Plattform Privatheit und selbstbestimmtes Leben in der digitalen Welt

Plattform Privatheit

Ramona Adair, Claudia Schlüfter, Angelika Diarra, Harald Zwingelberg, Diana Schneider, Ina Schiering, Nils B. Heyen

DIE INFORMIERTE EINWILLIGUNG BEDARFSGERECHT UMSETZEN

EIN LEITFADEN FÜR DIE TECHNISCHE GESTALTUNG DES PRIVATHEITSMANAGEMENTS BEI GESUNDHEITS-APPS

White Paper

Herausgegeben von Michael Friedewald, Alexander Roßnagel, Christian Geminn und Murat Karaboga

Impressum

Forschungsberichte der Plattform Privatheit Nr. 10

Herausgeber

Plattform Privatheit
Michael Friedewald[1], Alexander Roßnagel[2,3], Christian Geminn[2], Murat Karaboga[1]
(1) Fraunhofer-Institut für System- und Innovationsforschung ISI, Karlsruhe
(2) Universität Kassel, Projektgruppe verfassungsverträgliche Technikgestaltung (provet) im Wissenschaftlichen Zentrum für Informationstechnik-Gestaltung (ITeG)
(3) Hessischer Beauftragter für Datenschutz und Informationsfreiheit, Wiesbaden

Autorinnen und Autoren

Ramona Adair[1], Claudia Schlüfter[2], Angelika Diarra[3], Harald Zwingelberg[4], Diana Schneider[2], Ina Schiering[1], Nils B. Heyen[2]
(1) Ostfalia Hochschule für angewandte Wissenschaften, Institut für Verteilte Systeme, Wolfenbüttel
(2) Fraunhofer-Institut für System- und Innovationsforschung ISI, Karlsruhe
(3) Kanzlei für Gesundheitsrecht Prof. Schlegel, Hohmann, Diarra & Partner PartGmbB
(4) Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein ULD

Reihe

ISSN (Print)	2942-8874
ISSN (Online)	2942-8882
DOI	https://doi.org/10.24406/publica-10162

Veröffentlichung

September 2026, 1. Auflage
Fraunhofer-Institut für System- und Innovationsforschung ISI, Karlsruhe

Zitierempfehlung

Adair et al. (2026): Die informierte Einwilligung bedarfsgerecht umsetzen. Ein Leitfaden für die technische Gestaltung des Privatheitsmanagements bei Gesundheits-Apps. Forschungsberichte der Plattform Privatheit Nr. 10. Karlsruhe: Fraunhofer ISI. https://doi.org/10.24406/publica-10162

Inhaltsverzeichnis

1 Einleitung

Gesundheits-Apps können die Versorgungsqualität verbessern, Prävention vereinfachen, eine individuelle und personalisierte Behandlung ermöglichen oder Gesundheitsinformationen verwalten. Wenn eine Gesundheits-App nachgewiesenen klinischen Nutzen bietet und die Anforderungen der Verordnung für digitale Gesundheitsanwendungen (DiGA) erfüllt, kann sie zudem als DiGA eingetragen und wie ein Medikament „auf Rezept" von Ärzt:innen oder Psychotherapeut:innen verschrieben werden. Alle Gesundheits-Apps verarbeiten üblicherweise Gesundheits- und andere sensible Daten, die als besondere Kategorien personenbezogener Daten besonders geschützt sind, denn ihre Preisgabe birgt viele Risiken. So kann der Missbrauch von Daten unter anderem zu sozialer Isolation, finanziellen oder beruflichen Nachteilen führen.

Damit App-Nutzende der Verarbeitung ihrer Gesundheits- und personenbezogenen Daten durch die App-Anbieter vertrauen, ist es daher entscheidend, dass die Daten in ausreichendem Maße geschützt sind und ihre Erfassung und Verarbeitung transparent, nachvollziehbar und verständlich gestaltet ist. Schwer verständliche Datenschutzerklärungen, fehlende Kontrolle über die eigenen Daten oder unklare Zustimmungsprozesse führen dagegen zu Misstrauen von Nutzenden und können die Ablehnung der Gesundheits-App zur Folge haben.

In einem Markt mit steigendem Bewusstsein für Datenschutz ist eine transparente, verständliche und nutzerzentrierte informierte Einwilligung in die Datenverarbeitung (informed consent) nicht nur ethisch und rechtlich geboten, sondern auch ein Differenzierungsmerkmal. Sie stärkt das Vertrauen der Nutzenden und erhöht die Kundenbindung. Nutzende sind dann eher bereit, aktuelle und korrekte Informationen bereitzustellen, was die Datenqualität erhöht, und sensible Daten zu teilen, etwa für Forschungszwecke.

Dennoch bleibt die konkrete Umsetzung der informierten Einwilligung bei der Entwicklung von Gesundheits-Apps eine Herausforderung. App-Entwickler:innen fühlen sich in der Implementierung datenschutzkonformer Lösungen oft unsicher. Vielen Teams fehlen klare Leitlinien, wie Einwilligungen dynamisch, kontextabhängig und nachvollziehbar gestaltet werden können. Ohne adäquate Unterstützung durch technische Standards, ethische Rahmenbedingungen und praxisnahe Anleitungen bleibt die Einwilligung daher oft ein formaler Akt, der das Ziel der echten Selbstbestimmung und des vertrauensvollen Umgangs mit sensiblen Daten verfehlt.

Der vorliegende Leitfaden soll Ihnen als Entwickler:innen, Produktmanager:innen und Datenschutzverantwortliche, die eine datenschutzkonforme und nutzerzentrierte Umsetzung der informierten Einwilligung in digitalen Anwendungen anstreben, Orientierung und Hilfestellung geben. Durch die Kombination von rechtlichen Grundlagen, der Patienten- und Nutzerperspektive, technischen Umsetzungsempfehlungen und konkreten Beispielen ermöglicht der Leitfaden eine nachvollziehbare, anwendungsnahe Unterstützung. Wir bringen Ihnen pragmatische, praxisorientierte Privacy Best Practices (PBPs) für die informierte Einwilligung näher, die die Prinzipien des Privacy by Design in die Praxis umsetzen und den Schwerpunkt auf Klarheit, Benutzerfreundlichkeit und tatsächliche Nutzerkontrolle legen. Ergänzend zum Leitfaden bietet ein interaktiver Demonstrator (› prima-i.ostfalia.de) eine konkrete Anwendung der hier vorgestellten Privacy Best Practices, um die Umsetzung nachvollziehbar und greifbar zu machen.

Der Leitfaden entstand im Rahmen des Forschungsprojekts PRIMA[1] („Privatheitsmanagement bei Gesundheits-Apps entlang der Patient Journey"). Er basiert auf Literaturanalysen[2], rechtlichen Analysen[3] sowie einer empirischen Untersuchung der Perspektive von Patient:innen und App-Nutzenden[4]. Das Projekt wurde im Rahmen der Plattform Privatheit vom Bundesministerium für Forschung, Technologie und Raumfahrt (BMFTR) gefördert (FKZ: 16KIS1884K und 16KIS1885). Besonderer Dank gilt auch der Systemhaus ULM GmbH und der C&S Computer und Software GmbH für ihre

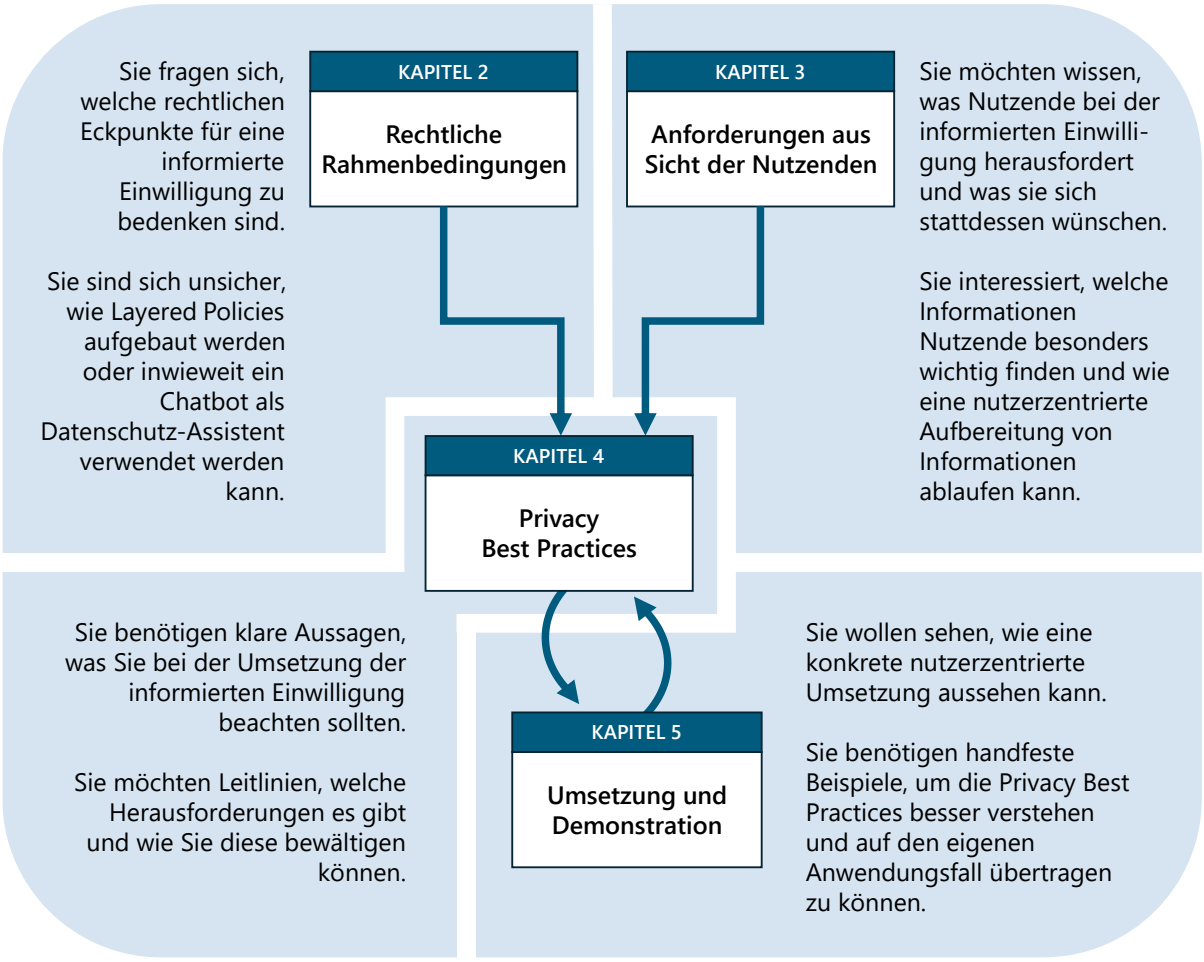
engagierte Mitwirkung, ihre fachliche Expertise und ihre Unterstützung während des Projekts. Ihre Beiträge haben die Qualität und Relevanz der Ergebnisse maßgeblich gestärkt.

1.1 Wie der Leitfaden zu nutzen ist

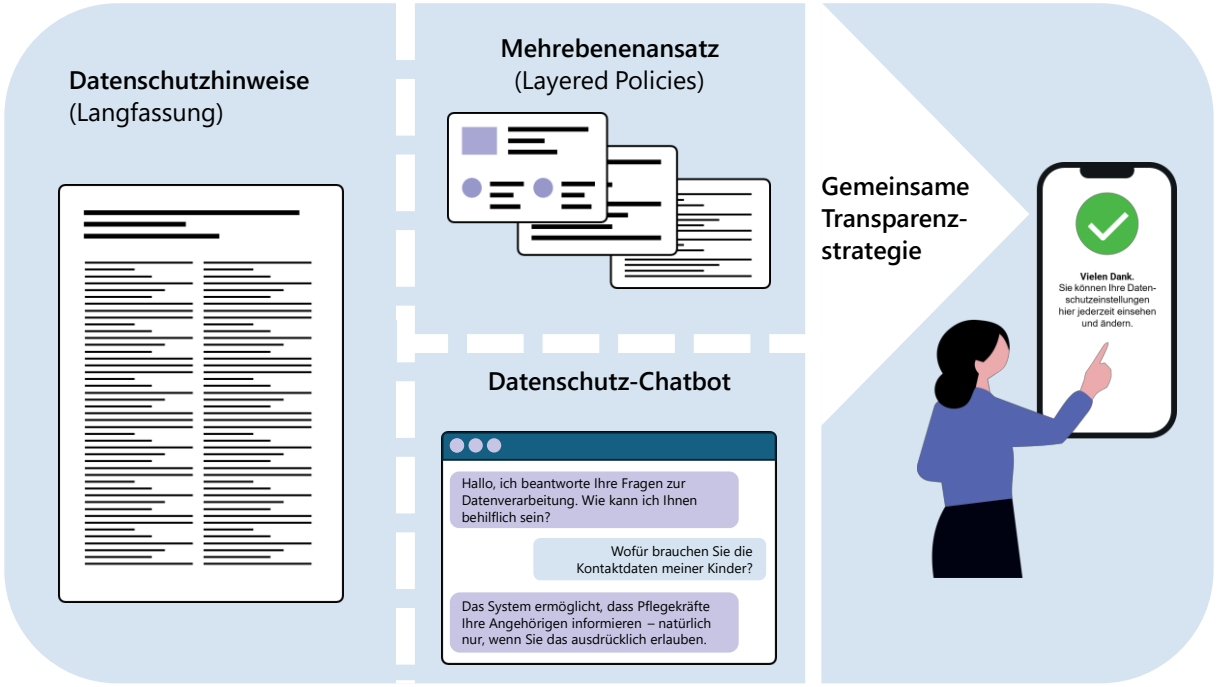
Dieser Leitfaden richtet sich insbesondere an Teams, die an der Entwicklung oder Weiterentwicklung von Gesundheits-Apps beteiligt sind, kann aber auch auf andere Bereiche übertragen werden. Das Dokument kann in verschiedenen Phasen des Entwicklungsprozesses genutzt werden: Bei der Konzeptphase zur Gestaltung von Einwilligungsprozessen, während der Implementierung zur Sicherstellung von Klarheit und Benutzerfreundlichkeit, oder auch zur Überprüfung und Verbesserung bestehender Systeme.

Der Leitfaden ist modular aufgebaut, das heißt, Sie können je nach Interesse bei unterschiedlichen Kapiteln einsteigen. Ein sequenzielles Lesen von Anfang bis Ende ist zwar empfehlenswert, aber nicht notwendig. › Abbildung 1 erläutert, welches Kapitel Sie als Einstieg wählen können, je nachdem welche Informationen Sie suchen. In › Kapitel 2 finden Sie Informationen zu den rechtlichen Eckpunkten und in › Kapitel 3 die Anforderungen aus Sicht der Nutzenden. Das Herzstück dieses Leitfadens bilden die Privacy Best Practices (PBP) als klare Leitlinien zur Umsetzung der informierten Einwilligung in › Kapitel 4. In den anderen Kapiteln wird auf diese an relevanten Stellen immer wieder querverwiesen (z.B. › PBP 1.1). In › Kapitel 5 finden Sie eine demonstrative Umsetzung der vorgestellten PBPs.

Abbildung 1: Einstiegspunkte in den Leitfaden



2 Rechtliche Rahmenbedingungen der informierten Einwilligung



Dieses Kapitel fasst die wichtigsten rechtlichen Eckpunkte und Erwägungen für eine transparente und verständliche Information über Datenverarbeitungen zusammen. Ziel der Darstellung ist, die aus rechtlicher Sicht nötigen Hintergrundinformationen für die in › Kapitel 4 vorgestellten Privacy Best Practices (PBPs) darzulegen. Dieses Kapitel kann daher nicht die datenschutzrechtlichen Voraussetzungen abschließend abbilden. Hierzu verweisen wir auf umfassendere Darstellungen und Leitfäden, etwa der europäischen Datenschutzaufsichtsbehörden zu Transparenz[5], AI[6], Einwilligung[7] oder Gesundheits-Apps[8].

Die nachfolgende Darstellung führt in die Grundlagen der Information über Datenverarbeitungen ein und zeigt am Beispiel der für eine informierte Einwilligung erforderlichen Informationen, welche Transparenzanforderungen grundsätzlich für Datenverarbeitungen gelten (› Kapitel 2.1). Anschließend werden Instrumente zur praktischen Umsetzung des Transparenzgebots erläutert (› Kapitel 2.2), insbesondere wie sich diese Transparenzanforderungen durch einen Mehrebenen Ansatz (Layered Policies) und den Einsatz eines KI Chatbots technisch umsetzen lassen.

