Umgang mit personenbezogenen Forschungsdaten

Rechtliche Grundlagen, Methoden und Hilfsmittel

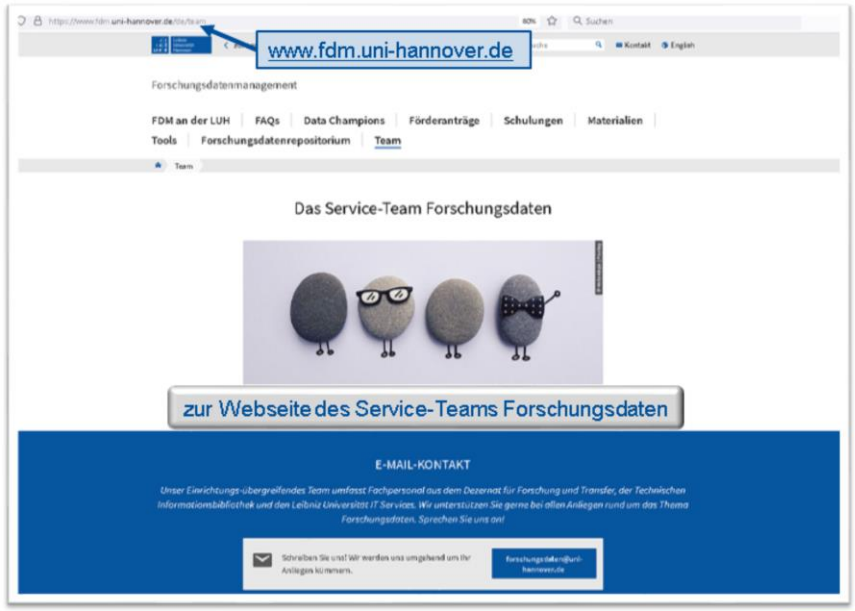
Image by delphinmedia: https://pixabay.com/de/photos/eye-tracking-blickuntersuchung-1791845/

Service-Team Forschungsdaten

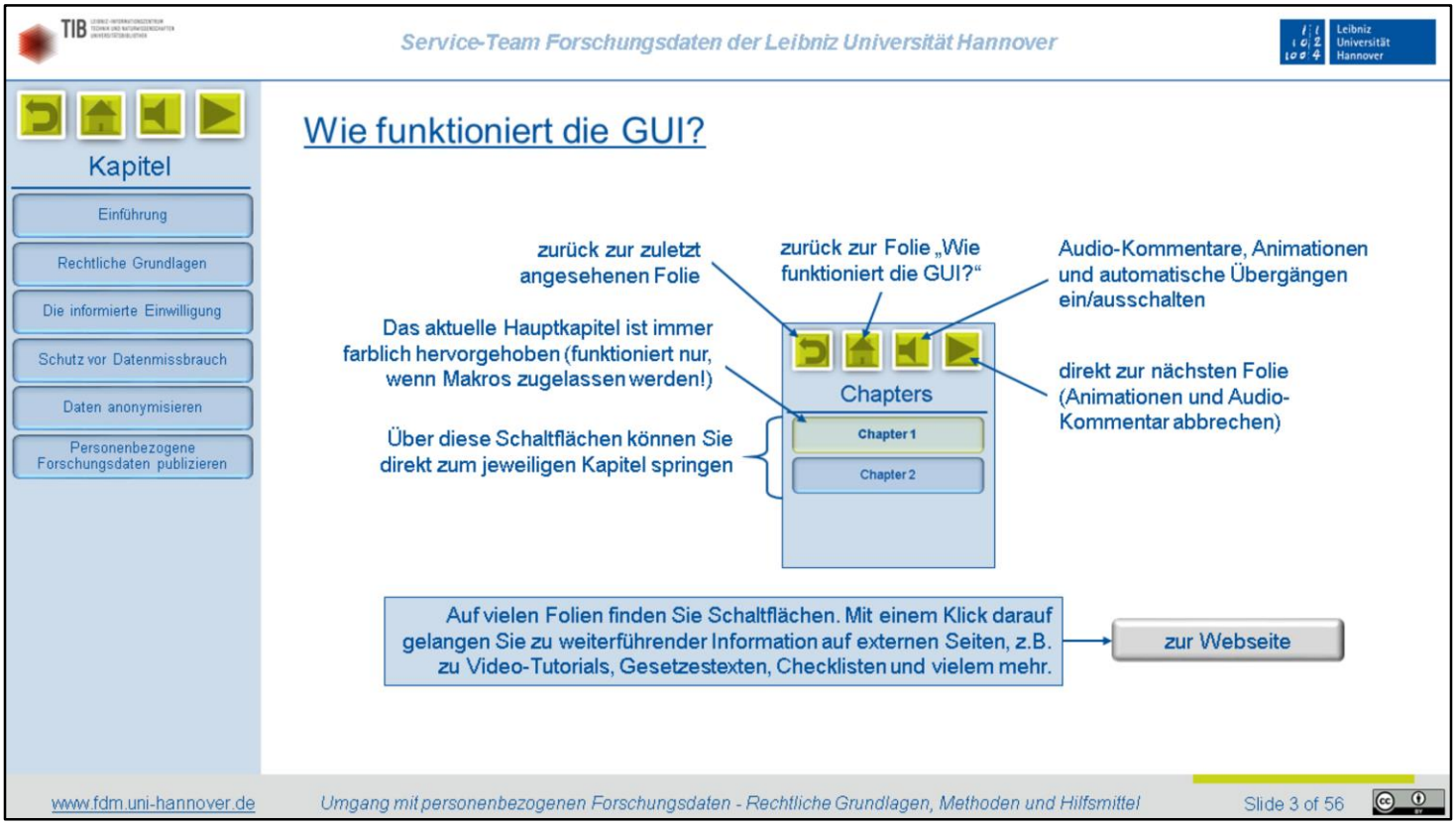
Stand: Juli 2024

DOI: 10.5281/zenodo.13305806

Herzlich willkommen!



Hallo und herzlich willkommen zum online-Kurs “Umgang mit personenbezogenen Forschungsdaten - Rechtliche Grundlagen, Methoden und Hilfsmittel“! Dieser Kurs wird vom Service-Team Forschungsdaten angeboten. Unser Team umfasst Personen aus den Publikationsdiensten der TIB, dem Forschungsdezernat der LUH sowie dem LUH-Rechenzentrum LUIS. Wenn Sie mehr über unsere Schulungs-, Beratungs- und Unterstützungsangebote erfahren möchten, schauen Sie doch mal auf unserer Webseite vorbei. Dort finden Sie umfangreiche Informationen zum Forschungsdatenmanagement allgemein. Gerne stehen wir LUH-Angehörigen auch für eine individuelle Beratung zur Verfügung.



Bevor es inhaltlich losgeht, noch ein paar Worte zur Funktionsweise der grafischen Benutzeroberfläche. Diese Präsentation ist für das selbständige Erarbeiten konzipiert. Sie sollen selbst entscheiden, mit welchen Kapiteln Sie sich in welcher Reihenfolge befassen möchten. Daher finden Sie links eine Liste der Hauptkapitel. Mit einem Klick auf die entsprechende Schaltfläche gelangen Sie zu der jeweiligen Kapitel-Übersicht. Von dort können Sie auch gezielt zu einer bestimmten Folie springen. Um die Orientierung zu erleichtern, wird das Hauptkapitel, zu dem die aktuell angezeigte Folie gehört, in der Seitenleiste grün unterlegt.

Wenn Sie zur zuletzt angesehenen Folie zurückkehren möchten, klicken Sie auf die grüne Schaltfläche mit dem gebogenen Pfeil oben links. Direkt daneben finden Sie einen Button, der Sie zu dieser Erklärungsfolie am Anfang der Präsentation zurückbringt. Der dritte grüne Button schaltet die Audio-Kommentare zu den Folien und die dazugehörigen Animationen ein oder aus. Möchten Sie sich eine Folie in Ruhe angucken, bevor es weitergeht, haben Sie bitte keine Hemmungen, ihn zu benutzen. Der ganz rechte Button führt Sie direkt zur nächsten Folie, falls Sie die Animationen und Audio-Kommentare auf der aktuellen Folie überspringen möchten.

Zuletzt noch der Hinweis, zu den grauen Schaltflächen, die Sie auf zahlreichen Folien finden. Wenn Sie diese betätigen, öffnet sich in der Regel ein Browserfenster, und Sie gelangen zu einer Webseite oder einem online-Dokument mit weiterführenden Informationen.

Einführung

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

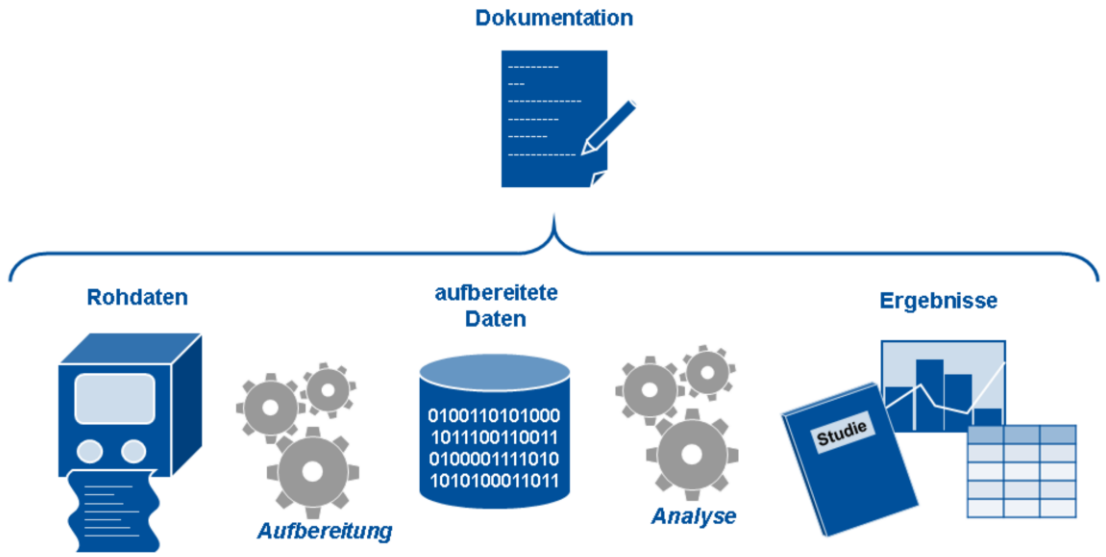
So, nun geht es endlich los! In diesem Einführungskapitel stellen wir kurz vor, was Sie inhaltlich erwartet. Außerdem wollen wir Sie mit ein paar grundlegenden Konzepten und Begrifflichkeiten vertraut machen, auf die wir uns später immer wieder beziehen werden. Das betrifft sowohl das Datenmanagement allgemein als auch im Besonderen den Umgang mit personenbezogenen Daten.

In diesem Kurs möchten wir Ihnen einen vertiefenden Überblick über die wichtigsten Aspekte im Umgang mit personenbezogenen Forschungsdaten geben. Natürlich kann es sein, dass Sie in Ihrem wissenschaftlichen Alltag auch mit weiteren personenbezogenen Daten zu tun haben, zum Beispiel mit Personaldaten von Projektbeteiligten. Solche Daten unterliegen teils noch anderen oder zusätzlichen Anforderungen und Bestimmungen. Diese sollen hier aber nicht berücksichtigt werden. In diesem Kurs geht es um Daten, die unmittelbar Gegenstand wissenschaftlicher Untersuchungen sind.

Nach dieser Einführung werden Sie die wichtigsten gesetzlichen Grundlagen kennenlernen. Wir erläutern anschließend, wie eine wirksame informierte Einwilligung eingeholt wird. In den folgenden Kapiteln zum Schutz vor Datenmissbrauch und zum Anonymisieren von Daten lernen Sie vor allem Methoden, Maßnahmen und Hilfsmittel kennen, die Sie direkt in Ihren Projekten einsetzen können. Zum Schluss erklären wir noch, unter welchen Voraussetzungen personenbezogene Daten publiziert werden dürfen.

Insbesondere bei rechtlichen Fragen zum Datenschutz können Sie sich jederzeit an die Stabsstelle Datenschutz wenden. Alle Kursinhalte, die rechtliche Fragen betreffen, sind eng mit dem juristischen Fachpersonal der Stabsstelle abgestimmt.

Was sind Forschungsdaten?



Da wir uns heute mit personenbezogenen Forschungsdaten beschäftigen wollen, sollten wir zunächst einmal klären, was denn überhaupt alles unter den Begriff „Forschungsdaten“ fällt. Wenn wir in diesem Kurs von „Forschungsdaten“ sprechen, dann ist damit Folgendes gemeint:

Da sind zum einen die sogenannten Roh- oder Primärdaten, also das, was unmittelbar neu generiert wird und noch in keiner Weise bearbeitet wurde. Im sozial- und wirtschaftswissenschaftlichen Kontext fallen zum Beispiel Audio-Aufnahmen von Interviews, Video-Aufnahmen bestimmter Kommunikationssituationen oder ausgefüllte Fragebögen darunter.

Diese Rohdaten werden üblicherweise in mehreren Schritten aufbereitet. Zum Beispiel werden Audio-Aufnahmen transkribiert, die Transkripte eventuell von mehreren Personen überprüft und anschließend noch annotiert. Bei Fragebögen werden vielleicht Antworten auf offene Fragen bestimmten Kategorien zugeordnet, oder es werden unvollständige Fragebögen aussortiert.

Der nächste Schritt ist die Analyse, bei der Daten häufig zusammengefasst werden. So können beispielsweise aus vielen individuellen Interviews und Fragebögen allgemeine Statistiken abgeleitet werden. Die Ergebnisse dieser Analysen werden üblicherweise als Fachliteratur veröffentlicht.

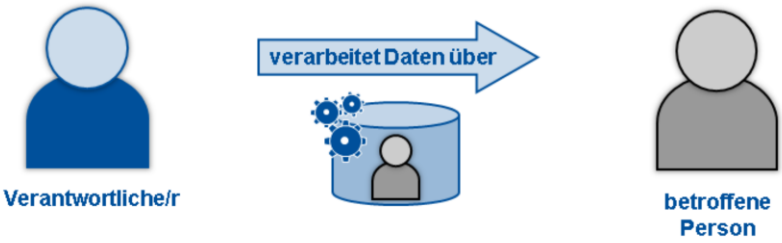
Rohdaten, aufbereitete Daten und Analyse-Ergebnisse sind alles Forschungsdaten. Hinzu kommt noch eine besonders wichtige Kategorie, nämlich die Dokumentation all dessen, was Sie im Laufe des Forschungsprozesses mit Ihren Daten tun. Zur Dokumentation gehören Beschreibungen von Methoden und Workflows ebenso wie das Protokollieren von Bearbeitungsvorgängen sowie systematisch gesammelte, strukturierte Metadaten zu den Dateien.

Da also meistens im gesamten Verlauf des Forschungsprozesses verschiedene Arten von Daten verarbeitet werden, ist auch das Management dieser Forschungsdaten etwas, was alle Stadien wissenschaftlichen Arbeitens begleitet. Genau genommen beginnt es sogar schon, bevor ein Projekt überhaupt startet, nämlich mit der Planung des Umgangs mit Daten. Und es endet auch nicht, wenn ein Projekt ausläuft, denn die entstandenen Daten werden in der Regel über längere Zeiträume archiviert oder gar publiziert und müssen in dieser Zeit les- und nutzbar bleiben.

In den verschiedenen Stadien eines wissenschaftlichen Projektes müssen Sie also passende Lösung für verschiedene Herausforderungen im Umgang mit Ihren Forschungsdaten finden. Welche Dokumentationssysteme kommen in Frage? Bietet die IT-Infrastruktur ausreichend Kapazitäten und ein angemessenes Sicherheitsniveau? Wie können Prozesse und Verantwortlichkeiten so geregelt werden, dass Forschungseffizienz, gute Datenqualität und Rechtskonformität jederzeit gewährleistet sind? Wer sich diese Fragen erst stellt, wenn schon die ersten Daten auf dem Tisch liegen, wird über viele Probleme stolpern. Daher nehmen Sie sich unbedingt die Zeit, Ihr Projekt mit viel Vorlauf detailliert durchzuplanen. Sie werden dann ein Vielfaches an Zeit allein dadurch einsparen, dass Sie nicht mitten im Projekt permanent gegen das Chaos ankämpfen müssen!

Zwar gilt dieser Rat grundsätzlich für jedes wissenschaftliche Projekt. Er ist aber besonders relevant, wenn Sie mit personenbezogenen Forschungsdaten arbeiten. Denn wenn Sie da nicht schon beim Erheben der Daten die einschlägigen Rechtsvorschriften beachten, kann es sein, dass Sie diese Daten gar nicht auswerten dürfen. Oder dass Sie sich sogar strafbar machen, wenn Sie es trotzdem tun.

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)

Bevor wir uns die rechtlichen Grundlagen näher ansehen, möchten wir ein paar zentrale Begriffe zum Thema Datenschutz erläutern. Eines vorweg: in Gesetzestexten wird in Deutschland üblicherweise nach wie vor allein die männliche Form verwendet, auch wenn alle Geschlechter gemeint sind. Es lässt sich hier also nicht immer vermeiden, ebenso zu verfahren, wenn auf juristisch definierte Begriffe oder Gesetzespassagen Bezug genommen wird.

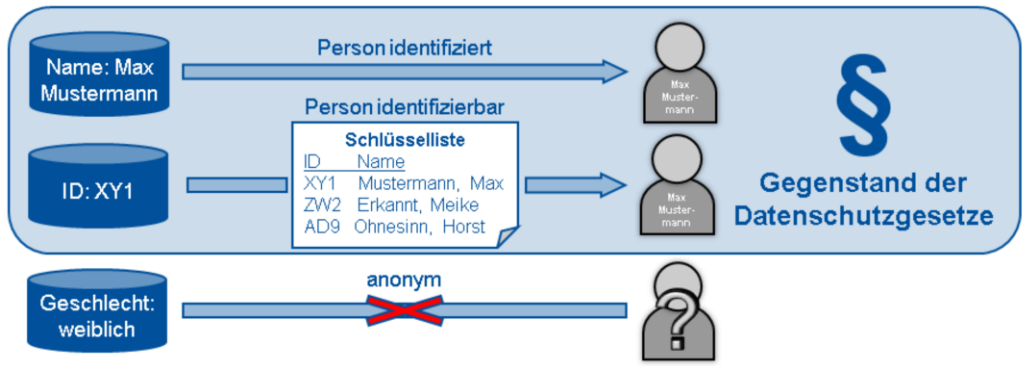
Beim Verarbeiten personenbezogener Daten gibt es immer zwei Parteien, nämlich den Verantwortlichen, der Daten verarbeitet und den Betroffenen, auf den sich diese Daten beziehen.

Mit Datenverarbeitung ist jegliche Art des Umgangs mit Daten gemeint, also zum Beispiel das Erheben, Zusammenstellen, Speichern, Übertragen, Analysieren oder Weitergeben.

Bei dem Betroffenen handelt es sich immer um eine sogenannte natürliche Person, also einen Menschen aus Fleisch und Blut

Beim Verantwortlich kann es sich hingegen auch um eine juristische Person handeln, also zum Beispiel einen Verein, eine Gesellschaft, eine Firma, eine Stiftung oder eine Behörde.

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

Die nächste Frage ist, wann Daten als personenbezogen gelten. Das ist in der Praxis nicht immer klar abgrenzbar. Eindeutig personenbezogen sind alle Informationen, von denen bekannt ist, auf wen sie sich beziehen. Wenn also auf einem ausgefüllten Fragenbogen der Name der Person steht, die ihn ausgefüllt hat, sind sämtliche darin enthaltenen Angaben personenbezogen, denn der Betroffene ist eindeutig identifiziert.

Ebenfalls personenbezogen sind aber auch Daten, bei denen der Betroffene nur mittelbar identifiziert werden kann. Das ist zum Beispiel der Fall, wenn in Datensätzen Merkmale wie Personennamen durch einen Alias ersetzt wurden, es aber eine Schlüsselliste gibt, auf er steht, hinter welchem Alias sich welcher echte Name verbirgt. Mithilfe dieser Liste wären die Betroffenen also identifizierbar. Hier spricht man von pseudonymen Daten. Doch selbst, wenn keine solche Schlüsselliste existiert, kann es möglich sein, Betroffene unter Zuhilfenahme allgemein verfügbarer Ressourcen zu identifizieren. Über eine einfache Google-Suche lassen sich oft viele Details über einzelne Personen erfahren. Führt man diese Informationen mit den scheinbar nicht personenbezogenen Daten zusammen, lässt sich manchmal doch sehr schnell herausfinden, um welche Personen es sich handelt. Alle Daten, bei denen die Betroffenen identifiziert oder identifizierbar sind, fallen in den Anwendungsbereich der Datenschutzgesetze!

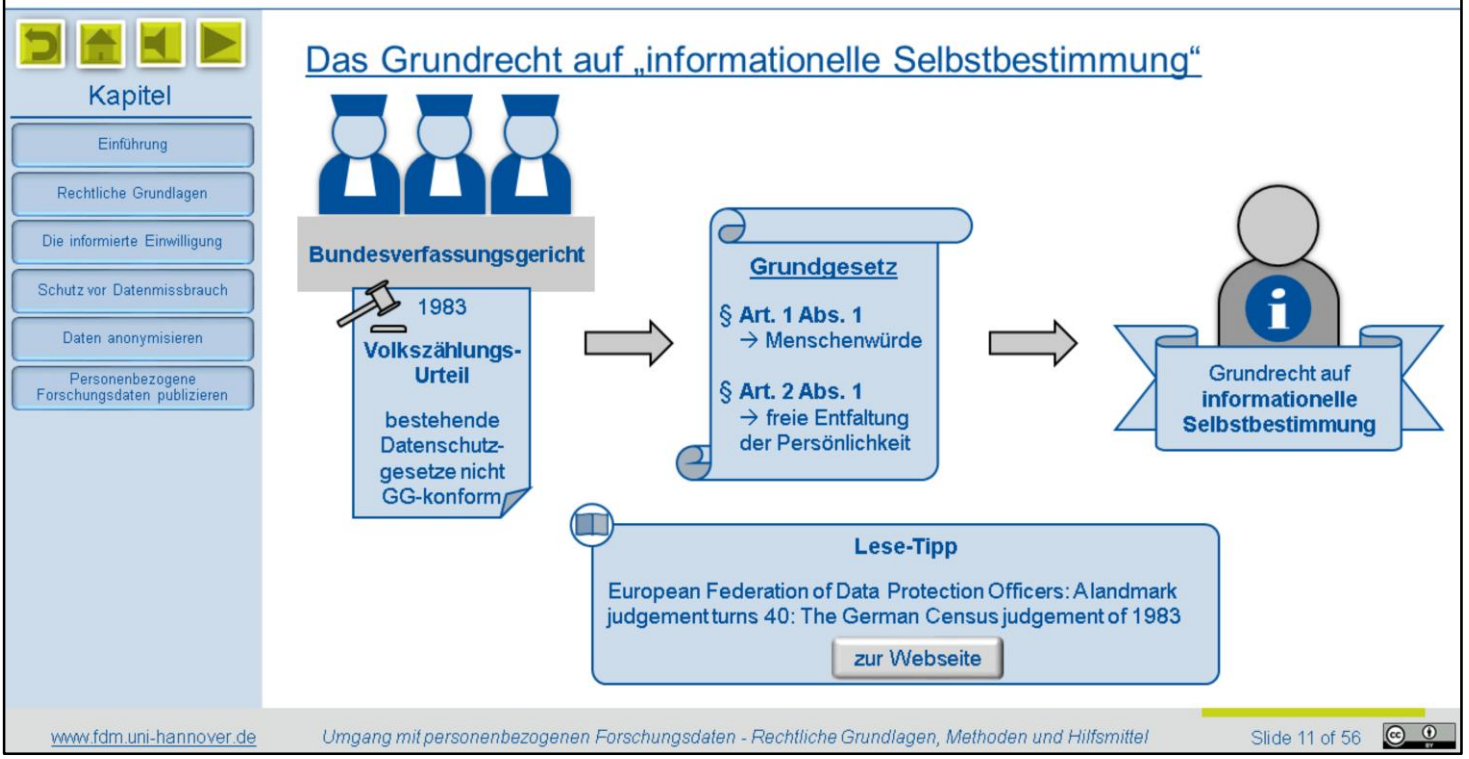
Von diesen gesetzlichen Regelungen ausgenommen sind lediglich vollständig anonyme Daten. Anonyme Daten beziehen sich entweder gar nicht auf Personen, oder sie sind so allgemein oder so verfremdet, dass sie selbst unter Einsatz weiterer Hilfsmittel und Datenquellen keine Rückschlüsse auf Einzelpersonen zulassen.

