

**ABSCHLUSSPUBLIKATION**

# WEARABLES UND INDIVIDUELLE DIGITALE SOVERÄNITÄT

MAI 2020 — APRIL 2023

**ABSCHLUSSPUBLIKATION**

# WEARABLES UND INDIVIDUELLE DIGITALE SOUVERÄNITÄT

MAI 2020 BIS APRIL 2023









- 7** DIE BEDEUTUNG  
MENSCHENZENTRIERTER  
TECHNIKEENTWICKLUNG  
FÜR DIGITALE SOUVERÄNITÄT
- 11** NUTZER\*INNENZENTRIERTE  
TECHNOLOGIEN FÜR MEHR  
TRANSPARENZ UND  
KONTROLLE IM DATENSCHUTZ
- 14** NUTZUNGSBEISPIELE  
DER PLATTFORM
- 20** PLATTFORMENTWICKLUNG –  
VOM MODELL ZUM TOOL
- 23** ETHISCHE BEWERTUNG  
DER AUSWIRKUNGEN  
VON WEARABLES AUF  
DIE AUTONOMIE DER  
NUTZER\*INNEN
- 30** SICHERE UND  
DATENSCHUTZFREUNDLICHE  
UMSETZUNG DER PLATTFORM
- 33** DER WERT VON  
TRANSPARENTEM  
DATENSCHUTZ



# EDITORIAL

ELISABETH SCHAUERMANN, GESELLSCHAFT FÜR INFORMATIK E.V.

Tragbare Gesundheitstechnologien, so genannte Wearables, finden immer mehr Verbreitung. Sowohl bei Freizeitsportler\*innen, die ihre Fitness und Lebensführung darüber nachvollziehen und quantifizieren möchten, als auch in der medizinischen Versorgung und Prävention, in der Altenpflege und in Industriebetrieben kommen sie zum Einsatz.

Mit einer Vielzahl an Sensoren erfassen diese Geräte sensible Gesundheitsdaten direkt am Körper sowie Standort- und Bewegungsdaten. Aus der Analyse und Verknüpfung dieser Informationen können je nach Einsatzbereich wertvolle Erkenntnisse gezogen werden. Jedoch ist es durch die Art der verarbeiteten, mitunter sehr intimen Daten und durch die Implikationen für die Privatsphäre besonders wichtig, dass Nutzenden Informationen niedrigschwellig angeboten und leicht verständlich aufbereitet werden.

Textbasierte Datenschutzerklärungen sind dabei aber für die meisten Menschen keine geeignete Auskunftswahl – zu

lang, in komplizierter Fachsprache verfasst und schwer auffindbar. Hersteller und datenverarbeitende Stakeholder verlassen sich aktuell dennoch hauptsächlich auf diese sperrige Form der Informationsdarbietung. Die in der Datenschutzgrundverordnung (DSGVO) festgelegten Rechte und Pflichten der Betroffenen und der Datenverarbeiter bleiben ebenfalls oft unklar.

Doch wie kann reflektierte Entscheidungsfindung, und damit individuelle digitale Souveränität im Hinblick auf die eigene Nutzung von Wearables und die eigenen Daten gelingen? Welche Alternativen und Innovationen sind denkbar und notwendig? Lassen sich diese auf andere Anwendungsbereiche übertragen?

Einblicke und Erkenntnisse dazu aus der dreijährigen Arbeit des Konsortiums InviDas sind in den folgenden Beiträgen verfasst.

## ÜBER DAS PROJEKT

Das Projektkronym InviDas steht für „Interaktive, visuelle Datenräume zur souveränen, datenschutzrechtlichen Entscheidungsfindung“. Genau diese zu erforschen, hat sich das Konsortium ab Mai 2020 zur Aufgabe gemacht. Über drei Projektjahre konnte mit Förderung des Bundesministeriums für Bildung und Forschung im Programm „Mensch-Technik-Interaktion für digitale Souveränität“ multiperspektivisch erarbeitet werden, welche Herausforderungen Nutzer\*innen haben, um Datenströme und Datenschutzinformationen bei Wearables zu verstehen. Daran anknüpfend stand die Frage im Fokus, wie interaktive Visualisierungen dazu beitragen können, informierte und reflektierte Entscheidungen zu unterstützen.

Der transdisziplinäre Forschungsverbund, bestehend aus Gesellschaft für Informatik, Stiftung Digitale Chancen, Garmin Würzburg GmbH, RWTH Aachen, Universität Bremen und Otto-Friedrich-Universität Bamberg, erforschte und entwickelte Ansätze und Lösungen, die den Nutzer\*innen von Wearables einen besseren Einblick in die Datenschutzimplikationen und Datenflüsse ermöglichen. Gemeinsam wurden alle Projektergebnisse, insbesondere die technischen Lösungen, iterativ und partnerübergreifend erarbeitet.

## ÜBER DAS KONSORTIUM

Die **Gesellschaft für Informatik** leitete den Forschungsverbund und setzte Maßnahmen zur Verbreitung der Projektergebnisse um, zum Beispiel über Veranstaltungen, Publikationen und im Austausch mit Wissenschaft, Wirtschaft und Zivilgesellschaft.

Die **Stiftung Digitale Chancen** brachte ihre Expertise und Netzwerke zu digitaler Teilhabe ein, vor allem im Hinblick auf die Einbindung auch unterrepräsentierter und weniger digital affiner Nutzer\*innen im Gestaltungsprozess.