2.1 Rechtsgrundlagen und Voraussetzungen der informierten Einwilligung[9]

Jede Datenverarbeitung von personenbezogenen Daten im Sinne der Europäischen Datenschutz-Grundverordnung (DSGVO) bedarf einer gesetzlichen Erlaubnis (Rechtsgrundlage). Das bedeutet, immer wenn Daten mit Personenbezug erhoben, gespeichert, übermittelt, analysiert oder anderweitig verarbeitet werden, darf das nur geschehen, wenn der hierfür Verantwortliche (z. B. ein App-Betreibende) auch eine Rechtsgrundlage dafür hat. Die Rechtsgrundlagen für die Datenverarbeitung sind in der DSGVO abschließend erfasst. Für die Verarbeitung durch Gesundheits-Apps kommt neben der Vertragserfüllung bei der App-Bereitstellung auch eine Einwilligung der Betroffenen nach Art. 6 Abs. 1 lit. a und Art. 9 Abs. 2 lit. a DSGVO in Betracht. (› PBP 1.11, › PBP 5.1)

Art. 6 DSGVO dient als Grundlage zur Verarbeitung personenbezogener Daten. Bei der Verarbeitung besonderer Kategorien personenbezogener Daten, etwa Gesundheitsdaten gilt: Gesundheitsdaten dürfen ausschließlich verarbeitet werden, wenn neben der Rechtsgrundlage aus Art 6 Abs. 1 DSGVO zusätzlich eine Ausnahme nach Art. 9 Abs. 2 DSGVO gegeben ist. Das Gesetz sieht für bestimmte Anwendungen zur Gesundheitsvorsorge im Rahmen von Verträgen mit Angehörigen eines Gesundheitsberufs[10] oder Verarbeitungen für das öffentliche Gesundheitsinteresse bereits Ausnahmen vor. Soll indes eine Gesundheits-App über die eigentliche Gesundheitsvorsorge oder Versorgung hinausgehende Zwecke verfolgen, etwa weil App-Anbietende auf Grundlage der Daten über die eigentliche Versorgung hinausgehende Funktionen wie Ernährungshinweise oder Erinnerungsdienste anbieten, ist eine ausdrückliche Einwilligung erforderlich.

Damit eine Einwilligung rechtswirksam ist, muss sie entsprechend den datenschutzrechtlichen Regularien konkrete Anforderungen erfüllen. Im Folgenden wird die Einwilligung als ein besonders transparenzsensibler Anwendungsfall genutzt: Die dargestellten Informationsanforderungen lassen sich jedoch in weiten Teilen auch auf andere Datenverarbeitungen übertragen.

2.1.1 Wie muss eine Einwilligung eingeholt werden?

Entscheidend bei der Einholung einer Einwilligung (› PBPs 1.1 ff) ist die aktive Zustimmung (› PBP 1.7) der betroffenen Person sowie bei Gesundheitsdaten zudem eine ausdrückliche Zustimmung (› PBP 1.10). Es muss also eine bestätigende Handlung durch die betroffene Person erfolgen, eine bloße fortgesetzte Nutzung genügt nicht. Die aktive Einwilligung lässt sich im digitalen Kontext durch verschiedene Varianten umsetzen:

- Ausfüllen eines elektronischen Formulars,
- Senden einer E-Mail,
- Abgabe einer bestimmten Handlung als Bestätigung wie beispielsweise dem Drücken eines Knopfes oder einer Taste oder ganz konkret bei einer App-Gestaltung: Ein Kästchen, das aktiv anzuklicken ist.

Checkbox-Lösung: Es darf keine Auswahl durch den Verantwortlichen vorgegeben werden, also das Feld darf nicht bereits vorab angeklickt sein und den Nutzenden lediglich eine Möglichkeit zur Abwahl (opt-out) geben werden. (› PBPs 1.8 f)

Bei der Verarbeitung von Gesundheitsdaten verlangt die DSGVO eine ausdrückliche Einwilligung. Nutzende müssen der Verarbeitung also – zusätzlich zur „aktiven" Erklärung – auch klar, bewusst und eindeutig zustimmen. Der Einwilligungstext sollte dazu die Art der besonders schutzbedürftigen Daten benennen. Wichtig ist, dass Nutzende vor der Zustimmung verstehen, welche Daten wofür verarbeitet werden. (› PBP 1.10)

Beispiel: *„Wir speichern ihre App-Tagebucheinträge inkl. Bewegungs-, Ernährungs- und Blutdruckdaten und erstellen in unserem KI-System damit Empfehlungen für Sie. Sie können diese Empfehlungen in der App einsehen; auf Wunsch können Daten und Empfehlungen mit Ihrem Arzt oder anderen von Ihnen benannten Empfängern geteilt werden."*

Nach der Rechtsprechung des Europäischen Gerichtshofs (EuGH) ist ausgeschlossen, dass „Stillschweigen, bereits angekreuzte Kästchen oder Untätigkeit" eine wirksame Einwilligung darstellen können[11]. In solchen Fällen lässt sich objektiv nicht feststellen, ob Nutzende der Verarbeitung ihrer personenbezogenen Daten tatsächlich zustimmen oder die voreingestellte Markierung nur beibehalten haben. Entsprechend ist eine aktive Einwilligung (opt-in) erforderlich[12], also eine eindeutig bestätigende Handlung, wie sie auch Erwägungsgrund 32 DSGVO verlangt. (› PBP 1.7)

Hinweis: In der Praxis eher verbreitet ist das Anklicken einer Checkbox als aktive Form der Einwilligung. Entscheidend ist, dass die betroffene Person eine Handlung durchführen muss, um die Einwilligung abzugeben. Das könnte beispielsweise auch im Rahmen einer Unterhaltung mit einem Chatbot erfolgen, solange die betroffene Person Sätze hierfür eintippen muss, beispielsweise *„Ja, ich willige in die Datenverarbeitung ein"* oder *„Ja, ich stimme der Datenverarbeitung zu"*. Die konkreten Formulierungen sind für jeden Einzelfall zu bestimmen.

2.1.2 Was bedeutet „in informierter Weise" einwilligen?

Neben der Art der Einholung einer Einwilligung muss diese auch in informierter Weise durch die betroffenen Person erfolgen. Betroffene müssen vor und bei Abgabe einer Einwilligung informiert sein. Das bedeutet, ihnen müssen alle notwendigen Informationen bereitgestellt werden, die eine sachliche Entscheidung zulassen (› PBPs 2.1 ff). Die betroffene Person muss verstehen, wofür sie konkret ihre Einwilligung abgibt, was mit ihren Daten passiert und welche Dritten diese Daten verarbeiten.

Hinweis: Nur wenn die betroffene Person informiert ist, kann diese eine wirksame Einwilligung abgeben und diese zum Beispiel auch widerrufen (› PBP 4.1 ff).

Damit Betroffene als informiert gelten, erachtet die EDSA[13] folgende Informationen als mindestens notwendig an (› PBP 2.1):

- Identität des Verantwortlichen bzw. aller gemeinsam Verantwortlichen,
- der Zweck jedes Verarbeitungsvorgangs, für den die Einwilligung eingeholt wird,
- die (Art der) Daten, die erhoben und verwendet werden,
- das Bestehen eines Rechts, die Einwilligung zu widerrufen,
- gegebenenfalls Informationen über die Verwendung der Daten für eine automatisierte Entscheidungsfindung gemäß Art. 22 Abs. 2 lit. c DSGVO, und
- Angaben zu möglichen Risiken von Datenübermittlungen ohne Vorliegen eines Angemessenheitsbeschlusses und ohne geeignete Garantien nach Art. 46 DSGVO.

Neben diesen zwingend erforderlichen Kerninformationen für die Einwilligung selbst gilt es zu beachten:

→ Daneben sind auch die Informationspflichten nach Art. 13, bzw. 14 DSGVO zu erfüllen (u.a. Name und Kontaktdaten des Verantwortlichen, Art der Datenverarbeitung, Zweck der Datenverarbeitung, Empfänger von Daten einschließlich Auftragsverarbeiter, etc.).

→ Insbesondere bei Einsatz von KI-Systemen ist gesondert zu erläutern, ob und wie automatisierte Entscheidungen oder Profiling eingesetzt werden und ob eine menschliche Überprüfung erfolgt.

→ Das bedeutet, betroffene Personen sollten bei Einwilligung über die in Erwägungsgrund 42 genannten Informationen (mindestens Angaben zu Verantwortlichen und die Verarbeitungszwecken) informiert sein. Im Übrigen sind sie auf die weiterführenden und ausführlicheren Informationen in der Datenschutzerklärung hinzuweisen, die sie direkt einsehen können (z.B. über einen Hyperlink). (› PBP 2.2)

Hinweis: Nutzen App-Betreiber/App-Hersteller bei der Entwicklung bestimmte Frameworks (z. B. auch plattformübergreifend), sind diese auf ihre eigene DSGVO-Konformität zu prüfen. Das bedeutet, enthalten die Frameworks Anbieter, die DSGVO-widrig die Daten der betroffenen Person verarbeiten und hierauf nicht oder nur mangelhaft hinweisen, dürfen diese nicht eingebunden werden.

Im Gesundheitsbereich ist der sogenannte Broad Consent eine verbreitete Ausnahme zur informierten Einwilligung. Diese Gestaltung ist vor allem für die wissenschaftliche Forschung gedacht. Wesensmerkmal der Forschung ist, dass man nicht vorhersagen kann, welche Forschungsfragen künftig eine Rolle spielen werden. Deshalb kann eine breitere Einwilligung dort in engen Grenzen statthaft sein, aber nur sofern zusätzliche Schutzmaßnahmen eingehalten werden[14,15]. Für normale Apps ist das aber keine Lösung: Dort sind Zweck und Datenverarbeitung möglichst konkret zu beschreiben. Eine offen gehaltene Sammel-Einwilligung für spätere, noch unklare Nutzungen ist nicht möglich. (› PBP 1.5)

Hinweis: „All-in-One-Einwilligungen" können problematisch sein, wenn diese in keinem Zusammenhang zur Dienstleistung/dem Produkt stehen und damit möglicherweise als unfreiwillig gelten.

2.1.3 Welche Merkmale muss eine Einwilligung erfüllen?

Eine Einwilligung muss

- freiwillig sein, (› PBP 1.6, › PBP 1.9)
- für bestimmte Zwecke abgegeben werden (› PBP 1.2) und
- unmissverständlich sein. (› PBP 1.10)

Außerdem muss die erforderliche *Willensbekundung* „für den konkreten Fall" erfolgen, was so zu verstehen ist, dass sie sich gerade auf die betreffende Datenverarbeitung beziehen muss und nicht aus einer Willensbekundung mit anderem Gegenstand abgeleitet werden kann.

Hinweis: In dem Fall des EuGH war die Einwilligung innerhalb des Vertragstextes enthalten, was der EuGH mit Verweis auf Art. 7 Abs. 2 S. 1 DSGVO ablehnte. Eine Einwilligung muss klar vom Vertragsschluss und anderen Erklärungen abgrenzbar sein.

Ebenfalls relevant ist die Transparenz der Datenverarbeitung, damit diese für die betroffene Person unmissverständlich ist. Neben der inhaltlichen Ausgestaltung spielt auch die Nachweisbarkeit der Einhaltung der Datenschutzgrundsätze eine zentrale Rolle. Nach Art. 5 Abs. 2 DSGVO ist der Verantwortliche verpflichtet, die Einhaltung der Grundsätze, einschließlich einer wirksam informierten Einwilligung, jederzeit belegen zu können. Dazu gehören unter anderem die Dokumentation, Versionierung und Protokollierung des Einwilligungsprozesses, damit Verantwortlicher und betroffene Person später nachvollziehen können, wann, worüber und in welcher Form eingewilligt wurde. (› PBPs 3.1 ff, › PBPs 5.2 ff)

2.1.4 Welche Transparenzanforderungen gelten?

Eine Einwilligung ist nur dann wirksam, wenn sie „in informierter Weise" erfolgt (› Kapitel 2.1.2). Informiertheit kann erst dann entstehen, wenn Informationen zur Datenverarbeitung auffindbar,

verständlich und zugänglich sind (› PBPs 2.2 ff). Sie müssen also transparent erfolgen. Die Informiertheit setzt Verständlichkeit voraus. (› PBPs 2.5 ff)

Die DSGVO verlangt hierfür „klare und einfache Sprache" (Art. 12 DSGVO). Das bedeutet:

- Kurze Sätze, aktive Formulierungen
- Keine abstrakten Sammelbegriffe ohne Konkretisierung („Verbesserung", „Services", usw.)
- Informationen müssen schnell erfassbar sein
- Kein „Informationsübermaß"
- Klare Gliederung und Hervorhebung zentraler Punkte
- Informationen müssen dauerhaft verfügbar und reproduzierbar für betroffene Personen sein, also kein temporäres Pop-up!
- Nachgelagerte Informationen (post-consent) reicht nicht
- Informationen nicht vermischen (z.B. Einwilligung in Datenschutzerklärung)
- Keine zu langen und zu juristischen Texte

Beispiel: Schreiben Sie nicht *„Wir nutzen Ihre Daten zur Verbesserung unserer Dienstleistungen"*. Sondern verdeutlichen Sie *„Wir analysieren Ihr Nutzerverhalten, um Ihnen personalisierte Produktempfehlungen anzuzeigen"*.

2.2 Instrumente zur praktischen Umsetzung des Transparenzangebots

Die Umsetzung der soeben skizzierten Transparenzanforderungen lässt für Verantwortliche und damit auch für App-Entwickler:innen Raum für eigene Gestaltungen. Dieses Unterkapitel soll mögliche Wege aufzeigen und zur Umsetzung anregen. Gerade zielgruppenspezifische Anpassungen - etwa für Kinder oder Personen mit Einschränkungen - sind zulässig und erwünscht. Aus der Breite denkbarer „Transparenz by Design"-Lösungen sollen dazu nachfolgend zwei Konzepte vorgestellt werden, die sich für die Umsetzung bei Apps unserer Ansicht nach besonders eignen. Zum einen die Darstellung der Informationen im Mehrebenen-Ansatz (Layered Policies) (› Kapitel 2.2.1). Informationen zum Datenschutz werden in mehreren Schichten (Layern) bereitgestellt. Das Ziel ist es, Nutzenden das Wesentliche sofort verständlich zu machen. Wer tiefergehende Details sucht, kann diese gezielt abrufen. Zum anderen erscheint der Rückgriff auf einen KI-Chatbot (› Kapitel 2.2.2) als Übersetzer zwischen dem juristischen Fachtext einer Datenschutzerklärung hin zu verständlichen Antworten im Stil der Fragesteller eine sich im digitalen Kontext heute aufdrängende Lösung.

2.2.1 Mehrebenen-Ansatz (Layered Policies)

Nach Artikel 12 DSGVO müssen Informationen in präziser, transparenter, verständlicher und leicht zugänglicher Form sowie in einer klaren und einfachen Sprache übermittelt werden. Nutzerstudien zeigen jedoch, dass Patient:innen klassische Datenschutzerklärungen oft als zu lang, unübersichtlich, ermüdend und fachsprachlich empfinden (vgl. › Kapitel 3.1). Mit Layered Policies wird dieses Problem adressiert, indem sie die Informationsflut strukturieren und nutzergerecht portionieren (› PBP 2.6). Dabei nimmt die Detailtiefe der Informationen von Schicht zu Schicht zu (› Abbildung 2).

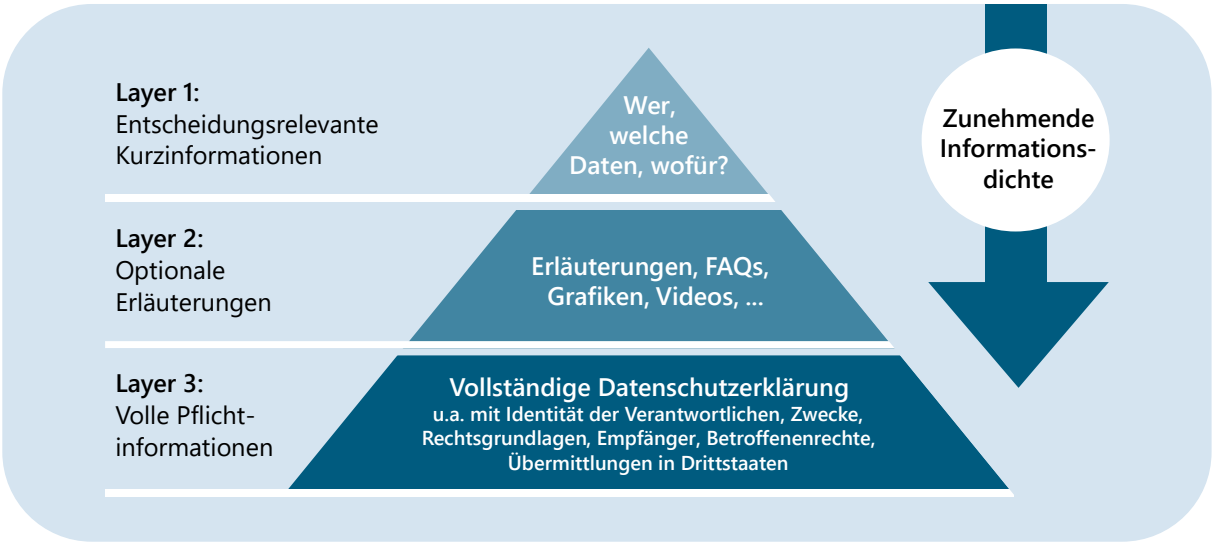
Die erste Schicht (Layer 1, Spitze der Pyramide) befindet sich direkt an der Stelle, an der über die Datenverarbeitung informiert wird bzw. wo die Einwilligung in der App eingeholt wird. Sie beantwortet die wichtigsten Fragen aus Nutzersicht in wenigen einfachen Worten: Wer verarbeitet welche

Daten zu welchen Zwecken? Insbesondere sind Verarbeitungen und Zwecke zu nennen, die mit besonders starken Auswirkungen für betroffene Personen verbunden oder schlicht überraschend sind. Daneben gehört hierhin ein Hinweis auf die Betroffenenrechte. (› PBP 2.1, › PBP 2.8)

Die zweite Schicht enthält optionale Erläuterungen und Details (Layer 2, Mitte der Pyramide): Durch Interaktion (zum Beispiel über ein Pop-up-Fenster oder eine Schaltfläche „Mehr erfahren") erhalten Nutzende konkretisierende Erklärungen. Es können beispielsweise spezifische Akteure (etwa „Krankenkassen" oder „technische Dienstleister" statt nur der Begriff „Dritte") genannt oder konkrete Speicherfristen erklärt werden.