Kapitel

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

Nun kommen wir zu den rechtlichen Grundlagen, also den einschlägigen Datenschutzgesetzen. Das mag etwas trocken sein, aber wer mit personenbezogenen Daten arbeitet, sollte in diesem Bereich zumindest über ein paar Grundkenntnisse verfügen.



Der Kernbegriff des Datenschutzes ist das „Recht auf informationelle Selbstbestimmung“. Damit ist gemeint, dass im Grundsatz jede Person selbst entscheiden können soll, wer was über sie wissen darf. Für Ausnahmen von diesem Grundsatz, zum Beispiel für die öffentliche Verwaltung, bedarf es einer gesetzlichen Grundlage.

1983 entschied das Bundesverfassungsgericht in seinem berühmten Volkszählungsurteil, dass die bestehenden Bundes- und Landesgesetze zum Datenschutz nicht mit dem Grundgesetz vereinbar sind. Es bezog sich dabei insbesondere auf Artikel 1, Absatz 1 und Artikel 2, Absatz 1 des Grundgesetzes. Darin heißt es: „Die Würde des Menschen ist unantastbar. Sie zu achten und zu schützen ist Verpflichtung aller staatlichen Gewalt“. Und weiter: „Jeder hat das Recht auf die freie Entfaltung seiner Persönlichkeit, soweit er nicht die Rechte anderer verletzt und nicht gegen die verfassungsmäßige Ordnung oder das Sittengesetz verstößt“.

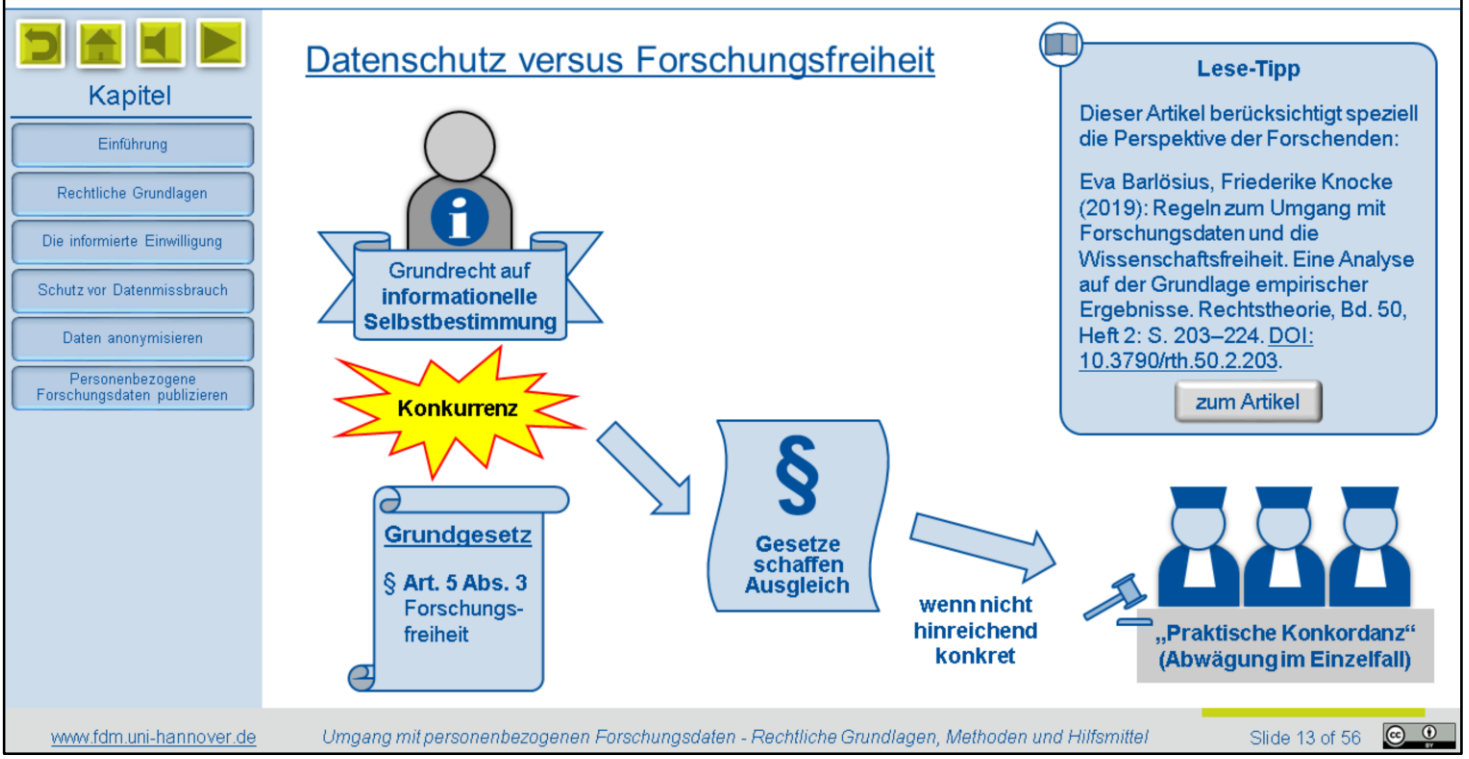
Aus diesen Artikeln leitete das Gericht ein Grundrecht auf informationelle Selbstbestimmung ab. Wer mehr zum Hintergrund dieses Meilensteins der Rechtsgeschichte wissen möchte, sollte einmal einen Blick auf die Webseite des Bundesdatenschutzbeauftragten werfen.

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

Das Thema Datenschutz hat gerade in Deutschland eine lange Tradition. Es war das Bundesland Hessen, das 1970 das weltweit erste Datenschutzgesetz verabschiedet hat. 1977 folgte die erste Fassung des Bundesdatenschutzgesetzes. Sie hatte allerdings nur bis zum Volkszählungsurteil von 1983 Bestand. In dessen Folge wurden die Datenschutzgesetze von Bund und Ländern zwischen 1986 und 1990 novelliert.

Die juristische Kontroverse in Deutschland hatte aber auch erheblichen Einfluss auf die Gesetzgebung der EU. Zwischen 1995 und 2018 galt die Europäische Datenschutzrichtlinie, an der sich die jeweiligen nationalen Gesetze orientierten. Seit 2009 ist der Datenschutz auch in der Europäischen Grundrechtecharta verankert. Und seit 2018 gilt nun die Europäische Datenschutzgrundverordnung, kurz DSGVO. Sie löst die alte Richtlinie von 1995 ab. Im Gegensatz zu dieser ist die DSGVO aber nicht einfach ein Orientierungsrahmen für nationale Gesetze, sondern unmittelbar geltendes Recht, das im Zweifel über den nationalen Gesetzen steht. Die deutschen Datenschutzgesetze von Bund und Ländern wurden daher noch einmal entsprechend angepasst.



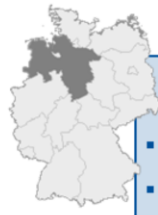
Neben dem indirekt abgeleiteten Recht auf informationelle Selbstbestimmung garantiert das Grundgesetz aber auch die Forschungsfreiheit. Dazu heißt es in Artikel 5, Absatz 3: „Kunst und Wissenschaft, Forschung und Lehre sind frei.“ Möchte also jemand mit personenbezogenen Daten forschen, so konkurriert das Recht der Betroffenen auf informationelle Selbstbestimmung mit dem Recht der Forschenden auf eine freie Wissenschaft.

Wenn gleichrangige Grundrechte konkurrieren, so sollen Gesetze einen Ausgleich schaffen, damit keines der Grundrechte übermäßig eingeschränkt wird. Es kommt allerdings immer wieder vor, dass die gesetzlichen Regelungen nicht hinreichend konkret sind. In diesen Fällen sind es letztlich die Gerichte, die im Einzelfall abwägen müssen. Im Juristendeutsch spricht man bei solchen Abwägungen von „praktischer Konkordanz“. Solche Urteile sind oft schwer vorhersagbar, zumal, wenn sie durch mehrere Instanzen gehen. Aufgrund dieser Unsicherheiten ist es ratsam, personenbezogene Daten auf einer möglichst eindeutigen Rechtsgrundlage zu verarbeiten. In der Praxis ist das meist das ausdrückliche Einverständnis der Betroffenen in die Datenverarbeitung.

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)

Seit 2018 ist die Europäische Datenschutzgrundverordnung als EU-weit unmittelbar geltendes Recht in Kraft. Etwas vereinfacht gesagt, gilt sie bei jeder Verarbeitung personenbezogener Daten innerhalb der EU. Sie gilt also auch, wenn die Betroffenen selbst keine EU-Bürger sind. Außerdem gilt sie für die Datenverarbeitung weltweit, wenn sie durch Stellen erfolgt, die ihren Sitz in der EU haben. Die DSGVO enthält wichtige Grundsätze, verweist an vielen Stellen aber auch auf die nationale Gesetzgebung, wenn es um die konkrete Ausgestaltung geht.

In Deutschland handelt es sich bei den nationalen Gesetzen vor allem um das Bundesdatenschutzgesetz und die entsprechenden Gesetze der einzelnen Bundesländer. Diese Gesetze stehen nicht in einer hierarchischen Beziehung zueinander. Das Bundesgesetz ist den Landesgesetzen also nicht übergeordnet. Vielmehr haben Bundes- und Landesgesetze unterschiedliche Geltungsbereiche, wie wir später noch sehen werden.

Im Folgenden werden wir uns zunächst mit den wichtigsten Regelungen der DSGVO beschäftigen. Dabei verwenden wir vereinfachte Formulierungen. Wer den genauen Wortlaut des Gesetzes nachlesen möchte, gelangt über die Schaltfläche zur offiziellen deutschen Fassung.

Bei der Verarbeitung personenbezogener Daten sind die folgenden Grundsätze zu beachten:

- Die Verarbeitung muss rechtmäßig sein, das heißt, sie darf nur auf einer der gesetzlichen Grundlagen erfolgen, die wir auf der nächsten Folie erläutern.
- Die Verarbeitung muss für die Betroffenen transparent und nachvollziehbar sein und darf nicht gegen Treu und Glauben verstoßen. Informieren Sie die Betroffenen also ausführlich und verständlich. Halten Sie, was Sie versprechen, und versprechen Sie nichts, was Sie nicht halten können!
- Der Zweck der Verarbeitung muss vorab klar definiert sein. Nachträgliche Zweckänderungen sind in der Regel nur auf einer entsprechenden gesetzlichen Grundlage möglich, zum Beispiel bei einer erneut erteilten Einwilligung der Betroffenen. Ausnahmen gibt es unter anderem, wenn vorhandene Daten für Forschungszwecke nachgenutzt werden.
- Ferner gilt das Prinzip der Datensparsamkeit. Es dürfen also nur so viele Daten verarbeitet werden, wie für den Verarbeitungszweck notwendig.
- Die Daten müssen auch sachlich richtig sein, soweit es sich um objektiv nachprüfbare Informationen handelt. Wenn also ein Zahlendreher bei einem Geburtsdatum auffällt, sollte dieser umgehend korrigiert werden.
- Personenbezogene Daten dürfen nur solange gespeichert werden, wie es für den Verarbeitungszweck unbedingt erforderlich ist. Anonymisieren Sie Ihre Daten daher so schnell wie möglich.
- Und schließlich sind die Verantwortlichen verpflichtet, geeignete technische und organisatorische Maßnahmen zu ergreifen, um die Daten vor Verlust, unbefugtem Zugriff und Missbrauch zu schützen. Dazu kommen wir später im Kapitel „Schutz vor Datenmissbrauch“.

Eine Verarbeitung personenbezogener Daten darf nur auf einer gesetzlichen Grundlage erfolgen. In Artikel 6 der DSGVO sind sechs mögliche Grundlagen aufgeführt. Im Forschungskontext kommen in aller Regel aber nur zwei Grundlagen infrage: Entweder haben die Betroffenen wirksam in die Verarbeitung ihrer Daten eingewilligt. Dies ist meist die sicherste Grundlage. Oder es besteht ein schutzwürdiges öffentliches Interesse an der Datenverarbeitung. Das könnte zum Beispiel bei Flächen-Studien zur Ausbreitung einer ansteckenden Krankheit der Fall sein, wenn diese der Eindämmung der Epidemie und damit dem Schutz von Leben und Gesundheit breiter Bevölkerungskreise dienen. Wenn Sie sich auf diese Rechtsgrundlage beziehen wollen, lassen Sie sich vorher bitte unbedingt eingehend juristisch beraten!

Ansonsten ist eine Verarbeitung ebenfalls zulässig,

- wenn sie zur Erfüllung eines Vertrages erforderlich ist,
- wenn dadurch lebenswichtige Interessen natürlicher Personen gewahrt werden,
- wenn der Verantwortliche gesetzlich zur Verarbeitung verpflichtet ist oder
- wenn die berechtigten Interessen des Verantwortlichen die Interessen des Betroffenen überwiegen.

Auf diesen letztgenannten „Gummiparagraphen“ beziehen sich besonders gerne privatwirtschaftliche Unternehmen. Er gilt aber ausdrücklich nicht für staatliche Stellen und damit auch nicht für staatliche Universitäten.

„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!

In Artikel 9 der DSGVO sind die so genannten „besonderen Kategorien“ personenbezogener Daten definiert. Das sind

- Daten zur rassischen und ethnischen Herkunft,
- genetische und biometrischen Daten sowie Gesundheitsdaten,
- Daten zu politischen Meinungen und religiösen oder weltanschaulichen Überzeugungen, oder zu einer Gewerkschaftszugehörigkeit und
- Daten zum Sexualleben oder zur sexuellen Orientierung.

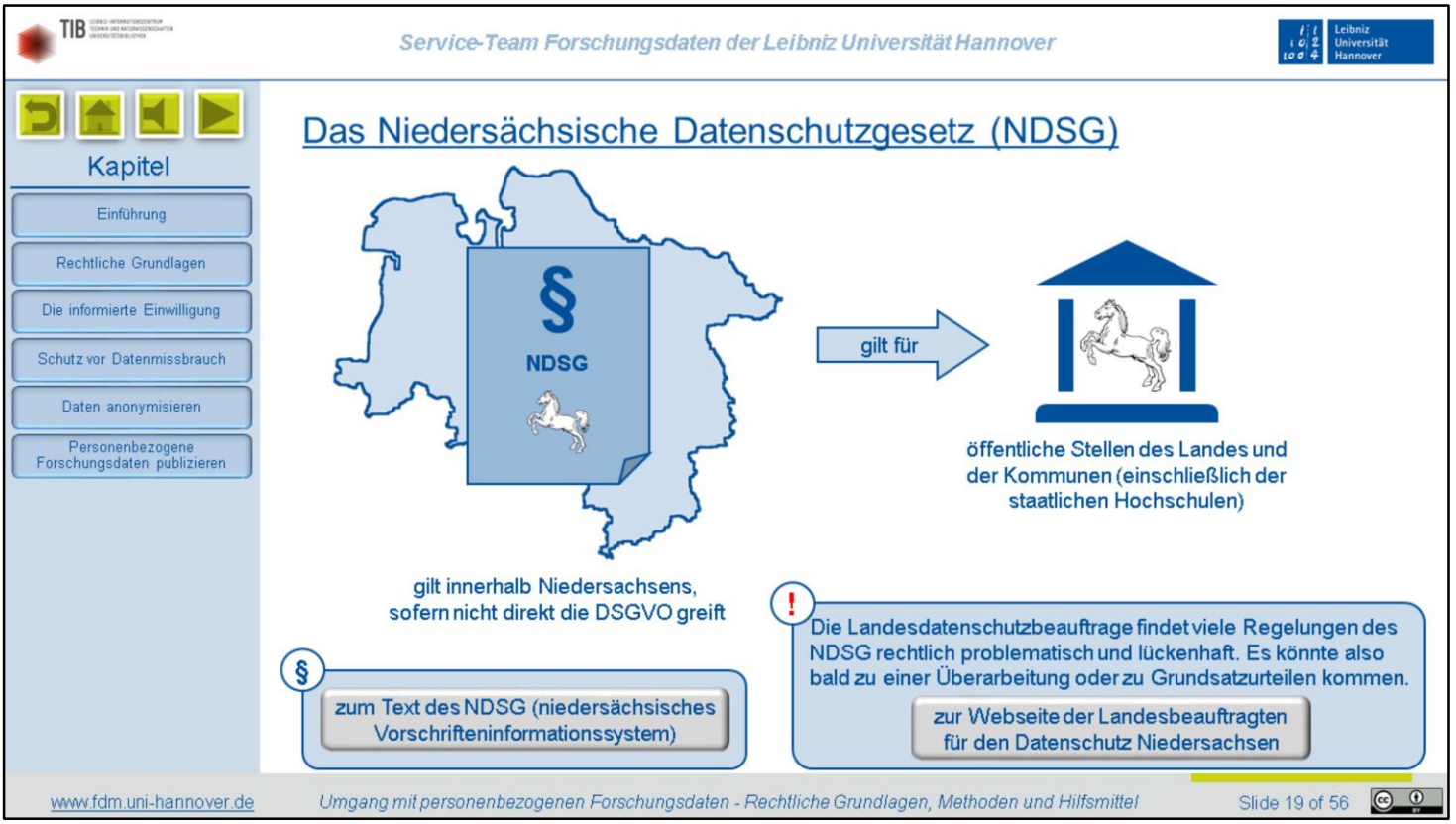
Da Daten dieser Kategorien sehr sensibel sind, ist ihre Verarbeitung nur in bestimmten Fällen und unter besonders strengen Auflagen erlaubt. Für Forschungszwecke dürfen solche Daten in der Regel nur mit ausdrücklicher Einwilligung der Betroffenen verarbeitet werden und sind dann besonders sorgfältig zu schützen!

Die DSGVO enthält zahlreiche sogenannte Öffnungsklauseln. Das bedeutet, dass die nationale Gesetzgebung einzelne Bestimmungen der DSGVO konkretisieren, ergänzen oder modifizieren kann. In Deutschland stehen solche Detailregelungen unter anderem im Bundesdatenschutzgesetz und in den Landesdatenschutzgesetzen.

Das Bundesdatenschutzgesetz gilt also für Datenverarbeitung innerhalb Deutschlands, aber nur soweit, wie die DSGVO nicht direkt selbst greift. Es gilt für öffentliche Stellen des Bundes. Für öffentliche Stellen der Länder gilt es nur, wenn diese im Auftrag des Bundes handeln, oder es für bestimmte Fälle keine entsprechenden Reglungen in dem jeweiligen Landesdatenschutzgesetz gibt.

Außerdem gilt das Bundesdatenschutzgesetz für nicht-öffentliche Stellen wie Privatunternehmen, soweit es um automatisierte oder teilautomatisierte Datenverarbeitung geht. Das betrifft zum Bespiel das Speichern von IP-Adressen bei Website-Besuchen oder die Eingabe von Bank- und Adressdaten in online-Formularen.

Bitte beachten Sie, dass für die Forschung an staatlichen Hochschulen nicht das Bundesdatenschutzgesetz gilt, sondern das jeweilige Landesdatenschutzgesetz!



Das niedersächsische Datenschutzgesetz gilt demnach für die Verarbeitung personenbezogener Daten in Niedersachsen. Anders als das Bundesdatenschutzgesetz gilt es aber ausschließlich für öffentliche Stellen des Landes und der Kommunen. Dazu gehören auch die in Niedersachsen ansässigen staatlichen Hochschulen, darunter die Leibniz Universität Hannover.

Der Landesdatenschutzbeauftrage kommentiert die Ausgestaltung des Gesetzes auf seiner offiziellen Webseite allerdings folgendermaßen:

„Viele Regelungen sind aus Sicht der Landesbeauftragten für den Datenschutz Niedersachsen […] rechtlich problematisch. Bereits im Gesetzgebungsverfahren wurde seitens der [Landesbeauftragten] kritisiert, dass das [Gesetz] u[nter] a[nderem] erhebliche Lücken mit Blick auf die vollständige Umsetzung des sog[enannten] EU-Datenschutzpakets aufweist. Eine zeitnahe Überarbeitung des NDGS wird daher für erforderlich gehalten.“ Zitat Ende.

Aber schauen wir uns mal an, was das Gesetz zum Umgang mit personenbezogenen Forschungsdaten sagt.

Für die wissenschaftliche Datenverarbeitung ist insbesondere der Paragraph 13 relevant. Er regelt die „Verarbeitung personenbezogener Daten zu wissenschaftlichen oder historischen Forschungszwecken“. Demnach ist eine Verarbeitung zulässig, wenn mindestens eine von zwei Bedingungen zutrifft:

Entweder sind keine schutzwürdigen Interessen der Betroffenen berührt oder das öffentliche Interesse überwiegt die schutzwürdigen Interessen der Betroffenen. Die Abwägung, wann genau das der Fall ist, wird allerdings den Verantwortlichen überlassen. Sie müssen jedoch dokumentieren, wie sie zu ihrer Entscheidung gekommen sind, und die geplante Verarbeitung dem Datenschutzbeauftragten der datenverarbeitenden Stelle melden. Im Fall der LUH wäre das die Stabsstelle Datenschutz.

