Fraunhofer IESE

Denis Feth & Svenja Polst

Benutzerfreundliche Umsetzung von Datensouveränität in Digitalen Ökosystemen

Zusammenfassung

Das Wichtigste in Kürze

Produkte und Dienstleistungen werden zunehmend in sogenannten Digitalen Ökosystemen gehandelt, deren Kern eine digitale Plattform ist. Dabei spielt auch die Verarbeitung sensibler Daten eine große Rolle. Neben der Umsetzung des Datenschutzes, welcher sich auf den Schutz personenbezogener Daten bezieht, sollte es immer auch Ziel sein den »Datengebern« (z. B. Konsumenten) größtmögliche Transparenz und Kontrolle über die Verarbeitung ihrer Daten zu geben. Dieses Konzept nennt sich Datensouveränität. Dabei ist es zum einen extrem herausfordernd komplexe Prozesse, Datenflüsse und Schutzmaßnahmen für den Nutzer in verständlicher und nachvollziehbarer Weise darzustellen. Zum anderen gilt es bei Einstellungen und Einwilligungen dem Nutzer die Konsequenzen seiner Wahl bewusst zu machen – ohne ihn aber unangemessen zu beeinflussen. All dies fordert ein stark nutzerzentriertes Vorgehen und das Anwenden von Prinzipien des Forschungsfelds »Usable Security & Privacy«.

Dabei sind die Nutzer Digitaler Ökosysteme stark heterogen in ihren Bedürfnissen und Fähigkeiten. Ebenso gibt es einige fundamentale Grenzen bei der Umsetzung von Datensouveränität zu beachten, welche teils auf menschlichen Eigenschaften (Privacy-Paradoxon), teils auf sich widersprechende Qualitätseigenschaften zurückgehen. Vor diesem Hintergrund kann man schlussendlich zielgruppenorientiert Maßnahmen zur Erreichung von Transparenz (z. B. durch benutzerfreundliche Datenschutzerklärungen, einheitliche Bildsymbole und die Nachverfolgbarkeit von Datenflüssen) und Selbstbestimmung (z.B. durch durchgängiges Einwilligungsmanagement und nutzerfreundliche Einstellungen) umsetzen.

Dazu schlagen wir vor sich am Human-Centered-Design zu orientieren. Dieser Prozess wird in der Praxis bereits häufig angewendet, berücksichtigt aber in der Regel weder Security, noch Datenschutz und Datensouveränität explizit. Daher stellen wir eine Reihe von Erweiterungen für diesen Prozess vor. Für die technische Umsetzung von Datensouveränität stellen wir zudem das Konzept der Datennutzungskontrolle vor. Dieses erlaubt es die vom Nutzer getroffenen Einstellungen in Regeln abzubilden und beispielsweise durch Filterung oder Maskierung der Daten umzusetzen.

Mit diesem Überblick hoffen wir, Leser dabei zu unterstützen Datensouveränität benutzerfreundlich umzusetzen. Die Kernbotschaften fassen wir dazu für jedes Kapitel kurz zusammen und sammeln sie zum Schluss in einem kompakten Fazit.

Inhalt

MOTIVATION & ÜBERBLICK 4

TEIL 1: KONTEXT & GRUNDLAGEN 6

1 Digitale Ökosysteme 8

2 Datensouveränität 10

3 Usability & User Experience 12

4 Usable Security & Privacy 13

TEIL 2: ZIELE & GRENZEN 14

5 Zielgruppen 16

6 Grenzen 18

7 Transparenz 20

8 Selbstbestimmung 22

TEIL 3: METHODEN & WERKZEUGE 24

9 Vorgehen 26

10 Technische Durchsetzung 30

TEIL 4: FAZIT 32

11 Unsere Kernbotschaften 34

12 Über die Autoren 35

REFERENZEN 36

Motivation & Überblick

Benutzerfreundliche Datensouveränität als Erfolgsfaktor digitaler Geschäftsmodelle

Produkte und Dienstleistungen (sogenannte Assets) werden zunehmend digital getauscht und gehandelt. Anbieter und Konsumenten finden dabei immer häufiger in sogenannten Digitalen Ökosystemen zueinander, was im Kern durch eine digitale Plattform ermöglicht wird. Beispielsweise können Konsumenten Unterkünfte über Airbnb buchen, Handwerkerleistungen über MyHammer beauftragen oder Produkte über die Marktplätze von Otto oder Amazon kaufen. Digitale Ökosysteme bieten vielfältige Chancen für ihre Teilnehmer. Hierunter zählen die Erschließung neuer Geschäftsfelder, die Gewinnung neuer Kunden und das Anstoßen von Innovationen in der eigenen Branche, welche durch die Generierung von Mehrwerten durch Daten entstehen. Skalen- und Netzwerkeffekte sind zentraler Bestandteil Digitaler Ökosysteme und der Plattformökonomie. Daher profitiert der Plattformanbieter ebenso wie Konsumenten, Anbieter und weitere Partner des Digitalen Ökosystems.

Bei all dem spielen Daten eine große Rolle. So verarbeiten die Anbieter der Assets und die Anbieter der Plattform in aller Regel personenbezogene Daten, um das Asset bereitzustellen. Es gibt sogar diverse Beispiele, bei denen es sich bei dem gehandelten Asset selbst um Daten handelt, z. B. bei Caruso, Advaneo, GovData oder Infra-Bau 4.0.

Dabei wird sowohl seitens der Gesetzgebung (im Rahmen der DSGVO) als auch seitens der Nutzer (also primär der Anbieter und Konsumenten) selbst immer häufiger gefordert, dass Nutzern gewisse Informations- und Mitspracherechte bezüglich der Nutzung »ihrer« Daten zugestanden wird. Diese Art der informierten Selbstbestimmung wird auch als Datensouveränität bezeichnet.

In Anbetracht dessen, dass Digitale Ökosysteme aus einem schwer durchschaubaren und hochgradig dynamischen Verbund von Teilnehmern bestehen, welche außerdem meist ein kommerzielles Interesse an den Daten haben, ist Datensouveränität umso wichtiger.

Damit Datensouveränität funktionieren kann, müssen einige Voraussetzungen erfüllt sein:

1. Nutzer müssen mit angemessenem Aufwand verstehen, nachvollziehen und kontrollieren können, wie ihre Daten verwendet und weitergegeben werden.

2. Nutzern muss die Möglichkeit gegeben werden, Einfluss auf die Verarbeitung ihrer Daten nehmen zu können.

3. Nutzer müssen verstehen, welche Auswirkungen bestimmte Entscheidungen auf sie haben (z. B. das Erteilen einer Einwilligung).

4. Nutzer müssen bei ihrer Entscheidung frei und unbeeinflusst sein.

Diese Voraussetzungen beziehen sich direkt auf die Usability (also die Effektivität, Effizienz und Zufriedenheit) der angebotenen Maßnahmen sowie auf die User Experience (UX; in unserem Zusammenhang z. B. das Vertrauen in den Anbieter). Ganz allgemein lässt sich die Wechselwirkung zwischen Datensouveränität und UX wie folgt zusammenfassen: Einerseits kann fehlende Datensouveränität einen negativen Einfluss auf wichtige UX-Aspekte wie Zufriedenheit oder Vertrauen haben. Daher kann Datensouveränität eine Voraussetzung für gute UX sein. Andererseits kann Datensouveränität nur dann erreicht werden, wenn die Maßnahmen auch benutzerfreundlich umgesetzt sind. Andernfalls werden Nutzer sie nicht (oder zumindest nicht korrekt) einsetzen und somit indirekt ihrer Souveränität beraubt. Im schlimmsten Fall können falsch getroffene Einstellungen sogar das genaue Gegenteil von dem bewirken, was der Nutzer eigentlich möchte.

Wir vermitteln in diesem Bericht die Bedeutung einer benutzerfreundlichen Umsetzung von Datensouveränität, gehen auf die speziellen Herausforderungen ein und zeigen entsprechende Lösungsansätze.

Teil 1: Kontext & Grundlagen

In Teil 1 unseres Berichts schaffen wir zunächst eine gemeinsame Basis. Hier beschreiben wir wichtige Hintergrundinformationen zu Digitalen Ökosystemen (Kapitel 1), Datensouveränität (Kapitel 2), Usability und User Experience (Kapitel 3), sowie dem für uns sehr relevanten Querschnittsthema »Usable Security & Privacy« (Kapitel 4).

Teil 2: Ziele & Herausforderungen

In Teil 2 widmen wir uns der Frage, wie sich Datensouveränität benutzerfreundlich umsetzen lässt. Wir gehen insbesondere näher auf unsere Zielgruppen ein (Kapitel 5) und beschreiben grundlegende Grenzen (Kapitel 6). Anschließend widmen wir uns den Kernzielen von Datensouveränität, nämlich der Schaffung von Transparenz (Kapitel 7) und Selbstbestimmung (Kapitel 8).

Teil 3: Methoden & Werkzeuge

In Teil 3 werfen wir einen Blick auf aktuelle Designpraktiken und schlagen eine Vorgehensweise basierend auf dem Human-Centered Design vor (Kapitel 9). Außerdem stellen wir das Konzept der »Datennutzungskontrolle« vor, welches einen wesentlichen Baustein zur technischen Durchsetzung von Datensouveränität darstellt (Kapitel 10).

Teil 4: Fazit

In Teil 4 fassen wir die wichtigsten Erkenntnisse und Kernbotschaften der vorherigen Kapitel kompakt zusammen. Außerdem stellen sich die Autoren vor und beschreiben wie das Thema der benutzerfreundlichen Umsetzung von Datensouveränität sie in ihrer täglichen Arbeit betrifft und angehen.

Die wichtigsten Erkenntnisse

Datensouveränität ist besonders in Digitalen Ökosystemen von hoher Relevanz, da diese im Kern auf dem Austausch sensibler Daten beruhen. Es gilt: Eine gute UX ist Voraussetzung für Datensouveränität UND Datensouveränität kann die UX positiv beeinflussen.

TEIL 1: KONTEXT & GRUNDLAGEN

1 Digitale Ökosysteme
2 Datensouveränität
3 Usability & User Experience
4 Usable Security & Privacy

1 Digitale Ökosysteme

Digitale Ökosysteme, Plattformen und Plattformökonomie

Digitale Ökosysteme und Plattformen wie Uber, Airbnb und eBay entstehen nicht nur in den USA, sondern auch in Europa und in Deutschland. Laut einer McKinsey-Studie werden Digitale Ökosysteme im Jahr 2025 etwa 30 Prozent des weltweiten Umsatzes generieren. Es ist daher nicht verwunderlich, dass im August 2020 mit Delivery Hero das erste deutsche Unternehmen, dessen Geschäftsmodell in der Plattformökonomie verortet ist, im DAX aufgenommen wurde. Digitale Ökosysteme bieten vielfältige Chancen für ihre Teilnehmer. Hierunter zählen die Erschließung neuer Geschäftsfelder, die Gewinnung neuer Kunden und das Anstoßen von Innovationen in der eigenen Branche, welche durch die Generierung von Daten entstehen. Skalen- und Netzwerk-effekte sind zentraler Bestandteil Digitaler Ökosysteme und der Plattformökonomie. Dadurch profitiert der Plattformanbieter ebenso wie alle Teilnehmer und Partner des Ökosystems.

Beteiligte Rollen

An einem Digitalen Ökosystem sind diverse Rollen beteiligt (siehe Abbildung 1). Kern eines jeden Digitalen Ökosystems ist eine digitale Plattform, welche einen Ökosystem-Service bereitstellt (z. B. das Vermitteln von Dienstleistungen oder Produkten), von dem wiederum die entsprechenden Ökosystemteilnehmer profitieren. Eine zentrale Rolle nimmt dabei der Broker (Vermittler, Makler) ein. Der Broker ist ein Unternehmen, das für die Vermittlung von Assets (Dienstleistungen, Daten, digitale Produkte oder Güter) zwischen den Konsumenten und Anbietern zuständig ist. Das Asset im Beispiel von eBay sind Güter aller Art. Im Play Store von Google sind die vermittelten Assets mobile Apps für Android-Geräte.

Anbieter sind Unternehmen oder Privatpersonen, die ein Asset anbieten, und Konsumenten sind Unternehmen oder Privatpersonen, die das Asset erwerben und in der Regel auch konsumieren.

Dabei kann in einem Digitalen Ökosystem ein Unternehmen oder eine Privatperson sowohl Konsument als auch Anbieter sein, zum Beispiel bei eBay-Kleinanzeigen oder Parship. Dahingegen treten bei Online-Marktplätzen wie Amazon Marketplace und mediamarkt.de die dahinterstehenden Unternehmen als Broker sowie als Anbieter auf. Anbietern, Brokern und Konsumenten kommen unterschiedliche Pflichten und auch Rechte bezüglich Datensouveränität zu. Insbesondere agieren alle Parteien voneinander unabhängig und haben ihre jeweils eigenen Geschäftsmodelle, Prozesse, AGBs und Datenschutzerklärungen. All dies macht es natürlich nicht gerade einfacher, sich seiner Rollen und Verantwortlichkeiten sowie der Verarbeitung seiner Daten klar zu werden.

Definition »Digitales Ökosystem«

Ein Digitales Ökosystem ist ein sozio-technisches System, in dem Unternehmen und Menschen kooperieren, die zwar unabhängig sind, sich von der Teilnahme aber einen gegenseitigen Vorteil versprechen. Ein Digitales Ökosystem hat in seinem Zentrum eine digitale Plattform, die diese Kooperation über Ökosystem-Dienste besonders gut unterstützt.
Ein Digitales Ökosystem adressiert tatsächliche Bedürfnisse potenzieller Konsumenten, liefert einen Mehrwert, der ohne den Ökosystem-Dienst bisher nicht erzielbar war, ist attraktiv sowohl für Anbieter als auch für Konsumenten von Leistungen und bietet Mehrwerte für sämtliche Partner, die am Ökosystem-Dienst beteiligt sind.
Der Gesamtnutzen eines Digitalen Ökosystems ergibt sich somit aus der Kombination der digitalen vermittelnden Plattform und einer großen Menge an Partnern, die zum gegenseitigen Nutzen am Digitalen Ökosystem teilnehmen und durch ihre Interaktionen über die Plattform zu Netzwerkeffekten führen.