Für das **Institut für Arbeitswissenschaft der RWTH Aachen** stand die nutzer\*innenzentrierte Forschung im Vordergrund und mündete in empirisch validierten Gestaltungsempfehlungen für transparente Mensch-Technik-Interaktion und den Umgang mit interaktiven Visualisierungen. Gemeinsamer Beitrag des Instituts für Arbeitswissenschaft und der Stiftung digitale Chancen. → ab Seite 7

Die Arbeitsgruppe Mensch-Technik-Interaktion der **Universität Bremen** beschäftigte sich mit Forschungsfragen zu interaktiven Visualisierungen von Datenschutzinformationen und einer menschenzentrierten Gestaltung der technischen Lösungen. → ab Seite 11

Der **Lehrstuhl für Software Engineering der RWTH Aachen** entwickelte und gestaltete anhand modellbasierter Softwareentwicklung die im Projekt entstandene Plattform datenschutzlotsin.de und ein Escape Game, das Nutzende zur Reflexion über Datenschutz anregt. → ab Seite 20

Das **Institut für Angewandte Ethik der RWTH Aachen** untersuchte die ethischen Implikationen von Wearables und deren Nutzung. Außerdem fokussierten sie sich auf die konzeptuelle und normative Klärung verschiedener Autonomie-Konzepte → ab Seite 23

Der **Lehrstuhl Privatsphäre und Sicherheit in Informationssystemen der Universität Bamberg** erforschte und analysierte Sicherheitsrisiken und Möglichkeiten für eine technik-unterstützte Erhebung von Diskrepanzen zwischen Datenschutzerklärung und der tatsächlichen technischen Umsetzung. → ab Seite 30

**Garmin Würzburg** stellte als Praxispartner den Bezug zur Herstellerperspektive her und beriet zu Fragen der wirtschaftlichen Verwertbarkeit und Nutzbarkeit. → ab Seite 33



# DIE BEDEUTUNG MENSCHZENT- RIERTER TECHNIK- ENTWICKLUNG FÜR DIGITALE SOUVERÄNITÄT

CLEMENS GRUBER, JUTTA CROLL, STIFTUNG DIGITALE CHANCEN  
MATTHIAS AREND, SEBASTIAN PÜTZ, VERENA NITSCH, RWTH AACHEN

Der Schutz der eigenen Privatsphäre ist vielen Menschen wichtig – auch im Internet. Dennoch teilen sie ihre privaten Daten in sozialen Netzwerken, beim Online-Shopping oder auf anderen Webseiten, häufig sogar mit Personen außerhalb des eigenen Freundes- oder Bekanntenkreises. Dieses Phänomen wird als Privatsphäre-Paradoxon (engl. Privacy Paradox) beschrieben.<sup>1</sup> Das Spannungsfeld zwischen dem Wunsch, die eigene Privatsphäre zu wahren, und dem Teilen kritischer persönlicher Daten, um digitale Plattformen oder Dienstleistungen in Anspruch zu nehmen, wird besonders bei der Nutzung von Smart Wearables deutlich. Diese Geräte sammeln zahlreiche persönliche Informationen und Daten, die sich oft auf sensible Bereiche wie die Gesundheit beziehen.

Die Ergebnisse aus einer im Projekt durchgeführten Umfrage mit insgesamt 204 Personen legen jedoch nahe, dass das Privatsphäre-Paradoxon auch die Nutzerinnen und Nutzer von Smart-Wearables betrifft: Während 75 Prozent der Personen, die zum Zeitpunkt der Studie einen Fitnesstracker nutzten, angaben, dass Datenschutzaspekte oft oder immer ihre Entscheidung zur Nutzung eines digitalen Produkts oder einer digitalen Dienstleistung beeinflussen, gaben nur 34 Prozent dieser Gruppe an, Datenschutzerklärungen oft oder immer zu lesen. Die Angaben der weiteren Teilnehmerinnen und Teilnehmer legen einen ähnlichen Effekt nahe (siehe Abbildung). Wie lässt sich das erklären? Häufig sind zum Lesen von Datenschutzerklärungen mindestens 30 Minuten notwen-

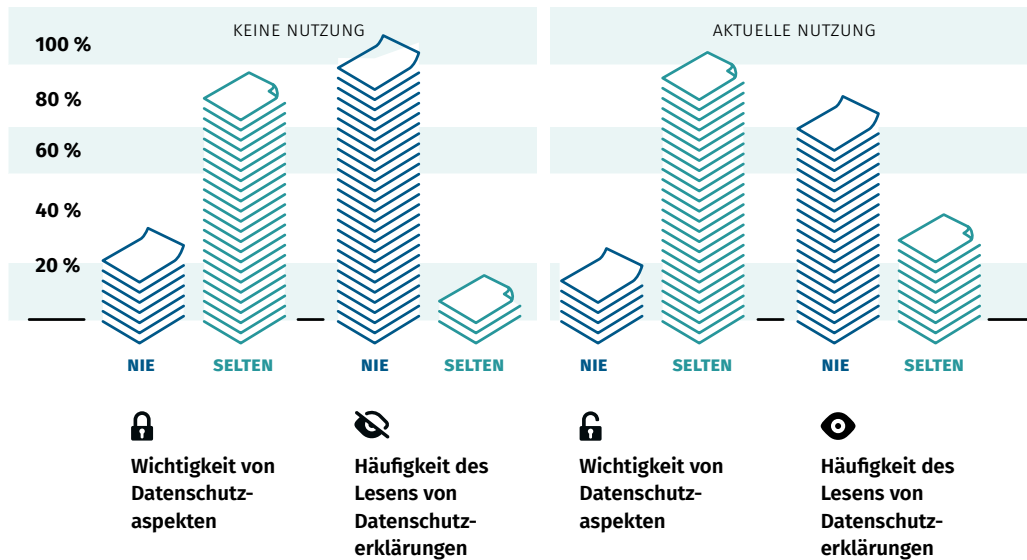


Abbildung 1: persönliche Einschätzung der Wichtigkeit des Themas Datenschutz vs. wie oft tatsächlich Datenschutzerklärungen gelesen werden