Die zwingend erforderliche dritte Schicht enthält die vollständige Datenschutzerklärung (Layer 3, Basis der Pyramide). Hier sind die vollständigen Informationen verfügbar mit allen nach Artikel 13 und 14 DSGVO verpflichtenden Angaben, wie Details zu Betroffenenrechten. Die vollständige Datenschutzerklärung sollte jederzeit von allen Ebenen aufrufbar sein. Sie ist auch nicht ersetzbar, sondern wird durch die anderen Ebenen erläuternd ergänzt. (› PBP 2.2)

Abbildung 2: Datenschutzinformationen gemäß Layered Policies



Optionaler Layer 4: Als Erweiterung könnte eine vierte Schicht zusätzliche Dokumente wie eine bereinigte Version des Verzeichnisses von Verarbeitungstätigkeiten anbieten. Dies erhöht die Transparenz weiter, sollte aber wegen möglicher Haftungsrisiken nur gegenüber Zielgruppen genutzt werden, die derartige Informationen benötigen (etwa Verantwortliche, die als Kunden von Auftragsverarbeitern ihrerseits Detailkenntnisse über Verarbeitungsvorgänge benötigen).

Die Aufteilung in Schichten deckt sich mit den Erwartungen der Patient:innen und erleichtert ihnen das Verständnis (vgl. › Kapitel 3.3).

Hinweis: Die DSGVO fordert *vollständige* und *verständliche* Informationen. Layered Policies helfen, diesen Widerspruch aufzulösen: Layer 1 sichert das schnelle Verständnis zentraler Informationen, Layer 3 gewährleistet die rechtliche Vollständigkeit.

2.2.2 KI-Chatbot als Datenschutz-Assistent

Um die verschiedenen Layer umzusetzen, eignen sich auch Tools wie ein KI-Chatbot. Dieser kann gezielte Informationen zu Fragen der betroffenen Personen geben und die Informationen verständlicher machen (› PBP 2.9 ff). Als interaktive Datenschutzerklärung kann er so zur Transparenz beitragen.

Ein KI-Chatbot kann als dynamische Komponente innerhalb eines Transparenzkonzepts eingesetzt werden, um die Informationsvermittlung interaktiv zu unterstützen. Er fungiert als intuitiver Übersetzer zwischen komplexen Fachtexten und den konkreten Fragen der Nutzenden, stößt dabei jedoch an klare rechtliche Grenzen. Ein solcher Chatbot kann weder die Pflichtangaben nach Art. 13 und 14 DSGVO noch eine formwirksame und rechtsverbindliche Einholung der Einwilligung ersetzen.

Rechtliche Anforderungen an den Chatbot

Ein KI-Chatbot wäre im oben (› Kapitel 2.2.1) vorgestellten Mehrebenen System auf der zweiten Ebene als optionale Ergänzung zu verstehen. Bei einem Einsatz eines Chatbots ist demgemäß zu beachten:

- → Der Chatbot stellt eine Datenverarbeitung dar, so dass die Datenschutzerklärung über den KI-Chatbot aufklären muss, u.a. zu Zweck, verarbeitete Daten, Speicherdauer, Verantwortlicher.
- → Die Antworten müssen inhaltlich korrekt sein, so dass die KI diese ausschließlich aus der Datenschutzerklärung oder anderer dafür freigegebener Dokumente schöpfen darf (FAQs, Ausschnitte des Verzeichnisses der Verarbeitungstätigkeiten). Die Korrektheit des Antwortverhaltens ist vor Inbetriebnahme zu testen.
- → Ein Halluzinieren ist zu unterbinden und stattdessen auf das Fehlen der Informationen hinzuweisen.
- → Die KI darf durch die Fragen nicht trainiert werden.
- → Wird ein KI-Chatbot eines Drittanbieters genutzt, muss mit diesem ein Auftragsverarbeitungsvertrag abgeschlossen werden. Der Vertrag muss sicherstellen, dass Daten umgehend gelöscht werden und nicht zum KI-Training verwendet werden (Zero-Data-Retention-Agreement).
- → Drittanbieter außerhalb der EU/EWR sollten vermieden werden, da andernfalls schon vor der Nutzung des Chatbots eine ausdrückliche Einwilligung erforderlich sein kann, erhöhte Transparenz-Anforderungen greifen und weitere Voraussetzungen für einen Datentransfer aus der EU heraus bestehen können.
- → Schutz vor aufgedrängten Informationen und ungewollten Eingaben: Da bei Texteingaben nicht verhindert werden kann, dass Nutzende personenbezogene Daten einschließlich Gesundheitsdaten oder Diagnosen eingeben, sind geeignete Vorkehrungen zu treffen. Mindestens sind die Nutzenden deutlich darauf hinzuweisen, keine personenbezogenen Daten einzugeben, und eingegebene Daten sind umgehend zu löschen. Für hochsensible Daten wie Angaben zur Gesundheit oder zum Sexualleben sollten Vorab Filter diese erkennen und durch Platzhalter ersetzen, bevor eine Weitergabe an das KI-Modell erfolgt.
- → Daten sind nach Beendigung des Dialogs zu löschen.

Hinweis zu Beginn der Nutzung

Um das Risiko von Falschinformationen zu minimieren und die Transparenz zu maximieren, müssen bei der Programmierung des Chatbots (insbesondere bei der Prompt-Gestaltung) folgende Prinzipien beachtet werden:

- Verweis auf die vollständige Datenschutzerklärung nebst Verlinkung und dem Hinweis, dass der Chatbot lediglich übersetzend tätig ist.
- Transparenzhinweis, dass ein KI- System eingesetzt wird (Art. 50 KI-VO).
- Hinweis, dass der Chatbot keine personenbezogenen Daten besonderer Kategorien verarbeitet und diese nicht eingegeben werden sollen.
- Klarstellung, dass der Chatbot fehlerhafte Antworten liefern könnte.

Beispiel für einen solchen Hinweis: *„Dieser KI-Assistent kann Ihnen erklären, wie die App Ihre personenbezogenen Daten verarbeitet. Alle Antworten basieren auf unserer Datenschutzerklärung, die Sie jederzeit hier (Verlinkung) lesen können.*

Bitte beschränken Sie sich auf Fragen zur Datenverarbeitung und machen Sie insbesondere keine Angaben über sich (Name, Krankheiten, Sonstiges). Der Chatbot speichert Ihren Dialog für die Dauer des Austausches. Antworten einer künstlichen Intelligenz können Fehler enthalten, für wichtige Fragen und verbindliche Information schauen Sie bitte in die Datenschutzerklärung."

Anforderungen an den Chatbot

Um das Risiko von Falschinformationen so gering wie möglich zu halten, sollte bei der Auswahl oder bei der Programmierung eines KI-Chatbots das Folgende beachtet werden:

→ Fokus: Der Chatbot soll nur datenschutzrechtliche Fragen zur Verarbeitung von personenbezogenen Daten im Allgemeinen Kontext beantworten können.

→ Wahrheitsbindung: Alle Antworten sollen ausschließlich auf den dafür freigegebenen und bereitgestellten Informationen basieren (vollständige Datenschutzerklärung) und bei jeder Antwort auf diese verlinken. Halluzinationen sind technisch zu minimieren.

→ Vorformulierte Kurzinformation: Der Einstieg erfolgt über eine vorformulierte Kurzinformation mit den Angaben, wer welche Daten zu welchen Zwecken verarbeitet und dass Betroffenenrechte bestehen. (Layer 1)

→ Verständlichkeit ohne Sinnverfälschung: Der Prompt muss den Chatbot dazu anleiten, die Sprache zu vereinfachen, ohne juristische oder medizinische Fakten inhaltlich zu verändern. Bei Gefahr einer zu starken Vereinfachung soll der Chatbot automatisch eine präzisere Fassung (z. B. in 3 bis 5 Bulletpoints) anbieten.

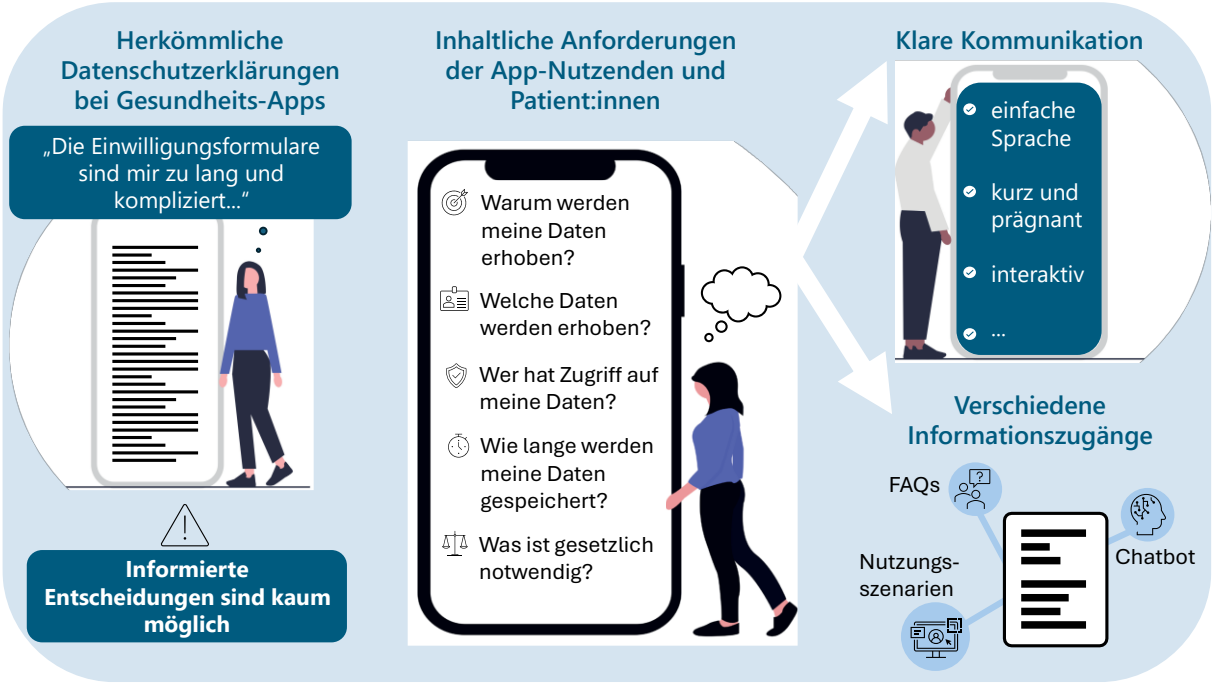
→ Fragen ohne Datenschutzbezug können mit einem vorformulierten Textbaustein beantwortet werden. Beispiel: *„Der Assistent kann nur Fragen zur Datenverarbeitung [der App / des Unternehmens] beantworten."*

→ Bei allen Fragen, die sich nicht auf die Datenschutzerklärung beziehen, sollte es eine einheitliche Antwort als vorformulierten Textbaustein geben. Beispiel: *„Hierzu liegen mir keine Informationen vor."*

Hinweis: Der Betreiber des KI-Chatbots kann nach aktueller Rechtsprechung für falsche Aussagen des Chatbots haften.[16]

---

3 Anforderungen an die informierte Einwilligung aus Sicht der Nutzenden



Dieses Kapitel widmet sich der nutzerfreundlichen Gestaltung von Datenschutzerklärungen und Einwilligungsprozessen sowie deren Wahrnehmung seitens der Nutzenden von Gesundheits-Apps, die oftmals Patient:innen sind.[17]

Zunächst werden die wesentlichen Herausforderungen beleuchtet (› Kapitel 3.1) mit denen Nutzende im Umgang mit Datenschutzerklärungen bei Gesundheits-Apps konfrontiert sind. Ein tiefes Verständnis dieser Hürden bildet die Grundlage dafür, das Vertrauen der Nutzenden in die Anwendung nachhaltig zu stärken.

Darauf aufbauend werden die Bedürfnisse und Erwartungen der Nutzenden an informierte und verständliche Datenschutzerklärungen und den Einwilligungsprozess dargelegt (› Kapitel 3.2). Die Perspektive der Nutzenden unterstützt Sie dabei, Datenschutzinformationen so zu gestalten, dass sie tatsächlich gelesen, verstanden und als vertrauenswürdig empfunden werden.

Im weiteren Verlauf des Kapitels werden konkrete Anforderungen an eine nutzerzentrierte Gestaltung von Datenschutzerklärungen und Einwilligungsprozessen formuliert (› Kapitel 3.3). Diese Anforderungen dienen als praxisorientierter Orientierungsrahmen für die Entwicklung und Überarbeitung von Datenschutzerklärungen und Einwilligungsprozessen.

Abschließend werden mit FAQs (› Kapitel 3.4) und Nutzungsszenarien (› Kapitel 3.5) zwei empirisch erprobte Formate vorgestellt, die eine nutzerzentrierte Umsetzung in der Praxis veranschaulichen und als Inspiration für die konkrete Anwendung dienen sollen.

3.1 Herausforderungen aus Sicht der Nutzenden

Patient:innen empfinden aktuelle Einwilligungsformulare in Gesundheits-Apps in der Regel als zu komplex, umfangreich und wenig benutzerfreundlich. Die Formulare haben aus Sicht der Patient:innen drei zentrale Schwächen:

- Umfang: Die Dokumente sind schlicht zu lang.

- Sprache: Juristische und technische Fachbegriffe machen den Text schwer verständlich.
- Struktur: Die Informationen sind unübersichtlich aufbereitet und schwer zu durchschauen.

Für die Nutzergruppe von Patient:innen kommt hinzu, dass im Kontext von Gesundheits-Apps folgende Faktoren erschwerend auf die informierte Einwilligung wirken können:

- Stresssituationen (z. B. Krankheit), in denen Zeit und Geduld sowie physische und psychische Belastbarkeit fehlen oder eingeschränkt sind
- Vage Formulierungen (z. B. „Dritte"), die keine klare Identifikation der jeweiligen Akteur:innen ermöglichen
- Fehlende Wahlmöglichkeiten, wenn Apps durch medizinische Fachkräfte verschrieben werden und die Nichteinwilligung den Zugang zur gewünschten Versorgung verhindert.

Das Ergebnis ist, dass die Mehrheit der Patient:innen in die Verarbeitung ihrer Gesundheitsdaten einwilligt, ohne die entsprechenden Dokumente gelesen zu haben, dabei jedoch oftmals ein mulmiges Gefühl verspürt. Lediglich Nutzende, die selbst Erfahrungen mit Datenschutzverletzungen oder Cyberkriminalität gemacht haben oder Datenschutz bewusst als Auswahlkriterium für eine App heranziehen, nehmen sich die Zeit für eine detaillierte Prüfung. Auch wenn eine reibungslose Einwilligung ohne kritische Auseinandersetzung aus technischer Sicht kurzfristig als vorteilhaft erscheinen mag, birgt sie mittelfristig das Risiko von Vertrauensverlust. Vertrauen in die Anwendung und das anbietende Unternehmen ist jedoch ein wichtiger Faktor, der die Nutzerbindung stärkt, die Reputation des App-Anbieters schützt und die Krisenresilienz des Anbieters gegenüber öffentlichem Vertrauensverlust erhöht – etwa, wenn Datenschutzvorfälle bekannt werden. Diese empirisch fundierte Beobachtung legt nahe, dass eine veränderte technische und gestalterische Umsetzung der Einwilligungsprozesse dazu beitragen kann, die Informiertheit der Nutzenden und damit das Vertrauen zu verbessern.

Viele Nutzende sind mit den gesetzlichen Grundlagen der Datenverarbeitung nicht vertraut. Besonders unklar sind gesetzlich vorgeschriebene Mindestaufbewahrungsfristen, die einer vollständigen Datenlöschung auf Wunsch entgegenstehen können, zeitlich definierte Zugriffsrechte wie sie etwa bei der elektronischen Patientenakte (ePA) gelten, sowie der Unterschied zwischen dem Widerruf einer Einwilligung und der tatsächlichen Datenlöschung. Diese Wissenslücken können zu Frustration und Vertrauensverlust führen, wenn Nutzende beispielsweise annehmen, Daten vollständig löschen zu können, dies aber gesetzlich nicht möglich ist. Die App sollte daher nicht nur die eigenen Möglichkeiten zur Datenkontrolle, sondern auch die gesetzlichen Grenzen dieser Kontrolle klar und verständlich kommunizieren.

Hinweis zur medizinischen vs. datenschutzbezogenen Einwilligung: Die informierte Einwilligung begegnet Patient:innen in zwei grundlegend verschiedenen Kontexten. Bei der medizinischen Einwilligung – etwa vor einem operativen Eingriff – erfolgt die Aufklärung typischerweise in einem persönlichen Gespräch mit einer medizinischen Fachkraft. Offene Fragen können direkt gestellt und Unsicherheiten im Dialog geklärt werden. Die schriftliche Einwilligung dokumentiert im Anschluss einen bereits stattgefundenen Verständigungsprozess.