Quelle: Fraunhofer IESE | https://www.digitale-oekosysteme.org

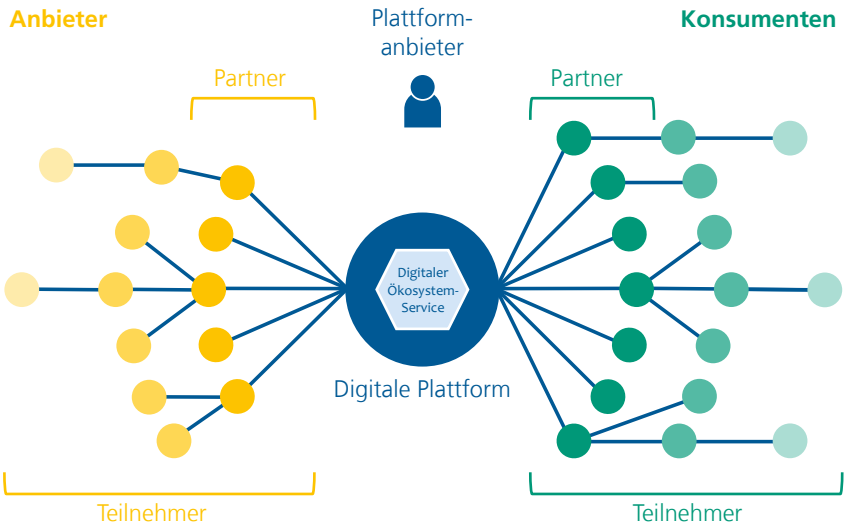

Abbildung 1: Rollen in Digitalen Ökosystemen

Sensible Daten als Treiber

In Digitalen Ökosystemen spielen sensible und personenbezogene Daten eine wichtige Rolle, da sie die Grundlage für datengetriebene Geschäftsmodelle sind. Selbst wenn es sich bei dem Asset selbst nicht um Daten, sondern um Dienstleistungen oder physische Waren handelt, ist die Verarbeitung personenbezogener Daten teils unerlässlich, teils aber auch einfach nur sehr vorteilhaft für die Beteiligten, wie folgende Beispiele zeigen:

- Stammdaten: Diese Daten sind eine Voraussetzung, um die Funktionalitäten, zumindest die Grundfunktionalitäten, eines Digitalen Ökosystems nutzen zu können. Bei einigen Digitalen Ökosystemen wird sogar eine Verifikation der Teilnehmer durchgeführt, um gesetzlichen Pflichten nachzukommen oder um das Vertrauen in das Digitale Ökosystem und die anderen Teilnehmer zu stärken.

- Nutzungsdaten: Bei der aktiven Nutzung des Digitalen Ökosystems fallen weitere Daten an. Die Teilnehmer generieren Daten, zum Beispiel indem sie ein Produkt kaufen, einen Anbieter bewerten oder persönliche Informationen mit einer Community teilen.

- Tracking-Daten: Daneben entstehen auch Daten ohne das direkte Zutun der Nutzer. Unter anderem können Daten über das Verhalten, auch außerhalb der Plattform, getrackt werden. Die Nutzer des Digitalen Ökosystems sind sich teils nicht darüber im Klaren, dass solche Daten erhoben werden.

Grundsätzlich kommt der Plattform aufgrund ihrer Zentralität eine besondere Rolle beim Datenaustausch zu. Allerdings ist es gar nicht zu verhindern, dass Teilnehmer auch außerhalb des Digitalen Ökosystems Daten verarbeiten oder teilen. Zum Beispiel spielt sich die Bezahlung bei eBay-Kleinanzeigen oder nebenan.de meist außerhalb der Plattform ab. Bei Digitalen Ökosystemen im B2B-Bereich werden die Unternehmen zwar miteinander über das Digitale Ökosystem vernetzt, Verträge zwischen den Unternehmen werden jedoch nicht zwangsläufig über das Digitale Ökosystem geschlossen. Somit fließen sensible Daten auch außerhalb der Plattform zwischen den Teilnehmern. Diese Eigenheit ist deshalb für uns relevant, da Umsetzung und Ausübung von Datensouveränität tendenziell einfacher sind, wenn mehr Daten zentral über die Plattform verwaltet werden. Da dies in der Praxis aber häufig nicht so ist, ist es eine große Herausforderung, Datensouveränität unternehmensübergreifend umzusetzen.Für tiefergehende Informationen zum Thema Digitale Ökosysteme verweisen wir aus Platzgründen auf unsere Webseite: https://www.digitale-oekosysteme.org

Die wichtigsten Erkenntnisse

Die Verarbeitung sensibler Daten ist eine Voraussetzung für die Funktionalität von Digitalen Ökosystemen, vor allem für die Vermittlung zwischen Konsumenten und Anbietern.
Es braucht Vertrauen, um Daten zu teilen, jedoch braucht es auch Daten, wie Bewertungen, um das Vertrauen aufzubauen.

2 Datensouveränität

Informiert und selbstbestimmt in der digitalen Welt

Im Hinblick auf den Wert und die Kritikalität der in Digitalen Ökosystemen verarbeiteten Daten muss man sich die Frage stellen, wie erreicht werden kann, dass alle Teilnehmer die Hoheit über ihre Daten wahren können. Wichtig dafür sind dabei primär zwei Aspekte: Zum einen gilt es, Transparenz zu schaffen, also den Teilnehmern die Möglichkeit zu geben, jederzeit nachvollziehen zu können, was mit den eigenen Daten passiert. Zum anderen gilt es Selbstbestimmung zu ermöglichen, also den Teilnehmern die Möglichkeit zu geben, Einfluss auf die Verarbeitung zu nehmen.

Definition »Datensouveränität«

Datensouveränität bezeichnet größtmögliche Kontrolle, Einfluss- und Einsichtnahme auf die Nutzung der Daten durch den Datengebenden. Dieser soll zu einer informationellen Selbstbestimmung berechtigt und befähigt werden und Transparenz über die Datennutzungen erhalten. Datensouveränität wird häufig als Teilgebiet der Digitalen Souveränität verstanden.

Quelle: Fraunhofer IESE

Das dahinterliegende Konzept nennt sich Datensouveränität und bezieht sich auf den Schutz sowohl von personenbezogenen Daten als auch von Unternehmensdaten. In der Praxis gilt es, eine Balance zwischen den folgenden Extremen zu finden:

1. Man bringt die eigenen Daten in das Ökosystem ein und profitiert dadurch direkt (z. B. wenn die Daten Grundlage für die Erbringung des Dienstes sind) oder indirekt (z. B. wenn mir der Dienst aufgrund meiner Datengabe kostenlos angeboten wird). Dies geht dann in der Regel aber mit einem Kontrollverlust über die Daten einher.

2. Die eigenen Daten verbleiben in der eigenen Obhut. In der Folge können sie dann aber nicht nutzbar gemacht werden, ihr Wert wird nicht genutzt und Opportunitäten für digitale Geschäftsmodelle werden verspielt.

Datensouveränität und Informationssicherheit

Um Datensouveränität zu erreichen, ist es zunächst einmal essenziell, für eine angemessene Informationssicherheit zu sorgen. Sogenannte Schutzziele bilden dabei die Eckpfeiler der Informationssicherheit. Die drei wichtigsten werden auch als CIA-Triade bezeichnet: Vertraulichkeit (Confidentiality), Integrität (Integrity) und Verfügbarkeit (Availability). Solche und andere Schutzziele (wie beispielsweise Authentizität, Zurechenbarkeit, Nichtabstreitbarkeit und Verlässlichkeit) werden durch die Planung und Umsetzung von technischen und organisatorischen Maßnahmen (TOM) erreicht. Die konkrete Ausgestaltung von TOMs kann auch innerhalb eines einzigen Digitalen Ökosystems stark variieren, da deren Planung und Umsetzung im Großen und Ganzen den einzelnen Teilnehmern obliegt. Dennoch kann es durchaus zielführend sein, dass der Plattformanbieter einige zentrale Auflagen vorgibt und ihre Einhaltung sicherstellt (z. B. durch die Forderung einer TISAX-Zertifizierung im Automobilbereich).

Datensouveränität und Datenschutz

Im Gegensatz zu Datensouveränität handelt es sich beim Datenschutz um ein klar definiertes Feld. Datenschutz bezeichnet den Schutz natürlicher Personen vor unrechtmäßiger Verarbeitung personenbezogener Daten. Gemäß der Datenschutz-Grundverordnung (DSGVO) [EU16] sind personenbezogene Daten »alle Informationen über eine bestimmte oder bestimmbare natürliche Person (die »betroffene Person«). »Als identifizierbar wird eine natürliche Person angesehen, die direkt oder indirekt, insbesondere mittels Zuordnung zu einer Kennung wie einem Namen, zu einer Kennnummer, zu Standortdaten, zu einer Online-Kennung oder zu einem oder mehreren besonderen Merkmalen, die Ausdruck der physischen, physiologischen, genetischen, psychischen, wirtschaftlichen, kulturellen oder sozialen Identität dieser natürlichen Person sind, identifiziert werden kann.« [EU16]

Definitionen
»Privatheit«, »Privatsphäre« und »Datenschutz«

Privatheit (engl. privacy) bezeichnet den Zustand eines Menschen, in dem dieser ungestört und »für sich« ist. Im Grunde geht es hierbei um die Unversehrtheit der Privatsphäre.

Privatsphäre (engl. private sphere) bezeichnet einen autonomen Bereich privater Lebensgestaltung, in dem der Einzelne Individualität entwickeln kann. Die Privatsphäre ist räumlich und thematisch zu bestimmen, wobei in räumlicher Hinsicht Bereiche erfasst sind, zu denen andere keinen Zugang haben, und in thematischer Hinsicht solche Bereiche, die typischerweise als privat einzustufen sind und bei denen eine Offenlegung als unangemessen empfunden würde, wie z. B. Tagebucheinträge, private E-Mails oder Details einer Beziehung oder Ehe.

Datenschutz (engl. data protection) bezeichnet den Schutz vor unrechtmäßiger Verarbeitung personenbezogener Daten. Personenbezogene Daten sind nach Art. 4 Nr. 1 DSGVO solche, die sich auf identifizierte oder identifizierbare Personen beziehen. Der Schutz personenbezogener Daten ist gesetzlich in Art. 8 der europäischen Grundrechtecharta normiert. Bei »Datenschutz« geht es indes nicht um den Schutz der personenbezogenen Daten selbst, sondern um den Schutz des Persönlichkeitsrechts der betroffenen Person.

Quelle: D'accord-Projekt | https://www.daccord-projekt.de

Ähnlich wie bei der CIA-Triade für die Informationssicherheit lassen sich auch beim Datenschutz grundlegende Datenschutzziele formulieren, auch wenn dies in der Literatur weniger verbreitet ist. Beispielsweise wird im Standard-Datenschutzmodell [SDM20] die CIA-Triade dahingehend um die folgenden vier Gewährleistungsziele erweitert:

- Datenminimierung (also Reduzierung der Erhebung, Speicherung und Verarbeitung von Daten auf das notwendige Minimum)
- Nichtverkettung (also Verhinderung des Zusammenführens von Daten, die eigentlich zu unterschiedlichen Zwecken erhoben wurden)
- Transparenz (also Schaffen von Nachvollziehbarkeit von Verarbeitungstätigkeiten)
- Intervenierbarkeit (also Umsetzung der zustehenden Rechte auf Benachrichtigung, Auskunft, Berichtigung, Löschung, etc.)

In diesem Zusammenhang ist es außerdem wichtig, sich der Trennung der Begriffe »Privatheit«, »Privatsphäre« und »Datenschutz« bewusst zu sein, da diese in der Praxis häufig vermischt werden (siehe Info-Kasten).

Wie steht nun aber Datensouveränität zum Datenschutz? Wie bereits beschrieben steckt hinter Datensouveränität die Idee, Nutzer zu befähigen, selbstbestimmt über »ihre« Daten verfügen zu können. Dabei ist Datensouveränität kein Ersatz für Datenschutz. Ganz im Gegenteil: Die in der DSGVO geregelten Rechte und Pflichten schaffen häufig überhaupt erst die Voraussetzung dafür, dass Nutzer selbstbestimmt handeln können (z. B. im Rahmen von Einwilligungen oder dem Löschrecht). Auf der anderen Seite bezieht sich Datenschutz eben nur auf personenbezoge Daten. Was ist aber mit Daten ohne Personenbezug? Schaut man genauer hin, herrschen hier häufig ähnliche Anforderungen der Anbieter und Konsumenten. So nehmen Unternehmen häufig nur dann an digitalen Geschäftsmodellen teil, wenn sie weiterhin die Kontrolle über »ihre« Daten (z. B. Produktionsdaten, IIoT-Daten) haben. Die vom Datenschutz zugesprochenen Rechte lassen sich also sehr gut auch auf Daten ohne Personenbezug anwenden, wenngleich es hier keine entsprechende rechtliche Regelung gibt.

Hinweis: Obwohl wir argumentiert haben, dass Privacy und Datenschutz (bzw. Data Protection) zwar verwandt, aber nicht identisch sind, verwenden wir die Begriffe in diesem Bericht teilweise synonym. Der Grund dafür ist der sehr enge Bezug zum Themenfeld »Usable Security & Privacy« (vgl. Kapitel 4). Der Begriff »Usable Privacy« ist hier in der Literatur weitaus gebräuchlicher als »Usable Data Protection«, auch wenn letzteres unserer Meinung nach zutreffender wäre.