dig, da diese sehr umfangreich sind. Dem widerspricht der nachvollziehbare Wunsch, das bereits gekaufte oder installierte Produkt möglichst bald zu nutzen. Weiterhin ist bei der ersten Nutzung des Produkts typischerweise zunächst die Zustimmung zu der gesamten Datenschutzerklärung nötig, was die Motivation zur gründlichen Auseinandersetzung mit dem Text ebenfalls reduziert. Die in juristischer Fachsprache formulierten Texte sind außerdem für viele Personen schwer oder nicht verständlich. Das Projekt InviDas geht daher einen anderen Weg: Im Projektverbund wurde eine interaktive visuelle Darstellung einer Datenschutzerklärung geschaffen, mit dem Ziel, die Informationen für Nutzende übersichtlich und schnell zugänglich machen. Dafür wurde ein menschenzentrierter Ansatz gewählt, der schon für den Beginn der Systemgestaltung die speziellen Fähigkeiten und Anforderungen der späteren Nutzenden berücksichtigt. Dafür wurden zu Projektbeginn sogenannte „Personas“ entwickelt. Personas sind realitätsnahe, aber stereotypische Beschreibungen fiktiver Personen, die auf Grundlage der gesammelten Informationen über reale Nutzende erstellt werden. Sie helfen Entwicklungsteams, unterschiedliche Bedürfnisse und Perspektiven von potentiellen Nutzerinnen und Nutzern bei der Gestaltung technischer Systeme zu berücksichtigen. Im Fokus stand dabei die digitale Souveränität, also die Fähigkeit und Möglichkeit von Personen, in der digitalen Welt selbstständig, selbstbestimmt und sicher zu agieren. So wurde zum Beispiel die Persona des Technik-Enthusiasten Martin entwickelt, der immer online ist. Mit den aktuellen Datenschutzkonzepten ist er vertraut und auch am Thema sehr interessiert. Er möchte auf der Datenschutzlotsin, der

InviDas-Plattform, Details aus der Datenschutzerklärung einfach finden und für die unterschiedlichen Geräte eine datenschutzbezogene Übersicht nutzen. Ina, als Persona der „digital Mithaltenden“, hat ganz andere Anforderungen. Sie nutzt ihr Handy primär für Online-Aktivitäten und vermeidet soziale Netzwerke eher. Sie ist besorgt um ihre persönlichen Daten und möchte daher eine genaue Übersicht, was mit ihren Daten im Netz wo passiert. Die Persona Frank ist in Rente, nutzt kein Handy und ist als nur gelegentlicher Internetnutzer eher „digital abseitsstehend“. Er informiert sich nicht aktiv über Datenschutz-Themen, möchte aber seine persönlichen Daten nicht weitergeben. Zum Thema Datenschutz kam er durch eine Smart-Watch, die ihm als Fitnessgerät empfohlen wurde. Nach einem Schlaganfall fällt es ihm schwer, lange und komplexe Texte zu lesen. Stattdessen benötigt er gut strukturierte Informationen. Um die verschiedenen Anforderungen von Nutzerinnen und Nutzern zu verstehen und für die menschengerechte Gestaltung der Plattform zu berücksichtigen, sollten Perspektiven von Personen mit unterschiedlich hoher digitaler Souveränität, wie sie in den beschriebenen Personas skizziert wurden, abgebildet werden. In einer fragebogenbasierten Untersuchung wurden die Anforderungen und Bedürfnisse von Personen, die Smart-Wearable-Geräte nutzen, mit denen von Personen, die diese aktuell nicht nutzen, verglichen. Dabei konnte zum Beispiel festgestellt werden, dass einfachere Darstellungsformen wie interaktive oder nicht-interaktive Grafiken mit Stichpunkten von beiden Nutzungsgruppen gewünscht werden. Unterschiede zeigten sich hingegen bezüglich der erwünschten Unterstützung vor dem Kauf eines Wearables,



bei der die Nutzerinnen und Nutzer einen geringeren Bedarf berichteten. In Anbetracht der oben genannten Hürden zum Lesen der Datenschutzerklärungen nach dem Kauf war daher die Vermittlung von Datenschutzzinhalten für Personen vor dem Kauf eines Wearables ein zentrales Ziel für die Plattformentwicklung, das sich aus der Analyse der Anforderungen ergab.

Nachdem der erste Prototyp des Systems entwickelt war, wurden Interviews mit Personen unterschiedlichen Alters durchgeführt, wobei vor allem Unterschiede zwischen einer jüngeren (zwischen 20 und 39 Jahre alt) und einer älteren Technikgeneration (zwischen 57 und 81 Jahre alt) betrachtet werden sollten. Allgemein standen ältere Personen der Nutzung von Smart Wearables wesentlich kritischer gegenüber



👤 27 Jahre alt

🎓 Masterabschluss  
in Architektur

💍 Single

🎮 Verfolgt ein Hobby  
Software Projekt

## Martin

### TECHNIK-ENTHUSIAST

#### DIGITALISIERUNG

##### Nutzung/Kompetenz

Nutzt viele Geräte, darunter auch Smartwatch und VR Brille

11 Stunden am Tag online, die Hälfte davon privat

Hohe technische Kompetenz

#### DATENSCHUTZ

##### Nutzung/Kompetenz

Ist mit grundlegenden Datenschutzzinhalten vertraut

Beschäftigt sich im Alltag nur wenig mit dem Datenschutzprofil seiner Geräte

##### Einstellung

Begeistert sich für die Nutzung neuer Geräte und Technologien

Für ihn ist das Internet ein fester Teil von Berufs und Alltagslebens

##### Einstellung

Ist am Thema Datenschutz interessiert

Eine Optimale Nutzungserfahrung (Bequemlichkeit, Vernetzung in sozialen Netzwerken) ist für ihn jedoch wichtiger als vollkommener Datenschutz

