtliche Grundlagen
- Die informierte Einwilligung
- Schutz vor Datenmissbrauch
- Daten anonymisieren
- Personenbezogene Forschungsdaten publizieren

Pseudonymisierungsverfahren

Anonymisierungsprotokoll

- Merkmale werden durch ähnliche Angabe mit vergleichbaren Eigenschaften 1:1 ersetzt
- Protokoll hält fest, welche Originaldaten durch welche Pseudonyme ersetzt wurden

Schlüsselliste

- Den betroffenen Personen wird ein Pseudonym (z.B. ein Alias, eine ID-Nummer oder ein Code) zugeordnet.
- Auf Fragebögen etc. erscheinen keine Namen der Betroffenen, sondern ausschließlich die Pseudonyme
- Eine Schlüsselliste hält fest, welches Pseudonym zu welcher natürlichen Person gehört

i

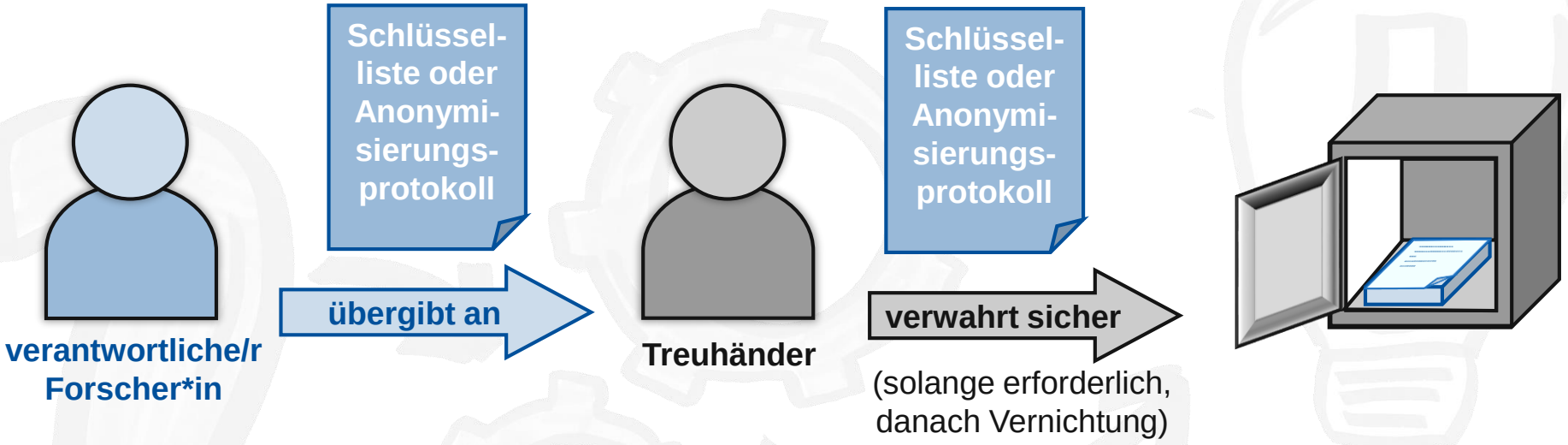
Anonymisierungsprotokolle und Schlüssellisten dürfen nur angefertigt und aufbewahrt werden, wenn für den Forschungszweck oder zur Erfüllung gesetzlicher Vorgaben eine spätere De-Anonymisierung erforderlich werden kann. Sie müssen an einem sicheren Ort und von den Daten selbst strikt getrennt aufbewahrt werden!

CC BY

Kapitel

- Einführung
- Rechtliche Grundlagen
- Die informierte Einwilligung
- Schutz vor Datenmissbrauch
- Daten anonymisieren
- Personenbezogene Forschungsdaten publizieren

Einsatz von Datentreuhändern bei pseudonymisierten Daten



i Als Datentreuhänder kommen z.B. Datenschutzbeauftragte, Anwälte oder Notare in Frage.