Bei der Verarbeitung sind aber ein paar Gebote unbedingt zu befolgen:

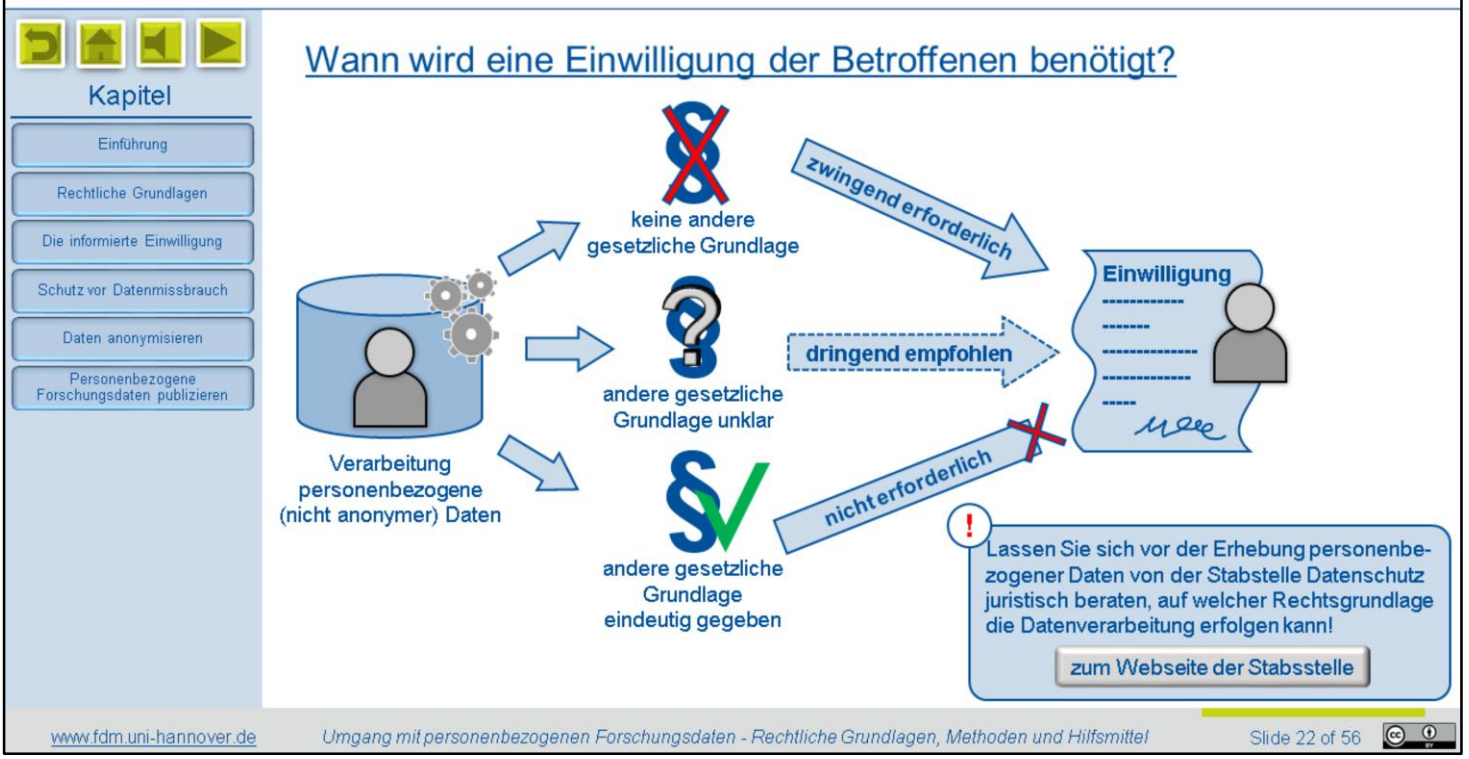
- Die Daten müssen sofort pseudonymisiert werden,
- sie dürfen ausschließlich zum Zweck des Forschungsvorhabens verarbeitet werden,
- sie sind zu anonymisieren, sobald der Forschungszweck dies zulässt und
- es sind angemessene technische und organisatorische Schutzmaßnahmen zu ergreifen. Diese werden in Paragraph 17 näher benannt.

Eine Veröffentlichung der Daten ist nur zulässig, wenn die Betroffenen eingewilligt haben oder wenn dies für die „Darstellung von Forschungsergebnissen über Ereignisse der Zeitgeschichte“ unerlässlich ist. Zur Datenpublikation gibt es am Ende dieser Präsentation noch ein Extra-Kapitel.

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

Wie wir gesehen haben, ist die im Forschungskontext wohl häufigste rechtliche Grundlage für eine Verarbeitung personenbezogener Daten eine Einwilligung der betroffenen Personen. Damit solche Einwilligungen rechtswirksam sind müssen sie bestimmte formale Anforderungen erfüllen. Außerdem müssen die Betroffenen angemessen zu den Hintergründen, Art und Zweck, sowie möglichen Folgen der beabsichtigten Datenverarbeitung informiert werden. In diesem Kapitel schauen wir uns die entsprechenden Vorgaben der DSGVO im Einzelnen an.

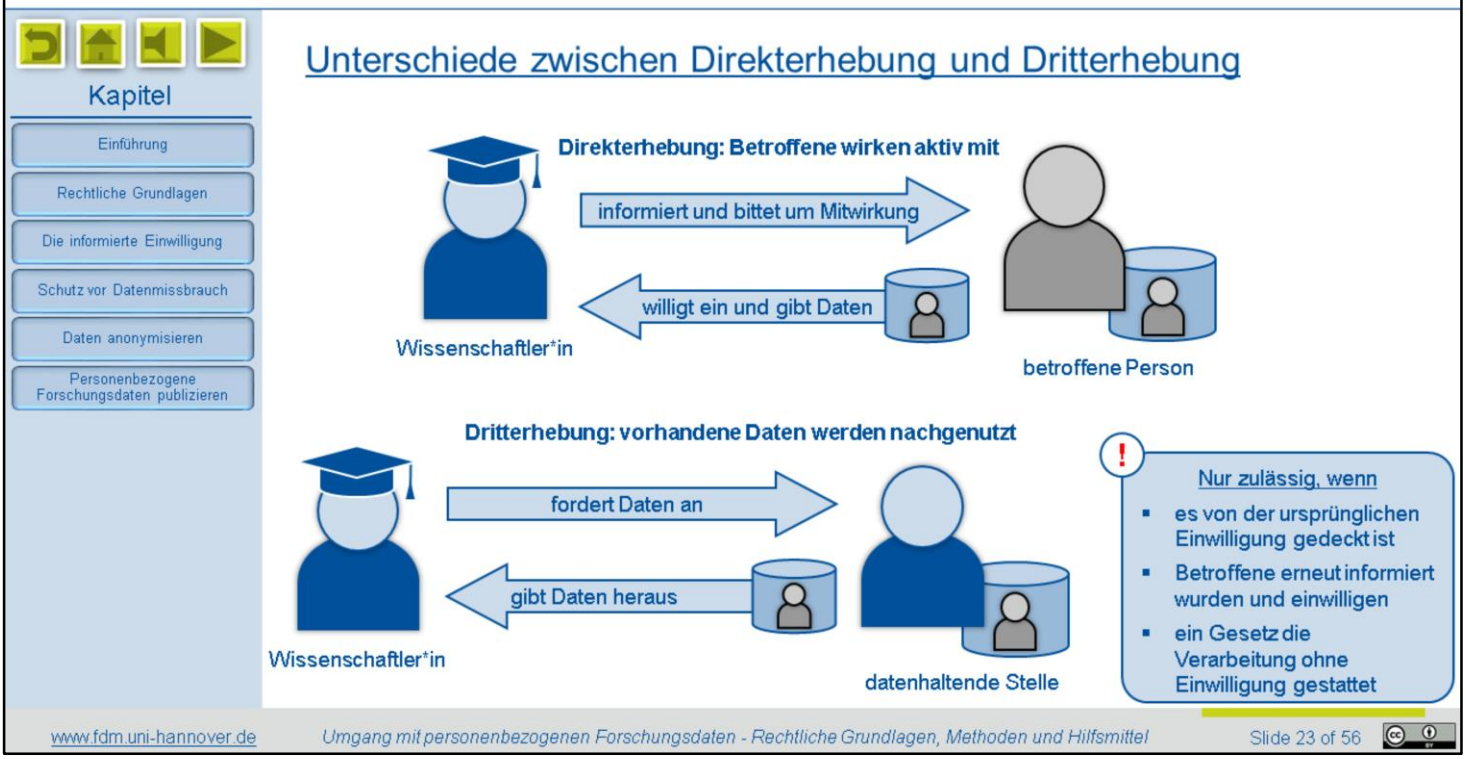


Wenn Sie personenbezogene Daten verarbeiten, müssen Sie eine Einwilligung der Betroffenen auf jeden Fall immer dann einholen, wenn keine andere Rechtsgrundlage infrage kommt. Welche Grundlagen das sein könnten, haben wir im Kapitel „rechtliche Grundlagen“ erläutert.

Manchmal ist es nicht ganz eindeutig, ob eine andere Grundlage greifen könnte. Einige Forschende neigen dann etwas vorschnell dazu, keine Einwilligungen einzuholen, um den damit verbundenen Aufwand zu sparen. Dieser Schuss kann aber schnell nach hinten losgehen, wenn es zu einem Rechtsstreit kommen sollte. Wir empfehlen daher dringend, im Zweifel lieber eine Einwilligung einzuholen und so Rechtssicherheit zu schaffen. Das heißt aber auch, dass Sie dann an alle darin angegeben Bestimmungen gebunden sind, selbst dann, wenn sich später herausstellen sollte, dass doch auch eine andere Rechtsgrundlage vorhanden gewesen wäre.

Nur wenn wirklich ganz eindeutig eine andere Rechtsgrundlage gegeben ist, kann auf das Einholen der Einwilligung verzichtet werden. Im Forschungskontext kommt hierfür wohl vor allem ein überragendes öffentliches Interesse an den Forschungsergebnissen infrage, wenn gleichzeitig der Aufwand für das Einholen von Einwilligungen unverhältnismäßig hoch wäre.

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

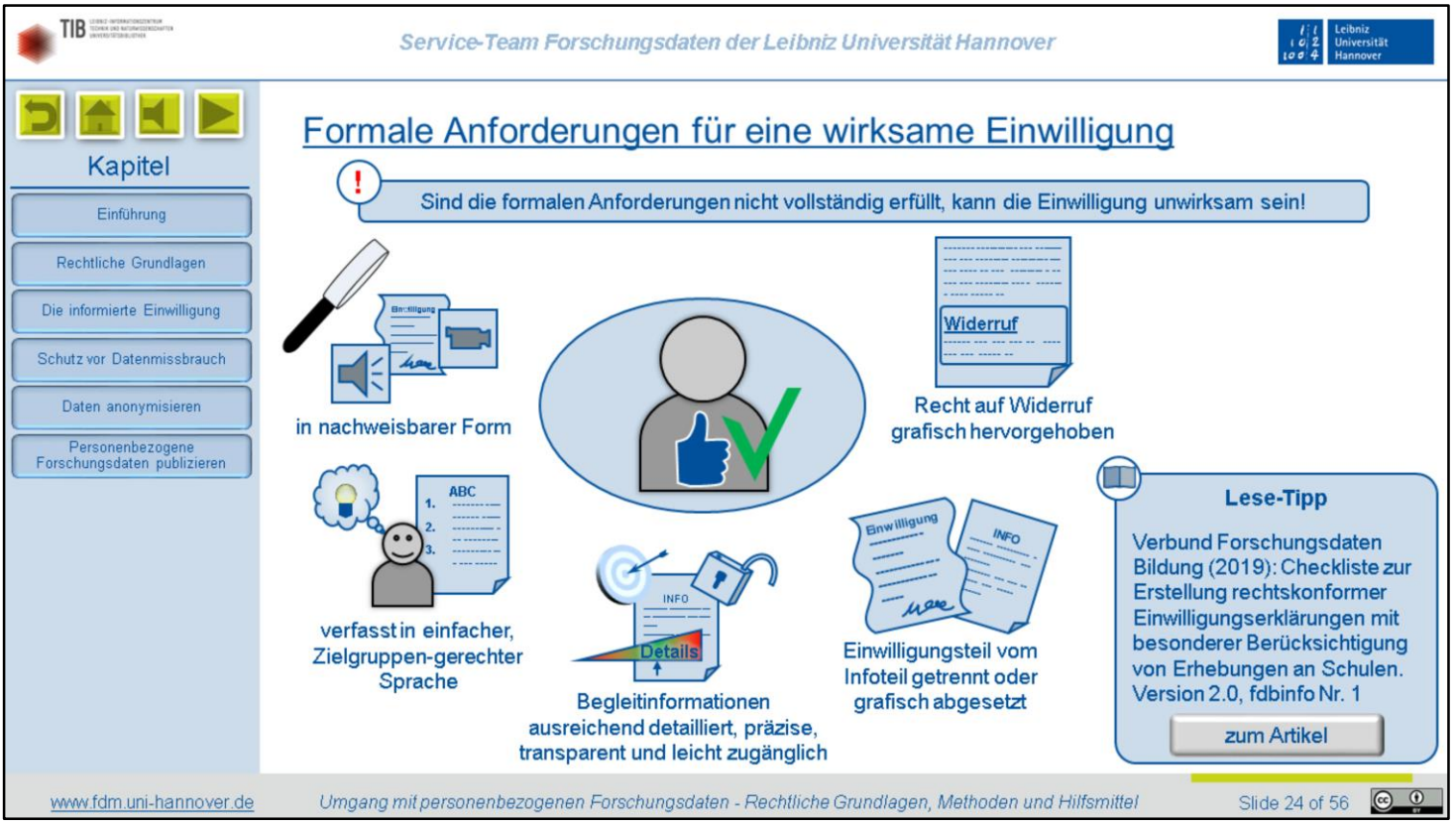


Bevor wir zu den formalen Anforderungen an eine Einwilligungserklärung kommen, noch eine Erläuterung zur Art der Datenerhebung. Wenn Sie selbst Daten bei den Betroffenen sammeln, handelt es sich um eine Direkterhebung. Im sozialwissenschaftlichen Kontext wäre das zum Beispiel der Fall, wenn Sie Personen interviewen oder wenn Sie Umfragen durchführen. Sie informieren dann die Betroffenen darüber, was Sie vorhaben und bitten sie um ihre aktive Mitwirkung. Die Betroffenen geben Ihnen dann also ihre Daten selbst.

Im Unterschied dazu handelt es sich bei einer Dritterhebung um eine Verarbeitung bereits vorhandener Daten ohne aktive Mitwirkung der Betroffenen. Das könnten zum Beispiel Daten des sozioökonomischen Panels sein. Diese Daten wurden von Anfang an per Direkterhebung zu wissenschaftlichen Zwecken gesammelt. Bei einer Nachnutzung würden die Betroffenen aber nicht erneut aktiv mitwirken müssen. Daher würde es sich bei der Nachnutzung dann um eine Dritterhebung handeln. Ein anderes Beispiel wäre die Auswertung von Daten, die von Behörden oder Social Media-Plattformen ursprünglich für einen nichtwissenschaftlichen Zweck gesammelt wurden. Solche Daten würden Sie bei der datenhaltenden Stelle anfordern. Diese Stelle sollte erst prüfen, ob sie die Daten überhaupt an Sie weitergeben darf und gibt sie dann gegebenenfalls an Sie heraus.

Eine Dritterhebung ist nur zulässig, wenn mindestens eine der folgenden Voraussetzungen zutrifft:

- Zunächst ist es möglich, dass die Betroffenen bereits bei der ursprünglichen Erhebung zugestimmt haben, dass die Daten später zu wissenschaftlichen Zwecken weitergegeben werden dürfen.
- Wenn nicht, könnten auch alle Betroffenen über die beabsichtigte neue Datenverarbeitung informiert und um ihr Einverständnis gebeten werden.
- Als letzte Möglichkeit könnte es sein, dass ein Gesetz die Verarbeitung gestattet, ohne dass die Betroffenen einwilligen müssen. Es kann aber sein, dass sie dennoch informiert werden müssen. Näheres regelt Art. 14 Absatz 5 der DSGVO.

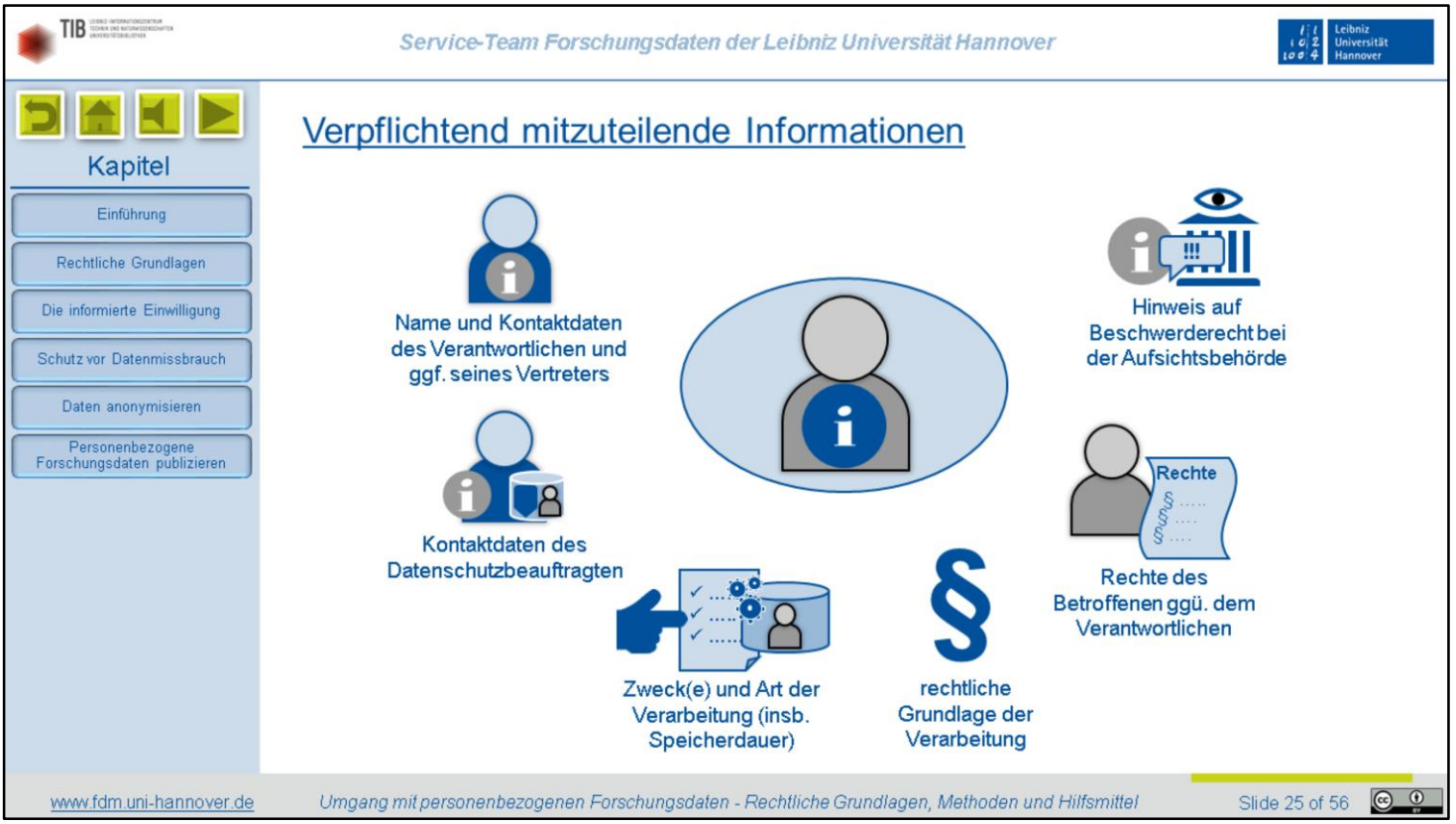


Damit eine Einwilligung der Betroffenen rechtlich wirksam ist, muss sie ein paar wichtige formale Anforderungen erfüllen. Zunächst einmal muss die Einwilligung nachweisbar sein. In dem meisten Fällen wird das durch die Unterschrift der Betroffenen unter ein entsprechendes Formular sichergestellt. Ebenfalls möglich wäre eine Ton- oder Video-Aufnahme und theoretisch sogar auch eine mündliche Aussage vor Zeugen ohne Aufzeichnung. Letzteres ist aber sehr unsicher, insbesondere wenn es um Zeiträume von mehreren Jahren geht.

Außerdem muss sichergestellt sein, dass die Betroffenen realistisch einschätzen können, in was sie einwilligen. Die Einwilligungserklärung und begleitende Informationsmaterialien müssen daher in einfacher, der Zielgruppe angemessener Sprache verfasst sein. Also verzichten Sie, soweit es geht, auf Bandwurm-Sätze, Substantivierungen, Passiv-Konstruktionen und Juristenkauderwelsch. Bedenken Sie, dass zum Beispiel Kinder oder Personen, deren Muttersprache nicht Deutsch ist, bestimmte Begriffe eventuell nicht verstehen.

Damit die Betroffenen wissen, in was sie einwilligen, müssen sie über alle relevanten Sachverhalte zum Zweck und zur Art der Datenverarbeitung in Kenntnis gesetzt und über ihre Rechte aufgeklärt werden. Diese Information muss angemessen detailliert, präzise, transparent und leicht zugänglich sein, zum Beispiel über ein Info-Blatt oder eine Webseite.

Die eigentliche Einwilligungserklärung muss von der begleitenden Information deutlich getrennt sein. Bei einer schriftlichen Einwilligung könnte es für beides jeweils ein eigenes Dokument geben, aber es ist auch möglich, die Einwilligung im selben Dokument grafisch abzuheben, zum Beispiel durch eine andere Schriftart oder Hintergrundfarbe. Innerhalb der Einwilligungserklärung ist wiederum das Widerrufsrecht hervorzuheben, zum Beispiel durch Fettdruck oder eine Umrahmung. Weitere Erläuterungen finden Sie in der Checkliste des Verbunds „Forschungsdaten Bildung“.



Wir haben in den vorherigen Folien bereits mehrfach darauf hingewiesen, wie wichtig es ist, dass die Betroffenen korrekt informiert werden, wenn ihre Daten verarbeitet werden sollen. Die DSGVO macht dazu sehr konkrete Vorgaben. Folgendes sollten Sie den Betroffenen am besten in Schriftform mitteilen:

Da wären zunächst der Name und die Kontaktdaten des Verantwortlichen. Im Forschungskontext ist das normalerweise die Projektleitung. Bei größeren Projekten könnte zusätzlich noch eine Person angegeben werden, die die Daten stellvertretend für die Projektleitung verarbeitet und primäre Ansprechstelle für die Betroffenen sein soll.