#### KERNANFORDERUNGEN

Möchte Konzepte des Datenschutzes aus eigenem Wissensdrang tiefer durchdringen

Braucht eine Aufbereitung, die sein hohes technisches Verständnis berücksichtigt und eine entsprechende Genauigkeit (hohen Detailgrad) bietet

Braucht aufgrund seiner vielen verschiedenen Geräte eine Übersicht, die ein breites Spektrum an Datenschutzzinhalten berücksichtigt und Informationen aggregiert





### DATENSCHUTZ FÜR KINDER UND JUGENDLICHE

Im Projektverlauf identifizierten wir eine weitere Zielgruppe, für die das Thema des persönlichen Datenschutzes eine immer relevanter werdende Rolle einnimmt: Kinder und Jugendliche. Dieser Bedarf entstand aus dem vermehrten Angebot spezieller Smart-Watches für Kinder, die von Herstellern wie Garmin als Industriepartner im InviDas-Projekt immer häufiger angeboten werden. Hier kann ein weiteres Spannungsfeld zustande kommen, da datenschutzrechtliche Entscheidungen häufig von den Eltern getroffen werden (müssen), die damit jedoch über die Privatsphäre der Kinder entscheiden. Daraus ergibt sich die zentrale Frage, wie Kinder oder Jugendliche selbstbestimmt und transparent informiert über ihre eigenen Daten bestimmen können und wie die Kommunikation zwischen ihnen und ihren Erziehungsberechtigten zu diesem Thema unterstützt werden kann.

als jüngere. Außerdem fiel den älteren Teilnehmerinnen und Teilnehmern die Nutzung der Plattform schwerer, was sich in einer höheren Fehleranzahl bei Interaktionsaufgaben (z.B. „Finden Sie heraus, zu welchem Zweck Garmin Ihre E-Mail-Adresse erfasst“) zeigte. Um diese Nachteile bei der weiteren Gestaltung der visuellen Darstellung der Datenschutzerklärung möglichst weitestgehend auszumerzen, wurden verschiedene konkrete Gestaltungsempfehlungen aus den Ergebnissen abgeleitet. Außerdem wurden Nutzungspräferenzen erfragt. So zeigte sich beispielsweise, dass ältere Personen eine aus dem Alltag bekannte alphabetische Sortierung von Datenpunkten präferieren, wohingegen sich jüngere Personen eine Einordnung und Sortierung nach technischen Kategorien wünschen. Darüber hinaus äußerten jüngere Personen eine Präferenz für grafische Datenschutzzinformationen, ältere hingegen für textuelle. Entsprechend enthielt der zweite Prototyp, der aus diesen Ergebnissen hervorging, mehr Möglichkeiten zur individuellen Anpassung der Inhalte: Grafische sowie textuelle Elemente konnten beispielsweise individuell in der Darstellung hinzugefügt oder entfernt werden.

Somit soll die Plattform Menschen aus verschiedenen Technikgenerationen und mit unterschiedlichen Bedarfen eine individualisierbare und anpassbare Art der Vermittlung von Datenschutzzinhalten ermöglichen. Um digital souveräne



-  55 Jahre alt
-  Verkäuferin im Einzelhandel
-  Verheiratet, hat drei Kinder und einen Hund
-  Verbringt so viel Zeit wie möglich mit ihren Kindern

## Ina

### DIGITAL MITHALTENDE

#### DIGITALISIERUNG

##### Nutzung/Kompetenz

Geht ausschließlich mit dem Smartphone online

Nutzt hauptsächlich Messenger und tauscht Fotos mit Bekannten aus

Muss häufig auf die Hilfe ihrer Kinder hoffen

#### DATENSCHUTZ

##### Nutzung/Kompetenz

Vermeidet soziale Netzwerke

Häufig unsicher mit Sicherheitseinstellungen

Kaum Kenntnisse darüber, was mit ihren Daten im digitalen Raum geschieht

##### Einstellung

Wenig Zeit und Interesse dafür, digitales Wissen auszubauen

Nimmt nur die Aspekte der Digitalisierung an, die aus ihrer Sicht Nutzen stiften

##### Einstellung

Möchte im Internet möglichst wenige Spuren hinterlassen, macht daher häufiger Falschangaben

Gefühl mangelnder Kontrolle über ihre Daten





#### KERNANFORDERUNGEN

Möchte anfangen zu verstehen, was mit ihren Daten im Internet geschieht und so das Gefühl von Kontrolle über ihre Daten zurück gewinnen

Möchte Erklärungen dafür, welchen Mehrwert die Freigabe von Daten für sie bringt

Braucht kurze, am besten grafisch veranschaulichte Übersichten und geringen Interaktionsaufwand da sie bei drei Kindern und Hund keine Zeit hat, sich in komplexe digitale Sachverhalte einzuarbeiten



-  71 Jahre alt
-  Ehemaliger Schreiner
-  Verheiratet
-  Arbeitet gerne mit seiner Frau im Garten

## Frank

### DIGITAL ABSEITSSTEHENDER

#### DIGITALISIERUNG

##### Nutzung/Kompetenz

Besitzt kein Smartphone

Nutzt das Internet nur selektiv, vor allem Suchmaschinen, ab und zu Kommunikations-Dienste