! Datentreuhänder und Projektverantwortliche müssen dafür Sorge tragen, dass die Dokumente professionell vernichtet werden, sobald sie nicht mehr benötigt werden!

Kapitel

- Einführung
- Rechtliche Grundlagen
- Die informierte Einwilligung
- Schutz vor Datenmissbrauch
- Daten anonymisieren
- Personenbezogene Forschungsdaten publizieren

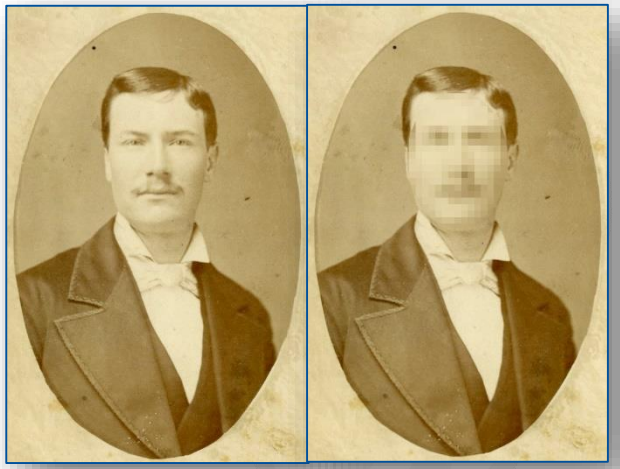
Verfremden von Ton und Bild

Szenen nachstellen,
Stimmen nachsprechen

Stimmen verzerren

original ***verzerrt***

(für dieses Beispiel wurde WavePad verwendet)



Gesichter, Nummernschilder etc. verpixeln (z.B. mit Paint.net)

! Bei Bildern, Videos und Audio-Aufnahmen lassen sich Verfremdungen mit speziellen Tools und Fachkenntnissen teilweise kompensieren, so dass Gesichter, Stimmen usw. wieder zu erkennen sind!

Lese-Tipp

Ryan Dahl, Mohammad Norouzi, Jonathon Shlens (2017): Pixel Recursive Super Resolution, arXiv:1702.00783

zum Artikel

CC BY

Kapitel

- Einführung
- Rechtliche Grundlagen
- Die informierte Einwilligung
- Schutz vor Datenmissbrauch
- Daten anonymisieren
- Personenbezogene Forschungsdaten publizieren

Vergröbern personenbezogener Merkmale in strukturierten Daten

!

Erheben Sie Daten nur in dem Detailgrad, wie es für den Forschungszweck nötig ist! Wenn Sie existierende Daten nachnutzen:

- nicht benötigte Merkmale löschen
- unnötig detaillierte Angaben vergröbern

Originaldaten	vergröberte Daten
Alter: 34	Altersgruppe: 30-39
Geschlecht: weiblich	Geschlecht: weiblich
Anschrift: Hinter dem Mond 42, 99999 Kuhkaff	Bundesland (Wohnort): Bayern
Bundesland: Bayern	Bundesland (Arbeitsort): Bayern
Branche: Unternehmensberatung	Branche: Unternehmensberatung
Arbeitgeber: Grasshopper Consulting GmbH, München	Arbeitgeber: mittelgroße Firma, 50-200 Angestellte
Brutto-Jahreseinkommen: 436.000 €	Brutto-Jahreseinkommen: 250.000-500.000 €
→ über eine Kombination der Merkmale wäre die betroffene Person vermutlich schnell identifizierbar	**→ durch die Vergröberung einiger Merkmale ist eine Identifikation der betroffenen Person unwahrscheinlich**

CC BY

Kapitel

Einführung

Rechtliche Grundlagen

Die informierte Einwilligung

Schutz vor Datenmissbrauch

Daten anonymisieren

Personenbezogene Forschungsdaten publizieren

Anonymisieren eines Transkripts

Original-Transkript eines Interviews

Interviewer: Und wie haben Sie die Folgen Ihrer Privatinsolvenz schließlich überwunden?