Die Einwilligung zur Datenverarbeitung in Gesundheits-Apps hingegen treffen Patient:innen in der Regel vollständig ohne professionelle Begleitung – häufig unter Zeitdruck, in gesundheitlich belastenden Situationen und ohne die direkte Möglichkeit, Rückfragen zu stellen. Hinzu kommt, dass in bestimmten Kontexten neben der Datenschutzeinwilligung auch eine Schweigepflichtentbindungserklärung (§ 203 StGB) erforderlich sein kann, was die Komplexität weiter erhöht.

Für die Softwareentwicklung bedeutet das: Was in der Medizin durch das Aufklärungsgespräch geleistet wird, muss bei der Datenverarbeitung durch Design, Sprache und Struktur der

Benutzeroberfläche übernommen werden. Datenschutzinformationen müssen so aufbereitet sein, dass sie auch ohne begleitendes Fachgespräch vollständig verstanden werden können.

3.2 Worüber Nutzende informiert werden wollen

Patient:innen und App-Nutzende haben klare Vorstellungen davon, welche Informationen sie bei der Einwilligung in die Datenverarbeitung erwarten. Im Mittelpunkt stehen drei übergeordnete Fragen:

- Welche Daten werden verarbeitet?
- Wer hat Zugriff auf die Daten?
- Warum wird dieser Zugriff benötigt?

Diese drei Fragen ziehen sich als roter Faden durch alle weiteren Informationsbedürfnisse und sollten als Mindeststandard für die Informationsarchitektur jeder datenschutzbezogenen Oberfläche in Gesundheits-Apps gelten. (› PBP 2.1, › PBP 2.8)

Im Detail wünschen sich Nutzende Informationen zu folgenden Bereichen

→ In Bezug auf Art und Umfang der verarbeiteten Daten sind Patient:innen oftmals unsicher, welche Daten konkret verarbeitet werden. Sie unterscheiden dabei nicht intuitiv zwischen verschiedenen Datenkategorien. Für die Entwicklung bedeutet dies: Die Benutzeroberfläche muss klar zwischen selbst eingetragenen Daten, automatisch erhobenen Daten (z. B. durch Sensoren) und extern zugespielten Daten (z. B. aus Arztpraxen) unterscheiden und dies für Nutzende sichtbar machen.

→ Bei zugriffsberechtigten Akteuren wird der Begriff „Dritte" von Nutzenden als zu unspezifisch empfunden. Hier wird die Benennung von konkreten Akteurskategorien (z. B. behandelnde Ärzt:innen, Krankenkassen, Forschungseinrichtungen, technische Dienstleister) als hilfreich empfunden und idealerweise auch die Bereitstellung einer Übersicht über aktuelle Zugriffsberechtigte in der App.

→ Ein zentrales Nutzerbedürfnis ist die Möglichkeit, Personen- oder fachrichtungsspezifische Zugriffsrechte zu vergeben. Nutzende möchten nicht pauschal allen Behandelnden Zugang zu allen Daten gewähren, sondern sie möchten anhand granularer Zugriffsrechte differenzieren können. Dies impliziert die Notwendigkeit eines rollenbasierten Zugriffsmodells mit nutzerseitig konfigurierbaren Berechtigungen auf Datenfeld- oder Kategorieebene. Gleichzeitig signalisieren Nutzende, dass eine zu feinkörnige Steuerung auch überfordern kann – daher sind sinnvolle Voreinstellungen essenziell, die Nutzende nach Bedarf anpassen können. Viele Nutzende äußerten zudem den Bedarf einer Zugriffhistorie. Sie wünschen sich eine transparente Übersicht darüber, wer wann auf welche ihrer Daten zugegriffen hat.

Fragen rund um die Speicherung und Löschung von Daten sind für viele Nutzende wichtig, aber häufig unklar. Dabei werden folgende Aspekte thematisiert:

- Wie lange werden Daten gespeichert?
- Können Daten nach Account-Löschung vollständig entfernt werden?
- Was passiert mit den Daten nach dem Tod der betroffenen Person?

Relevant ist hier auch, dass Nutzende Schwierigkeiten haben, gesetzlich geregelte Aufbewahrungsfristen von selbst gewählten Speicherzeiten zu unterscheiden. Diese Differenzierung muss in der Benutzeroberfläche explizit gemacht werden – insbesondere dann, wenn gesetzliche Vorgaben einer vollständigen Datenlöschung entgegenstehen (siehe auch › Kapitel 2.1).

In Bezug auf technische Sicherheitsmaßnahmen und den Speicherort spielen für die Nutzenden technische Details eine wichtige Rolle für das Vertrauen in einen App-Anbieter. Hierbei sind besonders die Art der Verschlüsselung, die Prozesse der Anonymisierung und Pseudonymisierung sowie der geografische Speicherort der Daten (EU vs. andere Staaten) von Bedeutung. Für die Entwicklung bedeutet dies: Informationen zum Serverstandort und zu Sicherheitsstandards sollten leicht auffindbar und klar kommuniziert werden – nicht nur im Kleingedruckten der Datenschutzerklärung, sondern idealerweise in einem dedizierten „Datensicherheits"-Bereich der App.

Durch die DSGVO bereits adressierte Informationspflichten

Das Recht verpflichtet App-Betreibende bereits dazu, über den Zweck der Datenverarbeitung (Art. 13 Abs. 1 lit. c DSGVO), gesetzliche Aufbewahrungsfristen (Art. 13 Abs. 2 lit. a), Betroffenenrechte wie Löschung, Auskunft und Widerruf (Art. 13 Abs. 2 lit. b, Art. 17), die verantwortlichen Datenverarbeitenden (Art. 13 Abs. 1 lit. a) sowie Empfänger:innen bzw. Kategorien von Empfänger:innen (Art. 13 Abs. 1 lit. e) zu informieren. Bei Transfers in Drittstaaten gelten zusätzliche Informationspflichten zum Speicherort (Art. 13 Abs. 1 lit. f, Art. 46 DSGVO).

Diese rechtlichen Anforderungen gelten für jede Gesundheits-App (vgl. › Kapitel 2.1) – die Herausforderung liegt jedoch zusätzlich in der verständlichen und nutzergerechten Umsetzung dieser Anforderungen, nicht im rechtlichen Rahmen selbst.

Über die DSGVO hinausgehende Nutzerbedürfnisse

Mehrere Informationsbedürfnisse sind gesetzlich nicht oder nur teilweise vorgeschrieben und sollten als vertrauensbildende Maßnahmen zusätzlich umgesetzt werden. Dazu gehören:

- → Granulare Zugriffsrechte je Fachrichtung oder Akteur:in: Die Möglichkeit, Zugriffsrechte gezielt nach Fachrichtung oder beteiligter Person individuell einzuschränken oder zu erweitern (z.B. mehr Zugriffsrechte für Hausärzt:innen als für Orthopäd:innen)
- → Zugriffshistorie: Eine einsehbare Protokollierung aller Zugriffe (wer, wann und auf welche Daten).
- → Notfalldatensatz mit automatischem Zugriff für medizinisches Personal: Ein zum Beispiel in der ePA hinterlegter, vorab definierter Datensatz mit medizinisch relevanten Informationen (z. B. Vorerkrankungen, Medikamente, Allergien) ist für medizinisches Personal im Notfall immer abrufbar – als geregelte Ausnahme von den sonst geltenden Zugriffsbeschränkungen.
- → Separate Einwilligung für anonymisierte Daten: Auch wenn anonymisierte Daten nicht unter die DSGVO fallen, stärkt eine explizite Einwilligung das Vertrauen der Nutzenden.
- → Information zum Umgang mit den Daten nach dem Tod: Transparente Informationen zu Löschung oder Zugang zu den Daten durch Angehörige.

3.3 Prinzipien nutzerzentrierter Gestaltung

Aus den Nutzerbedürfnissen lassen sich sieben übergeordnete Gestaltungsprinzipien für die Datenschutzinformationen und den Einwilligungsprozess ableiten (› PBPs 2.5 ff):

- Klarheit bedeutet, einfache, alltagssprachliche Formulierungen zu verwenden – ohne Fach- oder Fremdwörter, die den Lesefluss unterbrechen.
- Kürze erfordert prägnante Darstellungen von Kerninformationen.
- Formatierung umfasst klare Absätze, Fettdruck für Schlüsselbegriffe und ausreichend Weißraum für eine angenehme Lesbarkeit.

- Multimodalität bedeutet, Informationen nicht nur als Text, sondern ergänzend z.B. als Videos, Grafiken und Audios bereitzustellen. Damit kann auch die Barrierefreiheit adressiert werden.
- Gliederung in mehrere Ebenen beschreibt einen mehrstufigen Aufbau: Überblick zuerst, Details auf Abruf – damit Nutzende selbst entscheiden können, wie tief sie einsteigen möchten.
- Interaktivität meint schrittweise Zustimmungen anstelle einer undifferenzierten Einwilligung zu allem am Ende des Dokuments oder Prozesses.
- Augenhöhe meint, Erklärungen so zu formulieren, dass Nutzende auf Basis der Information selbst entscheiden können – ohne das Gefühl, von Juristen oder Technikexpert:innen überwältigt oder bevormundet zu werden.

Das am häufigsten genannte Wunschformat ist ein mehrstufiger Aufbau, der unterschiedlichen Informationsbedürfnissen gerecht wird. Dieses Wunschformat aus Patient:innensicht entspricht weitestgehend dem Konzept der Layered Policies (siehe › Kapitel 2.2.1). Die Umsetzung eines solchen Wunschformats lässt sich auf verschiedenen Ebenen vollziehen.

Zum einen sollten anstelle einer einzigen gebündelten Einwilligung am Dokumentende schrittweise Zustimmungen (Step-by-Step) nach jedem rückmeldepflichtigen Inhalt implementiert werden (vgl. z. B. den Onboarding-Prozess in › Kapitel 5.1). Dieses Format verfolgt zwei Ziele: Erstens wird der Leseprozess verlangsamt und ein bewussteres Durchlesen gefördert. Zweitens erlaubt es Nutzenden, einzelnen Verarbeitungszwecken differenziert zuzustimmen oder diese abzulehnen. Dabei sollten Pflichtfelder für den Kernbetrieb der App klar von optionalen Feldern – etwa für Forschungszwecke – unterschieden werden. Aus Sicht von Patient:innen werden hier insbesondere die schrittweise Zustimmung und das Aufzeigen von Entscheidungskonsequenzen positiv wahrgenommen, da sie das Gefühl einer freien Einwilligungsentscheidung vermitteln. (› PBPs 1.3 ff)

Zum anderen sollte es den Nutzenden leicht gemacht werden, schnell die Informationen zu finden, die sie primär interessieren, ohne sie zuvor in der ausführlichen Datenschutzerklärung suchen zu müssen. Dafür bieten sich insbesondere drei Tools an (› PBPs 2.8 ff):

- Frequently Asked Questions (FAQs)
- Funktionsbezogene Nutzungsszenarien
- Interaktiver KI-Chatbot

Das *FAQ-Format* bündelt empirisch belegte Nutzerbedürfnisse in alltagssprachlich formulierten Fragen und strukturierten Antworten – gegliedert nach Themenbereichen wie Zugriffsrechte, Datensicherheit oder Betroffenenrechte. So finden Nutzende gezielt die für sie relevanten Informationen, ohne die vollständige Datenschutzerklärung durchsuchen zu müssen.

Funktionsbezogene Nutzungsszenarien setzen direkt an konkreten App-Funktionen an – etwa der Registrierung oder dem Hochladen von Befunden – und erklären jeweils, welche Daten dabei verarbeitet werden, wer darauf zugreift und auf welcher Rechtsgrundlage dies geschieht. Nutzende erhalten so kontextgebundene Datenschutzinformationen genau in dem Moment, in dem sie mit der Datenverarbeitung in Berührung kommen.

Ein interaktiver *KI-Chatbot* ermöglicht es Nutzenden, Datenschutzfragen in natürlicher Sprache zu stellen und unmittelbar verständliche Antworten zu erhalten. Dies ist besonders hilfreich für individuelle oder situationsbezogene Fragen, die weder in den FAQs noch in den Nutzungsszenarien explizit abgedeckt sind. Entscheidend für den Nutzen des Chatbots ist aus Sicht von Patient:innen, dass die Antworten korrekt und verständlich aufbereitet sind. Um Vorbehalten gegenüber KI-Modellen entgegenzuwirken, kommt der Transparenz über die Funktionsweise des KI-Modells eine zentrale Rolle für die Vertrauensbildung zu.

Im Folgenden werden die beiden Tools bzw. Formate FAQs und Nutzungsszenarien näher dargestellt. Für den Einsatz eines KI-Chatbots sind insbesondere rechtliche Aspekte relevant (siehe › Kapitel 2.2.2).

3.4 FAQs zur Unterstützung der informierten Einwilligung

Die Grundlogik des FAQ-Formats folgt einem zweistufigen Aufbau: Jede Frage repräsentiert ein empirisch belegtes Nutzerbedürfnis, dem eine strukturierte Erwartungsbeschreibung gegenübersteht, die relevante Antwortaspekte bündelt. Dieser Aufbau ermöglicht es, Inhalte zielgerichtet zu formulieren und Nutzenden nur die jeweils für sie relevanten Informationen anzuzeigen.

Die typischen Fragen von Nutzenden sind in übergeordnete Themenbereiche gegliedert, die den gesamten Lebenszyklus der Datenverarbeitung abdecken – von der grundlegenden Frage nach Verantwortlichkeit und Rechtsgrundlage über konkrete Verarbeitungsvorgänge bis hin zu Handlungsmöglichkeiten und Rechtsdurchsetzungswegen, dargestellt in › Tabelle 1.

Tabelle 1: Thematische Struktur des FAQ-Formats

Themenbereich	Inhaltlicher Schwerpunkt
Verantwortlichkeiten und grundsätzliche Informationen	Rechtliche Grundlagen, Verantwortlichkeiten, Datenschutzerklärung
Datenerfassung und Datennutzung	Art, Umfang und Zweck der erhobenen Daten
Interessen des App-Anbieters	Nutzung der Daten durch das App-Unternehmen, Finanzierung der App
Datenspeicherung und Speicherort	Speichermedium, geografischer Ort, Cloud vs. lokal
Zugriffsrechte	Wer sieht was, Rollen- und Rechtemanagement, Dritte
Datensicherheit	Verschlüsselung, Datenpannen, Schutzmaßnahmen
Dauer der Datenspeicherung	Speicherfristen, Inaktivität, digitaler Nachlass
Richtigkeit der Daten	Einsehen und Ändern der Daten
Löschen der Daten	Löschvorgang, Archivierungspflichten, App-Deinstallation
Betroffenenrechte	Auskunft, Widerruf, Widerspruch, Datenübertragbarkeit

Logik Frage-Antwort-Paare: Jedem Themenbereich ist eine Reihe zentraler Fragen zugeordnet, die im › Anhang aufgeführt sind. Die Fragen sind bewusst alltagssprachlich formuliert und orientieren sich daran, wie Nutzende ein Informationsbedürfnis tatsächlich artikulieren würden. Die zugeordneten Antwortaspekte definieren die inhaltlichen Mindestanforderungen an eine vollständige Antwort – die konkrete Ausformulierung bleibt Aufgabe der Gestaltung. Beim Demonstrator ist die Anwendung des FAQs-Tools auf eine App, die als elektronische Patientenakte (ePA) fungiert, exemplarisch ausgearbeitet[18] (siehe auch › Kapitel 5.2).

Gesetzliche Anforderungen und darüber hinausgehende Bedürfnisse: Das FAQ-Format verbindet DSGVO-verpflichtende Informationspflichten mit Nutzerbedürfnissen, die gesetzlich nicht vorgeschrieben, für das nachhaltige Vertrauen in die App jedoch entscheidend sind. Es ist kein statisches Dokument, sondern muss mit der App und ihrem regulatorischen Umfeld mitwachsen. Die thematische Grundstruktur sollte dabei stabil bleiben – sie bildet das Navigationssystem, an dem sich Nutzende orientieren.

3.5 Funktionsbezogene Nutzungsszenarien zur Unterstützung der informierten Einwilligung

Bei diesem Format sollen Nutzende dort abgeholt werden, wo sie bei der Nutzung konkreter App-Funktionen tatsächlich mit der Datenverarbeitung in Berührung kommen. Die Grundlogik folgt einer konsequenten Nutzerperspektive. Ausgangspunkt ist nicht die Datenschutzerklärung des Anbieters, sondern die Handlungsabsicht der nutzenden Person, zum Beispiel *„Ich möchte mich registrieren und ein Nutzerkonto anlegen"* oder *„Ich möchte meine Behandlungsdaten und Befunde einsehen"*. Jedes dieser Nutzungsszenarien bildet eine eigene Informationseinheit, die entlang von sechs strukturierten Fragen aufgebaut und in › Tabelle 2 dargestellt ist:

Tabelle 2: Grundlogik des Formats Nutzungsszenarien

Strukturfrage	Inhaltlicher Fokus
Welche Daten werden verarbeitet?	Art und Umfang der betroffenen Datenkategorien
Wer greift auf die Daten zu?	Konkrete Akteure und technische Dienstleister
Wofür werden die Daten verarbeitet?	Zweck und Notwendigkeit der Verarbeitung im jeweiligen Funktionskontext
Woher stammen die Daten?	Selbsteingabe, automatische Erhebung oder externe Quellen
Was ist die Rechtsgrundlage?	Einwilligung, gesetzliche Pflicht oder berechtigtes Interesse
Wie kann ich meine Auswahl treffen?	Pflichtfeld oder optional – mit konkreter Handlungsoption

Diese sechs Fragen greifen, die im vorherigen Abschnitt identifizierten, zentralen Nutzerbedürfnisse, unmittelbar auf: Welche Daten werden verarbeitet? Wer hat Zugriff? Warum wird dieser Zugriff benötigt? Das Format übersetzt diese abstrakten Bedürfnisse in eine funktionsbezogene, kontextsensible Informationsarchitektur.