##### Einstellung

Oft von der Komplexität neuer Technologien überfordert – fühlt sich nicht berücksichtigt

Ist Entwicklungen der Digitalisierung daher skeptisch gegenüber eingestellt

#### DATENSCHUTZ

##### Nutzung/Kompetenz

Informiert sich nicht aktiv über das Thema Datenschutz

Keine Kenntnisse darüber, wie persönliche Daten online bewertet werden

##### Einstellung

Möchte nicht, dass seine persönlichen Daten weitergegeben werden

Möchte Technologien, die dies tun, lieber nicht nutzen

#### KERNANFORDERUNGEN

Möchte sichergehen, dass ein neues telemedizinisches Gerät nicht unzulässig in seine Privatsphäre eingreift

Braucht verständliche, gut strukturierte Informationseinheiten, da ihn das Lesen von langen Texten nach einem Schlaganfall vor vier Jahren ermüdet und es ihm schwerfällt komplexe Sachverhalte nachzuvollziehen

Braucht Erklärungen und eine Nutzerschnittstelle, die keine Vorkenntnisse in den Bereichen Technologienutzung und Datenschutz erfordern

Entscheidungen zu treffen, müssen Menschen befähigt werden, sich in der digitalen Welt selbstständig, selbstbestimmt und sicher zu bewegen. Die Nutzung von Smart Wearables stellt dabei eine kritische Schnittstelle dar, an der Daten aus dem analogen und digitalen Leben in der digitalen Welt gesammelt, verarbeitet und weitergegeben werden. Dabei ist den Nutzerinnen und Nutzern nicht immer klar, zu welcher Form der Sammlung, Verarbeitung und Weitergabe ihrer Daten sie ihre Zustimmung erteilt haben, wie diese Daten geschützt werden, und welche Rückschlüsse auf ihr nicht-digitales Leben damit möglich sind. Umso wichtiger ist es, diese Zusammenhänge für Menschen zu entschlüsseln,

um ein Bewusstsein für Datenschutz und damit individuelle digitale Souveränität zu ermöglichen. Für Nutzerinnen und Nutzer von Smart Wearables kann die menschenzentrierte Entwicklung der visuellen Darstellungen von Datenschutzerklärung im Projekt InviDas daher ein weiterer Schritt auf dem Weg zu höherer digitaler Souveränität sein.

<sup>1</sup> Kokolakis, S. (2017). *Privacy attitudes and privacy behaviour: A review of current research on the privacy paradox phenomenon*. *Computers & Security*, 64, 122-134. <https://doi.org/10.1016/j.cose.2015.07.002>



# NUTZER\*INNEN- ZENTRIERTE TECHNOLOGIEN FÜR MEHR TRANSPARENZ UND KONTROLLE IM DATENSCHUTZ

CAROLIN STELLMACHER, UNIVERSITÄT BREMEN

Datenschutzerklärungen begleiten uns täglich beim App-Download, Online-Einkauf oder beim Arztbesuch. Ihr Grundgedanke: Unternehmen klären Kund\*innen und Nutzende über die digitale Verarbeitung personenbezogener Daten auf, um deren informierte Zustimmung einzuholen. Die langen und schwer verständlichen Texte bleiben aber meist ungelesen. Die Zustimmung durch das berühmte Häkchen „Ja,

ich stimme der Datenschutzerklärung zu“ stellt somit keine informierte Einwilligung dar, sondern ist eher ein lästiges Übel. Somit verfehlen Datenschutzerklärungen oftmals ihren Zweck die Nutzenden über die Verarbeitung ihrer Daten aufzuklären. Die Gründe hierfür sind vielfältig: Die Texte sind zu lang, schwer lesbar und es mangelt an differenzierten Einwilligungsmöglichkeiten. Während der Grundgedanke, Nutzende über Datenschutzpraktiken zu informieren, sinnvoll ist und Nutzende in ihrer digitalen Selbstbestimmung ihrer eigenen Daten unterstützen soll, so scheitert das Vorhaben heutzutage in der Praxis. Neue Wege sind notwendig, die einen Zugang zu transparentem und kontrollierbarem Datenschutz ermöglichen und Nutzende bei der Ausübung ihrer digitalen Datensouveränität unterstützen. Im InviDas-Projekt haben wir erforscht, wie interaktive Visualisierungen mit spielerischen Elementen das Verständnis von Datenschutzerklärungen verbessern können.

Das Ziel interaktiver Visualisierungen von Datenschutzerklärungen ist die Verringerung komplexer Texte durch visuelle Elemente und mehr Kontrolle durch Interaktion. Bisherige Forschungsansätze erprobten kurze, kontextbezogene Datenschutzstatements, tabellarische Strukturen, Comics oder Escape Room Games. Unsere Forschung bewegt sich dabei in einem Spannungsfeld zwischen den rechtlichen Anforderungen der DSGVO, die eine umfangreiche Informationspolitik zur Sicherung der Datenschutzkonformität fordert, und den Bedarfen der Nutzenden. Während rechtliche Rahmenbestimmungen durch die DSGVO festgelegt sind, wurden zu Beginn des InviDas-Projekts die Bedarfe der Nutzenden erfasst. Die Studienerkenntnisse bestimmten somit von Anfang an den nutzer\*innenzentrierten Designprozess der angestrebten Plattform zur interaktiven Visualisierung von Datenschutzerklärungen. Zentrale Fragen während des Entwicklungsprozesses waren, wie die Art und Menge an datenschutzrechtlicher Information individuell angepasst werden kann, wie ein bestimmter Aspekt schnell aufgefunden werden kann und welche Informationen für Nutzende am relevantesten sind. Des Weiteren wurde das Design von Überlegungen bestimmt, welche textuellen Inhalte durch Grafiken kommuniziert werden können und wie neben der Transparenz auch die Kontrolle hervorgehoben werden kann.