Mandy Koslowski: Ja, also wir haben uns da an diese Beratungseinrichtung in Kleinkleckersdorf gewendet. Da hat uns die Frau Bauer dann so einen Plan ausgearbeitet, wie wir unsere Ausgaben aufschreiben sollen und so. Und mit dem Plan sind wir dann zu Herrn Miesepeter von der Kreissparkasse Kleinkeckersdorf gegangen. Der hat uns dann so ein Basiskonto eingerichtet.

Durch Verallgemeinerung anonymisiertes Transkript (sicherer aber weniger Analysepotential)

Interviewer: Und wie haben Sie die Folgen Ihrer Privatinsolvenz schließlich überwunden?

Interviewte Person: Ja, also wir haben uns da an diese Beratungseinrichtung in [Wohnort] gewendet. Da hat uns [Name der beratenden Person] dann so einen Plan ausgearbeitet, wie wir unsere Ausgaben aufschreiben sollen und so. Und mit dem Plan sind wir dann zu [Name der/des Bankangestellten] von [Name einer lokalen Bank] gegangen. [Der/die] hat uns dann so ein Basiskonto eingerichtet.

Durch 1:1-Verfremdung anonymisiertes Transkript (weniger sicher, mehr Analysepotential)

Interviewer: Und wie haben Sie die Folgen Ihrer Privatinsolvenz schließlich überwunden?

Cindy Kowalski: Ja, also wir haben uns da an diese Beratungseinrichtung in Hintertupfingen gewendet. Da hat uns die Frau Bäcker dann so einen Plan ausgearbeitet, wie wir unsere Ausgaben aufschreiben sollen und so. Und mit dem Plan sind wir dann zu Herrn Nörgelmichel von der Volksbank Hintertupfingen gegangen. Der hat uns dann so ein Basiskonto eingerichtet.

CC BY

Kapitel

- Einführung
- Rechtliche Grundlagen
- Die informierte Einwilligung
- Schutz vor Datenmissbrauch
- Daten anonymisieren
- Personenbezogene Forschungsdaten publizieren

Löschen personenbezogener Merkmale

Lorem ipsum dolor sit amet, [redacted] sadipscing elitr, sed diam nonumy [redacted] tempor invidunt ut labore et

x	y	z
lorem	12	**********
ipsum	99	Bla
dolor	225	Blub
tempor	11	**********
labore	78	palaver

Lese-Tipp

TU München (2019): Korrektes Schwärzen von personenbezogenen Daten. Online-Artikel vom 10.01.2019.

zu den Artikeln

Tonspuren anonymisieren: So kann´s gehen

Audacity: zum YouTube-Video (Greg)

Adobe Premiere: zum YouTube-Video (EN187)

CC BY

Kapitel

Einführung

Rechtliche Grundlagen

Die informierte Einwilligung

Schutz vor Datenmissbrauch

Daten anonymisieren

Personenbezogene Forschungsdaten publizieren

Personenbezogene Forschungsdaten publizieren

- Wann dürfen (ehemals) personenbezogene Daten publiziert werden?
- Daten über ein Fachrepositorium zur Verfügung stellen
- Wichtige Datenzentren und Fachdienste?

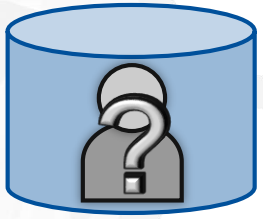
CC BY

Kapitel

Einführung
Rechtliche Grundlagen
Die informierte Einwilligung
Schutz vor Datenmissbrauch
Daten anonymisieren
Personenbezogene Forschungsdaten publizieren

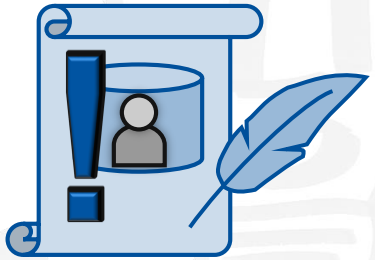
Wann dürfen (ehemals) personenbezogene Daten publiziert werden?