Jedes Nutzungsszenario enthält einen expliziten Verweis auf die einschlägige Rechtsgrundlage der Datenverarbeitung. Dies dient zwei Zwecken: Einerseits wird für alle Nutzenden sichtbar gemacht, auf welcher rechtlichen Basis eine Verarbeitung erfolgt. Andererseits erhalten Nutzende, die die rechtlichen Grundlagen vertiefend nachvollziehen möchten, einen direkten Einstiegspunkt in die einschlägigen Rechtstexte. Die Kurzformulierungen im Szenarioformat – etwa *„Das bedeutet: Sie stimmen ausdrücklich zu, dass …"* – übersetzen die juristische Rechtsgrundlage in alltagsverständliche Sprache, ohne den Bezug zum zugrundeliegenden Recht aufzugeben. Nutzende, die es genauer wissen möchten, finden die vollständigen gesetzlichen Regelungen in der Langfassung der Datenschutzerklärung.

Ein weiteres strukturelles Element dieses Formats ist die Unterscheidung zwischen technisch notwendigen Verarbeitungen und optionalen Diensten. Für jedes Szenario wird transparent gemacht, ob die Datenverarbeitung für den Kernbetrieb der App zwingend erforderlich ist – etwa bei der Registrierung – oder ob Nutzende frei entscheiden können, ob sie die jeweilige Funktion nutzen möchten. Die Beschreibung des Zwecks fällt dabei bewusst konkret aus: Es wird nicht nur allgemein auf die Funktionalität der App verwiesen, sondern aufgezeigt, welche Einschränkungen entstehen, wenn die Einwilligung nicht erfolgt. Dies erhöht die Nachvollziehbarkeit der jeweiligen Einwilligung und macht sowohl den Nutzen als auch die Konsequenzen einer Ablehnung für Nutzende greifbarer.

Das Format der funktionsbezogenen Nutzungsszenarien adressiert gezielt jene Herausforderungen, die bei klassischen Datenschutzerklärungen besonders ausgeprägt sind. Durch die Verknüpfung von gesetzlich geforderten Datenschutzinformationen mit konkreten Nutzungshandlungen wird der Abstraktionsgrad der Informationen für die Patient:innen deutlich reduziert. Darüber hinaus macht das Format die Rechtsgrundlage für jede einzelne Funktion sichtbar und verständlich – inklusive einer kurzen Erläuterung in alltagssprachlicher Formulierung, was die jeweilige Rechtsgrundlage für die nutzende Person bedeutet. Beim Demonstrator ist die Anwendung von Nutzungsszenarien auf eine App, die als elektronische Patientenakte (ePA) fungiert, exemplarisch ausgearbeitet[19] (siehe auch › Kapitel 5.2).

Dieses Format ergänzt das FAQ-Format, ersetzt es jedoch nicht. Während das FAQ-Format themenübergreifende Fragen beantwortet – etwa zur Datenlöschung, zu Betroffenenrechten oder zu technischen Sicherheitsmaßnahmen – liefert das Format der funktionsbezogenen Nutzungsszenarien kontextgebundene Informationen genau dann, wenn Nutzende eine bestimmte Funktion nutzen oder aktivieren wollen. Beide Formate zusammen bilden das im Konzept der Layered Policies (vgl. › Kapitel 2.2.1) vorgesehene mehrstufige Informationssystem: ausführliche Datenschutzerklärung (Langfassung), allgemeine Orientierung durch FAQs, funktionsspezifische Vertiefung durch Nutzungsszenarien.

4 Privacy Best Practices als handlungsleitende Prinzipien

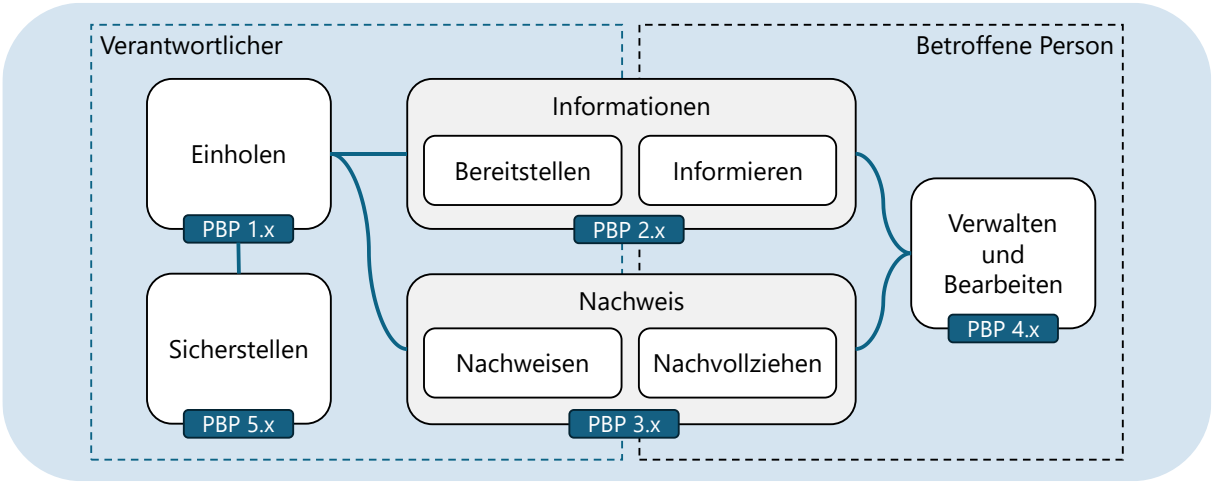
Die Umsetzung der informierten Einwilligung erscheint häufig komplex. Etablierte Ansätze wie Privacy by Design sind entscheidend für eine datenschutzbewusste Entwicklung. Sie stellen sicher, dass Datenschutz und Privatheit von Anfang an in den Entwicklungsprozess eingebunden werden. Privacy Patterns bieten bewährte Lösungsmuster für typische Datenschutzanforderungen. Dieses Kapitel stellt Privacy Best Practices (PBPs) vor, welche Sie durch pragmatische und prägnante Handlungsempfehlungen unterstützen, die informierte Einwilligung nachhaltig und nutzerfreundlich umzusetzen. Diese Prinzipien zeigen, wie Sie Transparenz schaffen, Komplexität vermeiden, Rechtskonformität einhalten und echte Entscheidungsfreiheit für Betroffene ermöglichen.

Die informierte Einwilligung beinhaltet mehrere Herausforderungen. Diese können in fünf Aspekte gefasst werden.

1) Einholen: Es muss die aktive und ausdrückliche Einwilligung der Nutzenden eingeholt werden.
2) Bereitstellen und Informieren: Damit die Einwilligung informiert erfolgen kann, müssen Informationen bereitgestellt werden und Nutzende befähigt sein sich zu informieren.
3) Nachweisen und Nachvollziehen: Anschließend darf die Einwilligung nicht in Vergessenheit geraten. Es ist wichtig Nachweise der Einwilligung bereit zu halten, um Nutzenden die Nachvollziehbarkeit zu ermöglichen und die Rechtmäßigkeit der Verarbeitung im Zweifelsfall belegen zu können.
4) Verwalten und Bearbeiten: Während der gesamten Anwendungsnutzung müssen Nutzende ihre Einwilligungsentscheidungen steuern können.
5) Sicherstellen: Auf der anderen Seite muss jederzeit sichergestellt werden, dass aktuelle Einwilligungsentscheidungen berücksichtigt werden.

Die Einwilligung einzuholen, sicherzustellen, sowie Informationen und Nachweise bereitzuhalten liegen in der Verantwortung des Verantwortlichen im Sinne der DSGVO (vgl. › Kapitel 2.1). Das Informieren, Nachvollziehen und Verwalten bzw. Anpassen sind Fähigkeiten, die Nutzenden als betroffene Personen zur Verfügung stehen sollten. Erhalten Sie einen Überblick in › Abbildung 3.

Abbildung 3: Herausforderungen bei der Umsetzung der informierten Einwilligung



Die folgenden Privacy Best Practices (PBPs) werden diesen fünf Aspekten zugeordnet. Rechtliche Einordnungen dazu sowie explizit zu den Fragen, wie eine Einwilligung eingeholt werden muss und was „in informierter Weise" bedeutet, können Sie in › Kapitel 2.1 nachlesen.

4.1 Einwilligung einholen

Der wichtigste Bestandteil der informierten Einwilligung ist das Einholen dieser. Dies muss vor der Erfassung und Verarbeitung personenbezogener Daten erfolgen. Sie finden die rechtliche Einordnung der Frage, wie eine Einwilligung eingeholt werden muss, in › Kapitel 2.1.1 sowie weitere Merkmale der Einwilligung in › Kapitel 2.1.3.

PBP 1.1 – Informierte Einwilligung muss informiert erfolgen.

Vor dem Einholen der Einwilligung müssen den Nutzenden alle relevanten Informationen zur Verfügung gestellt werden. Genauere Best Practices zur Bereitstellung von Informationen und wie Nutzenden die Möglichkeit gegeben werden kann informiert zu sein, gibt es in › Kapitel 4.2.

PBP 1.2 – Unterschiedliche Zwecke erfordern separate Einwilligungen bei trennbarer Verarbeitung.

Verschiedene Zwecke müssen klar voneinander abgegrenzt werden. Für jeden abtrennbaren Zweck sollten gegebenenfalls separate Einwilligungsoptionen bereitgestellt werden, damit die betroffenen Personen zwischen diesen wählen können. Erfordert ein Zweck mehrere Verarbeitungsvorgänge, kann eine einzige Einwilligung alle diese Vorgänge abdecken, sofern klar beschrieben wird, dass sie diesem Zweck dienen. Dient derselbe Verarbeitungsvorgang mehreren Zwecken (z. B. wird ein Datensatz für den Versand eines Produkts und für Marketingzwecke verwendet), müssen die jeweiligen

Zwecke klar erläutert, die dafür verwendeten Daten benannt und die Einwilligung sollte für jeden Zweck gesondert erteilt werden.

PBP 1.3 – Mehrere Einwilligungen können schrittweise eingeholt werden.

Sollten Sie mehrere separate Einwilligungen für verschiedene Zwecke einholen müssen, erfassen Sie diese schrittweise und separat. Verzichten Sie auf eine umfassende, am Ende des Dokuments angeordnete Einwilligungserklärung. Integrieren Sie stattdessen das Einholen der Einwilligung direkt in den jeweiligen Kontext. Bündeln Sie dafür die für einen bestimmten Zweck relevanten Informationen und holen Sie die Einwilligung unmittelbar und gezielt ein. Ein geeigneter Ansatz ist hierfür beispielsweise ein strukturierter Onboarding-Prozess.

PBP 1.4 – Der Prozess der informierten Einwilligung sollte transparent sein.

Erläutern Sie das Vorgehen zur informierten Einwilligung. Bei einem Onboarding-Prozess skizzieren Sie kurz den Ablauf. Erläutern Sie:

- dass die Einwilligung freiwillig ist.
- ob es eine Zusammenfassung gibt, in der vor der endgültigen Entscheidung nochmal alles angepasst werden kann.
- ob es in der Anwendung Möglichkeiten gibt, die Einwilligung im Nachgang anzupassen, wie diese nachträglich zu erteilen oder zu widerrufen. Sollte dies nicht der Fall sein, erläutern Sie kurz das Vorgehen, sollten Nutzende ihre Entscheidung ändern wollen.
- welche Informationsmöglichkeiten es gibt und wie diese zu erreichen sind.
- ob und wie die Informationen auch im Nachgang einsehbar sind.

Nutzen Sie klare Verlinkungen auf Informationsmöglichkeiten wie die Datenschutzerklärung, FAQs oder einen Chatbot. Sollte der Onboarding-Prozess über mehrere Seiten führen, verdeutlichen Sie den Fortschritt zum Beispiel durch einen Fortschrittsbalken. Ein Undurchsichtiger Onboarding-Prozess kann zu Ungeduld und uninformierten Entscheidungen führen. Vermeiden Sie es, Informationsmöglichkeiten zu verstecken, sodass Nutzende diese nur schwer finden können oder gegebenenfalls sogar keine Kenntnis von diesen erhalten.

PBP 1.5 – Informierte Einwilligung sollte individualisierbar sein.

Unterschiedliche Zwecke und Verarbeitungsprozesse sind zu trennen. Mit dem Modell des *Dynamic Consent* können Nutzende ihre Einwilligungen granular und zeitlich flexibel verwalten. Dies ermöglicht es, Entscheidungen zur Einwilligung für verschiedene Zwecke differenziert zu treffen und jederzeit anzupassen, wenn sich die Umstände oder Bedürfnisse ändern. *Broad Consent*, bei dem Nutzende einer umfassenden Datenverwendung zustimmen, ist zu vermeiden. Dieses Modell ist nur unter bestimmten Umständen zielführend, wie bei Forschungszwecken, bei denen die genaue Verarbeitung nicht absehbar ist (siehe auch › Kapitel 2.1.2). Vermeiden Sie Alles-oder-Nichts-Ansätze und halten Sie die Möglichkeit offen, einzelne Funktionen abzuwählen. Ermöglichen Sie Nutzenden gegebenenfalls Bedingungen festzulegen, unter denen die Einwilligung erteilt wird, wie beispielsweise zeitliche oder zugangsbezogene Einschränkungen. Wichtig ist, keine Abhängigkeiten zu erzeugen. Die Einwilligung muss unabhängig von anderen Einwilligungsentscheidungen für andere Zwecke sein.

PBP 1.6 – Informierte Einwilligung sollte optional sein.

Eine Einwilligung gilt nicht als freiwillig erteilt, wenn der Zugang zu einer Dienstleistung oder die Erfüllung eines Vertrags von der Einwilligung in eine Verarbeitung personenbezogener Daten abhängig gemacht wird, die für die Erfüllung dieses Vertrags nicht erforderlich ist, oder wenn für

verschiedene Verarbeitungsvorgänge keine gesonderte Einwilligung erteilt werden kann, obwohl dies angemessen wäre. Es muss stets die Möglichkeit bestehen, die Einwilligung zu verweigern.

PBP 1.7 – Informierte Einwilligung sollte aktiv sein.

Damit Nutzende eine bewusste Entscheidung treffen und nach außen eine erkennbare Willensbekundung vorliegt, sollte die Einwilligung in Form einer aktiven Handlung erfolgen. Dies kann durch Checkboxen, Swipe oder Drag-and-Drop realisiert werden. Vermeiden Sie Voreinstellungen.

PBP 1.8 – Im Default ist die Einwilligung abzulehnen.

Sollten Sie eine Standardoption anbieten, muss diese darin bestehen, die Einwilligung abzulehnen. Checkboxen müssen frei sein und andere Formate so eingestellt, dass sie einer Ablehnung entsprechen.

PBP 1.9 – Einwilligung und Ablehnung sollten gleichwertig sein.

Die Entscheidung für oder gegen eine Einwilligung sollte mit gleichem Aufwand möglich sein. Wenn eine Schaltfläche wie „Alle akzeptieren" angeboten wird, sollte dort auch eine gleichwertige Schaltfläche wie „Alle ablehnen" oder „Nur notwendige" vorhanden sein. Vermeiden Sie auffällige Hervorhebungen, ungleiche Button-Größen, irreführende Farben oder zusätzliche Zwischenschritte, die ausschließlich die Ablehnung erschweren.

PBP 1.10 – Informierte Einwilligung sollte eindeutig sein.

Unabhängig davon, welche Aktion für das Geben oder Ablehnen der Einwilligung gewählt wird, muss klar erkennbar sein, welche Aktion einer Einwilligung entspricht. Formulieren Sie Texte neben den Checkboxen klar aus. Vermeiden sie farblich kodierte Switches ohne eine Erklärung, welche Farbe und Position der Einwilligung entspricht.

Es muss zusätzlich klar erkennbar sein, zu was eingewilligt wird. Trennen Sie dafür die Informationen für die jeweiligen Zwecke klar voneinander. Bei besonderen Kategorien personenbezogener Daten, etwa Gesundheitsdaten, ist ausdrücklich mitzuteilen, dass solche und zu welchem konkreten Zweck genau diese besonders schutzwürdigen Daten verarbeitet werden. Präsentieren Sie die wichtigsten Informationen an der Stelle, an der auch die Entscheidung bezüglich der Einwilligung getroffen wird.

PBP 1.11 – Die Rechtsgrundlage sollte klar sein.

Unterscheiden Sie klar zwischen einer Verarbeitung auf der Grundlage einer Einwilligung und einer Verarbeitung auf der Grundlage anderer Rechtsgrundlagen (vgl. › Kapitel 2.1). Die Rechtsgrundlage, auf der die Verarbeitung beruht, ist eindeutig anzugeben. Beruht die Verarbeitung auf einer Einwilligung, muss der Verantwortliche in der Lage sein, einem Widerruf der Einwilligung nachzukommen, und darf später nicht auf eine andere Rechtsgrundlage zurückgreifen, um dieselbe Verarbeitung fortzusetzen. Kennzeichnen Sie eine Verarbeitung, die nach dem Recht der Europäischen Union oder der Mitgliedstaaten zwingend vorgeschrieben ist, als solche, um den falschen Eindruck zu vermeiden, dass die betroffene Person eine Wahlmöglichkeit hat.