### **DIE MÖGLICHKEITEN DER „DATENSCHUTZLOTSIN“**

Die im Projekt entstandene Plattform Datenschutzlotsin präsentiert Inhalte einer Datenschutzerklärung in Form eines Dashboards, welches das aktive Explorieren von Datenschutz fördern soll. Um insbesondere für technikferne Nutzende einen besseren Zugang zu den verschiedenen Praktiken der Datenverarbeitung zu schaffen, setzt die Plattform auf die

Idee des Lebenszyklus der Daten. Der Prozess der Datenverarbeitung ist in drei Stationen aufgeteilt: Erhebung & Aufbereitung, Speicherung und Weitergabe. Diese werden durch Farben und Icons unterschieden. Die aktuelle Version der Plattform fokussiert zunächst die Transparenz von Datenschutz anhand innovativer Visualisierungskonzepte. Zukünftige Erweiterungen könnten die aktive Kontrolle durch Datenschutzeinstellungen stärker integrieren. Doch schon jetzt hebt das Dashboard Möglichkeiten zur Kontrolle und Widerruf visuell hervor. Icons bieten visuelle Repräsentationen der drei möglichen Kontrollgrade: grundlegend verpflichtend, funktionsabhängig verpflichtend und freiwillig und vermitteln Wege des Widerrufs. Das Herzstück der Datenschutzlotsin-Plattform sind die Funktionen zur individuellen Anpassung des Dashboards an den eigenen Informationsbedarf. Umfangreiche Möglichkeiten zur Filterung und Sortierung ermöglichen ein schnelles An- und Abwählen von datenschutzrechtlichen Details. So können Nutzende weniger relevante Aspekte ausblenden und das Dashboard mit für sie bedeutsamen Details befüllen.