Die wichtigsten Erkenntnisse

Transparenz und Selbstbestimmung sind Eckpfeiler der Datensouveränität. Bei personenbezogenen Daten greifen hier primär die Rechte und Pflichten aus der DSGVO. Bei sonstigen sensiblen Daten gibt es keine durchgängigen gesetzlichen Regelungen – viele Konzepte lassen sich aber übertragen und bieten in Summe Vorteile für alle Teilnehmer von Digitalen Ökosystemen.

3 Usability & User Experience

Der Mensch im Mittelpunkt

Ein System kann seinen Zweck nur dann erfüllen, wenn es von den Nutzern wie vorgesehen verwendet wird. Das bedeutet aber auch, dass Systeme so gestaltet werden müssen, dass ihre Nutzer sie effizient, effektiv und auf zufriedenstellende Weise nutzen können. Dies wird als »Usability« (dt. Gebrauchstauglichkeit oder Benutzerfreundlichkeit) bezeichnet.

Definition »Usability«

Usability bezieht sich auf das »Ausmaß, in dem ein System, ein Produkt oder eine Dienstleistung von bestimmten Benutzern verwendet werden kann, um bestimmte Ziele in einem bestimmten Nutzungskontext mit Effektivität, Effizienz und Zufriedenheit zu erreichen.

Quelle: ISO 9241

Dabei gibt es eine ganze Reihe von Systemeigenschaften, die Voraussetzung für eine gute Usability sind (vgl. [Nie94]). Beispielsweise sollte ein System die Nutzer dabei unterstützen, Fehler bei der Benutzung zu vermeiden, und falls doch Fehler auftreten, die Nutzer dabei unterstützen, diese zu korrigieren. Darüber hinaus sollte das System die Sprache des Nutzers sprechen und die Begriffe einheitlich verwenden. Außerdem sollte das Design ästhetisch und minimalistisch sein, d.h. der Nutzer sollte nur die für ihn notwendigen Informationen angezeigt bekommen, um Ablenkungen zu vermeiden [Nie94].

Die wichtigsten Erkenntnisse

Hohe Usability und positive UX sind eine Voraussetzung für die Akzeptanz eines Systems. Dabei können in Digitalen Ökosystemen auch vermeintlich lokale Probleme (z. B. bei einem Dienst) negative Auswirkungen auf die UX des gesamten Ökosystems haben.

Wichtig ist, dass ein System nicht für alle Nutzer in jedem Kontext benutzerfreundlich sein muss. Usability bezieht sich vielmehr auf eine vorher festgelegte Kombination aus Zielgruppen und deren Zielen in einem konkreten Nutzungskontext.

Neben einer guten Usability, welche einen klaren Fokus auf die direkte Nutzung eines Systems hat, gilt es eine ganze Reihe weiterer Faktoren zu beachten, die sich direkt auf die Akzeptanz auswirken und für das (erwartete und tatsächliche) »Benutzungserlebnis« relevant sind. Dies wird als User Experience (UX) bezeichnet.

Definition »User Experience« (UX)

User Experience (UX) bezieht sich auf »die Wahrnehmungen und Reaktionen einer Person, die sich aus der Verwendung und/oder der erwarteten Verwendung eines Produkts, Systems oder einer Dienstleistung ergeben.«

Quelle: ISO 9241

In Digitalen Ökosystemen sind gute Usability und UX besonders wichtig, um wettbewerbsfähig zu bleiben. Negative Erfahrungen und schlechte Bewertungen können schnell und nachhaltig dazu führen, dass man von Mitbewerbern verdrängt wird. Auf der anderen Seite können in Digitalen Ökosystemen auch vermeintlich lokale Probleme (z. B. bei Problemen eines einzelnen Dienstes) negative Auswirkungen auf die UX des gesamten Ökosystems haben. Daher setzt beispielsweise Apple von Anfang an sehr starke Richtlinien für Apps in seinem App-Store durch, was sich schlussendlich positiv auf die Zufriedenheit der Nutzer ausgewirkt hat.

Was Usability und UX im Zusammenhang mit Datensouveränität bedeuten, werden wir im nächsten Kapitel erörtern.

4 Usable Security & Privacy

Nutzerzentrierter Schutz sensibler Daten

Security- und Datenschutzmaßnahmen weisen quasi immer eine hohe Komplexität und Kritikalität auf. Dies macht es für die Entwickler, Anbieter und Administratoren von Sicherheitslösungen besonders herausfordernd, für eine gute Usability und UX zu sorgen. Gleichzeitig ist dies für die Akzeptanz und Effektivität der Lösungen absolut essenziell. Dies gilt ebenso für den Bereich Datensouveränität. Schon allein das Erreichen von Transparenz stellt in Anbetracht der mannigfaltigen Beziehungen zwischen den Ökosystemteilnehmern und der Menge an ausgetauschten Daten eine große Herausforderung dar. Dem nutzerzentrierten Schutz sensibler Daten widmet sich das Forschungsfeld »Usable Security & Privacy« (USP).

Definition »Usable Security & Privacy«

Usable Security & Privacy (USP) bezieht sich auf inter- und transdisziplinäre Methoden, um Maßnahmen zur Verbesserung der Security und des Datenschutzes so zu gestalten, dass (1) die Nutzer und Entwickler der Maßnahmen in ihren sicherheits- oder datenschutzrelevanten Zielen und Projekten bestmöglich unterstützt werden [GL14] [SSH+16], und (2) die Maßnahmen zu einer durchgehend positiven UX beitragen.

Quelle: basierend auf der Definition des Arbeitskreises USP der German UPA

Aufgrund der engen Verzahnung von Datensouveränität mit Datenschutz sind viele Herausforderungen, Erkenntnisse und Lösungen aus dem Bereich »Usable Privacy« auf Datensouveränität übertragbar. Wir werden uns daher in diesem Bericht, auch wenn wir über USP reden, verstärkt auf den Teilbereich »Usable Privacy« konzentrieren, was aber keineswegs die Bedeutung von »Usable Security« herabstufen soll.

Für USP sind insbesondere Stakeholder aus drei Bereichen relevant: aus dem Security-Bereich, aus dem HCI-Bereich und aus dem Datenschutzbereich. Darüber hinaus gelten die folgenden Grundprinzipien:

1. Security & Privacy by Design: Dieses Prinzip bedeutet, dass Sicherheits- und Datenschutzmaßnahmen von Anfang an in die Systemgestaltung und -entwicklung einbezogen werden. Ziel ist es, sicherzustellen, dass technische und organisatorische Maßnahmen nicht nachträglich in das System eingebaut werden, sondern tief und systematisch eingebettet sind, um Security und Datenschutz sowie eine reibungslose Mensch–Maschine-Interaktion zu gewährleisten.

2. Security & Privacy by Default: Bei diesem Prinzip geht es um benutzerfreundliche, sichere und datenschutzfreundliche Voreinstellungen. Die Idee dahinter ist, dass gute Security und guter Datenschutz nicht davon abhängig sein dürfen, dass die Nutzer zunächst entsprechende Einstellungen vornehmen. Stattdessen sollte gute Security und guter Datenschutz der Standardfall sein. Gleiches gilt natürlich auch bei der Datensouveränität. So sinnvoll dieses Prinzip ist, sollte man sich dennoch darüber im Klaren sein, dass restriktive Voreinstellungen zu einer eingeschränkten Funktionalität führen können. Es ist dann in der Verantwortung des Nutzers, zwischen Privatsphäre und Funktionalität abzuwägen.

Viele weitere Aspekte von USP werden wir in den folgenden Kapiteln des Berichts streifen, wenn es beispielsweise darum geht, welche Zielgruppen und Herausforderungen es bei der Umsetzung benutzerfreundlicher Datensouveränität zu beachten gilt und welche Lösungsansätze und -bausteine es gibt.

Die wichtigsten Erkenntnisse

Transparenz und Selbstbestimmung sind Eckpfeiler der Datensouveränität. Bei personenbezogenen Daten greifen hier primär die Rechte und Pflichten aus der DSGVO. Bei sonstigen sensiblen Daten gibt es keine durchgängigen gesetzlichen Regelungen – viele Konzepte lassen sich aber übertragen und bieten in Summe Vorteile für alle Teilnehmer von Digitalen Ökosystemen.

TEIL 2:
ZIELE & GRENZEN

5 Zielgruppen
6 Grenzen
7 Transparenz
8 Selbstbestimmung

5 Zielgruppen

Für wen benutzerfreundliche Datensouveränität wichtig ist

Bevor wir uns darüber Gedanken machen können, wie man Datensouveränität benutzerfreundlich umsetzt, müssen wir zunächst klären, wer hierfür überhaupt verantwortlich ist und welche Zielgruppen adressiert werden.

Um zu verstehen, wer für die gebrauchstaugliche Umsetzung von Datensouveränität verantwortlich ist, sollte man sich zunächst bewusst machen, dass Digitale Ökosysteme aus einer Vielzahl aufeinander aufbauender und voneinander abhängiger Systemkomponenten bestehen. Diese werden naturgemäß nicht von einem einzigen Anbieter entworfen, entwickelt und vertrieben. Es ergibt sich vielmehr eine Kette, wie Abbildung 3 verdeutlicht.

Abbildung 3: Kette von USP-Anbietern und USP-Nutzern

Auf der untersten Ebene stellen Technologieanbieter generische Sicherheitslösungen bereit. Die vom Fraunhofer IESE entwickelten »MYDATA Control Technologies« (kurz MYDATA) sind ein solches Beispiel. Diese Lösungen werden vom Plattformanbieter sowie von den Ökosystempartnern zur Entwicklung ihrer eigenen Systeme eingesetzt. Im Falle von MYDATA würde man so auf Plattform- und Dienstebene eine regelbasierte Maskierung und Filterung ermöglichen. Diese kann schlussendlich von den Endnutzern dazu verwendet werden, ihre Bedarfe hinsichtlich Datensouveränität festzulegen und durchsetzen zu lassen (z. B. durch das Entfernen des Personenbezugs).

Somit ist jede Ebene sowohl Anwender der Maßnahmen der darunterliegenden Ebene(n) als auch Anbieter von Maßnahmen für die darüberliegende(n) Ebene(n). Eine wenig benutzerfreundliche Umsetzung von Datensouveränität birgt also das Risiko, dass die höheren Ebenen Probleme bei der Verwendung haben oder Probleme an höhere Ebenen weitergeben.

Die Endnutzer sind natürlich unsere primäre Stakeholder-Gruppe, da sie diejenigen sind, die Datensouveränität am Ende ausüben. Auf den unteren drei Ebenen gibt es eine Vielzahl weiterer Stakeholder, wie Entwickler, Administratoren, Lieferanten, Systemintegratoren, Wartungspersonal sowie die Unternehmensleitung [HPD+16]. All diese Stakeholder haben sehr unterschiedliche Sichtweisen und müssen entsprechend bei der Anforderungserhebung und beim Lösungsdesign berücksichtigt werden (vgl. Kapitel 9). Dennoch fokussieren wir uns im Folgenden primär auf die Entwickler, da diese den direktesten Einfluss, bzw. den größten Mehrwert, von USP haben.

Entwickler

Generell gilt im Bereich der Security die allgemeine Empfehlung, so wenig Funktionalität wie möglich selbst zu entwickeln und stattdessen auf etablierte, möglicherweise sogar zertifizierte, Komponenten (z. B. Softwarebibliotheken) zurückzugreifen. Gleichzeitig ist leider festzustellen, dass es sowohl für Digitale Ökosysteme als auch für Datensouveränität bisher nur wenige etablierte Standardlösungen gibt. Schaut man sich die Forschungs- und Entwicklungslandschaft an, so ist es aber auch nur eine Frage der Zeit, bis sich dies ändert. Projekte wie GAIA-X, International Data Spaces und Lösungen wie MYDATA

verdeutlichen diesen Trend. Insofern ist der Hintergrund dieser Empfehlung – nämlich, dass Sicherheit und Datenschutz hochkomplexe Bereiche sind und sich daher bei einer Eigenentwicklung leicht Fehler oder Sicherheitslücken einschleichen können – selbstverständlich dennoch valide und in unserem Kontext relevant.

Dies macht die Entwickler solcher Lösungen selbst zu Anwendern, wenn sie bestehende Softwarebibliotheken oder Systemkomponenten nutzen – nur auf einer anderen, technischeren Ebene als die Endanwender. Im Gegensatz zur Endnutzerebene wirkt sich eine schlechte Usability oder UX der zu integrierenden Komponenten jedoch systematisch auf alle Ökosystemteilnehmer aus (z. B. durch Sicherheitslücken). Eine ähnliche Argumentation gilt im Übrigen für Systemadministratoren, die Sicherheitsmaßnahmen zuverlässig konfigurieren und warten müssen. Auch hier können kleine Fehler schwerwiegende Folgen haben. Von Usability-Problemen sind in solchen Fällen nicht nur einzelne Nutzer betroffen, sondern alle Teilnehmer.

Entwickler sind dabei stark heterogen. Steven Clarke [Cla10], der Probanden in einer Vielzahl von Usability-Studien beobachtet hat, klassifiziert Entwickler in drei verschiedene Benutzertypen:

- Opportunistische Entwickler: Konzentrieren sich darauf, ihre Aufgabe schnell zu lösen; verfolgen einen explorativen Bottom-Up-Ansatz; häufig anzutreffen.
- Gründliche Entwickler: Versuchen zunächst ein ganzheitliches Verständnis für die Technologie zu erlangen; verfolgen einen Top-Down-Ansatz; selten anzutreffen.
- Pragmatische Entwickler: Beginnen typischerweise mit einem Bottom-Up-Ansatz; wechseln bei Problemen zu einem Top-Down-Ansatz.