4.2 Informationen bereitstellen

Sowohl vor und während als auch nach der Einwilligung müssen den Nutzenden alle relevanten Informationen zur Verarbeitung persönlicher Daten zur Verfügung gestellt und verständlich aufbereitet werden. Was „in informierter Weise" aus rechtlicher Sicht bedeutet, finden Sie in › Kapitel 2.1.2 sowie die Anforderungen an Transparenz in › Kapitel 2.1.4. Finden Sie zudem die Herausforderungen und Anforderungen an Einwilligungsformulare aus Sicht der Nutzenden in › Kapitel 3.

PBP 2.1 – Informationen sollten vollständig und angemessen detailliert sein.

Informationen im Zusammenhang mit der Einwilligung müssen Folgendes enthalten: die Identität und die Kontaktdaten des Verantwortlichen oder dessen Vertretung, die Kontaktdaten des Datenschutzbeauftragten sowie Informationen über die Rechte der betroffenen Person, einschließlich des Rechts, die Einwilligung jederzeit zu widerrufen. Darüber hinaus müssen für jede einzelne Einwilligung Informationen über die Rechtsgrundlage, die zu verarbeitenden Daten und deren Zwecke sowie über die Empfänger der Daten, eine etwaige beabsichtigte Übermittlung personenbezogener Daten in ein Drittland und die Speicherdauer bereitgestellt werden. Für eine fundierte Entscheidung sollten auch die Folgen einer Einwilligung oder einer Verweigerung der Einwilligung dargelegt werden, d.h. welche Risiken bestehen und wie sich dies auf die Funktionalität der Anwendung auswirkt. Welche Informationen rechtlich notwendig sind und worüber Nutzende konkret informiert werden wollen, finden Sie in › Kapitel 2.1.2 und › Kapitel 3.2.

PBP 2.2 – Informationen sollten jederzeit erreichbar sein.

Bieten Sie den Zugang zu datenschutzrelevanten Informationen sowohl während als auch jederzeit vor und nach dem Einholen der Einwilligung. Neben direkt präsentierten Informationen während der Einwilligung, müssen Verlinkungen auf die vollständige Datenschutzerklärung klar erkennbar sein.

PBP 2.3 – Informationen und Einstellungen sollten leicht erreichbar sein.

Damit Informationen jederzeit, also auch nach einem möglichen Onboarding-Prozess, erreichbar sind und Einwilligungen jederzeit anpassbar bleiben, richten Sie einen spezifischen Reiter auf der obersten Ebene der Einstellungen ein. Vermeiden Sie lange Wege und verstecken Sie Informationen nicht unter mehreren Reitern.

PBP 2.4 – Links sollten an relevanten Punkten zur Verfügung stehen.

Ergänzen Sie Referenzen zu datenschutzrelevanten Informationen an Punkten, bei denen diese zu beachten sind. Dazu gehören Stellen, an denen personenbezogene Daten eingegeben oder angezeigt werden oder eine solche Funktion aktiv unterbunden wird. In solchen Fällen sollten Sie einen Link zu den Datenschutzeinstellungen bereitstellen, damit Nutzende ihre Präferenzen unter Umständen anpassen können, sobald sie der Verarbeitung ihrer persönlichen Daten oder der Möglichkeit dazu gewahr werden.

PBP 2.5 – Texte sollten verständlich sein.

Nutzen Sie klare und einfache Sprache. Vermeiden Sie komplexe Sätze sowie, wenn möglich, juristische Formulierungen und technische Fachbegriffe. Erklären Sie notwendige Fachbegriffe. Vermeiden Sie außerdem schwammige, undeutliche oder mehrdeutige Formulierungen. Bieten Sie kurze, prägnante Darstellungen von Kerninformationen.

PBP 2.6 – Informationen sollten strukturiert sein.

Unterteilen Sie die Informationen in mehrere Ebenen. Heben Sie wichtige Aspekte hervor und nutzen Sie Zusammenfassungen. Unterteilen Sie Informationen in Komponenten, sodass Nutzende die für sie relevanten Informationen schneller finden können. Ermöglichen Sie ausführlichere Informationen durch Detailebenen. Genauere Informationen zu Layered Policies finden Sie in › Kapitel 2.2.1.

PBP 2.7 – Informationen sollten anschaulich sein.

Nutzen Sie visuelle Ankerpunkte und Gliederungshilfen wie Icons, farbliche Abgrenzungen, Überschriften und Zwischenüberschriften. Visualisieren Sie komplexe Zusammenhänge und Abläufe durch Grafiken oder Diagramme.

PBP 2.8 – Informationen sollten nutzerzentriert aufbereitet werden.

Neben verständnisfördernder Aufbereitung notwendiger Informationen durch Strukturierungen und Visualisierungen sollten Sie beachten, welche Informationen für Nutzende relevant sind. Bereiten Sie Informationen beispielsweise über Nutzungsszenarien auf, wie in › Kapitel 3.5 beschrieben. Ergänzen Sie im Kontext Ihrer Anwendung relevante Informationen, zum Beispiel was mit den Daten nach dem Tod passiert oder den Zugang zu einer Zugriffshistorie. Formulierungen sollten auf Augenhöhe sein, sodass Nutzende sich nicht von juristischen oder technischen Texten überwältigt oder bevormundet fühlen. Mehr Informationen, zu Anforderungen aus Sicht der Nutzenden, finden Sie in › Kapitel 3.

PBP 2.9 – Informationen sollten barrierefrei sein.

Achten Sie auf Kontraste und beachten Sie Farbschwächen. Vermeiden Sie Informationen ausschließlich über Farbe zu kommunizieren, wie die Zustimmung und Abwahl über einen Rot-Grün-Switch (denn für Menschen mit einer Rot-Grün-Schwäche ist das nicht erkennbar). Ergänzen Sie in diesem Fall Text, um die Optionen deutlich zu machen. Ermöglichen Sie Text-to-Speech. Bieten Sie unterschiedliche sprachliche Varianten an, wie leichte Sprache und Fremdsprachen, die in Ihrem Nutzerkreis häufig vorkommen. Vermeiden Sie es, Informationen lediglich in einer langen und komplexen Datenschutzerklärung zur Verfügung zu stellen. Bieten Sie zusätzliche Hilfestellungen wie FAQs (vgl. › Kapitel 3.4) oder die Einbindung eines Chatbots (vgl. › Kapitel 2.2.2). Ermöglichen Sie Nutzenden Fragen zu stellen.

PBP 2.10 – Hilfestellungen sollten vorhanden sein.

Stellen Sie Hilfestellungen zur Verfügung wie FAQs, Chats und ähnliches. Beugen Sie so Unklarheiten vor und unterstützen Sie Nutzende beim Verständnis der Informationen durch unterschiedliche Medien und Aufbereitungen (vgl Kapitel › 3.4 und › 3.5). Darüber hinaus ist es wichtig, dass Ihre Kontaktdaten gut sichtbar sind, falls weitere Fragen auftreten sollten. Eine Einordnung eines KI-Chatbots als Datenschutz-Assistent finden Sie in › Kapitel 2.2.2.

PBP 2.11 – Informationen sollten multimodal sein.

Stellen Sie verschiedene Darstellungsformen zur Verfügung. Nutzen Sie neben Texten auch Videos, Grafiken, Tabellen, Diagramme, Audios oder ähnliches. Über Multimodalität können Sie Visualisierungen, Barrierefreiheit und Hilfestellungen kombinieren. Interaktionen wie beispielsweise eine schrittweise Einwilligung können eine bewusstere Auseinandersetzung fördern.

4.3 Einwilligung nachweisen

Der für die Verarbeitung Verantwortliche ist dafür zuständig, jederzeit die Einwilligung nachweisen zu können. Betroffene Personen müssen auf gleiche Weise in der Lage sein, ihre Einwilligung nachzuvollziehen.

PBP 3.1 – Informierte Einwilligung sollte nachvollziehbar sein.

Die Entscheidung, ob eingewilligt wurde oder nicht, sollte jederzeit einsehbar sein. Die Informationen, die während der Einwilligung zur Verfügung standen, sollten auch danach bei Bedarf einsehbar sein. Ebenso sollten die Einstellungen zeitlich einordbar sein. Zum Beispiel durch einen Zeitstempel wie *letzte Aktualisierung*.

PBP 3.2 – Informierte Einwilligung sollte nachweisbar sein.

Erstellen Sie für die Einwilligung einen Nachweis. In bestimmten Fällen kann es ebenso hilfreich sein, den Nachweis auch bei einer Ablehnung der Einwilligung zu erstellen. Protokollieren Sie neben der Einwilligung selbst auch die Informationen, wie die Einwilligung eingeholt wurde, welche Informationen wie bereitgestellt wurden und welche Daten durch die Einwilligung zu welchem Zweck verarbeitet werden können. Versionieren Sie unterschiedliche Informationstexte. Hinterlegen Sie auch die Gültigkeit, wann die Einwilligung gegeben und wann diese gegebenenfalls abgelaufen ist oder widerrufen wurde.

PBP 3.3 – Nachweise sollten transparent sein.

Ermöglichen Sie die Kommunikation des Nachweises und den Erhalt für Nutzende, zum Beispiel durch die Nutzung von *Consent Receipts* nach ISO/IEC TS 27560:2023 Bestätigen Sie den Nutzenden Änderungen wie die Erteilung oder den Widerruf einer Einwilligung. Informieren Sie Nutzende über Änderungen des Einwilligungsstatus, zum Beispiel bei Ablauf der Gültigkeit durch ein Zeitlimit.

PBP 3.4 – Einwilligung sollte vertraulich und fälschungssicher sein.

Auch die Entscheidung für oder gegen eine Einwilligung ist ein personenbezogenes Datum und sollte daher vertraulich behandelt werden. Ebenso wichtig ist, dass nachgewiesen werden kann, dass der Nachweis der Einwilligung der tatsächlichen Entscheidung der betroffenen Person entspricht und keiner Änderung durch Dritte unterliegen kann.

PBP 3.5 – Weitergabe von Daten sollten nachvollziehbar sein.

Protokollieren und dokumentieren Sie die Weitergabe von Daten an Dritte. Bei Änderungen der Einwilligung sowie bei Anträgen auf Berichtigung, Löschung oder Einschränkung müssen Sie in der Lage sein, Empfänger der Daten darüber zu informieren. Darüber hinaus müssen Sie in der Lage sein, auf Verlangen der betroffenen Person Auskunft über die Empfänger zu geben.

4.4 Einwilligung verwalten und bearbeiten

Während der gesamten Nutzungsdauer müssen Nutzende in der Lage sein, ihre Einwilligung zu verwalten und gegebenenfalls zu bearbeiten.

PBP 4.1 – Informierte Einwilligung sollte anpassbar sein.

Ermöglichen Sie während der gesamten Nutzung der Anwendung Einstellungsmöglichkeiten, um Einwilligungen zu widerrufen oder zu erteilen. Hierzu gehören auch Anpassungen von Bedingungen, an die die Einwilligung gegebenenfalls geknüpft ist, wie Zugriffsberechtigungen für bestimmte Personen, bestimmte Zeiträume oder Ablaufdaten und andere Einschränkungen.

PBP 4.2 – Einwilligung geben und widerrufen sollte gleichwertig sein.

Änderungen wie das Widerrufen einer Einwilligung müssen genauso einfach sein wie das Erteilen der Einwilligung. Bieten Sie konkrete Einstellungs- und Widerrufsmöglichkeiten. Implementieren Sie Funktionen, über die die Einwilligung widerrufen und personenbezogene Daten gelöscht werden können. Zudem sollten diese Funktionen für Nutzende einfach zu finden und zu bedienen sein.

PBP 4.3 – Informierte Einwilligung sollte aktuell gehalten werden.

Änderungen in Nutzerbedürfnissen oder Umständen können die Entscheidung zur Einwilligung verändern. Ermöglichen Sie daher Erinnerungen, um Datenschutzeinstellungen regelmäßig zu überdenken und an die aktuellen Gegebenheiten anpassen zu können.

PBP 4.4 – Informierte Einwilligung sollte auf Änderungen eingehen können.

Mit der Zeit können sich Verarbeitungsprozesse oder -zwecke sowie die rechtlichen Rahmenbedingungen ändern. Richten Sie daher die Möglichkeit ein, Nutzende über Änderungen zu informieren. Richten Sie Prozesse ein, um die Einwilligung gegebenenfalls erneut einzuholen.

4.5 Einwilligung sicherstellen

Wann immer personenbezogene Daten erfasst oder verarbeitet werden, deren Verarbeitung auf der Grundlage der Einwilligung beruht, muss sichergestellt sein, dass eine aktuelle Einwilligung vorliegt.

PBP 5.1 – Im Default sollten keine Daten erfasst werden.

Um zu verhindern, dass personenbezogene Daten vor der Informierung der betroffenen Person oder ohne Einwilligung erfasst und verarbeitet werden, sollte während des Starts einer Anwendung auf personenbezogene Daten vollkommen verzichtet werden. Tracking-Tools sind standardmäßig deaktiviert und müssen erst aktiv eingeschaltet werden. Laden Sie Inhalte, deren Zweck eine Einwilligung benötigt, erst wenn eine Einwilligung vorliegt.

PBP 5.2 – Einwilligung muss technisch durchgesetzt werden.

Überprüfen Sie vor jeder Datenerfassung und Datenverarbeitung die Rechtsgrundlage und, ob eine Einwilligung notwendig ist. Vor jeder Datenerfassung und -verarbeitung, für die eine Einwilligung notwendig ist, muss das System vorher prüfen, ob diese vorliegt. Systeme sollen die personenbezogenen Daten erst erfassen und speichern, wenn eine Einwilligung vorliegt. Sollte die Einwilligung widerrufen worden sein, muss sichergestellt werden, dass das System ab diesem Zeitpunkt keine weitere entsprechende Verarbeitung durchführen kann.

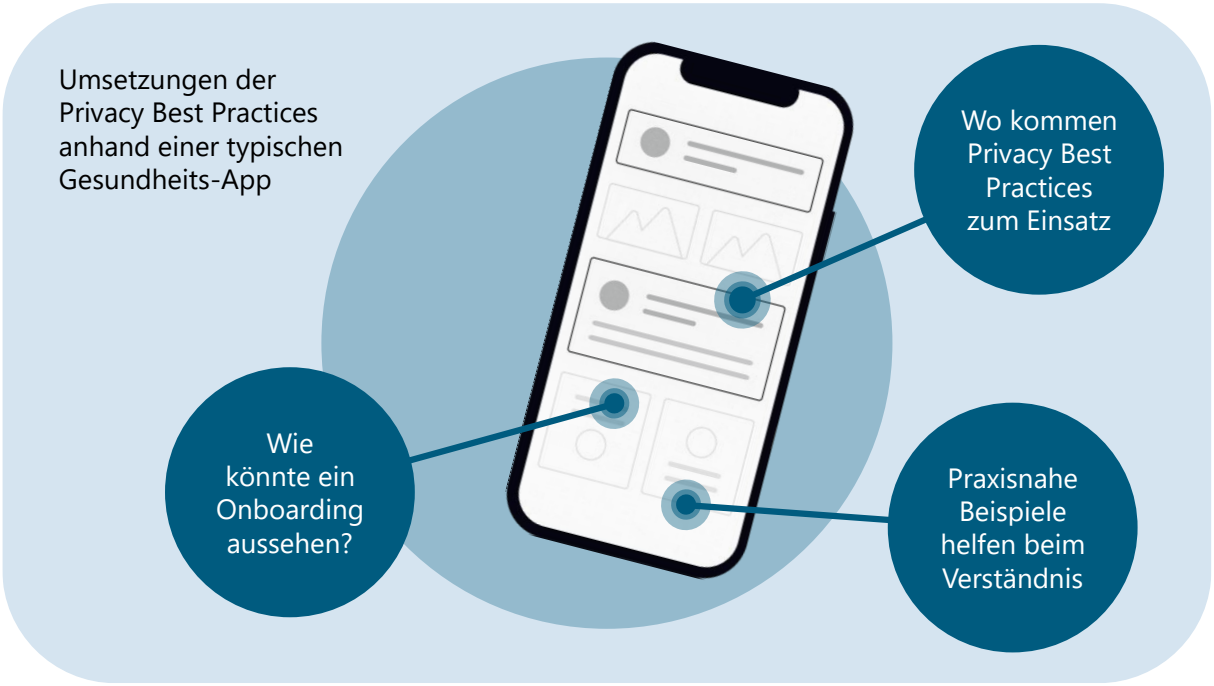
PBP 5.3 – Informierte Einwilligung sollte getestet werden.

Implementieren Sie automatische Tests. Testen Sie, dass die personenbezogenen Daten nur dann erfasst werden, wenn eine Einwilligung vorliegt. Testen Sie, dass die personenbezogenen Daten nicht mehr erfasst werden, wenn die Einwilligung entzogen wurde oder wenn Bedingungen, wie beispielsweise eine Zeitbeschränkung, abgelaufen sind. Testen Sie, dass vor jeder Verarbeitung der personenbezogenen Daten das Vorliegen einer gültigen Einwilligung überprüft und eine Verarbeitung beim Fehlen einer gültigen Einwilligung unterbunden wird.

PBP 5.4 – Weitergegebene Daten sollten an die Einwilligung gebunden sein.