! Eine Datenpublikation ist nur zulässig, wenn mindestens eine dieser Voraussetzung zutrifft:



Daten sind anonym (unsicher, da technischer Fortschritt berücksichtigt werden muss)

Betroffene haben in die Veröffentlichung eingewilligt

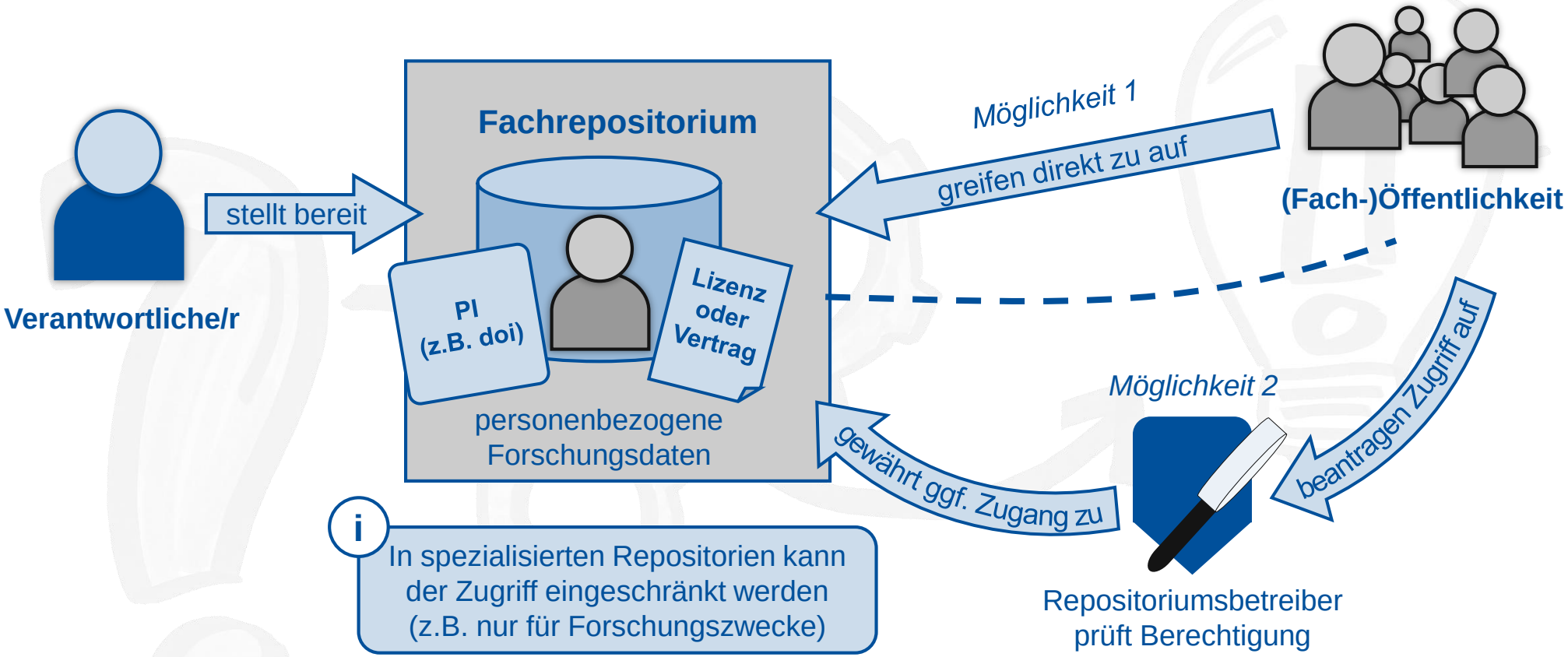


Publikation ist für die „Darstellung von Forschungsergebnissen über Ereignisse der Zeitgeschichte unerlässlich“