Die jeweiligen Eigenschaften und Herangehensweisen dieser Typen sollten bereits bei der der Gestaltung von Systemen (insb. deren APIs) und deren Dokumentation berücksichtigt werden.

Endnutzer

Wenn man über »den Endnutzer« redet, sollte man sich zunächst darüber bewusst sein, ob man im konkreten Fall über einen Nutzer redet, dessen sensible Daten verarbeitet werden (sog. »Datengeber«, bzw. »betroffene Personen« im Bereich Datenschutz) oder über einen Nutzer, der wiederum selbst sensible Daten anderer verarbeitet (sog. »Datennutzer«).

Darüber hinaus unterscheiden sich Nutzer stark in ihren individuellen Bedarfen und Fähigkeiten hinsichtlich Datensouveränität. Es lohnt sich daher, einen genaueren Blick auf die Klassifizierung von »Deutschland sicher im Netz« [DsiN21] zu werfen, die derzeit fünf Nutzertypen unterscheidet:

- Gutgläubige Nutzer (42,9 Prozent): Verfügen über Sicherheitskenntnisse, wenden diese aber nicht an, da sie nicht wissen, dass sie Sicherheitsbedrohungen ausgesetzt sind.
- Antreibende Nutzer (19,3 Prozent): Probieren gerne neue Dienste aus. Sie sind gut über Sicherheitsrisiken informiert und wenden Sicherheitsmaßnahmen an, indem sie beispielsweise Systeme regelmäßig aktualisieren.
- Fatalistische Nutzer (16,5 Prozent): Sehen überall Gefahren lauern, zweifeln an der Wirksamkeit von Sicherheitsmaßnahmen. Erwarten, dass Anbieter sich um ihre Privatsphäre und Sicherheit kümmern.
- Bedachtsame Nutzer (17 Prozent): Stehen neuen digitalen Diensten skeptisch gegenüber; denken über Sicherheitsfragen nach, bevor sie einen Dienst nutzen.
- Außenstehende Nutzer (4,3 Prozent): Sind von neuen Diensten überfordert; haben nur wenig Sicherheitswissen; wenden kaum Sicherheitsmaßnahmen an; wünschen sich stärkere Schutzbestimmungen durch den Staat.

Letztendlich helfen allgemeine Kategorisierungen nur bis zu einem bestimmten Grad, da Digitale Ökosysteme sich sehr stark unterscheiden. Und selbst innerhalb eines Digitalen Ökosystems kann es starke kulturelle Unterschiede geben. In einer Studie gaben zum Beispiel 65 Prozent der Teilnehmer aus Zypern an, dass sie bereit wären, ihre Gesichtsbilder mit der Regierung zu teilen, verglichen mit lediglich neun Prozent der Teilnehmer aus Deutschland [FRA20]. Daher sollte man seine eigene Nutzerschaft stets genau untersuchen, klassifizieren und beispielsweise mittels Personas beschreiben. Entsprechende Methoden und Vorlagen finden sich in der einschlägigen Literatur.

Die wichtigsten Erkenntnisse

Systeme und ihre Schutzmaßnahmen sollten sich an die Nutzer anpassen, nicht umgekehrt. Nicht alle Nutzer sind dabei gleich und es gibt bei Digitalen Ökosystemen sicherlich keine »Einheitslösung«. Wir empfehlen eine Klassifizierung von Nutzern, indem sie als Personas dokumentiert werden, um die spezifischen Merkmale der Zielgruppen im Auge zu behalten.

6 Grenzen

Teils paradox und absurd – umso wichtiger zu kennen

Egal, wie viel Mühe und Aufwand man investiert, um Datensouveränität benutzerfreundlich und mit positiver UX umzusetzen – man wird schlussendlich keine Lösung erreichen, die für jeden und in jeder Hinsicht perfekt ist. Das heißt natürlich nicht, dass man das Thema damit auf sich beruhen lassen sollte. Man muss sich aber einiger (teils unveränderlicher) Eigenschaften und Einschränkungen bewusst sein. Einige davon haben ihren Ursprung in der menschlichen Psyche. Andere resultieren daraus, dass man Qualitätseigenschaften wie Usability und UX natürlich nicht isoliert von anderen Eigenschaften betrachten kann.

Das Privacy-Paradoxon

Das Privacy-Paradoxon beschreibt eine Ambivalenz zwischen dem, was Nutzer in Bezug auf ihre Privatsphäre wollen, und dem, was sie wirklich tun. Mehrere Studien (z. B. [RFP18]) bestätigen, dass Nutzer ihre Privatsphäre zwar prinzipiell wertschätzen, sie sich aber nicht entsprechend verhalten.

Hierfür gibt es mehrere Gründe. Erstens erfordert die korrekte Einrichtung und Anwendung von Datenschutzmaßnahmen ein gewisses Maß an Wissen und bestimmte Fähigkeiten, über welche manche Nutzer schlicht nicht verfügen [GVG17]. Gerade in Digitalen Ökosystemen sind die Nutzergruppen extrem heterogen, sodass es in der Regel keine Lösung gibt, die für alle Nutzer gleichermaßen gut benutzbar ist. An dieser Stelle können Datenschutz-Personas helfen, die Nutzerschaft besser zu verstehen.

Ein weiterer Grund ist, dass Entscheidungen zum Schutz der Privatsphäre einen großen Einfluss darauf haben können, wie sich ein System verhält. So sind die Nutzer schon in »traditionellen Systemen« häufig dazu gezwungen, einen Kompromiss zwischen dem Schutz ihrer Daten und anderen Qualitäten, wie z. B. Komfort, einzugehen. In Digitalen Ökosystemen ist dieser Konflikt häufig noch größer, da der gesamte Mehrwert (inkl. diverser Geschäftsmodelle) des Digitalen Ökosystems auf der Bereitstellung und Nutzung von Daten basiert. Daher ist die Gefahr hier umso größer, dass Nutzer ihre Datensouveränität aufgeben, obwohl sie dies eigentlich nicht wollen.

Zu guter Letzt ist das Beschäftigen mit Datenschutz für den Nutzer immer mit Aufwand verbunden und daher eine Kosten-Nutzen-Abwägung. Dies machen Unternehmen sich durch sogenannte »Dark Patterns« teilweise sogar absichtlich zu Nutze, wie wir später in Kapitel 8 am Beispiel der Cookie-Banner noch sehen werden. Von solchen Praktiken ist natürlich, auch rechtlich, abzuraten. Stattdessen sollte man stets versuchen, die Einstiegshürde und den Aufwand für die Nutzer so gering wie möglich zu halten.

Streng betrachtet gefährdet das Privacy-Paradoxon eine wichtige Grundannahme hinter Datensouveränität, nämlich, dass Nutzer frei und entsprechend ihren Interessen selbstbestimmt handeln. Insofern können wir nur nochmals betonen, dass Datensouveränität den Datenschutz nicht ersetzen oder aufweichen darf, sondern ihn lediglich sinnvoll ergänzen sollte.

Datensouveränität ad absurdum

Es mag anfangs wenig plausibel erscheinen, ist aber durchaus ein reales Risiko: Datensouveränität kann auch negative Auswirkungen auf die Privatsphäre haben. Wir geben an dieser Stelle drei Beispiele, welche in [PF20] vertieft diskutiert werden:

Transparenz vs. Überwachung: Je stärker Datenflüsse und Datenverarbeitungen transparent gemacht werden, umso höher ist auch die Gefahr, dass dadurch sensible Informationen über jene Personen offengelegt werden, die die Daten verarbeiten. Wenn beispielsweise der genaue Zeitpunkt und die Person einer Datennutzung offengelegt wird, kann die betroffene Person Rückschlüsse auf das Arbeitsverhalten des Datennutzers ziehen. Anonymisierung kann diesen Konflikt zumindest teilweise auflösen.

Vertrauen vs. Misstrauen: Bei einer hohen Transparenz besteht die Gefahr, dass Nutzer die gezeigten Informationen nicht richtig einordnen können und fehlerhafte Schlüsse ziehen. Außerdem werden sie gegebenenfalls auf Sachverhalte aufmerksam, die ihnen überraschend erscheinen. Auch sollten die Gründe und Ziele bei neuen Maßnahmen (wie der Steigerung von Transparenz) klar gemacht werden. Die betroffenen Personen könnten sich sonst beispielsweise fragen, ob es einen Datenschutzvorfall gegeben hat, der zu dieser Einführung geführt hat.

Datensouveränität vs. sozialer Druck: Wenn sich Datengeber und Datennutzer kennen, z. B. wenn sie eine direkte Geschäftsbeziehung haben, kann der Datengeber sozialem Druck ausgesetzt sein, seine Daten bereitzustellen. Dies gefährdet dann natürlich direkt seine Souveränität.

Diese beschriebenen Beispiele verdeutlichen, dass es eine »ideale« Lösung nicht gibt oder geben kann. Selbst wenn die Umsetzung von Datensouveränität aus Sicht der Nutzer zunächst ideal umgesetzt zu sein scheint, müssen viele Faktoren beachtet und gegeneinander abgewogen werden.

In Bezug auf das Datenschutzparadoxon stellt sich die Frage, ob es überhaupt möglich ist, das Problem auf sinnvolle Weise zu lösen. Denn unabhängig davon, ob die Nutzer ihre Datensouveränität wahrnehmen oder nicht, ist die Privatsphäre eines anderen gegebenenfalls gefährdet. Die Maxime, den Nutzern möglichst viel Transparenz und Partizipation zu gewähren, ist daher nicht haltbar. Stattdessen sind eine Einzelfallbetrachtung und die Abwägung der Interessen unabdingbar.

Rechtliche und soziale Grenzen

Schlussendlich sollte es für alle Beteiligten klar sein, dass Datensouveränität natürlich nicht gleichbedeutend damit ist, dass Nutzer uneingeschränkte Freiheit hinsichtlich der Verarbeitung ihrer Daten haben. So gibt es natürlich diverse Situationen (z. B. Strafverfolgung) oder Gesetze (z. B. Aufbewahrungspflichten), die einen höheren Stellenwert haben als die Selbstbestimmung des Einzelnen. Dies ist auch in der DSGVO entsprechend geregelt (bspw. in Artikel 2, Absatz 2d oder Artikel 6, Absatz 1e). Schlussendlich gilt bei Datenschutz, wie auch bei Datensouveränität der Grundsatz: »Die Freiheit des Einzelnen endet dort, wo die Freiheit des Anderen beginnt.«

Die wichtigsten Erkenntnisse

Nur weil Nutzer sagen, dass sie ihre Privatsphäre schützen möchten, darf man nicht davon ausgehen, dass sie auch tatsächlich entsprechend handeln. In Digitalen Ökosystemen ist es für die Nutzer häufig besonders verlockend, Daten zu teilen.

Außerdem kann die Datensouveränität negative Auswirkungen haben. Schlussendlich müssen die Interessen aller Ökosystemteilnehmer gegeneinander abgewogen werden.

7 Transparenz

Datenverarbeitung nachvollziehen, überprüfen und bewerten

Transparenz bei der Verarbeitung sensibler Daten wird zunehmend von den Nutzern und, im Fall personenbezogener Daten, auch vom Gesetzgeber gefordert.

Definition »Transparenz«

Transparenz bedeutet, dass die Erhebung und Verarbeitung von Daten in Verfahren und deren Nutzung mit zumutbarem Aufwand geplant, nachvollzogen, überprüft und bewertet werden kann.

Quelle: basierend auf [RB11]

In der Praxis müssen hierzu komplexe Sachverhalte so aufbereitet werden, dass Nutzer sie verstehen und interpretieren können. Da in Digitalen Ökosystemen sensible Daten in großem Umfang verarbeitet werden und daran eine Vielzahl von Unternehmen beteiligt sind, ist dies kein leichtes Unterfangen. Wir gehen an dieser Stelle auf drei Möglichkeiten zur Schaffung von Transparenz in Digitalen Ökosystemen ein: nutzerfreundliche Datenschutz- erklärungen, einheitliche Bildsymbole und die Nachverfolgung von Datenflüssen.

Nutzerfreundliche Datenschutzerklärungen

In der Praxis sind Datenschutzerklärungen aktuell das (einzige) Mittel der Wahl, wenn es darum geht, den Nutzern Informationen über die Verarbeitung ihrer Daten zukommen zu lassen.

Nun ist allerdings hinreichend belegt, dass die Akzeptanz von Datenschutzerklärungen schon bei »traditionellen« Webseiten sehr gering ist. Umfragen (z. B. [OO20] [TEC+11] [Sym15]) zeigen, dass etwa drei Viertel der Nutzer Datenschutzerklärungen gar nicht lesen und die verbleibenden Nutzer sie höchstens überfliegen. Ansätze, die Lesbarkeit [EFB15] [MCG06], die Verständlichkeit [RBC+15], das Design [Wal18] oder den grundsätzlichen Aufbau [Fet18] [OGW+19] [Fet20] von Datenschutzerklärungen zu verbessern, haben bisher in der Praxis wenig Früchte getragen. Bei Digitalen Ökosystemen verstärkt sich dieses Problem noch, da es sich um ein für den Nutzer schwer zu überblickendes und intransparentes Netzwerk handelt, bei dem jedes teilnehmende Unternehmen seine eigene Datenschutzerklärung hat. Abhilfe schaffen kann hier der Plattformanbieter, indem er Vorgaben für Struktur und Gestaltung von Datenschutzerklärungen macht und den Nutzern aggregierte Informationen zur Verfügung stellt. Auch das Aufbrechen der Datenschutzerklärung in kleine, auf die jeweilige Nutzungssituation abgestimmte Häppchen (sogenannte kontextuelle Datenschutzerklärungen) erscheint hier als eine zielführende Strategie.