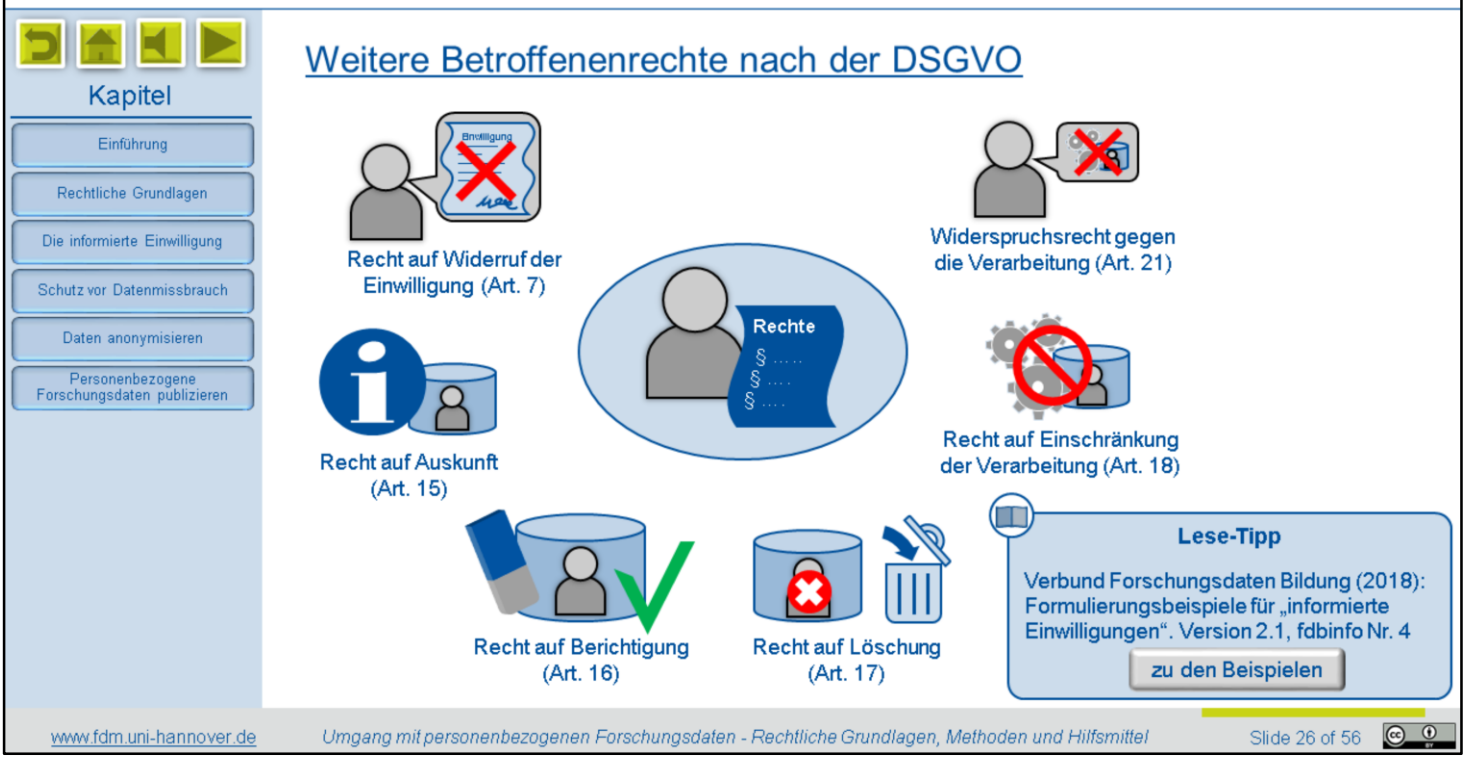
Ebenfalls anzugeben sind Name und Kontaktdaten der oder des Datenschutzbeauftragten der Institution, an der die Daten verarbeitet werden. Im Fall der LUH wäre das die Stabsstelle Datenschutz.

Ferner muss über Zweck und Art der Verarbeitung informiert werden. Hier ist insbesondere wichtig anzugeben, wo und wie lange die Daten in nicht-anonymer Form gespeichert werden sollen.

Des Weiteren ist die rechtliche Grundlage zu nennen, auf der die Verarbeitung erfolgen soll. Das wird meistens eine Einwilligung der Betroffenen sein. Aber auch in Fällen, in denen zwar keine Einwilligung erforderlich ist, wohl aber eine Informationspflicht besteht, darf diese Angabe nicht fehlen.

Außerdem haben die Betroffenen eine Reihe von Rechten gegenüber dem Verantwortlichen, die wir auf der nächsten Folie näher erläutern. Auf diese Rechte muss hingewiesen werden.

Und schließlich darf der Hinweis nicht fehlen, dass die Betroffenen ein Beschwerderecht bei der übergeordneten Aufsichtsbehörde haben. Das ist im Falle der LUH die niedersächsische Landesbeauftragte für den Datenschutz.



Zu Ihren Informationspflichten als Verantwortlicher gehört, dass Sie die Betroffenen auf ihre Rechte hinweisen.

Ganz wichtig ist das Recht auf Widerruf einer erteilten Einwilligung. Ein Widerruf muss jederzeit möglich sein. Die bereits erfolgte Verarbeitung vor Eingang des Widerrufs bleibt aber rechtmäßig. Sie sollten die Betroffenen ausdrücklich darauf hinweisen, dass ihre Mitwirkung bei der Datenerhebung freiwillig ist und dass ihnen im Falle eines Widerrufs keinerlei Nachteile entstehen. Denken Sie daran, dass dieses Recht bei einer schriftlichen Einwilligung grafisch hervorgehoben werden muss.

Die Betroffenen haben ferner das Recht, Auskunft zu verlangen, welche Daten über sie verarbeitet werden. Sollten die Daten offensichtlich fehlerhaft sein, besteht außerdem ein Recht auf Berichtigung. Klassische Fälle sind Zahlendreher in Adress- und Geburtsdaten oder Änderungen des Nachnamens aufgrund von Heirat oder Scheidung. Die Betroffenen können auch verlangen, dass die über sie gespeicherten Daten gelöscht werden, solange kein Gesetz die weitere Aufbewahrung gebietet. Bei den meisten zu rein wissenschaftlichen Zwecken erhobenen Daten besteht zwar kein gesetzliches Aufbewahrungsgebot. Sie dürfen aber unter Umständen trotzdem weiter aufbewahrt werden, wenn das für den Forschungszweck notwendig ist und bei einer informierten Einwilligung nichts Gegenteiliges zugesichert wurde. Das sollte dann von der Stabsstelle Datenschutz im Einzelfall geprüft werden.

Des Weiteren können die Betroffenen unter bestimmten Voraussetzungen verlangen, dass die Verarbeitung ihrer Daten eingeschränkt wird. In der Regel greift dieses Recht, wenn die Richtigkeit der Daten oder die Rechtmäßigkeit der Verarbeitung umstritten ist. Und schließlich gibt es noch das Recht, der Datenverarbeitung ganz zu widersprechen. Das gilt übrigens ausdrücklich auch für die Verarbeitung zu wissenschaftlichen Zwecken, wenn als Rechtsgrundlage keine Einwilligung, sondern ein „öffentliches Interesse“ nach Artikel 6, Absatz 1e herangezogen wurde.

In dem hier verlinkten Artikel finden Sie verschiedene Formulierungsbeispiele für DSGVO-konforme Einwilligungserklärungen.

Zusätzlich mitzuteilende Informationen in bestimmten Fällen

Wenn Daten an weitere Stellen übermittelt werden sollen

Empfänger der Daten
(oder Empfängerkategorien)

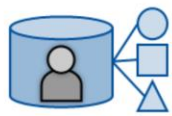
Bei Übermittlung ins Nicht-EU-Ausland:
Kann DSGVO-vergleichbarer
Datenschutz garantiert werden?

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?

Es gibt noch zwei Spezialfälle, in denen zusätzliche Informationspflichten bestehen: Wenn Sie beabsichtigen, die Daten an andere Stellen zu übermitteln, müssen Sie die Empfänger beziehungsweise die Empfängerkategorien benennen. Es könnte zum Beispiel sein, dass Sie Interviews von einem externen Fachdienst transkribieren lassen wollen. Darüber müssten Sie die Betroffen vorab informieren. Oder Sie bitten um Einwilligung, dass die Daten später auch in anderen Projekten ausgewertet werden dürfen. Dann wäre die Empfängerkategorie vielleicht „ausgewiesene Forschende aus dem Bereich der Sozial- und Wirtschaftswissenschaften“ oder so ähnlich.

Wenn Daten in ein Land außerhalb der EU oder an eine internationale Organisation übermittelt werden sollen, dann geben Sie an, ob ein Datenschutz-Niveau garantiert werden kann, das dem der DSGVO vergleichbar ist. Eine solche Garantie kann zum Beispiel ein Angemessenheitsbeschluss der EU-Kommission sein. Eine Liste der Drittstaaten, zu denen es solche Beschlüsse bereits gibt, finden Sie auf der hier verlinkten Webseite. Informieren Sie in jedem Fall, welche Art von Garantie es gibt und wo eine Kopie dieser Garantie verfügbar ist.

Der zweite Spezialfall ist die Dritterhebung, wenn Sie also Daten verarbeiten möchten, die bereits an anderer Stelle gesammelt wurden. Hier müssen Sie die betroffenen Personen darüber informieren, welche Kategorien von Daten Sie verarbeiten möchten, aus welchen Quellen diese Daten stammen und ob die Quellen öffentlich zugänglich sind.

Und nun noch einmal auf einen Blick, in welcher Reihenfolge Sie was unternehmen sollten, wenn Sie mit personenbezogenen Daten auf der Grundlage von Einwilligungserklärungen arbeiten. Als erstes sollten Sie den Umgang mit Daten im gesamten Projektverlauf detailliert durchplanen. Bedenken Sie dabei auch Aspekte, die über die Projektlaufzeit hinaus relevant sind. Das betrifft zum Beispiel eine Archivierung der Daten, eine Verwendung in der Lehre oder eine Neuauswertung in Folgeprojekten.

Entwerfen Sie dann die Einwilligungserklärung und das dazugehörige Info-Blatt. Stimmen Sie anschließend beides mit der Stabsstelle Datenschutz ab. Jetzt können Sie anfangen, die Betroffenen zu informieren und sie um ihre Einwilligung zu bitten. Erst wenn die vorliegt dürfen Sie mit der Datenerhebung und -verarbeitung beginnen!

Pseudonymisieren Sie die Daten möglichst unmittelbar nach der Erhebung und trennen Sie die Schlüsselliste von den übrigen Daten. Anonymisieren Sie Merkmale, über die eine Person indirekt identifiziert werden könnte, und vernichten Sie die Schlüsselliste sobald der Forschungszweck dies zulässt.

Sollte sich im Nachhinein ergeben, dass die Daten auf eine andere Art oder für einen anderen Zweck verarbeitet werden sollen, als ursprünglich mit den Betroffenen vereinbart, dann informieren Sie alle Betroffenen und bitten Sie sie erneut um ihre Einwilligung.

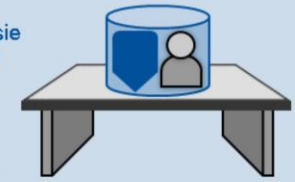
Falls ein Betroffener seine Einwilligung später widerruft, löschen Sie umgehend die Daten zu dieser Person. Wenn Sie mit den Betroffenen eine Höchstspeicherdauer vereinbart haben, sorgen Sie dafür, dass die Daten nach Ablauf dieser Frist auch tatsächlich gelöscht werden. Je länger die beabsichtigte Aufbewahrung, desto größer die Wahrscheinlichkeit, dass dies in Vergessenheit gerät… Falls Sie schon beim Archivieren ein Datum angeben können, an dem die Daten automatisiert gelöscht werden, sollten Sie diese Möglichkeit nutzen.

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

Wir nähern uns nun dem Ende des Teils, in dem es eher um die rechtlichen und formalen Fragen geht. Bevor wir in den nächsten Kapiteln zu den eher praktischen Dingen kommen, möchten wir noch einmal ausdrücklich auf die Unterstützungsangebote der Stabsstelle Datenschutz hinweisen.

Die Stabsstelle ist verpflichtet, alle an der LUH stattfindenden Verarbeitungen personenbezogener Daten in einem Verzeichnis zu erfassen. Da das auch die Forschung betrifft, sagen Sie dort bitte Bescheid, wenn Sie in Ihrem Projekt mit entsprechenden Daten arbeiten.

Wenn Sie Einwilligungserklärungen und Infoblätter entwerfen, stimmen Sie die Entwürfe bitte unbedingt mit der Stabsstelle ab.

Sollte es vorkommen, das personenbezogene Daten von Unbefugten eingesehen wurden oder das zumindest theoretisch möglich gewesen wäre, sind Sie verpflichtet, dass der Stabsstelle zu melden. Wenn beispielsweise ein unverschlüsselter USB-Stick mit sensible Daten verloren geht oder durch einen Hackerangriff Daten abgegriffen wurden, dann muss das angezeigt werden!

Ansonsten steht Ihnen die Stabsstelle auch bei allen weiteren Anliegen rund um das Thema Datenschutz gerne mit Rat und Tat zur Seite. Das gilt insbesondere auch für rechtliche Fragen.

Weitere Infos, Handreichungen, Vorlagen und Muster

Lese-Tipps

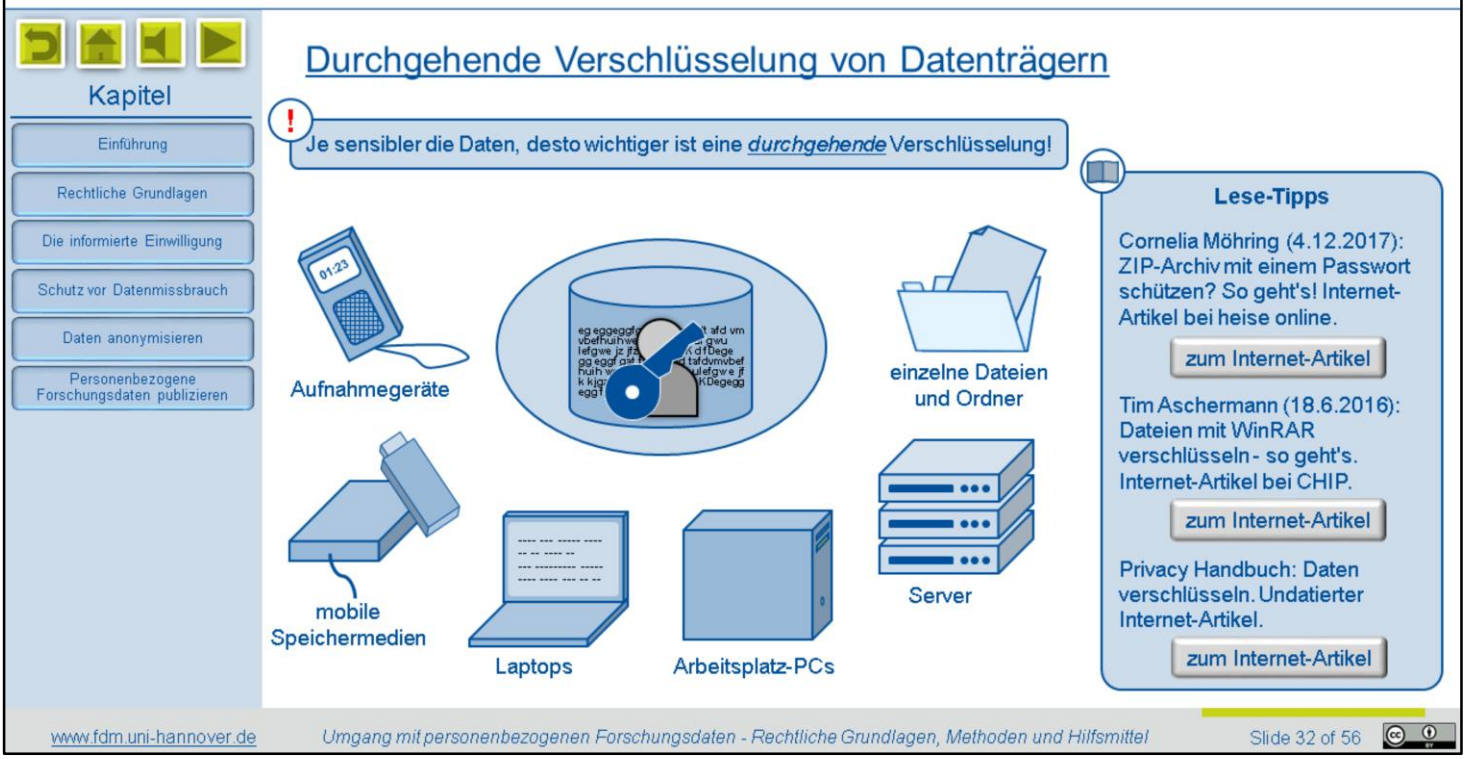
- Beschäftigtenportal der LUH (diverse Handreichungen und Vorlagen, nur aus dem LUH-Netz erreichbar)
- Zentrale Datenschutzstelle der baden-württembergischen Universitäten (Infos, Checklisten, Vorlagen rund um die DSGVO)
- Rat für Sozial- und Wirtschaftsdaten (Datenschutz allgemein)
- forschungsdaten.info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

Dies ist nun wirklich die allerletzte Folie dieses Kapitels. Hier haben wir noch ein paar Lesetipps und Links zu nützlichen Seiten mit weiterführender Information für Sie zusammengestellt. Dort finden Sie auch Praxisbeispiele und Vorlagen, die Sie für Ihr Projekt anpassen können.

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

Wie wir gesehen haben, verlangen sowohl die Europäische Datenschutzgrundverordnung als auch das Niedersächsische Datenschutzgesetzt, dass Sie als Verantwortliche angemessene technische und organisatorische Schutzmaßnahmen ergreifen. Welche das sein können, werden wir Ihnen in diesem Kapitel vorstellen.



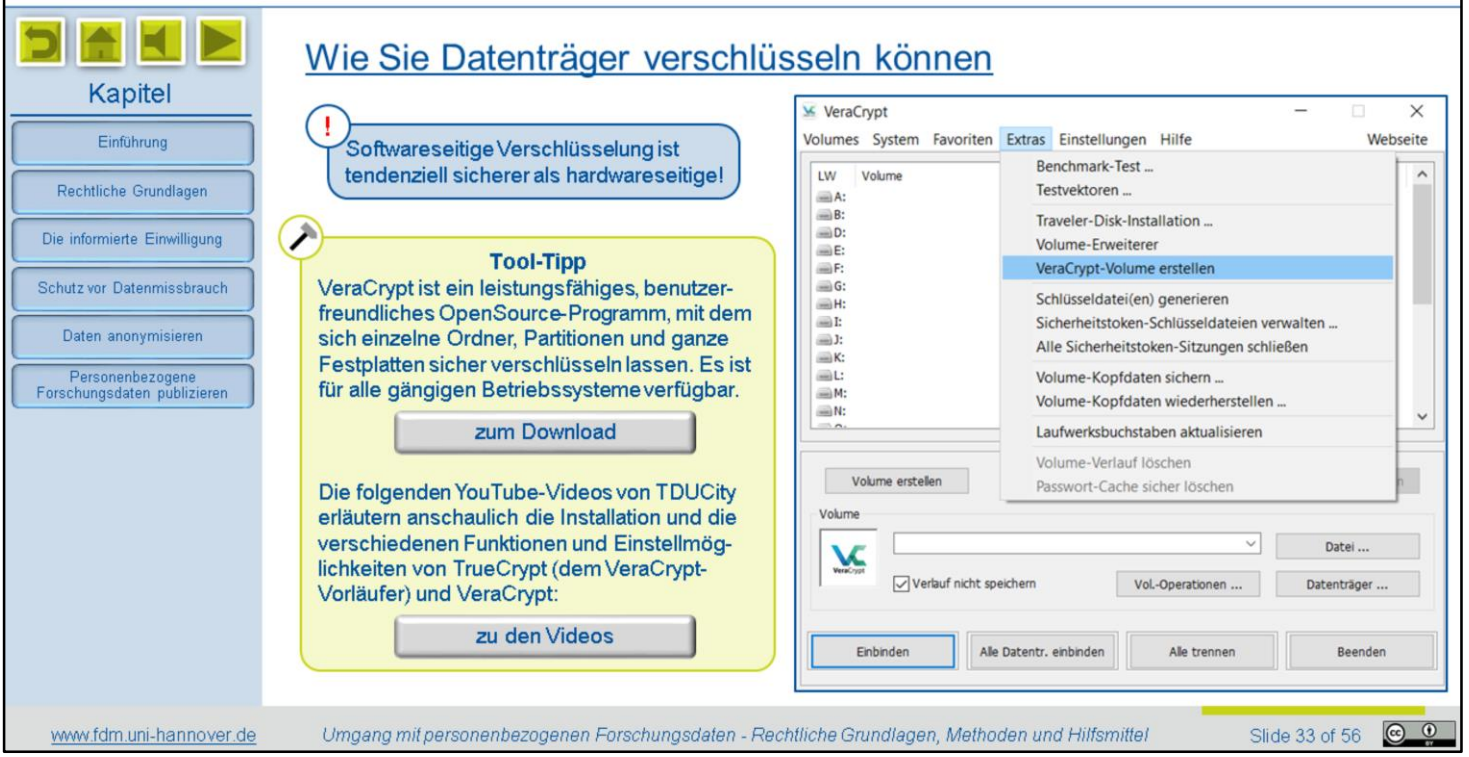
Die wichtigste technische Maßnahme zum Schutz Ihrer Daten ist die Verschlüsselung von Dateien und ganzen Datenträgern. Bitte machen Sie sich vor dem Sammeln von Daten Gedanken, auf welchen Medien im Laufe des Forschungsprozesses Daten gespeichert werden, und sei es auch nur temporär. So, wie bei verderblichen Lebensmitteln eine geschlossene Kühlkette wichtig ist, sollten Sie bei personenbezogenen Daten auf eine durchgehende Verschlüsselung achten.

Das beginnt bereits bei Aufnahmegeräten wie Diktiergeräten. Leider haben derzeit nur einige teure High-End-Modelle eine Verschlüsselungsfunktion. Dennoch sollten Sie diese Investition nicht scheuen, denn ein kleines mobiles Gerät geht schnell mal verloren. Bei unverschlüsselten Geräten könnte sich jeder zufällige Finder problemlos Ihre letzten Interviews anhören. Dasselbe gilt übrigens für USB-Sticks und externe Festplatten.

Auch bei Laptops mit unverschlüsselten Festplatten ist leicht an die Daten zu kommen. Das Login-Passwort Ihres Betriebssystems schützt Sie übrigens nicht, da man das Gerät zum Beispiel mit einer live-CD starten oder die Festplatte ausbauen und an ein anderes Gerät anschließen könnte. Laptops werden häufiger mal gestohlen oder in der Bahn vergessen…

Bei PCs ist die Wahrscheinlichkeit eines Verlustes geringer, aber auch Einbrüche in Uni-Gebäude kommen durchaus vor. Wenn Sie Originaldaten oder Backup-Kopien auf Servern Ihres Instituts oder Rechenzentrums gespeichert haben, stehen diese normalerweise in gut gesicherten Räumen.

Und zu guter Letzt: Denken Sie bitte auch ein einzelne Dateien oder Ordner, die Sie mal eben per E-Mail-Anhang verschicken oder bei einem kommerziellen File Hoster ablegen. Beides sollten Sie vermeiden. Aber wenn es wirklich unumgänglich ist, dann verschlüsseln Sie die Dateien vorher! Eine einfache Möglichkeit ist das Verschlüsseln beim Erstellen einer Archivdatei mit Programmen wie 7zip oder WinRAR, wie in unseren Lesetipps beschrieben. Zur Verschlüsselung ganzer E-Mails samt Anhang kommen wir gleich noch.