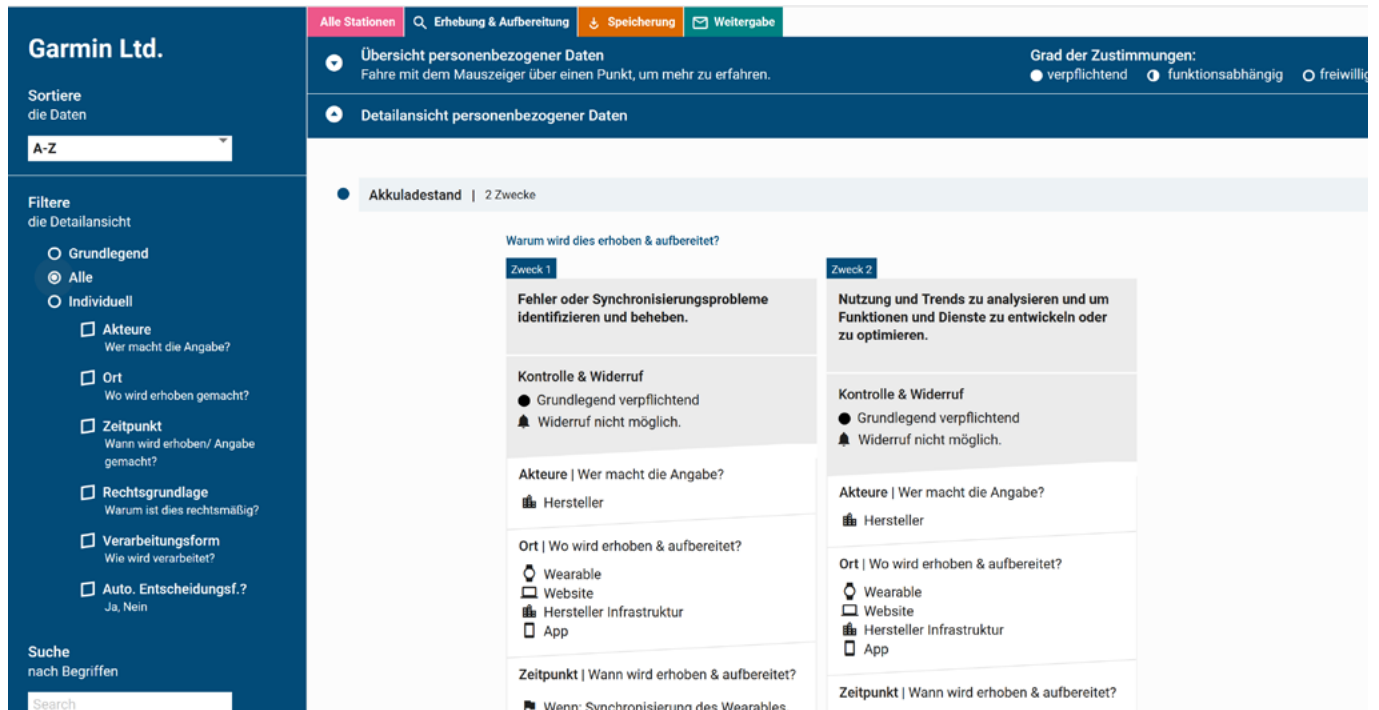


Abbildung 2: Screenshot der Plattform „Datenschutzlotsin“

## TECHNISCHER UND RECHTLICHER FORTSCHRITT GEHEN HAND IN HAND

Die Forschung im InviDas-Projekt, textuelle Datenschutzerklärung in interaktive Visualisierungen zu übertragen, hat gezeigt, dass innovativen Technologien bei der vereinfachten Kommunikation und Kontrolle von Datenschutz heutzutage noch Grenzen durch die DSGVO gesetzt sind. Diese schafft zurzeit Rahmenbedingungen, bei denen Nutzende vollumfänglich informiert werden müssen und die Verantwortung der informierten Zustimmung weiterhin auf den Schultern der Nutzenden platziert ist. Aber eine ausreichende Vermittlung datenschutzrechtlicher Kompetenzen, Unterstützung der Abwägung möglicher Konsequenzen und eine abschließende informierte und kompetente Einwilligung kann auch durch interaktive Visualisierungen nicht vollständig erreicht werden. Stattdessen sollte eine Trennung zwischen der rechtlichen Offenlegung der Datenkonformität eines Unternehmens durch Datenschutzerklärungen und der Einholung der informierten Zustimmung von Nutzenden gezogen werden. Die Entwicklung interaktiver Technologien zur Unterstützung der Transparenz und

Kontrolle des eigenen Datenschutzes sollte primär durch Bedarfe der Nutzenden bestimmt werden und losgelöst sein von den Vorgaben der datenschutzrechtlichen Bedingungen. Ansätze hierfür könnten Datenverarbeitungen bieten, deren Rechtsgrundlagen nicht auf der Zustimmung der Nutzenden basiert. In diesen Fällen kann ausschließlich Transparenz geschaffen werden. Die Ausübung von Kontrolle ist lediglich möglich bei Verarbeitungen, die explizit der Zustimmung der Nutzenden bedürfen. Eine Schärfung in der Kommunikation von Datenschutz auf diese kontrollierbaren Bereiche bietet Potenzial für mehr nutzer\*innenzentrierte Lösungen.



# NUTZUNGS- BEISPIELE

## ANHAND VON SCREENDESIGNS

CAROLIN STELLMACHER, UNIVERSITÄT BREMEN

### ALLGEMEIN

**NUTZENDE KÖNNEN DIE DATENSCHUTZRECHTLICHE VERARBEITUNG DER DATEN IN VISUELL AUFBEREITETER FORM SEHEN UND ANHAND VON DREI DATENVERARBEITUNGSSTATIONEN VERFOLGEN.**



● Datenpunkt relevant für die Station

Um die Datenverarbeitung für Nutzende transparenter zu gestalten, gliedert die Plattform den Verarbeitungsprozess in drei Stationen: Erhebung & Aufbereitung, Speicherung und Weitergabe. Sind personenbezogene Daten von einer der drei Verarbeitungsformen betroffen, so taucht jeweils ein repräsentativer Punkt in der entsprechenden Station auf. Wenn beispielsweise die E-Mail-Adresse sowohl erhoben und aufbereitet als auch gespeichert und weitergegeben wird, erscheinen in der Übersicht ein blauer, ein orangefarbener und ein türkiser Punkt. Wenn jedoch ein Datenpunkt nicht weitergegeben wird, endet der Verarbeitungsprozess in der Speicherung und wird nur durch einen blauen und einen orangefarbenen Punkt dargestellt.

### WELCHE DATEN?

#### NUTZENDE SEHEN, WELCHE DATEN VERARBEITET WERDEN.

In einer Datenliste wird genau aufgeführt, welche personenbezogenen Daten verarbeitet werden und von welcher Verarbeitungsstation diese betroffen sind. Zu Beginn jeder Zeile sind die entsprechenden Stationen durch Punkte abgebildet. Fehlt der dritte Punkt, so wird dieser personenbezogene Datenpunkt nicht weitergegeben.

Liste aller personenbezogener Daten aus allen Stationen			
			
			Abonnements <span>Mehr</span>
			Akkuladestand <span>Mehr</span>
			Aktivitätsgrad <span>Mehr</span>
			Analysedaten <span>Mehr</span>
			Datum <span>Mehr</span>
			Emailadresse <span>Mehr</span>
			Eventprotokolle <span>Mehr</span>
			Fitnessstudio <span>Mehr</span>
			Geburtsdatum <span>Mehr</span>

### WARUM?

#### NUTZENDE KÖNNEN DIE DATENSCHUTZRECHTLICHE VERARBEITUNG DER DATEN IN VISUELL AUFBEREITETER FORM SEHEN UND ANHAND VON DREI DATENVERARBEITUNGSSTATIONEN VERFOLGEN.

Die datenschutzrechtlichen Zwecke regeln, warum Daten verarbeitet werden. Jeder Zweck wird auf der Plattform durch eine „Karte“ dargestellt, die Nutzenden weitere Details liefert. Dabei bilden Informationen zur Kontrolle & Widerruf zusammen mit dem Namen des Zwecks die grau hinterlegten Basisdetails. Zusätzliche Aspekte wie „Akteure“ oder „Zeitpunkt“ werden ebenfalls aufgelistet und können individuell durch Filter aktiviert oder deaktiviert werden. Die optionale Anzeige dieser Aspekte ist durch schräge Linien und weißen Hintergrund gekennzeichnet.