Einheitliche Bildsymbole

Nach Art. 12 DSGVO müssen Informationen »in präziser, transparenter, verständlicher und leicht zugänglicher Form in einer klaren und einfachen Sprache« bereitgestellt werden. Wie bereits beschrieben, mündet dies in der Praxis meist in textuellen Datenschutzerklärungen. Dabei ist ausdrücklich die Möglichkeit vorgesehen, einheitliche Bildsymbole (Icons) für die Übermittlung von Datenschutzinformationen zu verwenden (vgl. DSGVO Artikel 12, Absätze 7 und 8). Diese Icons könnten z. B. dazu beitragen, die von den Nutzern so vehement ignorierten Datenschutzerklärungen in Zukunft benutzerfreundlicher zu gestalten. Gerade bei kontextuellen Datenschutzerklärungen können solche Bildsymbole einen großen Mehrwert liefern, wenn sie im gesamten Digitalen Ökosystem konsistent verwendet werden.

Es werden keine personenbezogenen Daten zu anderen Zwecken als denen, für die sie erhoben wurden, verarbeitet.

Es werden keine persönlichen Daten an kommerzielle Dritte weitergegeben.

Abbildung 4: Beispiele für Bildsymbole, die wegen ihres geringen Informationswerts abgelehnt wurden (nicht verwenden!).

Diverse Initiativen haben sich daran versucht, gute Symbole zu entwickeln, z. B. das »Privacy Icons Forum« (Abbildung 4). Leider hat sich bis heute kein Vorschlag durchgesetzt. Im Falle Digitaler Ökosysteme ist es daher am Plattformanbieter, für einheitliche Regelungen bzw. für eine einheitliche Beschreibung und Visualisierung zu sorgen.

Nachverfolgung von Datenflüssen

Ein weiteres Problem von Datenschutzerklärungen ist, dass sie statisch und allgemein sind. So erläutern Datenschutzerklärungen lediglich, dass gewisse Datenkategorien (z. B. Adressdaten) unter gewissen Umständen (z. B. bei einer Bestellung) an gewisse Partner (z. B. Versanddienstleister) weitergegeben werden könnten. Welches konkrete Datum aber tatsächlich bei welcher Bestellung an welchen Partner weitergegeben wurde, ist selten nachvollziehbar.

Gerade in Digitalen Ökosystemen, wo eine hohe Dynamik und eine hohe Anzahl an Teilnehmern eine Kerneigenschaft ist, würde sich aber genau hierdurch ein Mehrwert für die Nutzer ergeben. In gewissem Maß spielt uns die Zentralität Digitaler Ökosysteme an dieser Stelle sogar in die Karten, da es hier technisch häufig vergleichsweise einfach ist, Datenflüsse auf der Plattform zu protokollieren. Die größere Herausforderung besteht hier vielmehr darin, die zur Verfügung stehenden Daten verständlich und benutzerfreundlich aufzubereiten.

Abbildung 5 zeigt hier beispielhaft verschiedene Möglichkeiten um Datenflüsse darzustellen. Im oberen Beispiel kann man durch Klicken auf eine Datenkategorie sehen, welche Dienste im Digitalen Ökosystem Zugriff auf die Daten haben. Im mittleren Beispiel werden die Verarbeitungszwecke und die Speicherdauer beim Datenfluss noch einmal deutlicher hervorgehoben. Im unteren Beispiel kann man interaktiv nachverfolgen welche Daten wohin geflossen sind.

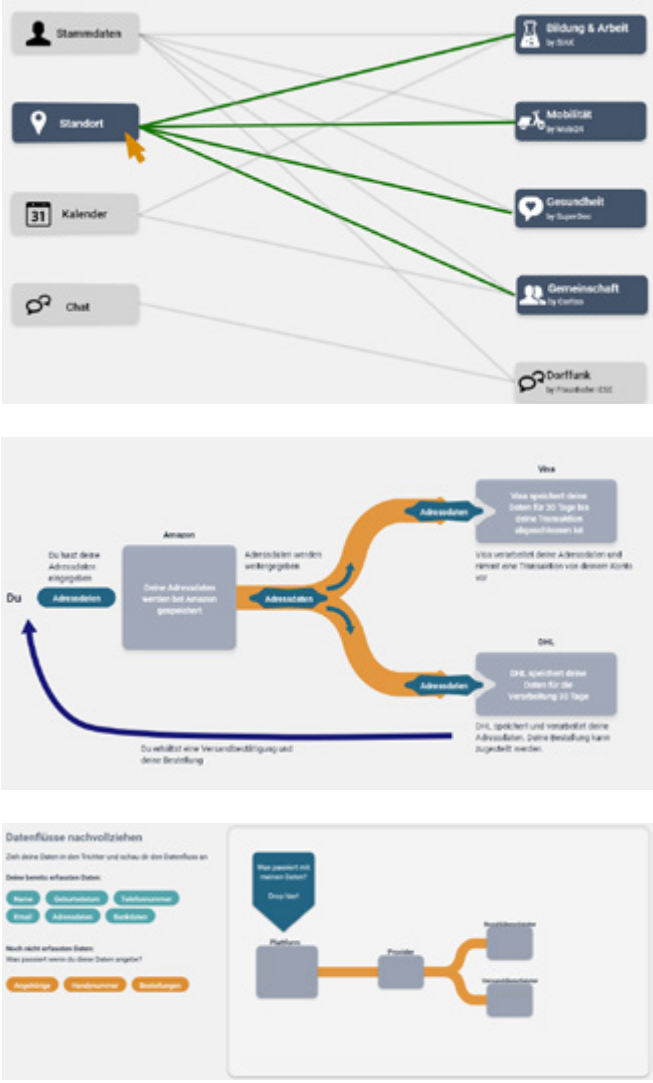

Abbildung 5: Möglichkeiten zur Darstellung von Datenflüssen

Die wichtigsten Erkenntnisse

Zur Schaffung von Transparenz muss die Nutzung der Daten mit zumutbarem Aufwand nachvollzogen, überprüft und bewertet werden können.

Dabei bedeutet Transparenz auch, konkret zu werden sowie Informationen zur Laufzeit zu erfassen und zugänglich zu machen.

8 Selbstbestimmung

Daten teilen, Kontrolle behalten

Auf Grundlage einer hohen Transparenz und Informiertheit kann man, unter Berücksichtigung der in Kapitel 6 beschriebenen Grenzen, davon ausgehen, dass der Datengeber selbst darüber entscheiden kann, wie seine Daten verwendet werden dürfen. Um dies zu ermöglichen, werden zwei Dinge benötigt:

1. Dem Datengeber muss die Möglichkeit gegeben werden, seine Bedarfe und Anforderungen hinsichtlich der Verarbeitung festzulegen.

2. Die festgelegten Regeln müssen verbindlich von allen beteiligten Teilnehmern umgesetzt werden.

Beide Aspekte sind sehr herausfordernd. Auf den ersten Aspekt werden wir direkt im Folgenden eingehen, indem wir uns die Herausforderungen beim Einwilligungsmanagement und bei Einstellungsmöglichkeiten generell ansehen. Auf den zweiten Aspekt kommen wir in Kapitel 10 zurück.

Durchgängiges Einwilligungsmanagement

Im Bereich Datenschutz sieht die DSGVO vor, dass Unternehmen personenbezogene Daten nur dann verarbeiten dürfen, wenn mindestens eine von sechs Voraussetzungen erfüllt ist. Eine dieser Voraussetzungen ist, dass die betroffene Person ihre Einwilligung gegeben hat. Bei Daten ohne Personenbezug gibt es solche Einschränkungen prinzipiell nicht, wenngleich sie durchaus plausibel übertragbar sind und der Selbstbestimmung des Datengebers zu Gute kommen.

Beim Datenschutz treten an dieser Stelle aber auch die Schattenseiten zu Tage: Aufgrund der durch die DSGVO geschaffenen Unsicherheiten werden die Nutzer oft mit Einwilligungsformularen konfrontiert, obwohl dies nicht notwendig ist. Dies wiederum führt zu einer erhöhten Belastung und möglicherweise sogar zu unnötigem Unbehagen bei den Nutzern. Als Betreiber sollte man daher sorgfältig prüfen, wann eine Einwilligung notwendig ist und wann nicht.

Umgekehrt gibt es einige Dinge zu beachten, wenn eine Einwilligung eingeholt wird. Zum Beispiel ist eine Einwilligung nur dann rechtsgültig, wenn sie freiwillig und unbeeinflusst erteilt wird. »Nudging«, wie es bei der Cookie-Einwilligung häufig vorkommt, ist daher nicht zulässig. Selbst kleine Gestaltungsmerkmale (sog. »Dark Patterns«) können eine Person dazu verleiten, eine Option zu wählen, welche nicht ihren Wünschen entspricht [CKG19]. In diesem Fall ist die Einwilligung nicht rechtens.

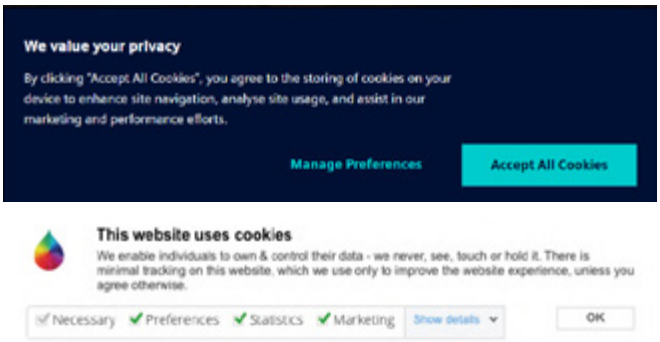

Abbildung 6: Dark Pattern bei Cookie-Einwilligungen

Nehmen wir das obere Beispiel in Abbildung 6. Hier werden Nutzer durch den stark hervorgehobenen Button dazu verleitet, auf »Accept All Cookies« zu klicken. Außerdem suggeriert die grünliche Farbe, dass ein Klick auf diesen Button eine »gute« Option für den Nutzer ist. Diese beiden Dark Patterns finden sich laut [NOYB21] auf 73 Prozent der untersuchten Webseiten. Ein weiterer Trick besteht darin, dem Nutzer auf der obersten Ebene gar nicht erst die Möglichkeit zu geben, alle Cookies abzulehnen. Auf diese Weise ist es für den Nutzer viel einfacher, zuzustimmen als abzulehnen. Dieses Dark Pattern findet sich laut [NOYB21] sogar 81 Prozent der untersuchten Webseiten. Im unteren Beispiel in Abbildung 6 werden standardmäßig alle Cookies ausgewählt und damit das Prinzip »Privacy by Default« verletzt. Dieses Dark Pattern ist zum Glück inzwischen nicht mehr so verbreitet wie zu Beginn der Cookie-Banner, findet sich aber immer noch auf 15 Prozent der untersuchten Webseiten [NOYB21].

Eine weitere Frage, die sich in diesem Zusammenhang stellt, ist die nach der notwendigen Detailtiefe und Darstellung der präsentierten Informationen (vgl. Kapitel 7). In einer Studie [KTS20] wurden Verbrauchern verschiedene Designs für das Einwilligungsmanagement vorgestellt. Auf der Grundlage dieser Studie wurde ein Best-Practice-Modell für ein innovatives Einwilligungsmanagement anhand verschiedener Praxisbeispiele entwickelt. Bei Digitalen Ökosystemen sollte man sich darüber hinaus noch die Frage stellen, ob es sinnvoll und gangbar ist, ein zentrales Einwilligungsmanagement über die Plattform anzubieten. Schlussendlich würde dies allen Ökosystemteilnehmern Arbeit ersparen und Sicherheit geben.

Nutzerfreundliche Einstellungen

Gerade große Plattformen bieten Nutzern bereits heute die Möglichkeit, über die Verwendung ihrer Daten zu bestimmen. Dazu können die Nutzer diverse Einstellungen vornehmen.

Dabei muss der Nutzer in der Regel einen Kompromiss zwischen Privatheit und anderen Qualitäten oder Ressourcen eingehen. So gehen beispielsweise restriktive Datenschutzeinstellungen (d. h. ein hohes Maß an Datenschutz) in der Google-Suche mit weniger personalisierten Vorschlägen einher (d. h. mit einem geringeren Maß an Effektivität). Dennoch sollten die Standardeinstellungen in jedem Fall datenschutzfreundlich sein, entsprechend des Prinzips »Privacy by Default«.

Unabhängig von dieser allgemeinen Herausforderung unterscheiden sich Einstellungsmöglichkeiten nach den Freiheitsgraden und der Unterstützung, die sie dem Nutzer bieten, sowie nach ihrem allgemeinen Interaktionsparadigma [Rud19]. Hier gibt es ein breites Spektrum – angefangen bei sehr groben Sicherheitsstufen, über Templates und Wizards, bis hin zu speziellen »Policy-Sprachen« (z. B. XACML, ODRL und proprietäre Sprachen wie die der MYDATA Control Technologies), um Bedarfe und Auflagen auszudrücken.

Welches Paradigma am besten geeignet ist, hängt von einer Vielzahl von Faktoren ab. Policy-Sprachen beispielsweise sind Experten vorbehalten, da sie detaillierte Kenntnis der Sprache und des zu steuernden Systems erfordern. Gleichzeitig bieten grobe Sicherheitsstufen den Experten nicht die gewünschte Flexibilität. Sie können ihnen höchstens zum Treffen von Grundeinstellungen dienen. Bei der Wahl und Umsetzung des Interaktionsparadigmas bedarf es also stets einer genauen Abstimmung auf die jeweiligen Merkmale und Bedarfe der Nutzergruppen.