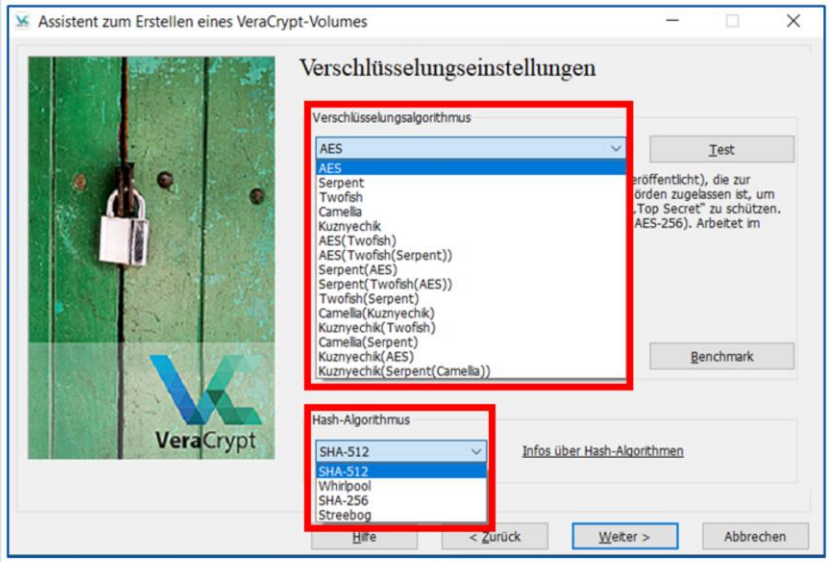


Viele aktuelle Geräte wie Laptops, Smartphones und externe SSD-Festplatten verschlüsseln von sich aus. Dabei übernimmt ein im Gerät verbauter Mikroprozessor die Verschlüsselung. Diese Funktion ist aber nicht immer ab Werk aktiviert. In der Vergangenheit sind bei solcher hardwareseitiger Verschlüsselung außerdem immer wieder gravierende Sicherheitslücken bekannt geworden, die sich oft selbst mit Firmware-Updates nicht beheben lassen.

Sicherer ist daher eine softwareseitige Verschlüsselung durch ein Verschlüsselungsprogramm. Das Windows-Betriebssystem beinhaltet dafür das Programm Bitlocker, allerdings nur in der Windows Pro-Version. MacOS bietet zur Verschlüsselung FileVault an. Wir empfehlen das kostenlose Open Source-Programm Veracrypt, das auf allen gängigen Betriebssystemen läuft.

Mit VeraCrypt können Sie Partitionen oder ganze Festplatten verschlüsseln, aber auch einzelne Container-Dateien. Ein solcher Container funktioniert wie ein Ordner, der beliebig viele Dateien und Unterordner enthalten kann. Er verhält sich ansonsten aber wie eine ganz normale Datei, die sich also auch einfach verschieben, verschicken oder löschen lässt. Der hier verlinkte YouTube-Kanal von TDUCity enthält sehr anschauliche Video-Tutorials, in denen die einzelnen Funktionen und Einstellmöglichkeiten von VeraCrypt und seinem Vorläufer TrueCrypt erklärt werden.

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

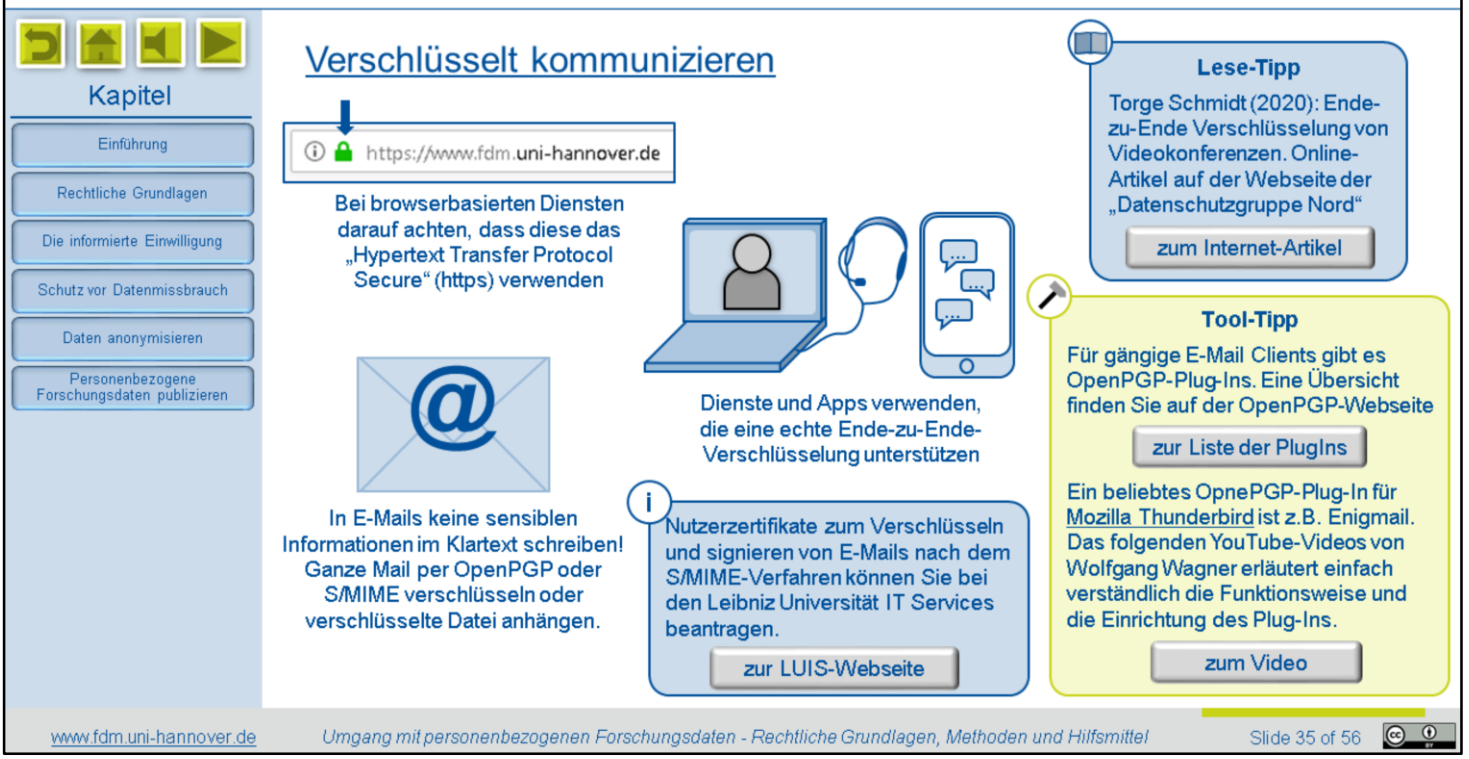
Beim Verschlüsseln werden nach einem bestimmten Algorithmus einerseits Werte durch andere ersetzt und andererseits die relativen Positionen dieser Werte verändert. Auf diese Weise geht der Sinnzusammenhang von Zeichenketten verloren, und Code ist nicht mehr ausführbar. Bei der Verschlüsselung von Datenträgern kommen gewöhnlich symmetrische Verschlüsselungsverfahren zum Einsatz. Das bedeutet, dass zum Ver- und Entschlüsseln derselbe Schlüssel verwendet wird. In der Regel ist das ein Passwort, aber es könnte auch ein Hardwareschlüssel oder ein biometrisches Merkmal, wie zum Beispiel ein Fingerabdruck, sein.

Moderne Algorithmen verschlüsseln Daten in Blöcken unterschiedlicher bit-Größe. Seit etwa 20 Jahren gibt es den Advanced Encryption Standard, kurz AES, der damals den nicht mehr ausreichend sicheren Data Encryption Standard DES ablöste. AES ist der bei symmetrischer Blockverschlüsselung wohl am häufigsten eingesetzte Algorithmus und gilt noch immer als sehr sicher. Es gibt verschiedene Varianten, die sich in der maximalen Größe der zu verschlüsselnden Datenblöcke unterscheiden. Je größer diese Wert, desto mehr kann die Blocklänge beim Verschlüsseln variieren, was die Sicherheit erhöht. Aktuell gilt AES-256-bit für die allermeisten Fälle als ausreichend sicher. Wenn Sie extrem sensible Daten verschlüsseln wollen, können Sie aber zusätzliche Sicherheitsmaßnahmen treffen.

Daten sind dann am sichersten, wenn ein potentieller Angreifer gar nicht weiß, dass sie existieren. Daher können Sie mit Veracrypt auch versteckte Partitionen erstellen, bei denen nicht erkennbar ist, dass sie überhaupt Daten enthalten. Dieses Vorgehen bietet sich an, wenn Sie in unsicheren Gegenden vor Ort Daten erheben, und die Gefahr besteht, dass Sie zur Herausgabe Ihres Passwortes gezwungen werden.

Ferner können Sie mehrere unterschiedliche Verschlüsselungsalgorithmen verschachteln. Die bereits verschlüsselten Daten werden dann also mit einem anderen Algorithmus noch einmal verschlüsselt. Sollte der äußere Algorithmus geknackt werden, sind die Daten dann immer noch geschützt. Der Nachteil ist, dass sich dadurch die Zugriffszeit erhöht, wenn Sie mit den Daten arbeiten.

Als weitere Maßnahme können Sie statt des voreingestellten SHA-512 Hash-Algorithmuses eine weniger verbreitete Alternative auswählen. Dadurch werden sogenannte Brute Force-Attacken erschwert, bei denen mit hohem Rechenaufwand einfach alle denkbaren Schlüssel in Kombination mit dem Hash durchprobiert werden. Da ein Angreifer wahrscheinlich zuerst die Standard-Einstellungen durchtesten wird, kann die Wahl ungewöhnlicher Verschlüsselungs- und Hash-Algorithmen den Angriff erheblich erschweren.



Verschlüsselung kann nicht nur beim Aufbewahren von Daten wichtig sein, sondern auch bei der Übertragung. Wenn Sie also mit digitalen Hilfsmitteln über sensible Informationen kommunizieren, nutzen Sie eine verschlüsselte Übertragung! Achten Sie bei allen browserbasierten Anwendungen darauf, dass diese das „Hypertext Transfer Protocol Secure“ verwenden. Die URL beginnt dann mit den Buchstaben „https“. Daneben sollte ein kleines Schloss-Symbol angezeigt werden.

Die meisten Messenger-Dienste und Telefonie-Programme werben inzwischen damit, eine sogenannte Ende-zu-Ende-Verschlüsselung implementiert zu haben. Das heißt eigentlich, dass die Datenpakete vor dem Senden verschlüsselt und erst nach Eingang auf dem Empfängergerät wieder entschlüsselt werden. Dadurch wird verhindert, dass auf dem Übertragungsweg Daten im Klartext von Dritten eingesehen werden können. De facto handelt es sich aber oft nur um eine Transportverschlüsselung bis zum Server des Dienstanbieters. Dort kann der Anbieter die Daten theoretisch einsehen, bevor Sie dann wieder verschlüsselt an die eigentlichen Kommunikationspartner weitergeleitet werden. Wenn es sich dabei um externe kommerzielle Anbieter handelt, deren Server zudem oft noch außerhalb des Gültigkeitsbereiches der DSGVO betrieben werden, kann das problematisch sein. Prüfen Sie daher, ob die von Ihnen verwendeten Apps und Dienste eine echte Ende-zu-Ende-Verschlüsselung unterstützen, bevor Sie sie für sensible Kommunikation verwenden. Für Video-Konferenzen können Sie sich dabei an der hier verlinkten Studie von Torge Schmidt orientieren. Dienste, die direkt von Ihrer Forschungsinstitution betrieben werden, sind normalerweise gut geschützt und vertrauenswürdig.

Für die Kommunikation per E-Mail bietet sich eine Verschlüsselung nach dem OpenPGP- oder dem S/MIME-Verfahren an. Das sind asymmetrische Verschlüsselungsverfahren, bei denen jeder Kommunikationsteilnehmer über einen öffentlichen und einen privaten Schlüssel verfügt. Den öffentlichen darf und soll jeder kennen. Damit kann eine Nachricht für die betreffende Person verschlüsselt werden. Zum Entschlüsseln wird aber zusätzlich der private Schlüssel benötigt, den ausschließlich derjenige kennt, für den die Nachricht bestimmt ist. Für beide Verfahren gibt es Plugins für E-Mail-Clients, wie Outlook und Thunderbird, oder die Clients haben bereits von Haus aus entsprechende Funktionen implementiert. Für das S/MIME-Verfahren benötigen Sie ein Nutzerzertifikat, dass Ihre Identität und Vertrauenswürdigkeit bestätigt. Solche Zertifikate könne Sie beim LUIS beantragen.

Rechtemanagement

Ordner, Dateien, Seitenbereiche

Rechte (Beispiele)

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

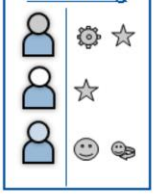
Das zuverlässige Einrichten und Verwalten von Berechtigungen erfordert IT-Fachkenntnisse und ggf. spezielle Software. Berücksichtigen Sie dies in Ihrer Projekt- und Ressourcenplanung!

Datensatz-Gruppen in Datenbanken

Nutzergruppen (Beispiele)

- IT-Admins
- Projektleitung
- Mitarbeitende
- Externe Partner

Gruppen-zuordnung



LOG

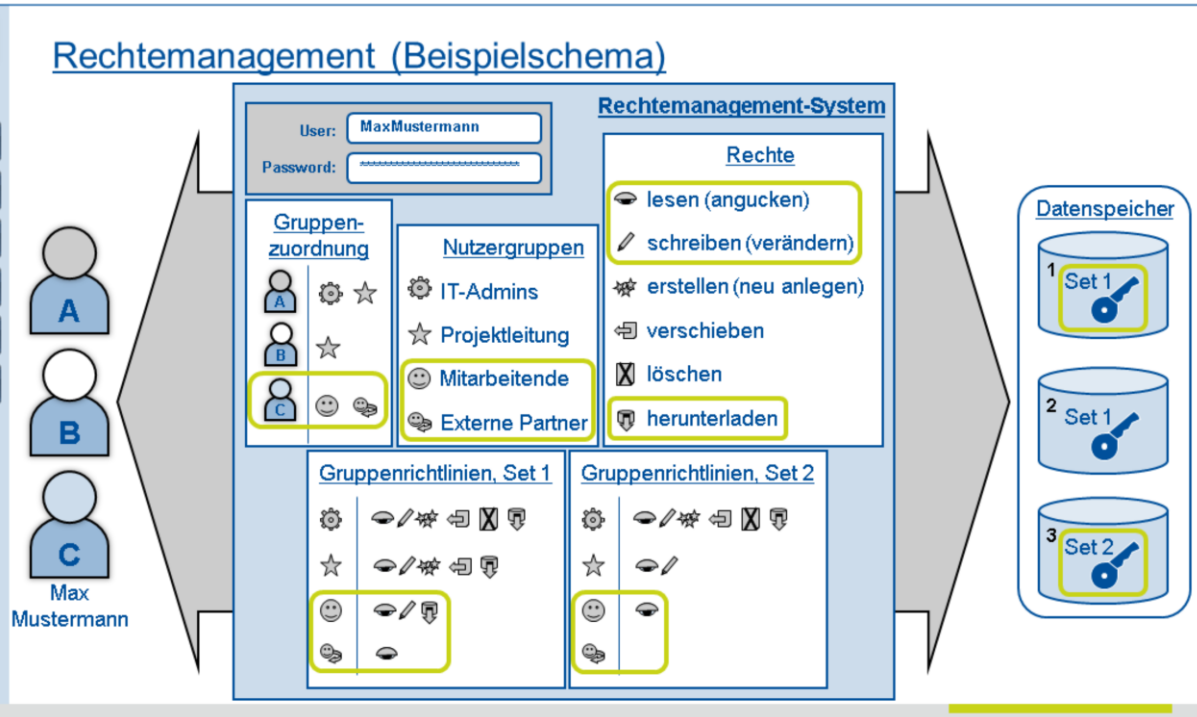
Datum	Uhrzeit	Nutzer	Aktion
.....	....	.....	.....
.....	.....	....	.....
.....	....	.....	.....
.....	.....	....	.....

Neben der Verschlüsselung ist das Einrichten eines angemessenen Managements von Berechtigungen eine sinnvolle Maßnahme, um unbefugte Datenzugriffe zu verhindern. Solche Rechte können sich auf einzelne Dateien und Ordner oder ganze Ordnerbäume beziehen, aber zum Beispiel auch auf bestimmte Gruppen von Datensätzen innerhalb einer Datenbank. Je nach Programm oder Dateisystem können Nutzerrechte unterschiedlich stark differenziert vergeben werden. Auf der einfachsten Ebene lässt sich meist unterscheiden zwischen kombinierten Lese- und Schreibrechten, reinen Leserechten und überhaupt keinen Zugriffsrechten. Die Schreibrechte lassen sich manchmal weiter differenzieren, so dass z.B. jemand das Recht haben könnte, eine Datei zu verändern, aber nicht, sie zu löschen.

In der Regel ist es ratsam, das Einstellen der Berechtigungen durch IT-Fachpersonal vornehmen zu lassen, da fehlerhafte Konfigurationen zu Datenverlust oder Sicherheitslücken führen können. Das sollten Sie in Ihrer Projekt- und Ressourcenplanung berücksichtigen.

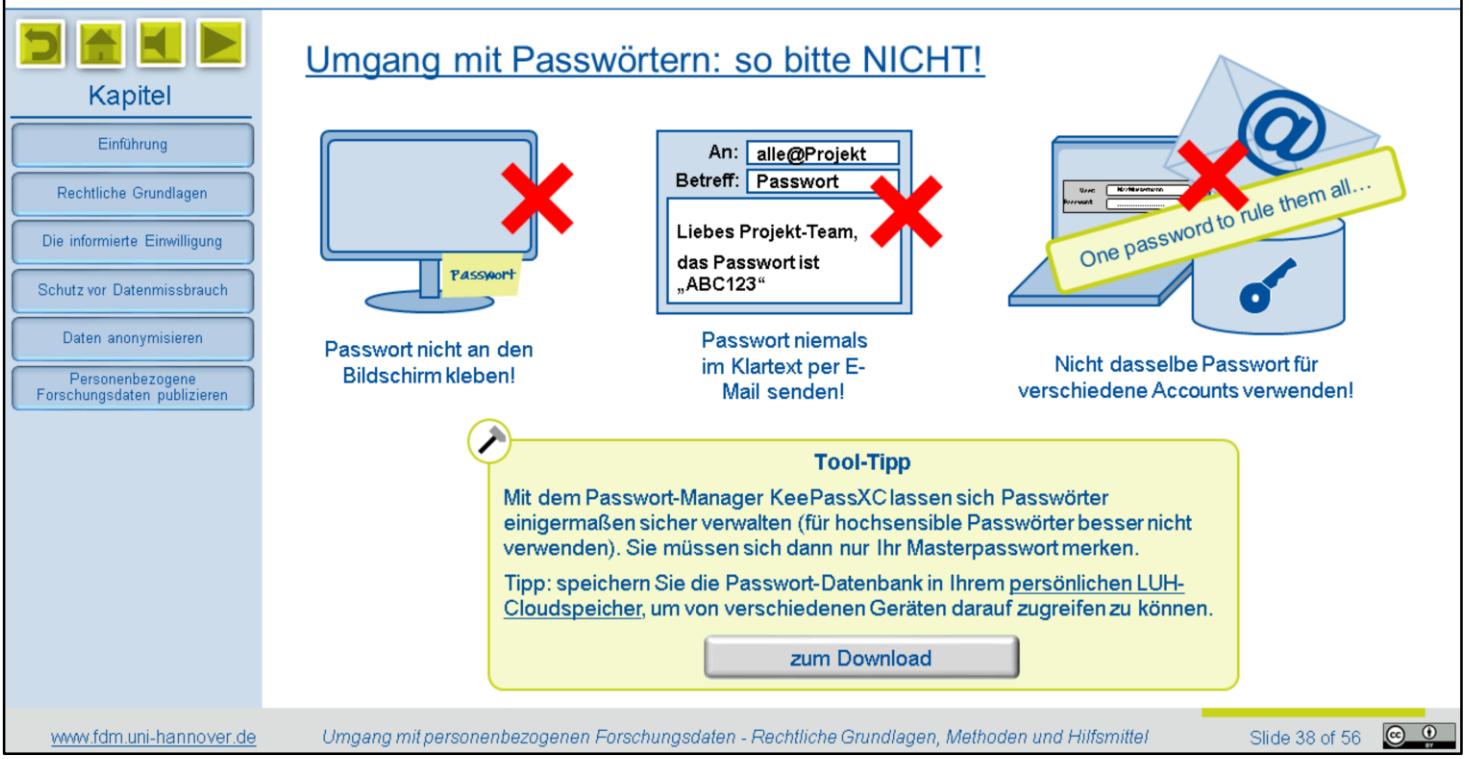
Berechtigungen können individuell vergeben werden. Bei größeren Systemen, die viele Nutzer verwalten, kommen aber gewöhnlich sogenannte Gruppenrichtlinien zum Einsatz. Dabei werden die Rechte für eine ganze Gruppe festgelegt und vererben sich an alle Personen, die Mitglied der jeweiligen Gruppe sind. Eine Person kann aber durchaus mehreren Gruppen angehören und deren jeweilige Rechte erben.

Viele Rechte-Management-Systeme bieten außerdem die Möglichkeit, Dateizugriffe mitzuloggen. Im Falle eines Sicherheitsvorfalls kann dann zum Beispiel nachvollzogen werden, über wessen Account Daten abgegriffen wurden.



Hier mal ein schematisches Beispiel, wie so ein Rechtemanagement-System funktionieren kann. Sagen wir, der Nutzer Max Mustermann möchte eine Datei aus dem Ordner 1 öffnen. Herr Mustermann loggt sich mit seinem Benutzernamen und Passwort ins System ein. Das System weiß, dass er den Gruppen „Mitarbeitende“ und „Externe Partner“ angehört. Nach dem Rechte-Set1 darf er Dateien aus dem Ordner 1 daher lesen, verändern und herunterladen, aber zum Beispiel nicht löschen oder neu erstellen.