Personenbezogene Daten auf der Grundlage einer Einwilligung sollten nur an solche Empfänger und für einen solchen Verarbeitungszweck weitergegeben werden können, wie er in der Einwilligung klar benannt wurde. Nutzen Sie beispielsweise zusätzlich *Sticky Policies*, bei denen Daten und Anforderungen an die Verarbeitung miteinander verknüpft werden. Dadurch stellen Sie sicher, dass Empfänger automatisch und nachvollziehbar wissen, unter welchen Bedingungen die Daten verarbeitet werden dürfen. Ist ein Auftragsverarbeiter Empfänger der Daten, muss sichergestellt sein, dass dieser klare Weisungen zum Umgang mit den Daten hat und die Einhaltung der Weisungen durch geeignete technische und organisatorische Maßnahmen überwacht wird.

5 Umsetzung und Demonstration einer nutzerzentrierten informierten Einwilligung



In diesem Kapitel sehen Sie, wie eine nutzerzentrierte informierte Einwilligung am Beispiel einer typischen Gesundheits-App aussehen kann und an welchen Stellen Privacy Best Practices zum Einsatz kommen. Sehen Sie sich die Umsetzung auch live im Demonstrator an unter prima-i.ostfalia.de[20]. Eine ausführlichere Erläuterung der Privacy Best Practices finden Sie in › Kapitel 4.

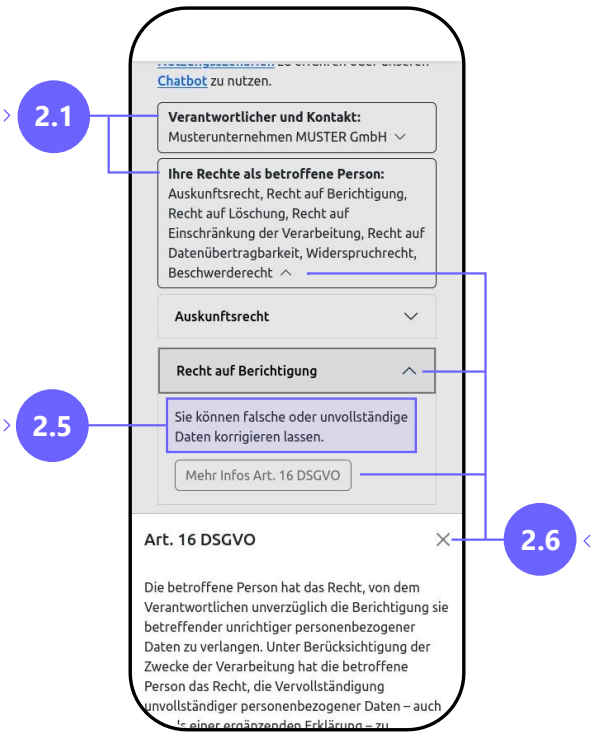
5.1 Vor der App-Nutzung – das Onboarding › Zum Demonstrator

Bevor personenbezogene Daten aufgenommen und verarbeitet werden, müssen die betroffenen Personen darüber informiert und gegebenenfalls eine Einwilligung eingeholt werden (› PBP 1.1). Ist die Anwendung nicht ohne die Verarbeitung personenbezogener Daten nutzbar, empfiehlt es sich, ein Onboarding anzulegen, bei dem Einwilligungen schrittweise eingeholt werden können (› PBP 1.3). Bei einer Gesundheits-App muss typischerweise zunächst ein Freischaltcode eingegeben und ein Profil erstellt werden. Das Onboarding kann nach dem Freischaltcode, sollte aber vor der Erstellung des Profils erfolgen.

Im ersten Schritt sollte Transparenz geschaffen werden (› PBP 1.4), siehe › Abbildung 4. Dazu wird dem Nutzenden kurz der Ablauf des Onboarding-Prozesses erklärt, sodass sich dieser darauf einstellen kann. Über einen Fortschrittsbalken können Nutzende nachvollziehen, wie viele Schritte der Prozess hat und an welcher Stelle sie sich gerade befinden, um vorschnelles Ablehnen oder uninformiertes Einwilligen zu vermeiden. In jedem Schritt sollten die vollständigen Informationen über die Datenschutzerklärung über einen Link einfach erreichbar sein (› PBP 2.2) sowie Hilfestellungen wie FAQs, Nutzungsszenarien oder ein Chatbot zur Verfügung stehen (› PBP 2.10).

Abbildung 4: Onboarding Start

Abbildung 5: Allgemeine Informationen



Zu allgemeinen Informationen, die unabhängig von Art und Zweck der Verarbeitungen aufzuzeigen sind, gehören vor allem, wer verantwortlich ist und welche Kontaktmöglichkeiten bestehen sowie die Aufklärung über die Rechte der betroffenen Person (› PBP 2.1), siehe › Abbildung 5. Die Informationen können gemäß der Layered Policies (› Kapitel 2.2.1) strukturiert werden. Sollten Nutzende genauere Informationen wünschen, können diese ausgeklappt werden (› PBP 2.6). Die einzelnen Rechte werden zunächst mit einfachen Worten kurz und prägnant beschrieben, wobei auf juristischen Wortlaut verzichtet wurde (› PBP 2.5), die genauen Gesetztestexte stehen in tieferen Ebenen zur Verfügung.

In den nächsten Schritten des Onboardings werden die Nutzenden für jeden trennbaren Zweck über die Verarbeitung der personenbezogenen Daten informiert und separat eine Einwilligung eingeholt (› PBP 1.2). Jeder Zweck stellt einen abgegrenzten Schritt dar (› PBP 1.3). Die Informationen sind über Icons, Überschriften und farbliche Abgrenzungen anschaulich aufbereitet (› PBP 2.7), siehe › Abbildung 6. Dabei wurde darauf geachtet, dass Informationen barrierefrei sind und nicht ausschließlich über Farbe kommuniziert wird (› PBP 2.9). Die Informationen sind in vier Bereiche geteilt: Den Zweck der Verarbeitung, die dafür verarbeiteten Daten, die Empfänger sowie die Rechtsgrundlage (› PBP 2.1, › PBP 2.8, › PBP 1.11).

Informationen für Zwecke, die eine Einwilligung erfordern, wurden durch einen Abschnitt *Konsequenzen Ihrer Entscheidung* ergänzt (› Abbildung 7). Über diesen Abschnitt können den Nutzenden die Konsequenzen bzw. Chancen und Risiken ihrer jeweiligen Entscheidung nähergebracht werden, um für eine Entscheidung alle notwendigen Informationen nutzerzentriert zur Verfügung zu haben (› PBP 2.1, › PBP 2.8). Dies beinhaltet zum Beispiel, welche Funktionen bei Ablehnung nicht genutzt werden können, aber auch was im Falle eines Datenschutzvorfalls auf welche Weisen passieren kann.

Abbildung 6: Erforderliche Datenverarbeitung

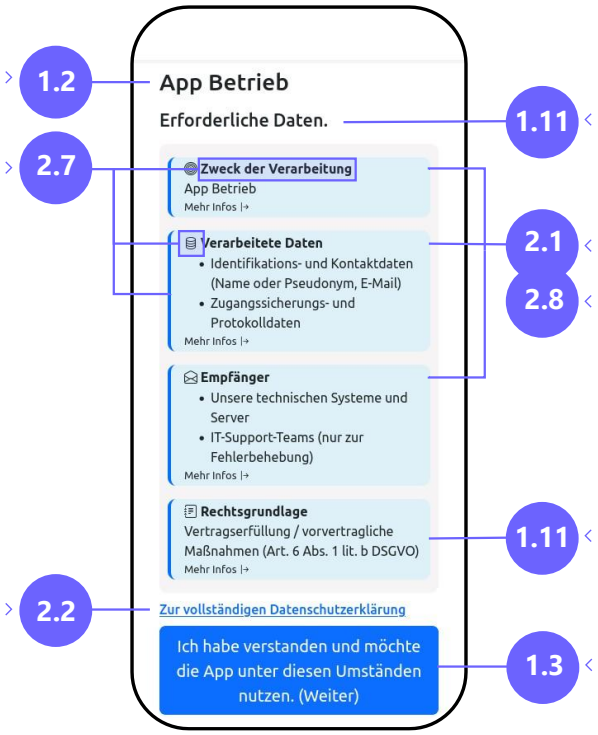
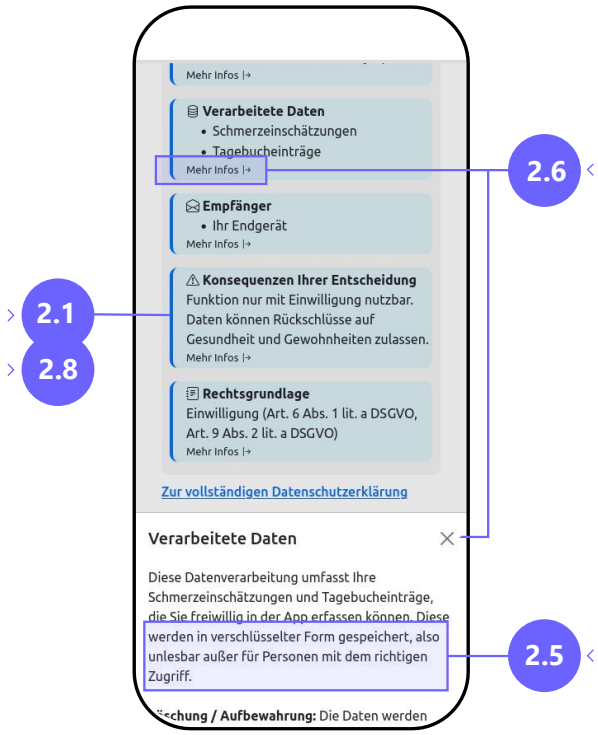


Abbildung 7: Optionale Datenverarbeitung



Weiterhin sind die Informationen gemäß dem Prinzip der Layered Policies strukturiert (› PBP 2.6). Auf der ersten Ebene sind die wichtigsten Informationen kurz festgehalten. Weiterführende Informationen sind in tieferen Ebenen einsehbar. In den Texten wird technischer und juristischer Wortlaut vermieden und gegebenenfalls erklärt, sodass diese verständlich bleiben (› PBP 2.5). Die visuellen Anker und Strukturen werden über die verschiedenen Zwecke beibehalten, sodass sich Nutzende nicht neu orientieren müssen (› PBP 2.6, › PBP 2.7). Der Zugang zur vollständigen Datenschutzerklärung ist, wie eingangs beschrieben, über einen klaren Link jederzeit möglich (› PBP 2.2). Neben den vollständigen Informationen können die Nutzenden durch weitere Hilfestellungen wie FAQs oder einen KI-Chatbot jederzeit unterstützt werden (› PBP 2.10). Ebenso wird ein Perspektivwechsel über Nutzungsszenarien angeboten, um verschiedene Modalitäten der Informationsaufnahme zu ermöglichen (› PBP 2.8, › PBP 2.11), siehe › Abbildung 8.

Abbildung 8: Einwilligung

Zunächst erfolgen alle Schritte, in denen Nutzende über Verarbeitungsprozesse von personenbezogenen Daten informiert werden, die auf einer anderen Rechtsgrundlage als der Einwilligung beruhen und daher für die Nutzung der App erforderlich sind (› PBP 1.11). Dies wird über einen Button bestätigt mit der Aufschrift *„Ich habe verstanden und möchte die App unter diesen Umständen*

nutzen" (› Abbildung 6). Anschließend folgen die Zwecke, für die eine Einwilligung erforderlich ist. Diese werden explizit als „Optional" gekennzeichnet (› PBP 1.6) (› Abbildung 9).

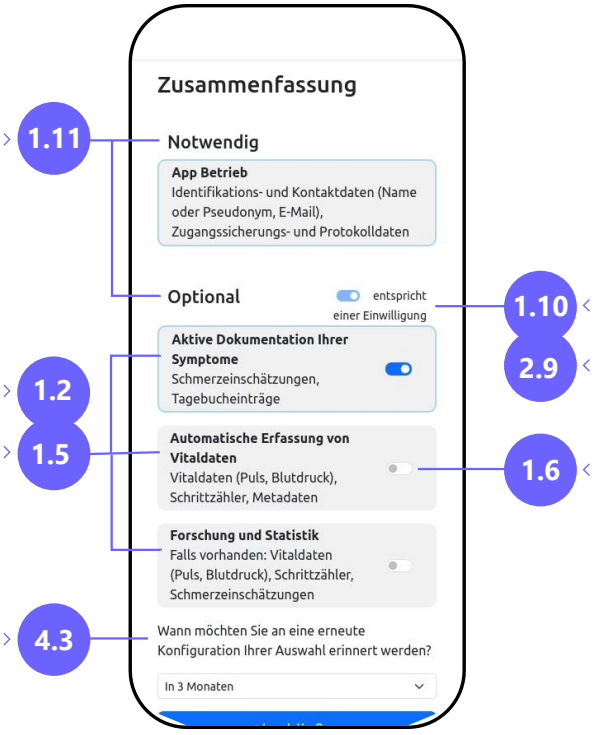
Anstelle einer Kenntnisnahme stehen Nutzenden zwei Buttons zur Verfügung: *„Ich willige ein*" und *„Ich willige nicht ein*" (› Abbildung 8). Nutzende müssen sich aktiv (› PBP 1.7) für einen Button entscheiden und es ist keine der Optionen vorausgewählt (› PBP 1.8). Ebenso sind die Buttons gleichwertig dargestellt und die Ablehnung einer Einwilligung ist auf derselben Höhe ohne Zwischenschritte möglich (› PBP 1.9). Die klare Beschriftung verdeutlicht eindeutig, welcher Button welcher Einwilligungsentscheidung entspricht (› PBP 1.10). Eine Ablehnung verhindert nicht die App-Nutzung, sondern schließt lediglich die spezifische Funktion aus, sodass die Einwilligung optional bleibt (› PBP 1.6).

Für die Verarbeitung von Daten für Forschungs- und Statistikzwecke wurde eine umfassendere Einwilligung umgesetzt, da die konkreten Zwecke nicht vorher absehbar sind. Um dennoch auf die individuellen Bedürfnisse der Nutzenden eingehen zu können, ist diese Einwilligung an eine zeitliche Bedingung geknüpft (› PBP 1.5). Nutzende können auswählen, ob ihre Daten unbegrenzt oder nur für fünf/drei Jahre genutzt werden dürfen, bevor eine erneute Einwilligung eingeholt werden muss (› Abbildung 9).

Am Ende des Onboarding-Prozesses erfolgt eine Zusammenfassung (› Abbildung 10). In dieser werden Verarbeitungen, die auf der Einwilligung beruhen und damit optional sind, klar von anderen Zwecken getrennt (› PBP 1.6, › PBP 1.11). Auf diese Weise kann die Einwilligung nochmals individuell an die Bedürfnisse der betroffenen Person angepasst werden (› PBP 1.5). Mit Hilfe eines Hinweises wird verdeutlicht, welche Stellung des Switches einer Einwilligung entspricht, sodass diese eindeutig (› PBP 1.10) und barrierefrei (› PBP 2.9) erfolgt. Um die Einwilligung aktuell zu halten und bei längerer Anwendung der App auf sich ändernde Umstände einzugehen, können Nutzende auswählen, wann Sie an eine erneute Konfiguration erinnert werden möchten (› PBP 4.3).

Abbildung 9: Weitere Einwilligungen

Abbildung 10: Zusammenfassung



5.2 Während der App-Nutzung

Die informierte Einwilligung ist ein Aspekt, der sich in vielen Teilen der Anwendung und während der gesamten Nutzungszeit widerspiegelt. Im Demonstrator gibt es beispielhaft eine Stelle, an der personenbezogene Daten eingetragen und auf Basis der Einwilligung erfasst werden, im Bereich Eintrag, und zwei Stellen, an denen diese angezeigt und verarbeitet werden, im Bereich Verlauf. In allen drei Fällen prüft das System, ob eine Einwilligung vorliegt (› PBP 5.2). In › Abbildung 11 liegt für die Verarbeitung von Schmerzwerten eine Einwilligung vor, für die automatische Erfassung des Blutdrucks aber nicht. An relevanten Stellen wie dieser wird direkt auf den Datenschutz verlinkt, damit Informationen leicht erreichbar bleiben (› PBP 2.4). Zusätzlich wird anstelle der Verarbeitung der Blutdruckwerte, ein Hinweis auf die Einstellungen angezeigt, sodass Nutzende auch nachträglich jederzeit ihre Einwilligungsentscheidung anpassen können (› PBP 4.1).

Zu Informationen zum Datenschutz sowie Datenschutzeinstellungen gelangen Nutzende auch über das Profil, ein Bereich, in dem typischerweise organisatorische Funktionen vorgesehen sind. Im Profil ist für den Datenschutz ein Reiter auf der obersten Ebene der Einstellungen angelegt (› PBP 2.3) (› Abbildung 12). Unter diesem sind alle Informationen und Hilfestellungen, die während des Onboardings zur Verfügung gestellt wurden, jederzeit aufrufbar (› PBP 2.2, › PBP 3.1). Zu den Hilfestellungen zählen FAQs (› Abbildung 14 und weitere Informationen in › Kapitel 3.4), die Aufbereitung der Datenschutzinformationen über Nutzungsszenarien (› Abbildung 15, › Kapitel 3.5) und ein KI-Chatbot, über den Fragen zu den Datenschutzinformationen gestellt werden können (› Kapitel 2.2.2).