Die wichtigsten Erkenntnisse

Nutzer können ihre Bedarfe nur dann effektiv, effizient und zufriedenstellend ausdrücken, wenn die angebotenen Einwilligungs- und Einstellungstools auf sie abgestimmt sind.

Einwilligungen sind nur dann gültig, wenn sie freiwillig und ohne Manipulation des Nutzers gegeben wurden. Das Prinzip »Privacy by Default« sollte beachtet werden.

TEIL 3: METHODEN & WERKZEUGE

9 Vorgehen
10 Technische Durchsetzung

9 Vorgehen

Datensouveränität mittels Human-Centered Design benutzerfreundlich umsetzen

In den vergangenen Jahrzehnten wurden eine Reihe von Produktentwicklungsmodellen und -methoden vorgeschlagen, um die Entwicklung sicherer Produkte zu unterstützen. Das bekannteste Beispiel ist sicherlich der Security Development Lifecycle (SDL) von Microsoft [Mic12]. Leider wird bei all diesen Methoden die Usability und UX der Lösung kaum berücksichtigt. Umgekehrt gibt es für viele Anwendungsdomänen noch keine Best Practices, wie Sicherheitsthemen bei einer nutzerzentrierten Gestaltung angemessen berücksichtigt werden können.

Wir möchten daher in diesem Kapitel unseren Ansatz zur Integration von USP in den Human-Centered-Design-Prozess (HCD) [ISO9241] vorstellen. HCD wird als interaktiver und iterativer Designprozess mit den Nutzern verstanden, bei dem die Designer Prototyping und Feedbackschleifen nutzen, um die Nutzer und ihre Anforderungen zu verstehen (siehe Abbildung 7). Zu jedem Schritt des HCD-Prozesses haben wir Aspekte hinzugefügt, die mit der benutzerfreundlichen Umsetzung von Datensouveränität zusammenhängen.

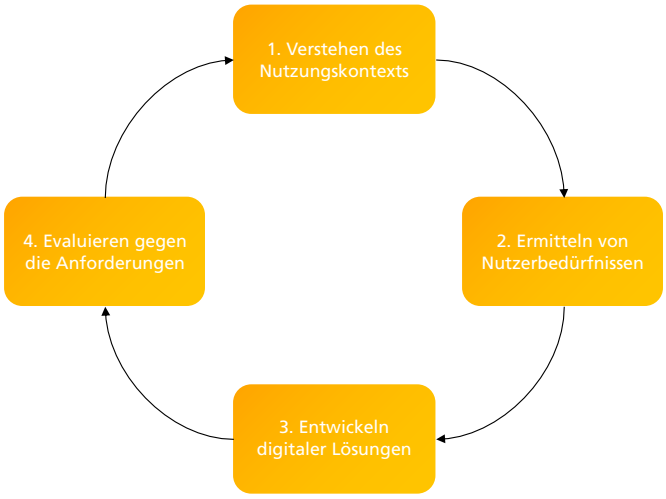

Abbildung 7: Der Human-Centered-Design-Prozess

Verstehen des Nutzungskontextes

Der erste Schritt im HCD ist das Verstehen des Nutzungskontexts. Nach ISO 9241 umfasst der Nutzungskontext Nutzer, Aufgaben, Ausrüstung (Hardware, Software und Materialien) sowie die physische und soziale Umgebung, in der ein Produkt verwendet wird. Wir stellen weitere Aspekte vor, unter anderem Daten, Datenschutzvorschriften und Merkmale der Nutzer mit Bezug zu benutzerfreundlicher Umsetzung von Datensouveränität in Digitalen Ökosystemen.

Daten im Digitalen Ökosystem verstehen: Zunächst sollte man sich darüber im Klaren sein, welche personenbezogenen Daten oder anderen sensiblen Daten in dem Digitalen Ökosystem verwendet werden oder verwendet werden sollen. Dies kann durch eine Analyse der Geschäftsprozesse, der Systemarchitektur und der Schnittstellen erfolgen. Danach sollte man unter anderem diese Fragen beantworten: Werden die Daten über ein öffentliches oder privates WLAN übertragen? Werden die Daten in eine Cloud gesendet? Wenn ja, befindet sich der Server innerhalb oder außerhalb der Europäischen Union? Steht er außerhalb, sollten geprüft werden, wie die Nutzer zu dieser Übertragung stehen. Sind sie damit einverstanden oder werden sie das System ablehnen, weil sie ihre Privatsphäre gefährdet sehen?

Datenschutzvorschriften verstehen: Des Weiteren sollte man Datenschutzvorschriften (insb. die DSGVO und das BDSG n.F.), Unternehmensrichtlinien und die AGB und Verträge des Digitalen Ökosystems kennen, um den Lösungsraum eingrenzen zu können. Außerdem decken diese Vorschriften zu einem gewissen Teil auch die Bedarfe der Nutzer ab.

Nutzermerkmale verstehen: Nutzer haben unterschiedliche Bedarfe und Eigenschaften in Bezug auf Datensouveränität. Endnutzer können unter anderem anhand der in Abbildung 8 dargestellten Merkmale unterschieden werden.

Abbildung 8: Merkmale der Endnutzer in Bezug auf Datensouveränität.

Diese Eigenschaften können sich auf das Design auswirken. Wenn zum Beispiel eine Person einen starken Bedarf nach Privatheit hat, könnten entsprechende Datenschutzfunktionen an prominenter Stelle platziert werden, sodass der Nutzer versteht, dass das System sich um den Datenschutz kümmert. Wenn ein Nutzer nur wenig über Datensouveränität weiß, könnte das System den Nutzer über die Bedrohungen und Möglichkeiten informieren. Sind die Fähigkeiten des Nutzers gering, könnte ein Tutorial ihn bei der Anwendung der Maßnahmen unterstützen. Wenn der Nutzer es nicht gewöhnt ist, souverän zu agieren, könnten Erinnerungen helfen, solche Gewohnheiten zu etablieren.

Ermitteln von Nutzerbedarfen

Der zweite Schritt im HCD ist die Ermittlung der Nutzerbedarfe. Dabei gibt es in unserem Fall zwei wichtige Arten von Nutzern – Datengeber und Datennutzer. Es ist wichtig, sie zu unterscheiden, da sie unterschiedliche Bedarfe haben, die miteinander in Konflikt stehen können.

Datengeber haben die folgenden Arten von Bedarfen:

- Datenschutzbedarf: der Wunsch, bestimmte Arten von Daten oder bestimmte Datenelemente zu schützen.
- Transparenzbedarf: der Bedarf oder der Wunsch nach Informationen über die Verwendung ihrer Daten.
- Selbstbestimmungsbedarf: der Bedarf oder der Wunsch nach Kontrolle über die Verwendung ihrer Daten.

Datennutzer haben die folgenden Arten von Bedarfen:

- Datenverarbeitungsbedarf: die Notwendigkeit, eine bestimmte Klasse von Daten zu verarbeiten, um eine Aufgabe zu erfüllen.
- Informationsbedarf über die Verarbeitung: der Bedarf einer Person nach Informationen über die Vorschriften für die Verarbeitung von Daten, z. B. Informationen darüber, für welche Zwecke das konkrete Datum verwendet werden darf.

Die genannten Bedarfe sind hierbei als Kategorie zu verstehen. Das heißt, es reicht nicht, zu wissen, dass die Nutzer Transparenzbedarfe haben, sondern es muss konkret erhoben werden, über welche Datenverarbeitungen Informationen bereitgestellt werden müssen.

Die Datenverarbeitungsbedarfe und die Datenschutzbedarfe können dabei gegensätzlich sein und zu einem Interessenskonflikt führen. Der Konflikt kann gelöst oder abgemildert werden, indem über die Notwendigkeit und die Vorteile der Datenverarbeitung sowie die Maßnahmen zum Schutz der Daten informiert wird.

Entwickeln digitaler Lösungen

Der dritte HCD-Schritt ist das Entwickeln von Lösungen. Hierbei sollte man Best Practices aus dem Bereich USP kennen und beachten. Das Projekt USecureD [Use17] hat solche Best Practices gesammelt und dabei drei Ebenen unterschieden: Prinzipien, Richtlinien und Patterns.

Prinzipien: Prinzipien sind allgemeine Regeln für die Gestaltung von Systemen. Sie beruhen auf Erfahrungen, sind relativ kurz und eignen sich gut, um ein Grundverständnis über USP zu erlangen. USecureD stellt eine Sammlung von 23 Grundsätzen online zur Verfügung, beispielsweise folgende:

- Gute Sicherheit jetzt [Gar05]: Mit der Einführung nicht warten, bis die Sicherheitsmaßnahme perfekt ist.
- Weg des geringsten Widerstands [Yee02]: Der Weg, den der Nutzer normalerweise nimmt, bzw. der Weg, der für den Nutzer am einfachsten ist, sollte auch der sicherste sein.
- Konditionierung [COB07]: Positive Verstärkung (Belohnung) hilft, gewünschtes Verhalten zu fördern.

Richtlinien: Richtlinien beschreiben, wie die Prinzipien umgesetzt werden können. Sie sind wichtig, um möglichst viele potenzielle Probleme bereits in einem frühen Stadium des Prozesses zu beseitigen [Bir13]. Sie helfen außerdem, einen hohen Qualitätsstandard zu gewährleisten und die Komplexität von Entwicklungsprojekten zu reduzieren. USecureD stellt online eine Sammlung von Richtlinien zur Verfügung, wie z. B. Richtlinien für brauchbare Krypto-APIs [GS16], zur Fehlervermeidung [SPC+16] und für standardisierte Verfahren [SM86] [HHS08].

Patterns: Patterns sind bewährte Lösungen für wiederkehrende Probleme, die bei der Systementwicklung auftreten. Heutzutage ist das Befolgen von Patterns eine integrale Strategie in der Softwareindustrie. Dies spiegelt sich in einer großen Anzahl von Sammlungen wider, die Patterns für verschiedene Bereiche der Softwareentwicklung dokumentieren, z. B. Architektur, Dokumentation, Gestaltung von Benutzeroberflächen oder eben auch Security. In den letzten Jahren sind auch vermehrt Patterns für USP entstanden. Sie befassen sich mit Aspekten wie Authentifizierung, Autorisierung, Schlüsselverwaltung, digitale Signaturen, Verschlüsselung, sichere Datenlöschung, Erstellung von Backups, benutzerfreundlichen APIs und der Gestaltung von Hinweisen, Warnungen und Systemzuständen [LSF+19]. USecureD hat auch hier online eine umfangreiche Sammlung zusammengestellt.

Evaluieren gegen die Anforderungen

Im letzten HCD-Schritt wird die entwickelte Lösung gegen die Anforderungen evaluiert. Nutzertests sind dabei zumeist sehr zeit- und kostenintensiv, da die Nutzer für ihre Teilnahme in der Regel zumindest eine Aufwandsentschädigung erhalten. Daher ist es ratsam, eine heuristische Evaluation mit Experten durchzuführen, bevor man in die Nutzertests einsteigt. Die heuristische Evaluation ist deutlich kostengünstiger, schneller und kann bereits viele Unzulänglichkeiten des Designs aufdecken. Zu diesem Zweck stellen Feth und Polst [FP19] eine Liste von 45 Heuristiken zur Bewertung von Systemen hinsichtlich USP vor. Diese Heuristiken decken die folgenden Aspekte ab und sind auf verschiedene Domänen und Anwendungen erweiterbar:

- Transparenz (z. B. wird klar angegeben, für welche Zwecke Daten verwendet werden)
- Authentifizierung (z. B. werden Passwortrichtlinien bei der Passwortvergabe direkt angezeigt)
- Kontrolle und Freiheit des Nutzers (z. B. kann der Nutzer inkorrekte Daten selbstständig aktualisieren oder löschen)
- Fehlererkennung, -diagnose und -behebung (z. B. informieren Fehlermeldungen über den Schweregrad des Problems)
- Benutzerunterstützung und -dokumentation (z. B. folgen Hilfe und Dokumentation den Prozessschritten)
- Zugänglichkeit (z. B. unterstützt das System die Verwendung von Textpasswörtern für sehbehinderte Nutzer)

Der Erfolg von Heuristiken hängt natürlich von ihrer richtigen Anwendung und Bewertung ab. Deshalb zeigen Feth und Polst auch, wie Heuristiken im HCD eingesetzt werden können (vgl. Abbildung 9).

Diese Integration basiert u.a. auf der Instanziierung eines spezifischen Modells für USP. Je nach Heuristik wird das Modell durch ein Werkzeug so gefiltert, dass es die Auswertung der jeweiligen Heuristik unterstützt. Weitere auf Heuristiken basierende Ansätze zur USP finden sich in [BSM07], [KFR+10], [YVP12], [RCH+16] und [JS19].