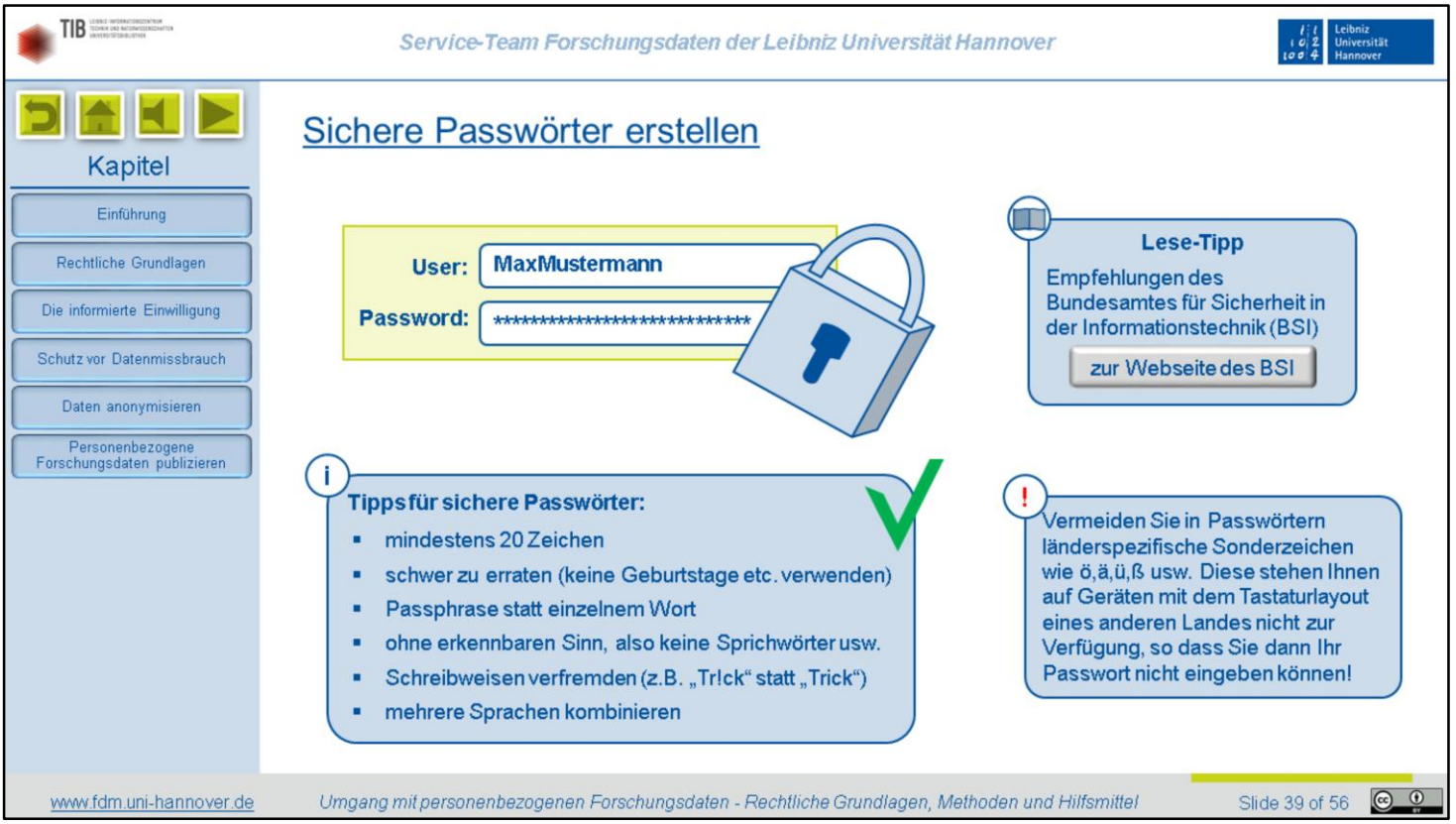
Nun möchte Herr Mustermann noch eine Datei aus dem Ordner 3 herunterladen. Jetzt wird er eine Fehlermeldung bekommen, dass er nicht die nötigen Rechte besitzt. Denn für Ordner 3 gilt das Rechte-Set 2 und nach dem darf Herr Mustermann als Mitarbeitender die Dateien nur lesen, aber nicht herunterladen. Wäre er nur externer Partner, dürfte er nicht einmal das.



Jede Hochsicherheits-Verschlüsselung und jedes noch so ausgeklügelte Rechtemanagement sind letztlich wertlos, wenn die verwendeten Passwörter unsicher sind oder nicht geheim gehalten werden. Die meisten Angriffe konzentrieren sich daher nicht auf das Brechen von Algorithmen oder das Umgehen von Rechte-Abfragen, sondern auf das Abgreifen von Passwörtern. Leider ist das häufig immer noch viel zu einfach möglich. Hier ein paar Tipps, die vielleicht banal klingen, aber trotzdem oft ignoriert werden:

- Bitte kleben Sie Ihre Passwörter nicht als Post-It an den Bildschirm! Jeder, der Zutritt zu Ihrem Büro hat, ist dann in der Lage, Ihre Daten zu entschlüsseln oder Ihre Zugänge zu nutzen! Das betrifft nicht nur Kolleginnen und Kollegen, sondern theoretisch auch Reinigungspersonal, Hausmeister oder auch Einbrecher. Grundsätzlich kann es durchaus sicherer sein, Passwörter aufzuschreiben, statt sie digital zu speichern. Aber verwahren Sie sie dann bitte an einem sicheren, abschließbaren Ort, z.B. in einem Tresor.
- Verschicken Sie Passwörter niemals im Klartext per E-Mail! Einerseits können unverschlüsselte E-Mails auf dem Übertragungsweg leicht abgefangen und mitgelesen werden. Andererseits werden Mails manchmal achtlos weitergeleitet, ohne vorher zu prüfen, ob irgendwo im Kommunikationsverlauf noch sensible Informationen enthalten sind, die nicht für den Empfänger der Weiterleitung bestimmt sind.
- Und schließlich sollten Sie auch darauf verzichten, für mehrere Accounts immer dasselbe Passwort zu verwenden. Sonst laufen Sie Gefahr, dass alle Ihre Nutzerkonten missbraucht werden können, sobald einmal das Passwort in falsche Hände gerät. Es ist klar, dass es in der Praxis völlig unrealistisch ist, sich für alles ein extra-Passwort zu merken. Aber gerade wenn es um sensible Daten oder kritische Infrastrukturen geht, denken Sie sich zumindest dafür jeweils eigene Passwörter aus.

Eine praktische Möglichkeit, Zugangsdaten für weniger sensible Systeme zu verwalten, bietet ein Passwort-Manager wie KeePass. In diesem Fall brauchen Sie sich nur ein einziges sicheres Masterpasswort zu merken.

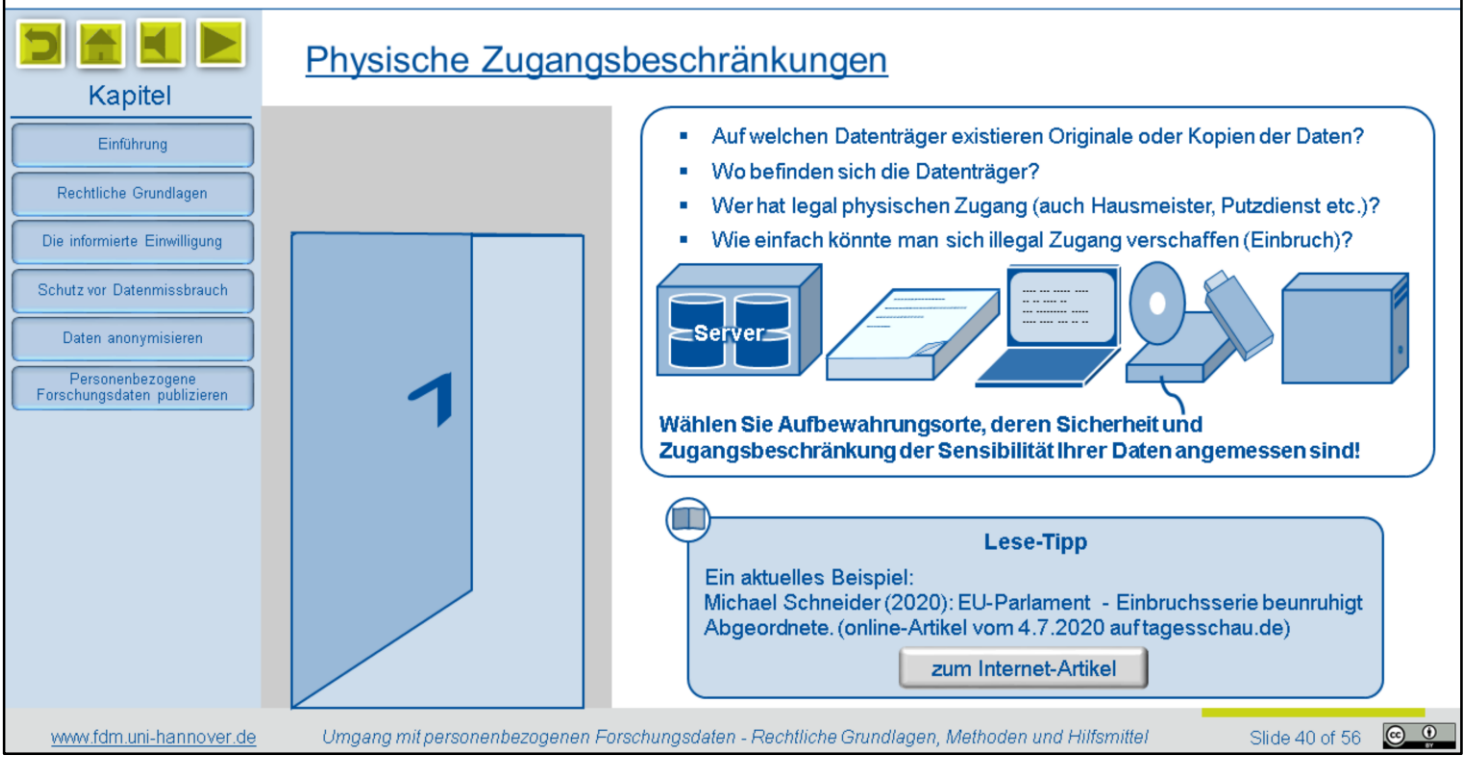


Wie sollte nun ein sicheres Passwort aussehen? Theoretisch hängt die Sicherheit eines Passwortes ausschließlich an dessen Länge. Das gilt jedenfalls, wenn es um Brute-Force-Attacken geht, bei denen einfach alle denkbaren Zeichenkombinationen durchgetestet werden. Nach derzeitigem Stand der Technik gibt es ab einer Länge von etwa 20 Zeichen so viele mögliche Kombinationen, dass nur wenige Angreifer über die nötige Rechenpower und Geduld verfügen. Daher sollten Passwörter für sensible Anwendungen mindestens 20 Zeichen lang sein.

In der Praxis werden Angreifer aber versuchen, zunächst besonders wahrscheinliche Zeichenkombinationen durchzutesten. Das können beliebte Passwörter wie „123456“ sein, oder Wörter, wie sie in einem elektronischen Wörterbuch stehen. Wenn der Angriff sehr gezielt erfolgt, werden eventuell auch recherchierte Daten der angegriffenen Person und ihres Umfeldes durchprobiert. Das sind zum Beispiel Geburtsdaten, Telefonnummern, Nummernschilder oder Kosenamen. Auch Kombinationen solcher Daten oder deren umgedrehte Zahlen- beziehungsweise Buchstabenreihenfolgen sind unsicher. Verwenden Sie daher keine recherchierbaren persönlichen Daten als Passwort!

Damit Sie sich auch ein langes Passwort gut merken können, können Sie eine Passphrase verwenden, also eine Zusammenstellung mehrerer Wörter. Diese sollte nicht unbedingt einen Sinn ergeben, damit sie schwerer zu erraten ist. Ein gängiges Sprichwort ist also eher nicht geeignet. Sie können außerdem die Schreibweise der Wörter verfremden, indem Sie zum Beispiel bestimmte Buchstaben durch ähnlich aussehende Sonderzeichen ersetzen. Und schließlich können Sie auch noch mehrere Sprachen kombinieren, also zum Beispiel deutsche und englische Wörter mischen. Sollten Sie zufällig Bretonisch beherrschen, umso besser… Weitere Tipps finden Sie auf der hier verlinkten Webseite des Bundesamtes für Sicherheit in der Informationstechnik.

Und noch ein letzter Hinweis: Vermeiden Sie in Ihren Passwörtern länderspezifische Sonderzeichen! Sie können sonst schlimmstenfalls Ihr Passwort nicht eingeben, wenn Sie an einem Gerät mit dem Tastaturlayout eines anderen Landes sitzen!



Die allermeisten Versuche, unbefugt Daten abzugreifen, erfolgen über das Internet. Doch selbst, wenn keine Netzanbindung besteht, könnte ein Angreifer so weit gehen, sich direkt physischen Zugang zu den Datenträgern zu verschaffen. Wenn Sie mit Daten arbeiten, die für sehr versierte und skrupellose Angreifer interessant sein könnten, machen Sie sich daher auch über die physischen Zugangsmöglichkeiten zu Ihren Datenträgern Gedanken. Insbesondere sollten Sie sich folgende Fragen stellen:

- Auf welchen Datenträger existieren Originale oder Kopien der Daten? Denken Sie dabei auch an E-Mail-Anhänge, externe Speichermedien, Papier-Ausdrucke und Backup-Server
- Wo befinden sich die Datenträger? Ein zusätzlichen Sicherheits-Backup auf dem privaten USB-Stick in der Hosentasche kann hier schnell zum Unsicherheitsfaktor werden. Bei der Nutzung von Cloudspeichern sollten Sie sich informieren, wo die Server stehen und wie sie gesichert sind. Sind solche Informationen nicht zu bekommen, verzichten Sie auf die Nutzung.
- Wer hat legal physischen Zugang? Wenn die Daten auf der Festplatte Ihres Arbeitsplatzrechners liegen sollten, hätten zum Beispiel Kolleginnen und Kollegen, der Hausmeister oder der Putzdienst Zugang. Bei zentralen Servern ist es mindestens das IT-Personal der Einrichtung, die die Server betreibt.
- Wie einfach könnte man sich illegal Zugang verschaffen, indem man also in die Räume einbricht, in denen die Datenträger aufbewahrt werden? Ein fensterloser Serverraum mit Stahltür ist da deutlich sicherer als ein Büroraum in Erdgeschoss mit großen Fenstern.

Wer solche Überlegungen für blanke Paranoia hält, dem sei unser Lesetipp ans Herz gelegt. Nach einer Einbruchsserie im EU-Parlament, bei der offenbar gezielt Datenträger entwendet wurden, rätselt man dort gerade, ob vielleicht sogar der eigene Sicherheitsdienst darin verstrickt ist…

Neben den vorgestellten technischen Vorkehrungen, sollten Sie die Sicherheit Ihrer Daten durch einfache organisatorische Maßnahmen weiter erhöhen. Ganz wichtig ist, dass alle Personen, die in Ihren Projekten personenbezogene Daten verarbeiten, angemessen geschult und sensibilisiert werden. Sie könnten also beispielsweise verpflichtet werden, sich einmal mit diesem online-Kurs zu beschäftigen, oder an einer Schulung der Stabsstelle Datenschutz teilzunehmen.

Ferner sollten Sie sensible Daten nicht an Orten ablegen, über die Sie keinerlei Kontrolle haben. Wenn Sie also kommerzielle Speicherdienste wie Google Drive oder Ähnliches nutzen, können Sie nicht mehr kontrollieren, wohin die Daten letztlich fließen und wer alles darauf Zugriff hat. Nutzen Sie solche Dienste daher bitte möglichst nicht! Wenn es wirklich gar nicht anders gehen sollte, dann legen Sie Daten dort nur in verschlüsselten Container-Dateien ab.

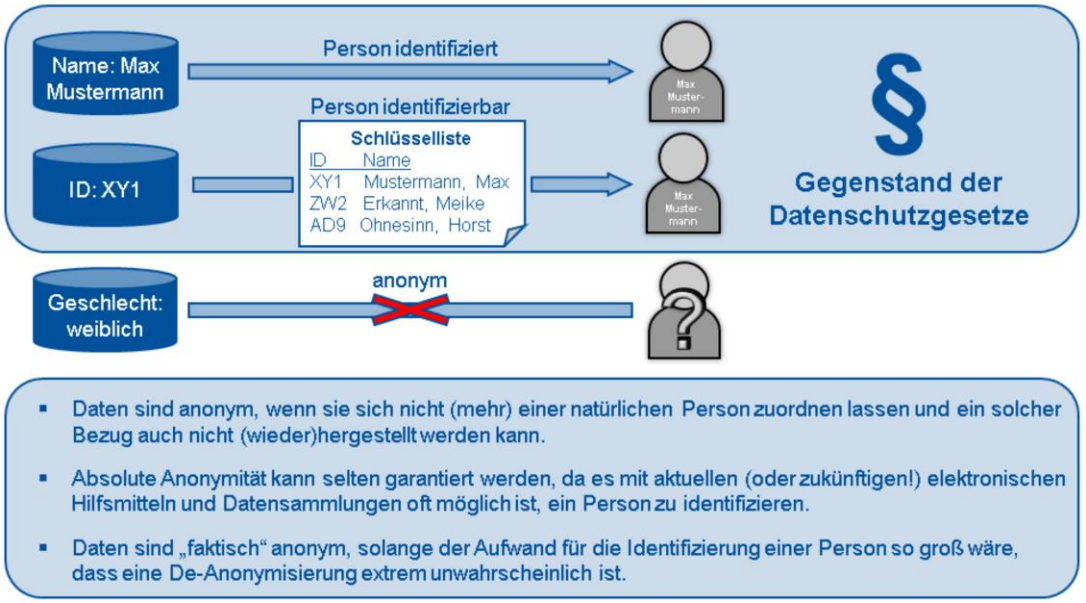
Ähnlich problematisch ist das Speichern auf mobilen Datenträgern, da diese besonders häufig verloren gehen oder gestohlen werden. Einerseits droht Ihnen dann ein Datenverlust, falls Sie kein aktuelles Backup haben, und andererseits könnten die Daten vom Dieb oder einem zufälligen Finder missbraucht werden. Dieses Risiko können Sie durch eine gute Verschlüsselung zwar minimieren, aber eben nicht ganz ausschließen.

Wenn Datenträger, auf denen einmal sensible Daten gespeichert waren, defekt sind, müssen sie professionell physisch vernichtet werden! Andernfalls besteht die Gefahr, dass sie aus dem Elektroschrott gefischt werden, um die Daten wiederherzustellen. Mit entsprechender Ausrüstung und Knowhow ist das oft nicht einmal besonders schwer. Sie können solche Datenträger beim Sachgebiet 12 im Welfenschloss abgeben, das sich dann um die sichere Vernichtung kümmert.

Zu guter Letzt sollten Sie in Ihren Projekten regelmäßige Kontrollen etablieren, um sicherzustellen, dass die Regeln im Umgang mit den Daten von allen eingehalten werden. Legen Sie dafür Workflows und Verantwortlichkeiten fest, und zwar am besten schriftlich in einem Datenmanagementplan oder einer Projekt-internen Richtlinie.

Der beste Schutz personenbezogener Daten vor missbräuchlicher Verarbeitung ist es, sie gar nicht erst zu erheben. Der zweitbeste Schutz ist es, sie so schnell wie möglich zu anonymisieren, also alle Merkmale, über die eine Person mittelbar oder unmittelbar identifiziert werden kann, zu löschen oder zu verfremden. Je nach Forschungszweck, Art und Sensibilität der Daten sind dafür verschiedene Verfahren möglich, die wir Ihnen in diesem Kapitel vorstellen möchten.

Wann sind Daten anonym?



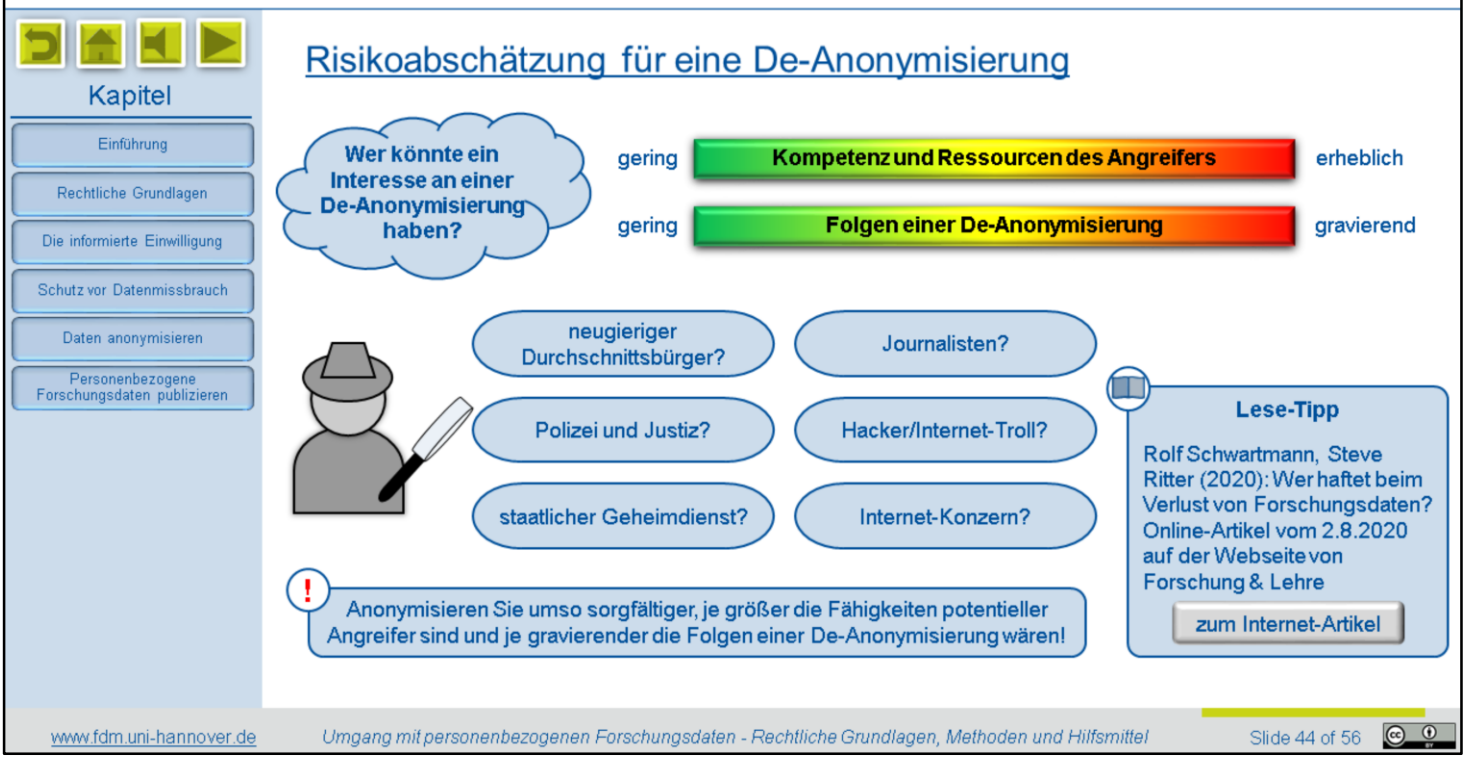
- Daten sind anonym, wenn sie sich nicht (mehr) einer natürlichen Person zuordnen lassen und ein solcher Bezug auch nicht (wieder)hergestellt werden kann.
- Absolute Anonymität kann selten garantiert werden, da es mit aktuellen (oder zukünftigen!) elektronischen Hilfsmitteln und Datensammlungen oft möglich 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.

Diese Folie kennen Sie in etwas abgewandelter Form aus dem Einführungskapitel. Da die Frage, wann Daten tatsächlich anonym sind, die Grundlage dieses Kapitels bildet, hier eine kurze Wiederholung:

Daten sind anonym, wenn sie sich nicht oder nicht mehr einer natürlichen Person zuordnen lassen und ein solcher Bezug auch nicht hergestellt oder wiederhergestellt werden kann.