Kapitel

- Einführung
- Rechtliche Grundlagen
- Die informierte Einwilligung
- Schutz vor Datenmissbrauch
- Daten anonymisieren
- Personenbezogene Forschungsdaten publizieren

Daten über ein Fachrepositorium zur Verfügung stellen



i In spezialisierten Repositorien kann der Zugriff eingeschränkt werden (z.B. nur für Forschungszwecke)

Kapitel

- Einführung
- Rechtliche Grundlagen
- Die informierte Einwilligung
- Schutz vor Datenmissbrauch
- Daten anonymisieren
- Personenbezogene Forschungsdaten publizieren

Wichtige Datenzentren und Fachdienste

Empfehlungen:

- Verwenden Sie vorzugsweise Repositorien mit Spezialisierung auf sozial- und wirtschafts-wissenschaftliche Daten
- Nehmen Sie Unterstützungs-angebote von Fachdiensten in Anspruch (z.B. Prüfung der Anonymität)!
- Stellen Sie Daten ggf. nur unter Bedingungen oder nur einem eingeschränkten Personenkreis zur Verfügung
- Beantragen Sie Mittel für Service-Leistungen und Publikations-gebühren!

Beispiele für relevante Datenzentren und Fachdienste:

Qualiservice data sharing

Spezialisiert auf Aufbereitung und Archivierung qualitativer Daten

gesis Leibniz-Institut für Sozialwissenschaften

Spezialisiert auf Aufbereitung, Archivierung und Publikation quantitativer Daten

VerbundFDB forschungsdaten-bildung.de

Umfassender Beratungsservice, hilfreiche Publikationen, unterstützt bei der Datenpublikation

RatSWD. Rat für Sozial- und WirtschaftsDaten

Repositorien-übergreifende Suche, Liste akkreditierter Datenzentren, hilfreiche Publikationen

CC BY

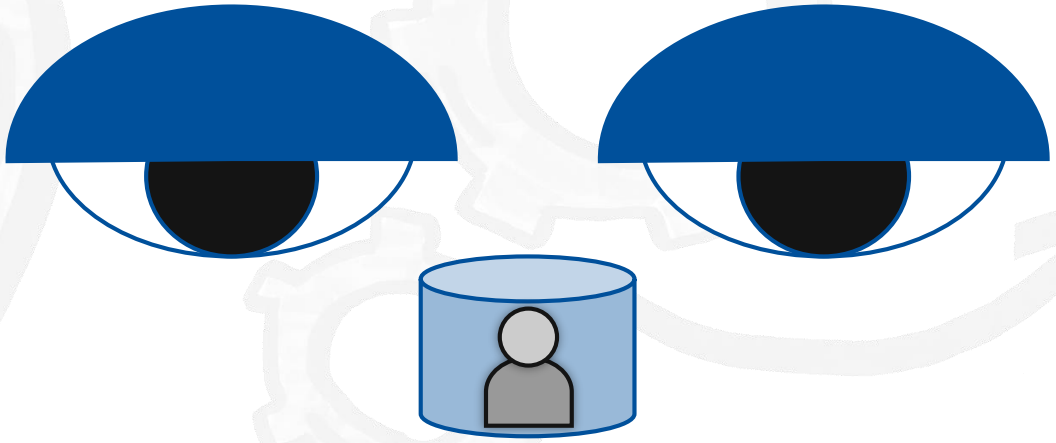
Kapitel

Einführung
Rechtliche Grundlagen
Die informierte Einwilligung
Schutz vor Datenmissbrauch
Daten anonymisieren
Personenbezogene Forschungsdaten publizieren

Vielen Dank für Ihr Interesse!

Herzlichen Glückwunsch! Sie sollten nun einen soliden Überblick über das Thema „personenbezogene Forschungsdaten“ haben.

Bei weiteren Fragen und für individuelle Beratungen wenden Sie sich gerne an die Stabsstelle Datenschutz oder das Service-Team Forschungsdaten.



! Und niemals vergessen: BIG BROTHER IS WATCHING YOU! ;-)