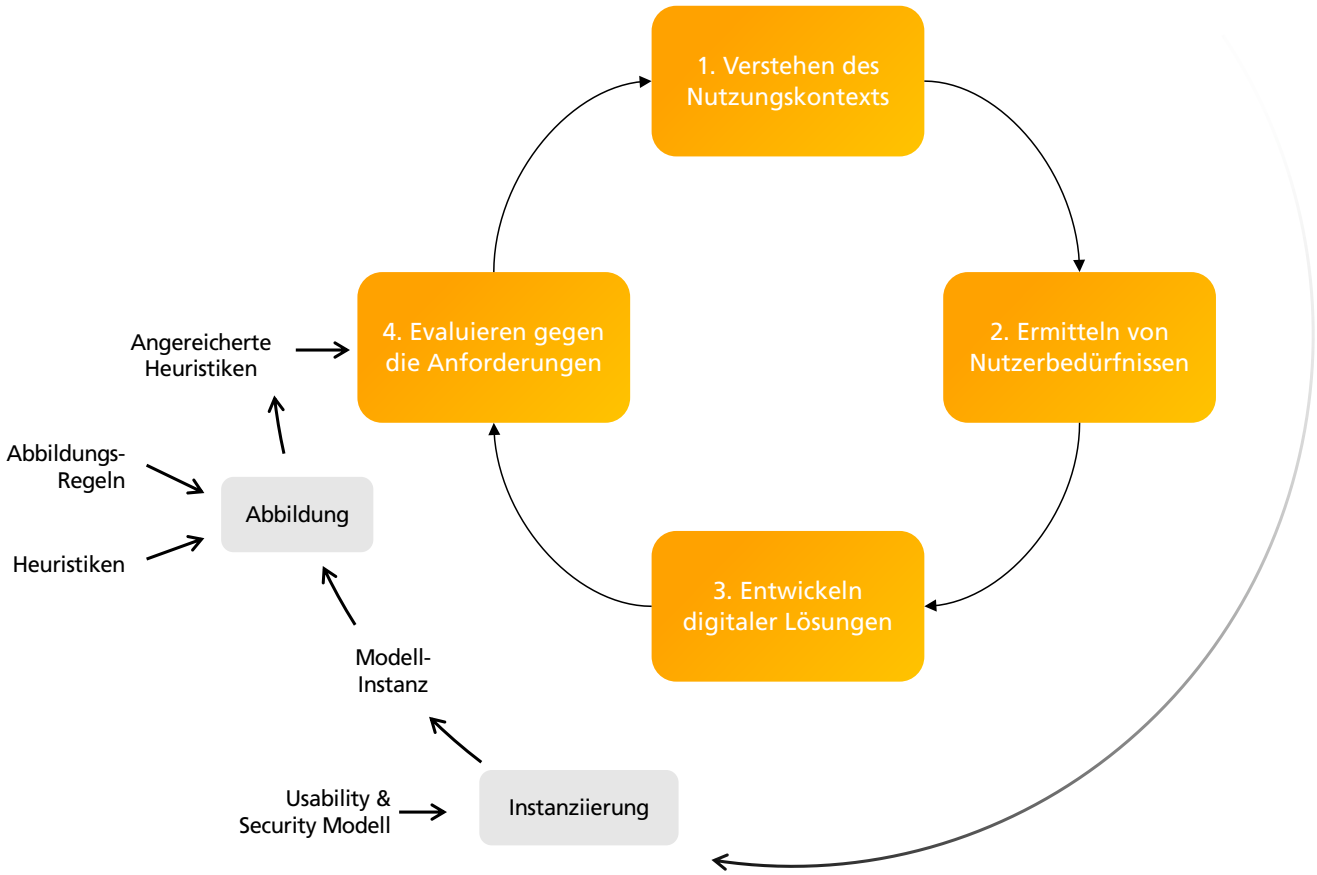

Abbildung 9: Heuristische Evaluation im HCD-Prozess [FP19]

Die wichtigsten Erkenntnisse

Usability und UX werden in Security-Prozessen häufig vernachlässigt und umgekehrt.

Ein nutzerzentriertes Vorgehen entlang des von uns vorgestellten HCD-Prozesses kann dabei helfen, die Nutzerbedarfe besser zu verstehen und Datensouveränität benutzerfreundlich umzusetzen.

Der HCD-Prozess sollte dabei eher als Inspiration gesehen werden und nicht als etwas, an das man sich immer halten muss.

10 Technische Durchsetzung

Informationelle Selbstbestimmung durch Datenfilterung und -maskierung

In den vorangehenden Kapiteln haben wir gesehen, welchen Herausforderungen man sich stellen muss, um Datensouveränität benutzerfreundlich umzusetzen. So werden Nutzer mittels verständlicher Datenschutzerklärungen, nachverfolgbaren Datenflüssen und konsistenter Terminologie und Ikonographie darüber informiert, wie ihre Daten verarbeitet werden. Auf dieser Grundlage können sie entsprechend ihrer Bedarfe Einwilligungen erteilen (oder eben nicht) sowie Datenschutzeinstellungen vornehmen. Aber wie kann man nun als Plattformanbieter oder Dienstanbieter in einem Digitalen Ökosystem solche Datenschutzeinstellungen technisch umsetzen?

Das Problem: Die Komplexität vieler Bedarfe und Einstellungen geht weit über das hinaus, was mit Standardmitteln (insbesondere der seit Jahrzehnten etablierten Zugriffskontrolle) umsetzbar ist. Insbesondere begegnen einem vermehrt Anforderungen, die über eine einfache binäre Zugriffsregel hinausgehen. Stattdessen gewinnen Filterungen (z. B. »Nur Datensätze der letzten 30 Tage«), Maskierungen (z. B. »Schwärze Felder mit gekauften Artikeln«), Anonymisierung und Nutzungsauflagen (z. B. »Lösche Daten nach 14 Tagen«, »Leite Daten nicht weiter« oder »Daten dürfen nur für den genannten Zweck verwendet werden«) an Bedeutung. Siehe dazu Abbildung 8. Daher widmen wir uns in diesem Abschnitt der »Datennutzungskontrolle« als treibendem Paradigma zur technischen Umsetzung von Datensouveränität.

Zur Umsetzung der vorgenannten Auflagen mittels Datennutzungskontrolle gibt es zwei Methoden: präventive und reaktive Mechanismen. Präventive Mechanismen stellen die Einhaltung der festgelegten Regeln sicher, indem sie unerwünschte Handlungen verhindern, wie etwa die Weitergabe von Daten. Im Gegensatz dazu können reaktive Mechanismen unerwünschte Handlungen nicht verhindern, sondern unterstützen lediglich die Aufdeckung von Verstößen gegen die Auflagen. Dieses Prinzip kann mit der Durchsetzung von Geschwindigkeitsbegrenzungen verglichen werden. Die Polizei kann zwar nicht verhindern, dass zu schnell gefahren wird, aber sie kann Verstöße aufdecken und Bußgelder auferlegen. Auf ähnliche Weise können durch Protokollierung von Datennutzungen und nachgelagerte Auditierungen Verstöße gegen die Auflagen aufgedeckt werden (vgl. Kapitel 7).

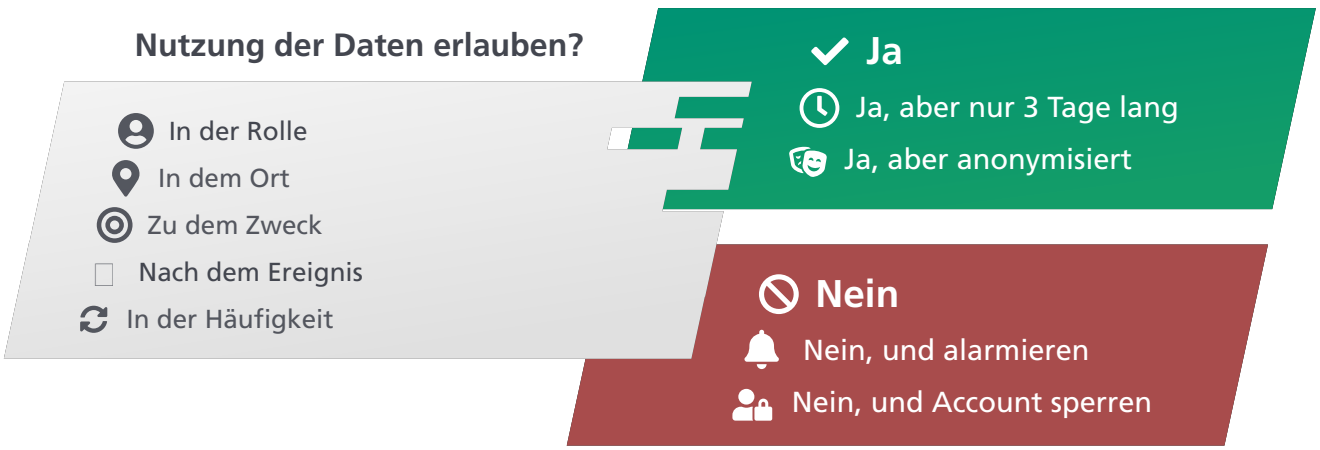

Abbildung 10: Feingranulare Regeln für Datensouveränität

Abbildung 11: MYDATA Control Technologies

Beide Arten von Mechanismen haben in verschiedenen Anwendungsszenarien ihre Vor- und Nachteile. Die optimale Lösung hängt daher vom Einsatzgebiet ab. Präventive Mechanismen haben den Vorteil, dass die Einhaltung der Nutzungsrestriktionen und Auflagen garantiert werden kann. Diese können aber zu einer geringeren Akzeptanz führen, da die Nutzer in ihrem Handeln eingeschränkt werden, wie man am Beispiel Digital Rights Management (DRM) häufig beobachten kann. Außerdem ist eine Integration präventiver Mechanismen in Bestandssysteme häufig schwerer oder teilweise gar nicht möglich. Reaktive Mechanismen sind hingegen einfacher umzusetzen (z. B. durch Protokollierung) und lassen dem Nutzer mehr Spielraum. Da sie unerwünschte Nutzungen aber nicht verhindern können, muss ein nachgelagerter Prozess für die Erkennung und Kompensierung des aufgetretenen Schadens etabliert werden.

Um Datennutzungskontrolle umzusetzen, müssen primär die folgenden Anforderungen erfüllt werden:

1. An relevanten Stellen im System, z. B. in der Plattform, müssen Datennutzungen und Datenflüsse kontrolliert werden.

2. Gewünschte Datennutzungen müssen gegen eine Vielzahl komplexer Regelungen abgeglichen werden, welche unter anderem aussagenlogische, kardinale und temporale Aspekte beinhalten können. Auch Kontextfaktoren müssen ggf. berücksichtigt werden.

3. Entsprechend der Auswertung der Auflagen müssen proaktive Aktionen (z. B. das Blockieren oder Filtern des Datenflusses) oder reaktive Aktionen (z. B. das Benachrichtigen des Nutzers oder Administrators) ausgeführt werden können.

4. Werden Daten weitergegeben, so müssen die Auflagen (»Lösche Daten nach 14 Tagen«) an das Zielsystem weitergegeben und dort entsprechend umgesetzt werden.

Während man die ersten drei Anforderungen in traditionellen Systemen noch mit halbwegs vertretbarem Aufwand selbst implementieren kann, ist dies spätestens bei einem unternehmensübergreifenden Datenaustausch in einem inhärent volatilen Digitalen Ökosystem im Hinblick auf die vierte Anforderung nicht mehr praktikabel. Hier sollten spezielle Frameworks und Softwarelösungen, wie die MYDATA Control Technologies, eingesetzt werden, welche die Spezifikation, Verwaltung und Durchsetzung von Datennutzungsregeln vereinen (vgl. Abbildung 9).

Die wichtigsten Erkenntnisse

Für die technische Umsetzung von Datensouveränität in Digitalen Ökosystemen ist traditionelle Zugriffskontrolle nicht mehr geeignet.

Datennutzungskontrolle bietet hier eine passende Erweiterung, welche z. B. mittels MYDATA Control Technologies umgesetzt werden kann.

TEIL 4: FAZIT

11 Unsere Kernbotschaften
12 Über die Autoren

11 Unsere Kernbotschaften

Zusammenfassung und Fazit

Wenn es um Datensouveränität geht, gilt: Systeme, die nicht sicher sind, haben eine schlechte UX und Sicherheitslösungen mit schlechter UX sind nicht sicher. Darüber hinaus fassen wir hier nochmals alle unsere Kernbotschaften zusammen:

1. Die Verarbeitung sensibler Daten ist eine Voraussetzung für die Funktionalität von Digitalen Ökosystemen, vor allem für die Vermittlung zwischen Konsumenten und Anbietern. Es braucht Vertrauen, um Daten zu teilen, aber auch Daten, wie Bewertungen, um das Vertrauen aufzubauen.

2. Transparenz und Selbstbestimmung sind Eckpfeiler der Datensouveränität. Bei personenbezogenen Daten greifen hier primär die Rechte und Pflichten aus der DSGVO. Bei sonstigen sensiblen Daten gibt es keine durchgängigen gesetzlichen Regelungen – viele Konzepte lassen sich aber übertragen und bieten in Summe Vorteile für alle Teilnehmer von Digitalen Ökosystemen.

3. Hohe Usability und positive UX sind eine Voraussetzung für die Akzeptanz eines Systems. Dabei können in Digitalen Ökosystemen auch vermeintlich lokale Probleme (z. B. bei einem Dienst) negative Auswirkungen auf die UX des gesamten Ökosystems haben.

4. Usable Security & Privacy deckt ein breites Spektrum von Querschnittsthemen und interdisziplinären Themen zwischen den Bereichen Security, Datenschutz und UX ab. Wir empfehlen, diese Themen immer ganzheitlich und von Anfang an zu betrachten und dabei die gegenseitigen Wechselwirkungen zu berücksichtigen.

5. Systeme und Schutzmaßnahmen sollten sich an die Nutzer anpassen, nicht umgekehrt. Nicht alle Nutzer sind dabei gleich und es gibt bei Digitalen Ökosystemen keine »Einheitslösung«. Wir empfehlen eine Klassifizierung von Nutzern mittels Personas um die spezifischen Merkmale der Zielgruppen im Auge zu behalten.

6. Nur weil Nutzer sagen, dass sie ihre Privatsphäre schützen möchten, darf man nicht davon ausgehen, dass sie auch entsprechend handeln. In Digitalen Ökosystemen ist es für die Nutzer häufig besonders verlockend, Daten zu teilen. Außerdem kann Datensouveränität auch negative Auswirkungen haben. Schlussendlich müssen die Interessen aller Ökosystemteilnehmer gegeneinander abgewogen werden.