Absolute Anonymität kann selten garantiert werden, da es mit aktuellen oder auch zukünftigen elektronischen Hilfsmitteln und Datensammlungen oft möglich ist, eine Person zu identifizieren. Bedenken Sie das insbesondere bei der langfristigen Archivierung oder gar Publikation von Daten! Große Internetkonzerne wie Facebook, Google, Amazon und Microsoft, oder auch staatliche Geheimdienste wie die NSA verfügen über gigantische und äußerst detaillierte Datensammlungen von Hunderten Millionen Menschen sowie über ausgereifte Analyse-Tools. Sie sind heute sehr wahrscheinlich in der Lage, viele der vor zehn Jahren gesammelten und anonymisierten Daten wieder zu de-anonymisieren.

In den allermeisten Fällen sind anonymisierte Daten daher nur „faktisch" anonym. Das bedeutet, dass der Aufwand für die Identifizierung einer Person so groß wäre, dass eine De-Anonymisierung extrem unwahrscheinlich ist. Auch dabei sollte aber bedacht werden, dass eine De-Anonymisierung, die noch vor zehn Jahren eine aufwändige Recherche durch Fachpersonal erfordert hätte, heute oft in Sekundenbruchteilen durch künstliche Intelligenz und das Einbeziehen von Big Data erfolgen kann.



Um abzuschätzen, ob Ihre Daten ausreichend vor einer De-Anonymisierung geschützt sind, sollten Sie sich drei Dinge fragen: Erstens: Wer könnte ein Interesse an einer De-Anonymisierung haben? Zweitens: Über welche Kompetenzen und Ressourcen verfügen potentielle Angreifer? Und drittens: Welche Folgen hätte eine De-Anonymisierung für die Betroffenen?

Hier ein paar mögliche Akteure, die entweder zufällig an Ihre Daten gelangen oder diese gezielt stehlen könnten: Die meisten Menschen sind neugierig. Finden sie durch Zufall Informationen, die eigentlich nicht für sie gedacht sind, werden viele wohl trotzdem mal einen Blick riskieren... Allerdings verfügen nur wenige über die Kenntnisse, die technische Ausstattung und die Motivation, um zum Beispiel verschlüsselte Daten zu knacken.

In der Vergangenheit gab es Fälle, in denen investigative Journalisten Daten de-anonymisiert haben, um die Verantwortlichen für politische Skandale zu ermitteln, zum Beispiel 2018 nach dem Giftanschlag auf den britisch-russischen Doppelagenten Skripal.

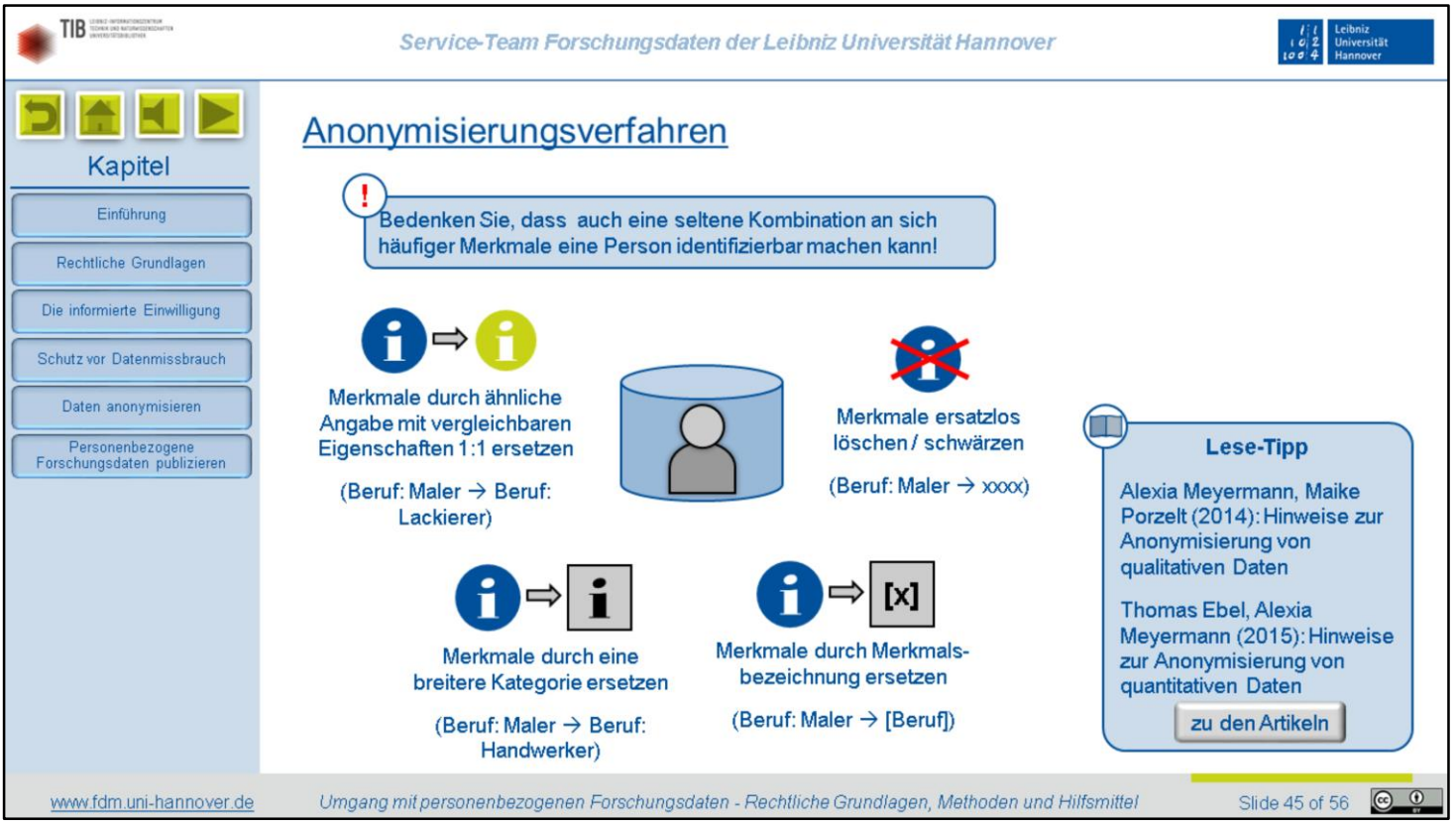
Polizei und Justiz sind schon von Amts wegen verpflichtet, zur Aufklärung von Straftaten alle legal gesammelten Informationen auszuwerten. Legal kann unter Umständen auch eine Beschlagnahmung von Datenträgern sein. Diese Institutionen verfügen auch in begrenztem Rahmen über das nötige Fachpersonal.

Einzelne Hacker sehen es manchmal als eine Art sportliche Herausforderung, technische Schutzmaßnahmen zu knacken. Sie sind dabei erschreckend oft erfolgreich, wie viele große Firmen, Organisationen und staatliche Einrichtungen schon leidvoll erfahren mussten. Einigen geht es aber gar nicht darum, Daten zu entwenden, sondern Sicherheitslücken aufzudecken.

Dagegen kommt es immer häufiger vor, dass bestens ausgestattete und ausgebildete Hacker im Auftrag staatlicher Geheimdienste Attacken ausführen, um Informationen abzugreifen oder Systeme zu sabotieren.

Eine häufig noch immer unterschätze Gefahr geht aber auch von den großen Internetkonzernen und ihren vermeintlich kostenlosen Angeboten aus. Deren Geschäftsmodell basiert auf personalisierter Werbung, die umso zielgerichteter geschaltet werden kann, je mehr Informationen über einzelne Personen zusammenkommen. Diese Firmen werden alle Daten nutzen, die sie bekommen können, und zwar häufig auch ohne Wissen oder gar Zustimmung der Betroffenen.

Grundsätzlich gilt: Anonymisieren Sie umso sorgfältiger, je größer die Fähigkeiten potentieller Angreifer sind und je gravierender die Folgen einer De-Anonymisierung wären! Bedenken Sie auch, dass unzureichende Schutzmaßnahmen zu Schadenersatzansprüchen der Betroffenen führen können, wenn Daten tatsächlich in falsche Hände geraten. Werfen Sie dazu gerne mal einen Blick in unseren Lese-Tipp.



Anonymisieren heißt also, alle Merkmale, über die eine Person unmittelbar oder mittelbar identifiziert werden kann, entweder zu entfernen oder so zu verändern, dass eine Identifizierung nicht mehr möglich ist.

Bedenken Sie dabei, dass auch seltene Kombination an sich häufiger Merkmale eine Person identifizierbar machen können. Es reicht also oft nicht, nur Angaben wie Name und Adresse zu ändern oder zu entfernen. Hier zunächst einmal ein Überblick, welche Anonymisierungsverfahren zum Einsatz kommen können. Wir werden diese gleich noch näher erläutern.

Um das Analysepotential so weit wie möglich zu erhalten, können Merkmale durch Angaben gleichen Detailgrades ersetzt werden, die vergleichbare Eigenschaften haben. Zum Beispiel könnte man in einem Transkript die Berufsangabe „Maler“ durch „Lackierer“ ersetzen.

Wenn für die Analyse allgemeinere Merkmale ausreichen, könnte die genaue Berufsbezeichnung durch eine breitere Kategorie wie „Handwerker“ ersetzt werden.

Vielleicht kommt es auch nur darauf an, dass an der betreffenden Stelle überhaupt der Beruf erwähnt wird. Dann könnte dort einfach der Platzhalter „Beruf“ stehen.

Die radikalste Methode bestünde darin, alle personenbezogenen Merkmale ersatzlos zu löschen oder zu schwärzen. Damit sind dann allerdings auch viele Analysen nicht mehr durchführbar.

Nähere Informationen und Beispiele zu diesen und weiteren Methoden finden Sie auch in unseren Lese-Tipps.

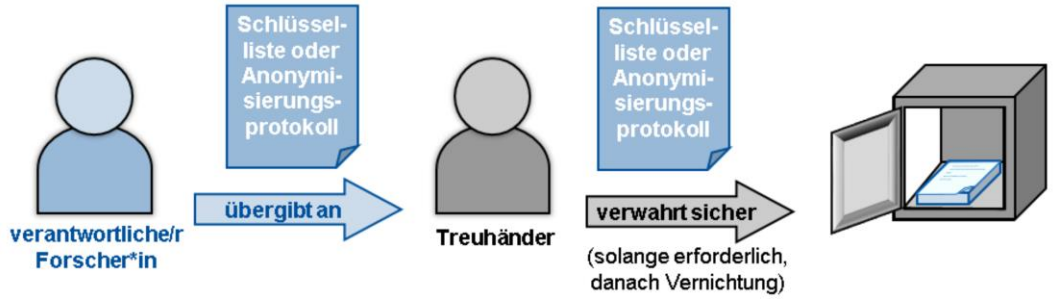
Manchmal ist es nicht möglich, Daten sofort zu anonymisieren. Das kann zum Beispiel der Fall sein, wenn eine Umfrage in bestimmten Intervallen mit denselben Personen wiederholt werden soll, um die Veränderungen zu messen. In solchen Fällen sind die Daten schnellstmöglich zu pseudonymisieren.

Dafür können dieselben Verfahren wie bei der Anonymisierung zum Einsatz kommen. Allerdings wird in einem Anonymisierungsprotokoll festgehalten, welche Originalmerkmale wodurch ersetzt wurden.

Wurde jeder betroffenen Person ein Pseudonym, wie ein Alias oder eine ID, zugeordnet, so hält eine Schlüsselliste fest, zu welcher Person welches Pseudonym gehört.

Denken Sie daran: Das Anfertigen von Anonymisierungsprotokollen und Schlüssellisten ist nur zulässig, wenn der Forschungszweck oder eine gesetzliche Vorgabe es erfordert! Diese Dokumente müssen dann von den pseudonymisierten Daten strikt getrennt und an einem sicheren Ort aufbewahrt werden.

Einsatz von Datentreuhändern bei pseudonymisierten Daten



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

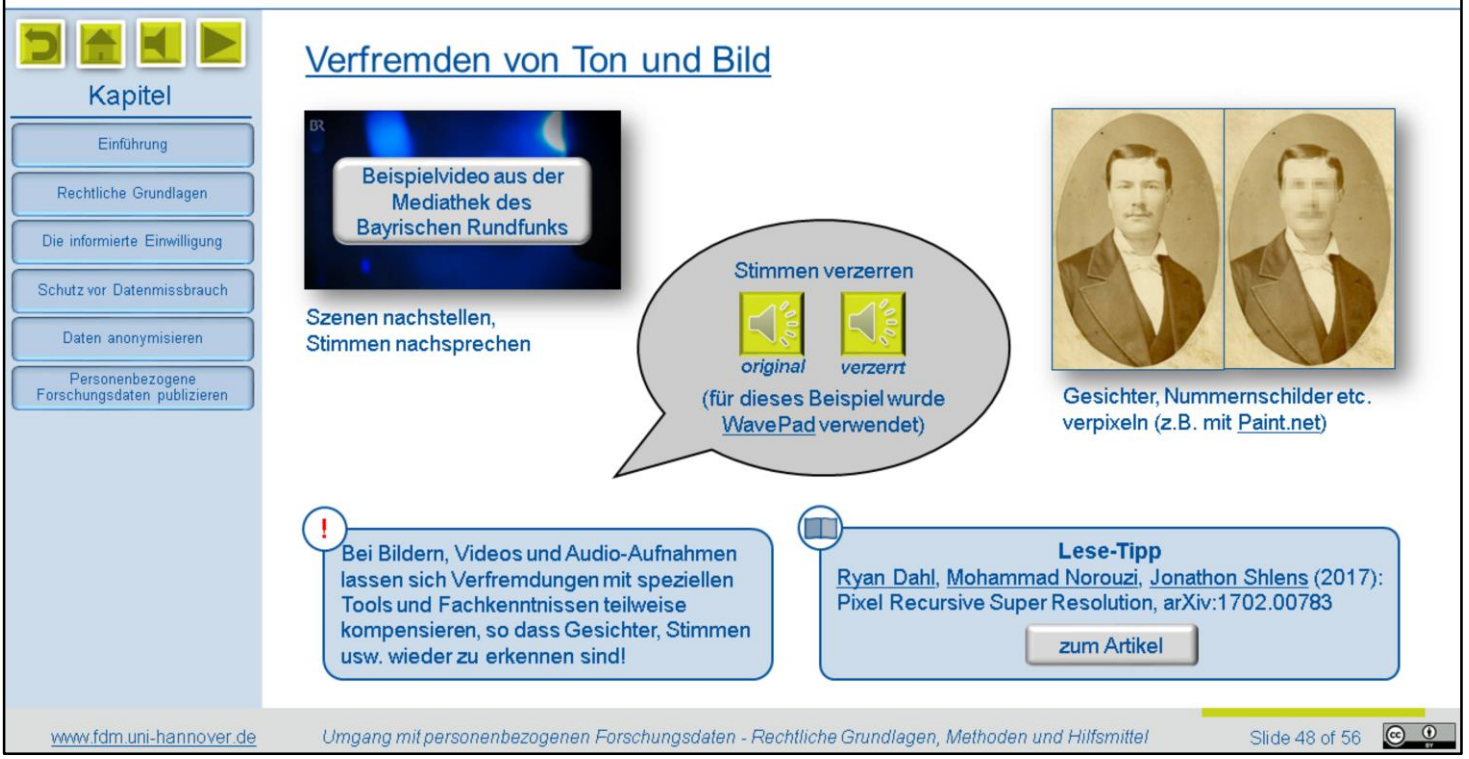
! Datentreuhänder und Projektverantwortliche müssen dafür Sorge tragen, dass die Dokumente professionell vernichtet werden, sobald sie nicht mehr benötigt werden!

Die sicherste Art, Schlüssellisten und Anonymisierungsprotokolle aufzubewahren, ist es, sie einem unabhängigen Datentreuhänder zu übergeben. Der Datentreuhänder verwahrt sie dann beispielsweise in einem Safe, wenn es sich um Papierformulare handelt, oder auf einem gut gesicherten und nur ihm zugänglichen Speichermedium.

Die weitere wissenschaftliche Analyse erfolgt dann also mit Daten ohne Personenbezug. Sollte es in Ausnahmefällen während des Forschungsprozesses erforderlich werden, einen Personenbezug wiederherzustellen, wäre das aber möglich. Das könnte zum Beispiel der Fall sein, wenn Betroffene ihre Einwilligung widerrufen und die Löschung ihrer Daten verlangen.

Als Datentreuhänder kommen zum Beispiel Datenschutzbeauftragte, Anwälte oder Notare in Frage. Anwälte und Notare gehören zu den Berufsgruppen, für die die Strafprozessordnung ein Zeugnisverweigerungsrecht nach Paragraph 53 und ein Beschlagnahmeverbot nach Paragraph 97 vorsieht. Sie könnten daher selbst im Fall polizeilicher Ermittlungen nicht ohne Weiteres zur Herausgabe der Listen gezwungen werden.

Ist der Forschungszweck erfüllt oder eine zuvor festgelegte Aufbewahrungsfrist abgelaufen, sollten Datentreuhänder und Projektverantwortliche gemeinsam dafür sorgen, dass Protokolle und Schlüssellisten professionell vernichtet werden.



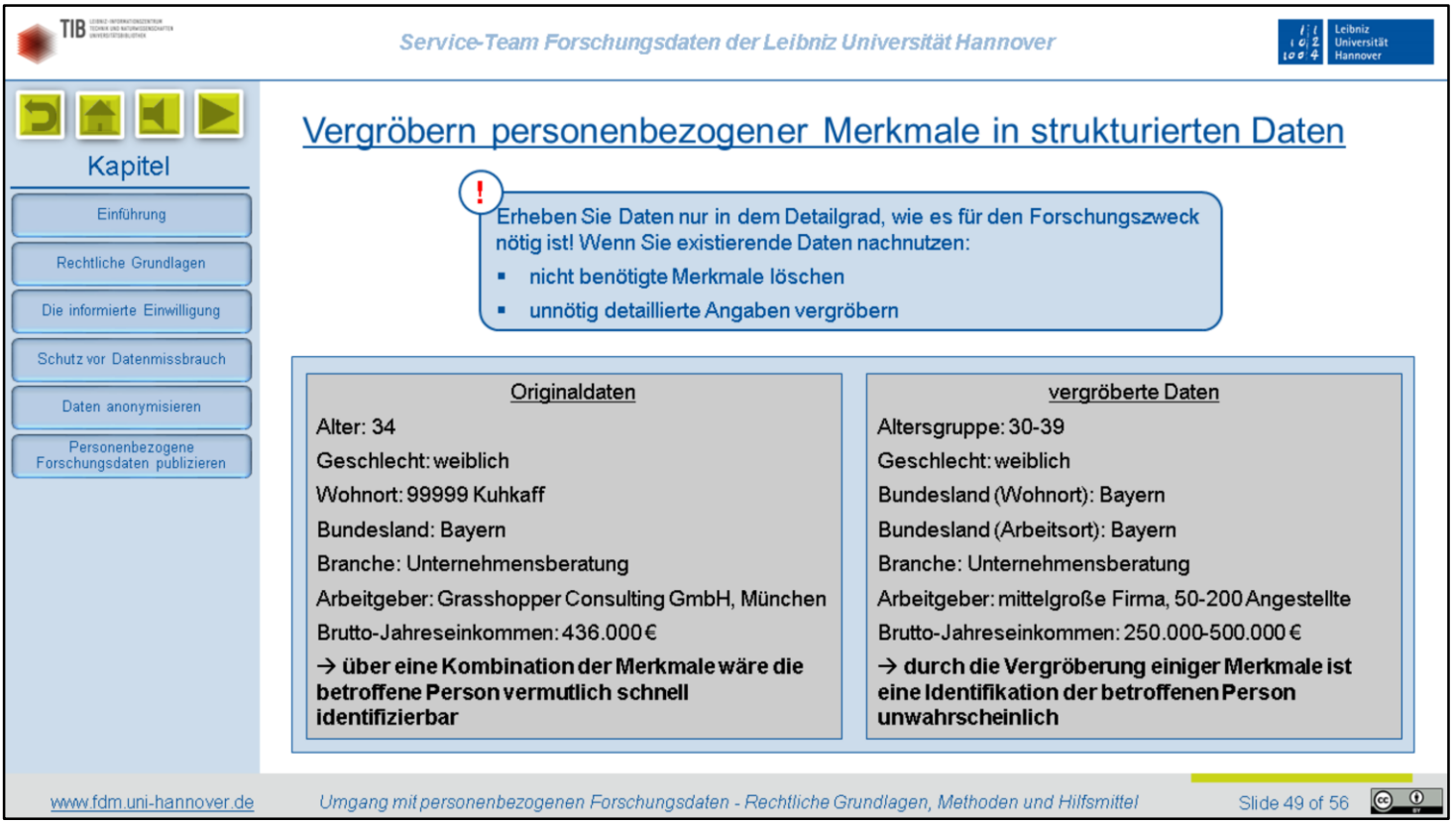
Kommen wir zum Anonymisieren von Daten durch Verfremdung. Je nach Datenart, Forschungszweck und Analysemethoden können dafür verschiedene Verfahren zum Einsatz kommen. Bei schriftlich vorliegenden Informationen, können Merkmale durch Angaben ersetzt werden, die den Originalen in jenen Eigenschaften ähneln, die für die Analyse wichtig sind. Aber auch Videos, Bilder und Tonaufnahmen lassen sich verfremden.

Geht es zum Beispiel bei einem Video nicht um die exakte Wiedergabe einer Szene, sondern nur um das grundsätzliche Setting, kann eine solche Szene auch nachgestellt und die Stimmen nachgesprochen werden. Diese Methode wird häufig in investigativ-journalistischen Fernsehsendungen verwendet. Die ursprünglich gefilmten Personen können so weder über ihre Stimme noch über ihr Erscheinungsbild identifiziert werden.

Bei Tonaufnahmen können Stimmen verfremdet werden. Das lässt sich relativ einfach mit diversen Software-Tools bewerkstelligen. In diesem Beispiel haben wir WavePad verwendet. Zunächst das Original. Und nun die verfremdete Version.

Bei Bildern können Bereiche verpixelt oder unscharf maskiert werden. Auch das ist mit fast allen gängigen Bildbearbeitungsprogrammen möglich, zum Beispiel mit paint.net. Hierbei geht es nicht nur um Gesichter, sondern zum Beispiel auch um Nummernschilder, Straßennamen und Hausnummer oder sonstige Dinge, die Rückschlüsse auf Personen zulassen.

Bitte bedenken Sie, dass sich Verfremdungen von Ton und Bild mit der nötigen Technik und Knowhow teilweise rückgängig machen oder kompensieren lassen. Wenn Sie befürchten, dass jemand gezielt versuchen könnte, auf diese Weise mithilfe Ihrer Daten Personen zu identifizieren, verlassen Sie sich daher nicht ausschließlich auf diese Techniken. In unserem Lesetipp erläutern zum Beispiel drei Google-Entwickler, wie sich unscharfe Bilder mit statistischen Verfahren „nachschärfen“ lassen. Wenn Sie dagegen Stimmen nachsprechen oder Szenen nachstellen, besteht diese Gefahr nicht. Eine Identifizierung wäre dann nur über den Inhalt des Gesprochenen möglich.