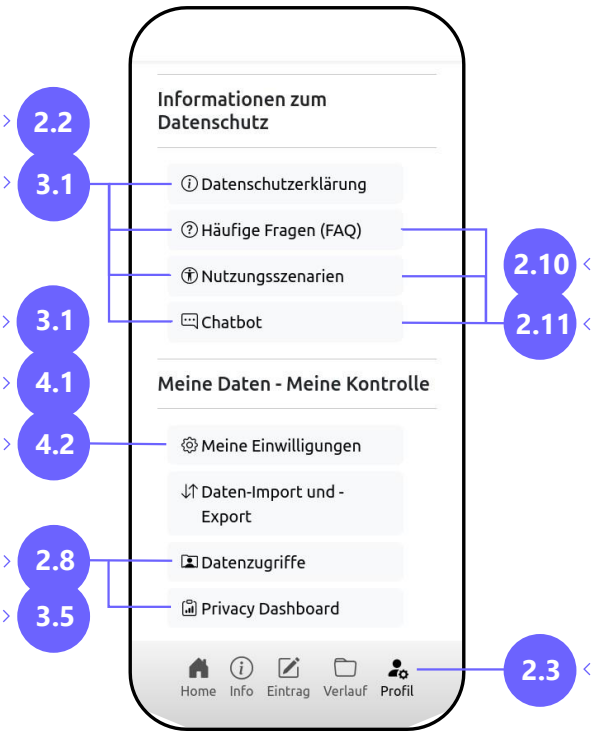
Im unteren Bereich stehen Nutzenden alle Funktionen zum Datenschutz zur Verfügung, die ihre eigenen Daten betreffen. Getätigte Einwilligungsentscheidungen können unter *Meine Einwilligungen* eingesehen (› PBP 3.1) und angepasst (› PBP 4.1) werden. Die einzelnen Zwecke sind wie in der Zusammenfassung des Onboardings übersichtlich dargestellt und Informationen auf Bedarf

Abbildung 11: Datenverarbeitung in der App

› Zum Demonstrator

Abbildung 12: Datenschutzeinstellungen

› Zum Demonstrator



aufklappbar (› Abbildung 13). Das Geben und Widerrufen der Einwilligung ist dabei wertfrei und beides über das Betätigen des jeweiligen Switches möglich (› PBP 4.2). Ein Hinweis *Letzte Aktualisierung* ermöglicht die zeitliche Einordnung (› PBP 3.1).

Zudem kann über ein Privacy Dashboard die Erfassung und Verarbeitung der Daten transparent sowie durch eine Auflistung der Datenzugriffe die Weitergabe von Daten nachvollziehbar (› PBP 3.5, › PBP 2.8) gemacht werden. In diesen Bereich fallen auch weitere Funktionen wie beispielsweise die Möglichkeit Daten zu exportieren oder zu importieren.

Abschließend ist zu beachten, dass die informierte Einwilligung nicht nur Aspekte beinhaltet, die in einer Beispielanwendung sichtbar gemacht werden können. Neben verständlichen Informationen, nutzerfreundlicher Aufbereitung, Anforderungen an Transparenz und Anpassbarkeit, ist auch im Hintergrund einiges zu beachten. Besonders wichtig ist, dass im Default zunächst keine personenbezogenen Daten erfasst werden (› PBP 5.1). Die Einwilligung darf nicht nur aufgesetzt sein, sondern muss technisch durchgesetzt werden (› PBP 5.2). Ebenso ist die Einwilligung wie jedes andere Feature zu testen (› PBP 5.3). Nutzen Sie Sticky Policies um weitergegebene Daten an die Einwilligung zu binden (› PBP 5.4). Stellen Sie sicher, dass Sie auf Änderungen in Verarbeitungsprozessen und rechtlichen Rahmenbedingen reagieren können (› PBP 4.4). Behalten Sie ebenso die Nachweisbarkeit im Auge und machen Sie sich hierzu zum Beispiel Consent Receipts zu Nutze (› PBP 3.3).

Abbildung 13: Zustimmungsverwaltung

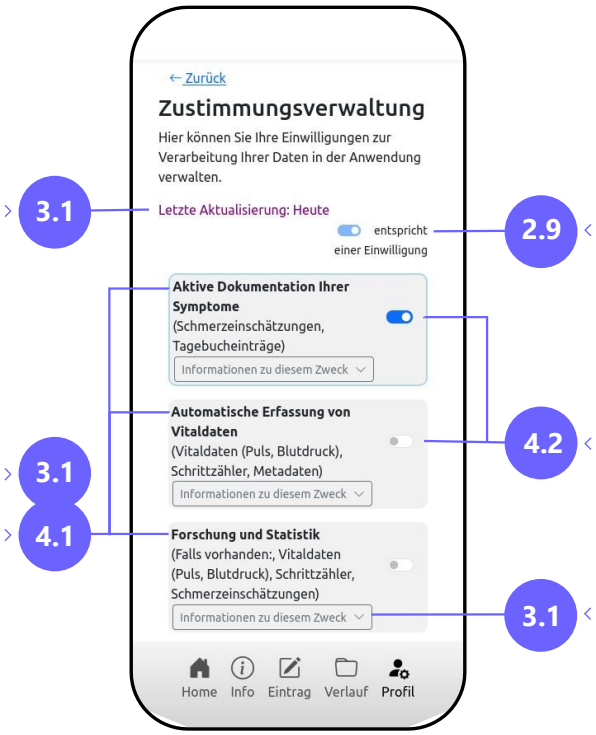


Abbildung 14: FAQ › Zum Demonstrator

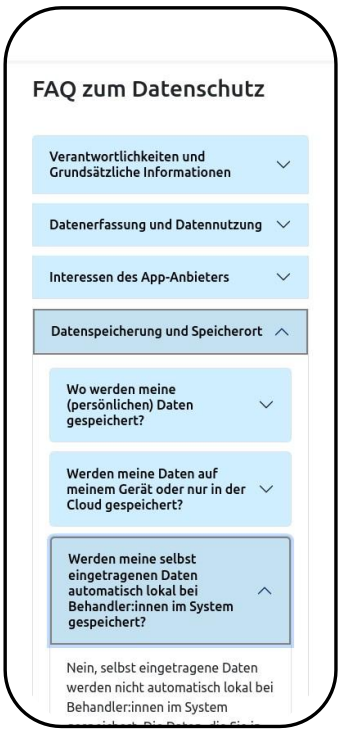


Abbildung 15: Nutzungsszenarien › Zum Demonstrator

Ich möchte...	Welche Daten werden verarbeitet?	Wer greift auf die Daten zu?	Wofür werden die Daten verarbeitet?	Woher stamme die Daten?
... meine Laborwerte eintragen, einsehen oder ändern.	Von Ihnen selbst eingetragene Laborwerte und Ihr Geschlecht aus den Stammdaten	Auf die eingetragenen Laborwerte: Sie selbst. Auf das Geschlecht aus den Stammdaten: IBM Deutschland GmbH.	Damit Sie Ihre Laborwerte jederzeit einsehen und bei Bedarf mit Leistungserbringenden teilen können. Ihr Geschlecht wird für Referenzwerte benötigt.	Sie selbst trage die Daten ein, b aus den Stammdaten Ihr ePA (Info zum Geschlecht).
.. Übungen für	Von Ihnen gewählte	Nur Sie selbst haben	Damit Sie Ihren	Sie wählen die

Anhang

Zentrale Fragen je Themenbereich der FAQs

Themenbereich	Zentrale Fragen
Verantwort-lichkeiten und grundsätzliche Informationen	Wer betreibt die Gesundheits-App und wer ist für den Datenschutz verantwortlich?
	Wie werde ich über Änderungen der Datenschutzrichtlinie informiert?
	Wo ist die Langfassung der Datenschutzerklärung erhältlich?
	An wen kann ich mich wenden, wenn ich Fragen oder Kritik zur App habe?
	An wen kann ich mich wenden, wenn ich Fragen zu der Verarbeitung meiner Daten habe oder ein Verstoß in der Verarbeitung meiner Daten feststelle?
Datenerfassung und Datennutzung	Welche Daten werden von mir erhoben? Welche Daten werden aus den Gesprächen (bspw. über Video oder Chat) erhoben bzw. erfasst?
	Wofür bzw. für welche Analysen werden meine Daten genutzt? Warum werden diese Daten genutzt?
Interessen des App-Bieters	Wofür kann das App-Unternehmen meine Daten über die App-Funktion hinaus nutzen?
	Wie finanziert sich die App?
Daten--speicherung und Speicherort	Wo werden meine (persönlichen) Daten gespeichert?
	Werden meine Daten auf meinem Gerät oder nur in der Cloud gespeichert?
	Werden meine selbst eingetragenen Daten automatisch lokal bei Behandler:innen im System gespeichert?
	Werden Videogespräche mit Behandler:innen (automatisch) gespeichert? Werden die Gesprächsdateien von anderen Kommunikationskanälen (z. B. Chats) gespeichert?
Zugriffsrechte	Wer kann auf meine Daten zugreifen, die ich innerhalb der App dokumentiere?
	Wer entscheidet, wer meine Daten (ein)sehen darf?
	Was sehe ich selbst, was sehen Behandler:innen, Betreuer:innnen oder Angehörige sowie Krankenkassen und Arbeitgeber:innen?
	Können Behandler:innen, Betreuer:innen oder Angehörige Daten ändern – oder nur einsehen?
	Werde ich benachrichtigt, wenn ein/e Behandler:in oder Einrichtung unerwartet auf meine Daten zugreift oder diese ändert?
	Wie kann ich einer Person den Zugang zu meinen Daten in der App wieder entziehen?
	Was passiert mit meinen Daten, wenn ich die/den Behandler:in oder die Betreuungseinrichtung wechsle?
	Mit welchen Partnern/Unbeteiligten arbeitet der App-Anbieter zusammen? Warum haben auch diese Zugriff auf bestimmte Daten von mir?
	Muss ich meiner Krankenkasse Zugriff auf meine Daten gewähren, zum Beispiel damit diese bestimmte Kosten erstattet? Auf welche Daten hat meine Krankenkasse Zugriff und warum?

Themenbereich	Zentrale Fragen
	Warum benötigt die App den Zugriff auf meine Kontaktdaten, Kamera und Standort?
Datensicherheit	Was passiert beim Einloggen mit meinen Daten – ist das sicher?
	Warum muss ich meine Log-In Daten regelmäßig erneuern?
	Wie werden meine Daten vor dem Zugriff unberechtigter Personen oder Einrichtungen bzw. vor Datenpannen geschützt?
	Was muss ich tun, wenn ich denke, dass meine Daten missbraucht oder von unberechtigten Personen abgerufen wurden?
	Was kann ich selbst tun, um Datenpannen zu verhindern?
Dauer der Daten-speicherung	Wie lange werden meine Daten gespeichert?
	Was passiert mit meinen Daten, wenn ich die App über einen längeren Zeitraum nicht nutze?
	Was passiert mit meinen Daten, wenn ich versterbe?
Richtigkeit der Daten	Wie kann ich meine Daten einsehen oder ändern (lassen)
Löschen der Daten	Wie lösche ich meine Daten beim App-Anbieter?
	Welche meiner Daten können gelöscht werden?
	Wie kann ich meine Daten in der App löschen?
	Was passiert mit meinen Daten, wenn ich die App deinstalliere?
	Was passiert, wenn ich mein Gerät verliere?
Betroffenen-rechte	Wie kann ich mein Recht auf **Auskunft** geltend machen?
	Wie kann ich mein Recht auf **Berichtigung** geltend machen?
	Wie kann ich mein Recht auf **Löschung** geltend machen?
	Wie kann ich mein Recht auf **Einschränkung** geltend machen?
	Wie kann ich mein Recht auf **Datenübertragbarkeit** geltend machen?
	Wie kann ich mein Recht auf **Widerruf einer Einwilligung** geltend machen?
	Wie kann ich mein Recht auf **Widerspruch** geltend machen?
	Wie kann ich mein Recht auf **Automatische Verarbeitung** geltend machen?
	Wie kann ich mein Recht auf **Beschwerde bei einer Aufsichtsbehörde** geltend machen?

Anmerkungen

Kapitel 1 – Einleitung

[1] Siehe die Projekt-Webseite: https://prima-projekt.de/
[2] Schmidt, Ramona; Schiering, Ina; Zwingelberg, Harald; Friedewald, Michael (2025). "Challenges and Solutions in Implementing Informed Consent in Digital Environments: A Scoping Review". In: *IEEE Access* 13, S. 71965–71983. https://doi.org/10.1109/ACCESS.2025.3562773
[3] Diarra, Angelika (2025). *Rechtliche Analyse der datenschutzrechtlichen Ausgestaltung von Gesundheits-Apps*. PRIMA-Arbeitspapier. Frankfurt und Karlsruhe.
[4] Schneider, Diana; Koch, Jana; Schlüfter, Claudia; Zwingelberg, Harald; Friedewald, Michael; Heyen, Nils B. (2026): Einwilligen, aber informiert: Die Perspektive von Patient:innen auf die informierte Einwilligung bei der Nutzung von Gesundheits-Apps. In: Friedewald, M., Roßnagel, A., Karaboga, M., Geminn, C. (eds.) Datenschutz und Digitalpolitik in krisenhaften Zeiten.

Kapitel 2 – Rechtliche Rahmenbedingungen

[5] Artikel 29-Gruppe, "Leitlinien für Transparenz gemäß der Verordnung 2016/679", 2018, Leitlinien für Transparenz gemäß der Verordnung 2016/679
[6] Europäischer Datenschutzausschuss, "Opinion 28/2024 on certain data protection aspects related to the processing of personal data in the context of AI models", 2024, https://www.edpb.europa.eu/documents/opinion-of-the-board-art-64/opinion-282024-on-certain-data-protection-aspects-related-to_en
[7] Europäischer Datenschutzausschuss, "Guidelines 05/2020 on consent under Regulation 2016/679", 2020, https://www.edpb.europa.eu/documents/guideline/guidelines-052020-on-consent-under-regulation-2016679_en
[8] Datenschutzkonferenz, Entschließung der 91. Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder - Wearables und Gesundheits-Apps – Sensible Gesundheitsdaten effektiv schützen!",2016, https://www.bfdi.bund.de/SharedDocs/Downloads/DE/DSK/DSKEntschliessungen/91DSK_EntschliessungWearables.html
[9] Diese Handreichung stellt wesentliche Aspekte einer informierten Einwilligung möglichst knapp und eingängig dar, um als Grundlage für Entwickler:innen zu dienen. Einzelfälle können immer Besonderheiten aufweisen, die eine differenzierte rechtliche Betrachtung erfordern. Diese Informationen in dieser Handreichung ersetzten daher nicht den Dialog mit der/Dem Datenschutzbeauftragten, sollen aber befähigen die wesentlichen Fragen stellen zu können.
[10] Art.9 Abs.2 lit. h in Verbindung mit Art. 6 Abs. 1 lit b DSGVO
[11] EuGH, Urt. v. 01.10.2019 – C-673/17, Planet49, Rn. 92
[12] BGH, Urteil v. 28.05.2020 – I ZR 7/16, Rn. 60 https://openjur.de/u/2241381.html
[13] Europäischer Datenschutzausschuss, Leitlinien 05/2020 zur Einwilligung gemäß Verordnung 2016/679, Version 1.1., https://www.edpb.europa.eu/documents/guideline/guidelines-052020-on-consent-under-regulation-2016679_de
[14] Datenschutzkonferenz, "Beschluss der 97. Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder zu Auslegung des Begriffs „bestimmte Bereiche wissenschaftlicher Forschung" im Erwägungsgrund 33 der DS-GVO 3. April 2019", 2019
[15] Thilo Weichert, Datenschutzrechtliche Rahmenbedingungen medizinischer Forschung, 2022, S. 97 ff.
[16] Der von einer Praxis für Schönheitsbehandlungen betriebenen KI wies die Ärzte, auch auf Rückfrage, fälschlich als Fachärzte aus. OLG Hamm, Urteil vom 12.05.2026 – AZ: 4 UKl 3/25. Noch nicht rechtskräftig.

Kapitel 3 – Anforderungen aus Sicht der Nutzenden

[17] Die hier dargestellten Erkenntnisse basieren auf leitfadengestützten Gruppen- und Einzelinterviews mit 20 Patient:innen zu vier verschiedenen Anwendungsszenarien von Gesundheits-Apps (Pflege,

chronische Erkrankungen, psychische Gesundheit sowie elektronische Patientenakte; vgl. Schneider et al. 2026) sowie auf drei Online-Workshops mit Patient:innen und App-Nutzenden zur Erprobung der entwickelten Formate und Tools.

[18] Finden Sie eine beispielhafte Umsetzung der FAQs im Demonstrator direkt unter: https://prima-i.ostfalia.de/profil/privacy/faq

[19] Finden Sie eine beispielhafte Umsetzung der Nutzungsszenarien im Demonstrator direkt unter: https://prima-i.ostfalia.de/profil/privacy/scenarios

Kapitel 5 – Umsetzung und Demonstration

[20] Finden Sie das Projekt auch unter: https://codeberg.org/R-Adair/PRIMA_Demonstrator.git

Plattform Privatheit

Gefördert durch:

Bundesministerium
für Forschung, Technologie
und Raumfahrt

BETEILIGTE INSTITUTIONEN

Ostfalia
Hochschule für angewandte
Wissenschaften

Fraunhofer
ISI

ULD
Unabhängiges Landeszentrum für
Datenschutz Schleswig-Holstein

Kanzlei für Gesundheitsrecht
PROF. SCHLEGEL, HOHMANN, DIARRA & PARTNER

ITeG
Wissenschaftliches
Zentrum für
Informationstechnik-
Gestaltung

UNIKASSEL
VERSITÄT