7. Zur Schaffung von Transparenz muss die Nutzung der Daten mit zumutbarem Aufwand nachvollzogen, überprüft und bewertet werden können. Dabei bedeutet Transparenz auch, konkret zu werden sowie Informationen zur Laufzeit zu erfassen und zugänglich zu machen. Idealerweise sorgt der Plattformanbieter hier für verbindliche Gestaltungsvorgaben.

8. Nutzer können ihre Bedarfe nur dann effektiv, effizient und zufriedenstellend ausdrücken, wenn die angebotenen Einwilligungs- und Einstellungstools auf sie abgestimmt sind. Einwilligungen sind nur dann gültig, wenn sie freiwillig und ohne Manipulation des Nutzers gegeben wurden. Das Prinzip »Privacy by Default« sollte in jedem Fall beachtet werden.

9. Usability und UX werden in Security-Prozessen häufig vernachlässigt und umgekehrt. Ein nutzerzentriertes Vorgehen entlang des von uns vorgestellten HCD-Prozesses kann dabei helfen, die Nutzerbedarfe besser zu verstehen und Datensouveränität benutzerfreundlich umzusetzen. Der HCD-Prozess sollte dabei eher als Inspiration gesehen werden und nicht als etwas, an das man sich immer halten muss.

10. Für die technische Umsetzung von Datensouveränität in Digitalen Ökosystemen ist traditionelle Zugriffskontrolle nicht mehr geeignet. Datennutzungskontrolle bietet hier eine passende Erweiterung, welche z. B. mittels MYDATA Control Technologies umgesetzt werden kann.

12 Über die Autoren

Zusammenarbeit zwischen Sicherheit und Usability

Denis Feth, M. Sc.

Expert »Data Sovereignty«
Abteilung Security Engineering, Fraunhofer IESE

»Ich habe Informatik mit den Schwerpunkten Security und HCI studiert. Seit 2011 arbeite ich in der Abteilung »Security Engineering« und forsche dort schwerpunktmäßig im Bereich Datensouveränität. Hier wurde beispielsweise die Komplexität unserer Lösung »MYDATA« schnell zu einer Herausforderung für Entwickler, Administratoren und Endanwender. So haben wir bereits früh begonnen, uns systematisch mit USP auseinanderzusetzen. Seitdem stehen wir im ständigen Austausch mit Kolleg*innen aus anderen Fachdisziplinen (z. B. UX, Design, Psychologie, RE) und profitieren von deren Expertise. In diversen Forschungsprojekten entwickeln wir gemeinsam Konzepte, um Security- und Datenschutzlösungen auf die Nutzer auszurichten – zum Beispiel in den Bereichen Wearables, Digitale Ökosysteme und Datentreuhänder. Um im Austausch mit der Forschungscommunity und Praktikern zu bleiben, bin ich Teil des Organisationsteams des »Usable Security & Privacy« Workshops auf der »Mensch und Computer«-Konferenz.«

Svenja Polst, M. Sc.

Senior Digital Innovation Designer
ehem. Abteilung Digital Innovation Design, Fraunhofer IESE

»Ich habe Psychologie mit dem Schwerpunkt Mensch-Computer-Interaktion studiert und sechs Jahre in der Abteilung »Digital Innovation Design« gearbeitet. In dieser Abteilung versucht man, die Bedarfe der Nutzer im Detail zu verstehen und Lösungen zu entwickeln, die diese Bedarfe so gut wie möglich erfüllen. Bei vielen Systemen ist Nutzern Privatheit und der Schutz ihrer Daten sehr wichtig. Sicherheitsmaßnahmen werden jedoch oft als alleinige Aufgabe von Security Engineers wahrgenommen. In Projekten mit Denis und anderen Security Engineers ist mir bewusst geworden, dass es auch die Aufgabe von User Experience Experten ist, dazu beizutragen, dass Systeme nicht nur benutzerfreundlich, sondern auch sicher sind. Auch in meinem neuen Job als User Researcher bei einem großen Medizintechnikunternehmen gibt es spannende Fragestellungen rund um Usable Security und Privacy und ich freue mich stets über einen Austausch zu diesem Thema.«

Referenzen

[AKS+03] Abran, A., Khelifi, A., Suryn, W., & Seffah, A. (2003). Usability meanings and interpretations in ISO standards. Software quality journal.

[Bir13] Birolini, A. (2013). Zuverlässigkeit von Geräten und Systemen. Springer-Verlag.

[BSM07] Braz, C., Seffah, A., & M'Raihi, D. (2007). Designing a trade-off between usability and security: A metrics based-model. Human-Computer Interaction–INTERACT …, 4663, 114–126.

[CKG19] Caraban, A., Karapanos, E., Gonçalves, D. & Campos, P. (2019). 23 Ways to Nudge: A Review of Technology-Mediated Nudging in Human-Computer Interaction. CHI ,19: Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems, 1–15.

[COB07] Chiasson, S., van Oorschot, P. C., & Biddle, R. (2007, July). Even experts deserve usable security: Design guidelines for security management systems. In SOUPS Workshop on Usable IT Security Management (USM).

[DsiN21] Deutschland sicher im Netz e.V. (2021). DsiN-Sicherheitsindex 2021. https://www.sicher-im-netz.de/dsin-sicherheitsindex-2021

[EFB15] Ermakova, T., Fabian, B., & Babina, E. (2015). Readability of Privacy Policies of Healthcare Websites. Wirtschaftsinformatik, 15, 1-15.

[EU16] European Parliament/Council of the European Union. (2016): Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation). https://eur-lex.europa.eu/eli/reg/2016/679/oj

[Fet18] Feth, D. (2018). Transparency through Contextual Privacy Statements. Mensch Und Computer 2017-Workshopband: Spielend Einfach Interagieren.

[Fet20] Feth, D. (2020). Modelling and Presentation of Privacy-Relevant Information for Internet Users. International Conference on HCI for Cybersecurity, Privacy and Trust.

[FP19] Feth, D., & Polst, S. (2019). Heuristics and Models for Evaluating the Usability of Security Measures. Proceedings of Mensch Und Computer 2019, 275–285.

[FRA20] European Union Agency for Fundamental Rights (2020). Your Rights matter: Data protection and Privacy, doi:10.2811/292617

[Gar05] Garfinkel, S. L. (2005). Design Principles and Patterns for Computer Systems That Are Simultaneously Secure and Usable. Gene, 31, 234–239.

[GL14] Garfinkel, S., & Lipford, H. R. (2014). Usable Security: History, Themes, and Challenges. Synthesis Lectures on Information Security, Privacy, and Trust, 5(2), 1–124.

[GS16] Green, M., & Smith, M. (2016). Developers are not the enemy!: The need for usable security apis. IEEE Security & Privacy, 14(5), 40-46.

[GVG17] Gerber, P., Volkamer, M., & Gerber, N. (2017). Das Privacy-Paradoxon–Ein Erklärungsversuch und Handlungsempfehlungen. In Dialogmarketing Perspektiven 2016/2017 Springer Gabler, Wiesbaden.

[HHS08] US Department of Health and Human Services. (2008). Research-based web design & usability guidelines.

[HPD+16] Holz, T., Pohlmann, N., Bodden, E., Smith, M., & Hoffmann, J. (2016). Human-Centered Systems Security: IT-Sicherheit von Menschen für Menschen. Verfügbar unter: https://www.ptj. de/lw_resource/datapool/_items/item_7794.

[ISO9241] International Organization for Standardization. (2019). Ergonomics of human-system interaction (ISO 9241).

[JS19] Johansen, J., & Fischer-Hübner, S. (2019). Making GDPR usable: a model to support usability evaluations of privacy. arXiv preprint arXiv:1908.03503.

[KFR+10] Kainda, R., Fléchais, I., Roscoe, A. W. A., & Flechais, I. (2010). Security and Usability: Analysis and Evaluation. 2010 International Conference on Availability, Reliability and Security, 275–282.

[KTS20] Kettner, S. E., Thorun, C., Spindler, G. (2020). Innovatives Datenschutzeinwilligungsmanagement. https://www.bmjv.de/SharedDocs/Downloads/DE/Service/Fachpublikationen/090620_Datenschutz_Einwilligung.pdf?__blob=publicationFile&v=1 Last accessed: 11/2021

[LSF+19] Lo Iacono, L., Schmitt, H., Feth, D., Jakobi, T., Gorski, P.L., Dölle, M., Nehren, P., Kropp, E., Hausmann, S., Hofmeister, A., Frydyada de Piotrowski, A., & Balthasar, M. (2018). Arbeitskreis Usable Security & Privacy: Nutzerzentrierter Schutz sensibler Daten.

[MCG06] Milne, G. R., Culnan, M. J., & Greene, H. (2006). A longitudinal assessment of online privacy notice readability. Journal of Public Policy & Marketing, 25(2), 238-249.

[Mic12] Microsoft (2012) Microsoft Security Development Lifecycle (SDL) - version 5.2 - https://www.microsoft.com/en-us/securityengineering/sdl

[Nie94] Jakob Nielsen, J. (1994). Usability Heuristics for User Interface Design. https://www.nngroup.com/articles/ten-usability-heuristics/

[NOYB21] NOYB – European Center for Digital Rights. Online: https://noyb.eu/de/noyb-setzt-dem-cookie-banner-wahnsinn-ein-ende. Last accessed: 08/2022

[OGW+19] Ortloff, A.-M., Güntner, L., Windl, M., Feth, D., & Polst, S. (2019). Evaluation kontextueller Datenschutzerklärungen. Mensch Und Computer 2018 Workshopband.

[OO20] Obar, J. A., & Oeldorf-Hirsch, A. (2020). The biggest lie on the internet: Ignoring the privacy policies and terms of service policies of social networking services. Information, Communication & Society, 23(1), 128-147.

[PF20] Polst, S., & Feth, D. (2020). Privacy ad Absurdum-How Workplace Privacy Dashboards Compromise Privacy. Mensch und Computer 2020-Workshopband.

[RB11] Rost, M., & Bock, K. (2011). Privacy by design und die neuen schutzziele. Datenschutz und Datensicherheit-DuD, 35(1), 30-35.

[RBC+15] Reidenberg, J. R., Breaux, T., Cranor, L. F., French, B., Grannis, A., Graves, J. T., ... & Ramanath, R. (2015). Disagreeable privacy policies: Mismatches between meaning and users' understanding. Berkeley Tech. LJ, 30, 39.

[RCH+16] Realpe, P. C., Collazos, C. A., Hurtado, J., & Granollers, A. (2016, September). A set of heuristics for usable security and user authentication. In Proceedings of the XVII International Conference on Human Computer Interaction.

[**RFP18]** Rudolph, M., Feth, D., & Polst, S. (2018). Why Users Ignore Privacy Settings and Policies - A survey and intention model for explaining user privacy behavior. International Conference on Human Aspects of Information Security, Privacy, and Trust.

[SDM20] AK Technik der Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder. (2020). Das Standard-Datenschutzmodell: Eine Methode zur Datenschutzberatung und -prüfung auf der Basis einheitlicher Gewährleistungsziele

[SM86] Smith, S. L., & Mosier, J. N. (1986). Guidelines for designing user interface software. Bedford, MA: Mitre Corporation.

[SPC+16] Shneiderman, B., Plaisant, C., Cohen, M. S., Jacobs, S., Elmqvist, N., & Diakopoulos, N. (2016). Designing the user interface: strategies for effective human-computer interaction. Pearson.

[SSH+16] Sasse, M. A., Smith, M., Herley, C., Lipford, H., & Vaniea, K. (2016). Debunking security-usability tradeoff myths. IEEE Security & Privacy, 14(5), 33-39.

[Sym15] Symantec (2015). State of Privacy Report 2015.

[TEC+11] Tsai, J. Y., Egelman, S., Cranor, L., & Acquisti, A. (2011). The effect of online privacy information on purchasing behavior: An experimental study. Information systems research, 22(2), 254-268.

[Use17] USecureD-Konsortium. (2017). UsecureD—Usable Security by Design. https://www.usecured.de

[Wal18] Waldman, A. E. (2018). Privacy, notice, and design. Stan. Tech. L. Rev., 21, 74.

[Whi04] Whitten, A. (2004). Making Security Usable. Computers Security, 26, 434–443.

[YAA+04] Yan, J., Alan, B., Anderson, R., & Grant, A. (2004). Password memorability and security: Empirical results. IEEE Security and Privacy, 2(5), 25–31.

[YT15] Choong, Y.-Y., & Theofanos, M. (2015). What 4,500+ People Can Tell You - Employees' Attitudes Toward Organizational Password Policy Do Matter. In T. Tryfonas & I. Askoxylakis (Eds.), Human Aspects of Information Security, Privacy, and Trust. Springer International Publishing.

[YVP12] Yeratziotis, A., Van Greunen, D., & Pottas, D. (2012). A Framework for Evaluating Usable Security: The Case of Online Health Social Networks. In HAISA (pp. 97-107).

[ZS96] Zurko, M. E., & Simon, R. T. (1996). User-centered security. In Proceedings of the 1996 workshop on New security paradigms - NSPW '96 (pp. 27–33). New York, New York, USA: ACM Press.

Das Fraunhofer IESE ist ein Institut der Fraunhofer-Gesellschaft.

Das Institut transferiert innovative Softwareentwicklungstechniken, -methoden und -werkzeuge in die industrielle Praxis, unterstützt Unternehmen beim Aufbau von bedarfsgerechten Softwarekompetenzen und hilft ihnen, sich im Wettbewerb zu positionieren.

Das Fraunhofer IESE wird von Prof. Dr.-Ing. Peter Liggesmeyer geleitet.

Fraunhofer-Institut für Experimentelles Software Engineering IESE

Fraunhofer-Platz 1
67663 Kaiserslautern

www.iese.fraunhofer.de