Schriftlich vorliegenden Daten können nicht nur durch Verfremdung sondern auch durch Vergröberung anonymisiert werden. Das bietet sich insbesondere bei strukturierten Daten aus Befragungen etc. an. Bei Dritterhebungen kann es sein, dass die Originaldaten in einem Detailgrad vorliegen, der für die beabsichtigte Analyse gar nicht notwendig ist. Dann ist es angebracht, diese Merkmale durch allgemeinere Kategorien oder Wertspannen zu ersetzen. Bei Direkterhebungen sollten Sie von Anfang an Daten nur in dem Detailgrad erheben, wie es für Ihren Forschungszweck nötig ist.

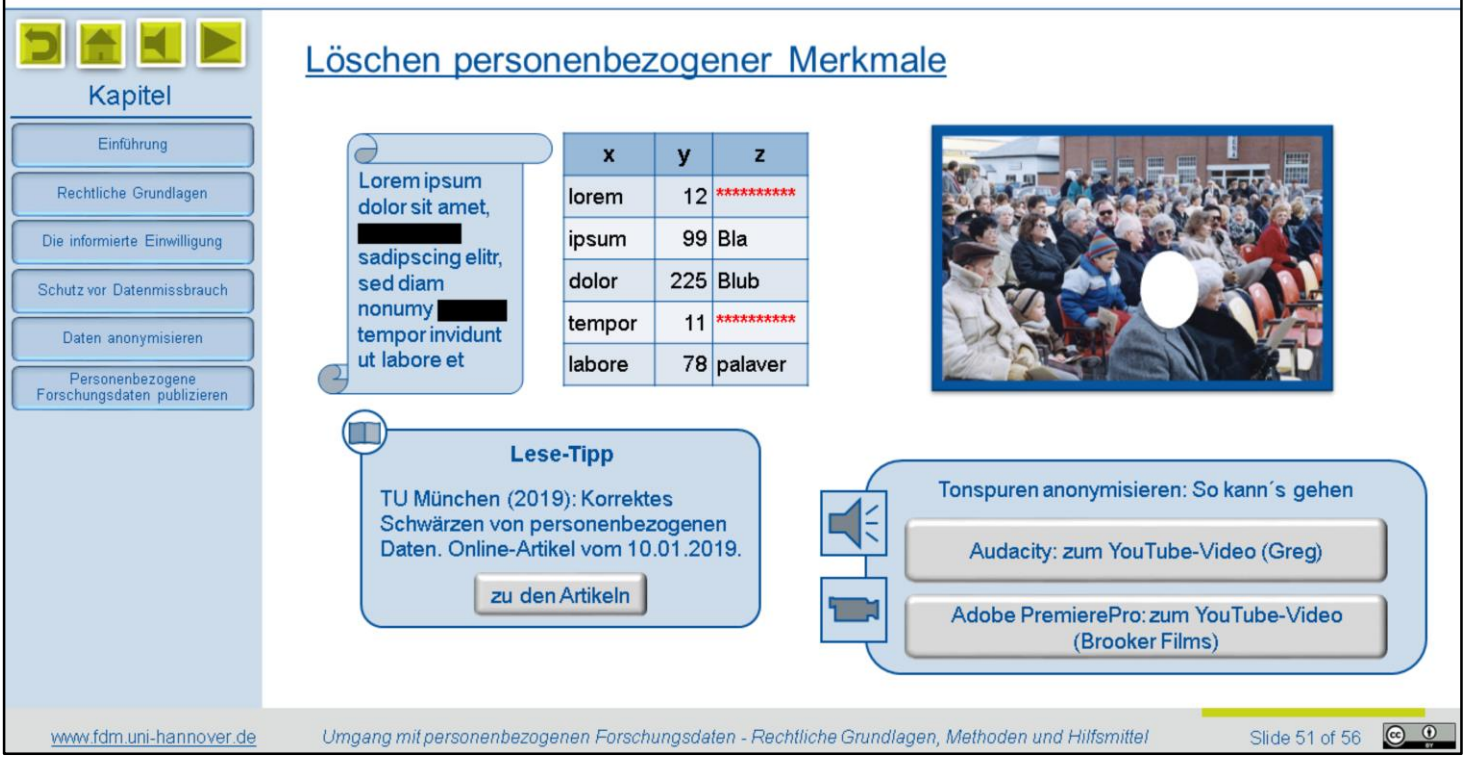
In diesem Beispiel nehmen wir einmal an, Sie haben bundesweit Befragungsdaten von Führungskräften aus der Privatwirtschaft erhoben. Sagen wir, Sie möchten untersuchen, in welchen Branchen und welchen Bundesländer es besonders viele junge weibliche Führungskräfte gibt. Die Originaldaten links sind so detailliert, dass die betroffene Person über die Kombination der Merkmale vermutlich leicht zu identifizieren wäre. In dem kleinen Dorf „Kuhkaff“ wird es wohl nur eine 34jährige gutverdienende Unternehmensberaterin geben, die bei Grasshopper Consulting arbeitet.

Auf der rechten Seite wurden die Merkmale so vergröbert, dass sie auch in ihrer Kombination keine Rückschlüsse auf eine einzelne Person mehr zulassen. Sie sind aber weiterhin geeignet, um auszuwerten, in welchen Branchen und welchen Bundesländer es besonders viele junge weibliche Führungskräfte gibt.

Insbesondere in den Sozial- und Wirtschaftswissenschaften entstehen viele Forschungsdaten durch das Aufzeichnen und anschließende Transkribieren von Interviews. Wörtliche Transkripte so zu anonymisieren, dass zwar einerseits eine De-Anonymisierung so weit wie möglich erschwert wird, andererseits aber die beabsichtigten Auswertungen möglich bleiben, ist eine Gratwanderung.

In diesem Beispiel haben wir einen Ausschnitt aus einem fiktiven Interview auf zwei verschiedene Arten verfremdet. In der ersten Version wurden alle personenbezogenen Angaben durch die jeweilige Merkmalskategorie ersetzt. Diese Vergröberung erhöht den Schutz vor einer De-Anonymisierung, vermindert aber das Analysepotential. Es wäre zum Beispiel nicht möglich, die Interviews mehrerer Betroffener zu vergleichen, die von derselben Person beraten wurden oder ein Basiskonto bei derselben Bank eröffnet haben.

In der zweiten Version wurden die Angaben durch Pseudonyme mit ähnlichen Eigenschaften ersetzt. Wenn in allen transkribierten Interviews immer dasselbe Pseudonym für dieselbe Person, dieselbe Bank und denselben Ort verwendet wurde, ließen sich dann später Aussagen treffen, ob zum Beispiel mehrere Personen ähnliche Erfahrungen mit derselben Bank gemacht haben, ohne dass die Bank selbst mit ihren echten Namen benannt wird.



Die radikalste aber auch sicherste Form der Anonymisierung ist das Löschen personenbezogener Merkmale. Wann immer Ihre Rohdaten Merkmale enthalten, die Sie für Ihre Analysen nicht benötigen, sollten Sie diese umgehend entfernen.

In editierbaren Texten und Tabellen ist das recht einfach durch das Löschen der entsprechenden Wörter oder das Ersetzen durch Platzhalter-Zeichen möglich. Anschließend sollte der gesamte Text aber in ein neues Dokument kopiert und gespeichert werden, da in der Originaldatei die Änderungshistorie gespeichert ist. In nicht editierbaren Texten, zum Beispiel Scanns oder Papierdrucken, bietet sich ein Schwärzen mit Bildbearbeitungsprogrammen beziehungsweise mit entsprechenden gut deckenden Farbstiften an. Weitere Tipps hat die TU München zusammengestellt.

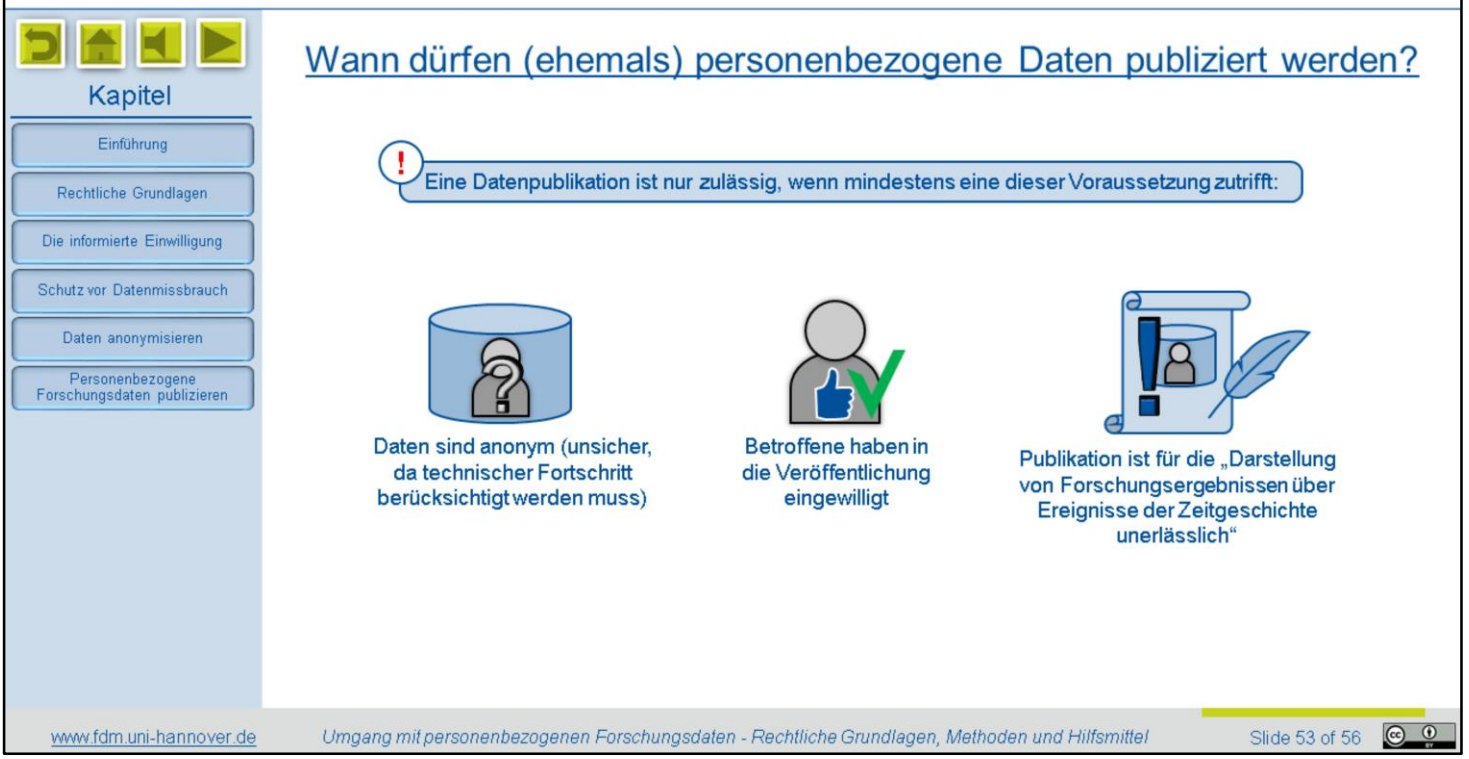
Bei Bildern lassen sich Gesichter und andere Merkmale mit jedem Bildbearbeitungsprogramm ausschneiden oder übermalen. Bitte speichern Sie die Dateien anschließend in einem Format, dass nur eine Ebene unterstützt, zum Beispiel jpg oder png. Die Herstellerformate von Photoshop, CorelDraw und so weiter können mehrere Ebenen speichern. Falls Sie also absichtlich oder versehentlich die Maskierung auf eine eigene Bildebene gelegt haben, bleiben die Originaldaten darunter erhalten.

Auch Tonspuren lassen sich so bearbeiten, dass sensible Passagen durch Pieptöne oder Ähnliches ersetzt werden. Auch hier sollten Sie darauf achten, dass nach der Bearbeitung die Tonspuren zusammengeführt werden und die Pieptöne nicht etwa auf einer extra-Tonspur laufen, die den O-Ton lediglich überdeckt, aber nicht überschreibt. Die hier verlinkten Video-Tutorials stellen die Vorgehensweise mit dem open source-Programm Audacity für reine Tonaufnahmen und dem kommerziellen Adobe Premiere für Videos vor. Es gibt aber viele weitere Tools, mit denen sich Ähnliches erreichen lässt.

Personenbezogene Forschungsdaten publizieren

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

Nun kommen wir zum letzten und kürzesten Kapitel dieses Kurses. In diesem erläutern wir, wie und unter welchen Voraussetzungen Sie Forschungsdaten publizieren können, die personenbezogene Merkmale enthalten oder ursprünglich enthalten haben.



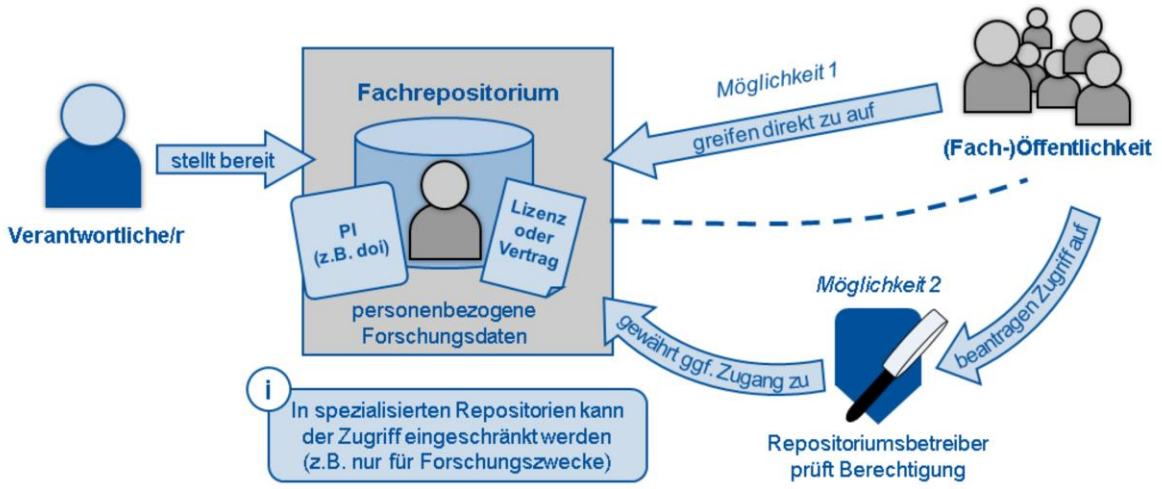
Grundsätzlich ist das Veröffentlichen personenbezogener oder ehemals personenbezogener Daten nur zulässig, wenn mindestens eine der folgenden drei Voraussetzungen zutrifft:

Die Daten sind so anonymisiert worden, dass ein Personenbezug auch mit technischen Hilfsmitteln und unter Einbeziehung weiterer Datensammlungen aus anderen Quellen nicht wiederhergestellt werden kann. Das kann zum Beispiel für viele Statistiken angenommen werden, wenn die Grundgesamtheit groß genug ist. Bei anonymisierten Fragebögen und erst recht bei wörtlichen Transkripten von Interviews kann jedoch eine solche absolute Anonymität auch für die Zukunft in aller Regel nicht gewährleistet werden.

Das Niedersächsische Datenschutzgesetz sieht in Paragraph 13 noch zwei weitere Fälle vor, in denen auch nicht-anonyme Forschungsdaten publiziert werden dürfen: Erstens können die Betroffenen in die Datenveröffentlichung einwilligen. Wenn Ihre Einwilligungserklärungen also entsprechende Klauseln enthalten und Sie Ihren Informationspflichten nachgekommen sind, sind Sie auf der sicheren Seite. Wenn Sie Ihre Daten nicht veröffentlichen wollen oder dürfen, können Sie sie eventuell zumindest für wissenschaftliche Zwecke unter Auflagen zur Verfügung stellen. Dafür können Sie die Dienste eines sozial- und wirtschaftswissenschaftlichen Fachrepositoriums in Anspruch nehmen, wie wir auf den folgenden Folien näher erläutern werden. Auch dafür benötigen Sie aber die Einwilligung der Betroffenen.

Zweitens ist eine Veröffentlichung zulässig, wenn „dies für die Darstellung von Forschungsergebnissen über Ereignisse der Zeitgeschichte unerlässlich ist“. Beispielsweise erschien 2010 eine vielbeachtete Studie zum Umgang des Auswärtigen Amtes mit seiner NS-Vergangenheit, in der detailliert das Verhalten der namentlich genannten Akteure und ihre fortgesetzte Karriere im Nachkriegsdeutschland nachgezeichnet wird. Eine solche Veröffentlichung sollte auch von der aktuellen Rechtslage gedeckt sein. Dennoch empfiehlt sich eine juristische Fachberatung durch die Stabsstelle Datenschutz, wenn Sie sich auf diese Rechtsgrundlage berufen wollen.

Daten über ein Fachrepositorium zur Verfügung stellen



Wenn Sie Ihre Daten veröffentlichen oder zumindest unter Auflagen einem eingeschränkten Nutzerkreis zu Verfügung stellen dürfen, laden Sie sie am besten in ein sozial- und wirtschaftswissenschaftliches Fachrepositorium. Ein Repositorium oder Datenzentrum speichert und verwaltet Dateien und die dazugehörigen Metadaten. Es funktioniert wie ein online-Archiv, in dem man über eine Suchdatenbank mit Metadaten relevante Datensätze finden kann.

Gute Repositorien sollten für jeden Datensatz einen sogenannten persistent identifier vergeben, also einen dauerhaft gültigen Link, über den die Daten oder zumindest deren Metadaten auch noch in vielen Jahren zuverlässig abgerufen werden können. Besonders bekannt sind die „Digital Object Identifier“, kurz doi.

Außerdem sollte festgehalten werden, ob und wie die hochgeladenen Daten von anderen Personen verwendet werden dürfen. Bei öffentlichen Daten geschieht das normalerweise über die Vergabe einer standardisierten Lizenz, zum Beispiel einer Creative Commons-Lizenz. Bei eingeschränkt zugänglichen Daten, kann stattdessen ein individueller Nutzungsvertrag abgeschlossen werden. Er enthält dann unter anderem Bestimmungen zur Vertraulichkeit und zum Schutz der Daten durch die Nachnutzenden. Einige sozial- und wirtschaftswissenschaftliche Fachrepositorien schränken den Datenzugang generell ein, wenn es sich um personenbezogene Daten handelt, oder bieten den Datengebenden die Möglichkeit, selbst festlegen, an wen Daten unter welchen Bedingungen weitergegeben werden dürfen.

Demnach gibt es also zwei Möglichkeiten für den Datenzugriff durch Dritte: Möglichkeit eins ist der direkte Zugriff durch jedermann, wenn die Daten vollständig öffentlich sind. Möglichkeit zwei ist ein Antrag auf Einsicht oder Erhalt einer Kopie, wenn der Zugriff beschränkt ist. Wer an den Daten interessiert ist, würde sich dann an die Betreiber des Repositoriums wenden. Diese prüfen, ob die betreffende Person grundsätzlich berechtigt ist, die Daten zu nutzen, also zum Beispiel, ob ein plausibel begründetes Forschungsinteresse vorliegt. Ist das Ergebnis positiv, wird ein Nutzungsvertrag geschlossen und anschließend der Zugang zu den Daten gewährt.

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

Im Gegensatz zu vielen anderen Fächern gibt es in den Wirtschafts- und Sozialwissenschaften bereits zahlreiche etablierte Datenzentren und Fachdienste.

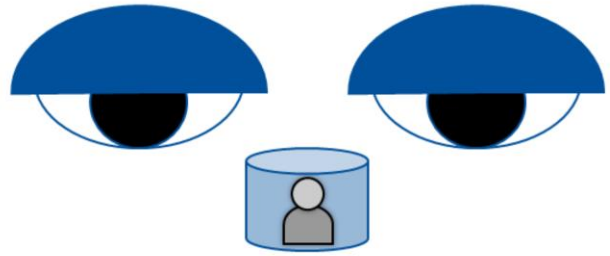
- Verwenden Sie vorzugsweise Repositorien mit Spezialisierung auf sozial- und wirtschaftswissenschaftliche Daten. Dann stehen Ihnen Service-Leistungen und technische Features zur Verfügung, die für das Archivieren und gegebenenfalls Publizieren personenbezogener Daten besonders wichtig sind.
- Nehmen Sie entsprechende Unterstützungsangebote von Fachdiensten und Repositoriumsbetreibern in Anspruch. Neben einer allgemeinen Projektberatung kann das zum Beispiel auch eine Prüfung der Datenqualität und -anonymität, ein Vervollständigen der Metadaten oder das Konvertieren in geeignetere Datenformate beinhalten.
- Stellen Sie personenbezogene Daten nur unter Bedingungen oder nur einem eingeschränkten Personenkreis zur Verfügung, sofern Ihnen keine Einwilligung der Betroffenen für eine vollständige Veröffentlichung vorliegt.
- Viele dieser Dienstleistungen sind nicht kostenlos. Beantragen Sie daher Mittel für Service-Leistungen und Publikationsgebühren! Die meisten Forschungsförderer sehen das inzwischen ausdrücklich vor.

Wenn Sie qualitative Daten, wie zum Beispiel Interview-Transkripte, aufbereiten und archivieren möchten, ist Qualiservice eine gute Anlaufstelle. Für quantitative Daten ist die GESIS einer der ältesten und bekanntesten Fachdienste, über den Daten auch archiviert und veröffentlicht werden können. Wer aus der Bildungsforschung kommt, kann die umfassenden Informations-, Beratungs- und Unterstützungsangebote des Verbunds Forschungsdaten Bildung in Anspruch nehmen. Viele hilfreiche Publikationen zum Umgang mit Daten, auch auf wissenschaftspolitischer Ebene, finden zu außerdem beim Rat für Sozial- und Wirtschaftsdaten. Dort gibt es auch eine Liste weiterer akkreditierter Datenzentren, die den fachüblichen Qualitätsstandards entsprechen.

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! ;-)

So, nun haben Sie es wirklich geschafft! Herzlichen Glückwunsch, Sie sollten nun einen soliden Überblick über das Thema „personenbezogene Forschungsdaten“ haben.

Wir hoffen, dass dieser Kurs gut verständlich war und Ihre Erwartungen erfüllen konnte. Wenn Sie Fragen haben oder eine individuelle Beratung suchen, wenden Sie sich gerne an die Stabsstelle Datenschutz oder das Service-Team Forschungsdaten.

Wir werden in den kommenden Monaten und Jahren weitere Kurse in einem asynchronen online-Format anbieten, also schauen Sie gerne ab und zu mal auf unserer Webseite vorbei. Für heute verabschieden wir uns und wünschen Ihnen viel Erfolg für Ihre Forschungsarbeit!

Und vergessen Sie nicht: Big Brother is watching you!