Emailadresse   6 Zwecke		
Warum wird dies erhoben & aufbereitet?		
Zweck 1	Zweck 2	Zweck 3
<b>Kontoanmeldung</b> <b>Kontrolle &amp; Widerruf</b> <ul style="list-style-type: none"> <li>● Grundlegend verpflichtend</li> <li>🔔 Widerruf nicht möglich.</li> </ul> <b>Akteure   Wer macht die Angabe?</b> <ul style="list-style-type: none"> <li>👤 Nutzerin</li> </ul> <b>Ort   Wo wird erhoben &amp; aufbereitet?</b> <ul style="list-style-type: none"> <li>🌐 Website</li> <li>📱 App</li> </ul> <b>Zeitpunkt   Wann wird erhoben &amp; aufbereitet?</b> <ul style="list-style-type: none"> <li>📅 Wenn: Erstellung eines Garmin-Kontos</li> </ul> <b>§ Rechtsgrundlage   Warum ist dies rechtmäßig?</b> Rechtsgrundlage	<b>Informationen zu Ihren Garmin-Produkten, -Services, -Apps oder -Konten senden</b> <b>Kontrolle &amp; Widerruf</b> <ul style="list-style-type: none"> <li>● Grundlegend verpflichtend</li> <li>🔔 Widerruf nicht möglich.</li> </ul> <b>Akteure   Wer macht die Angabe?</b> <ul style="list-style-type: none"> <li>👤 Nutzerin</li> </ul> <b>Ort   Wo wird erhoben &amp; aufbereitet?</b> <ul style="list-style-type: none"> <li>🌐 Website</li> <li>📱 App</li> </ul> <b>Zeitpunkt   Wann wird erhoben &amp; aufbereitet?</b> <ul style="list-style-type: none"> <li>📅 Wenn: Erstellung eines Garmin-Kontos</li> </ul> <b>§ Rechtsgrundlage   Warum ist dies rechtmäßig?</b> Rechtsgrundlage	<b>Versenden von Marketinginformationen</b> <b>Kontrolle &amp; Widerruf</b> <ul style="list-style-type: none"> <li>○ Freiwillig</li> <li>🔔 Widerruf möglich: In Präferenzen oder per Link in Mail.</li> </ul> <b>Akteure   Wer macht die Angabe?</b> <ul style="list-style-type: none"> <li>🏢 Hersteller</li> </ul> <b>Ort   Wo wird erhoben &amp; aufbereitet?</b> <ul style="list-style-type: none"> <li>🏢 Hersteller Infrastruktur</li> </ul> <b>Zeitpunkt   Wann wird erhoben &amp; aufbereitet?</b> <ul style="list-style-type: none"> <li>🔄 Kontinuierlich</li> <li>📅 Wenn: Zustimmung zum Erhalt von Marketinginformationen.</li> </ul> <b>§ Rechtsgrundlage   Warum ist dies rechtmäßig?</b> Rechtsgrundlage

## KONTROLLE & WIDERRUF

### NUTZENDE ERKENNEN AUF EINEN BLICK DEN GRAD IHRER KONTROLLE UND DEN PROZESS DES WIDERRUFS.

Um den hohen Bedarf der Nutzen- und Kontrolle zu erfüllen, bilden die relevanten Informationen zusammen mit dem Namen des Zwecks die grundlegenden datenschutzrechtlichen Basisinformationen. Zur Unterstützung der schnellen Auffindbarkeit sind diese Basisinformationen durch einen grauen Hintergrund visuell hervorgehoben. Zusätzlich zeigen zwei verschiedene Punkte-Icons den Grad der Nutzerzustimmung auf: Ein gefüllter Punkt markiert eine grundlegende Verpflichtung, bei der die Zustimmung nur durch das Beenden der Geräte-Nutzung erteilt werden kann. Bei optionalen Funktionen wird die Freiheit der Zustimmung durch einen halb-gefüllten Punkt angezeigt. Nutzende können dann selbst entscheiden, ob sie der Datenverarbeitung zu diesem Zweck

#### Zweck 2

Informationen zu Ihren Garmin-Produkten, -Services, -Apps oder -Konten senden

##### Kontrolle & Widerruf

- Grundlegend verpflichtend
- 🔔 Widerruf nicht möglich.

#### Zweck 3

Versenden von Marketinginformationen

##### Kontrolle & Widerruf

- Freiwillig
- 🔔 Widerruf möglich: In Präferenzen oder per Link in Mail.

#### Zweck 5

Kunden benachrichtigen, die gegen unsere Bedingungen verstoßen haben.

##### Kontrolle & Widerruf

- Grundlegend verpflichtend
- 🔔 Widerruf nicht möglich.

#### Zweck 6

Versenden von Marketinginformationen.

##### Kontrolle & Widerruf

- ◐ Funktionsabhängig verpflichtend
- 🔔 Widerruf möglich: Erhalt der Benachrichtigungen ablehnen oder Email-Benachrichtigungen deaktivieren

zustimmen, um die entsprechende Funktion zu nutzen. Sollte die Funktion nicht genutzt werden wollen, kann diese Zustimmung widerrufen werden.



## WEITERGABE

## NUTZENDE KÖNNEN EINSEHEN, WELCHE DATEN AN WELCHE AKTEURE WEITERGEGEBEN WERDEN.

**Hersteller**

- **Aktivitätsdaten** | 1 Zweck  
z.B. Position

Warum wird dies weitergegeben?

**Zweck 1**

Damit sie die Qualität der bereitgestellten Inhalte oder Funktionen optimieren können, und wir teilen oder verkaufen sie mit bzw. an andere Dritte zu Forschungs- oder anderen Zwecken

Kontrolle & Widerruf

- Grundlegend verpflichtend
- 🔔 Widerruf nicht möglich.

**Externer Datenbereinsteller**

- **Segmente** | 1 Zweck

Warum wird dies weitergegeben?

**Zweck 1**

Aktivitätsinformationen in Garmin Connect mit Informationen aus Drittanbieter Apps ergänzen

Um einzusehen, welche Daten an welche Akteure weitergegeben werden, bietet die Plattform eine entsprechende Listensortierung. Dabei werden die Empfängertypen differenziert, wie zum Beispiel Hersteller, externe Datenempfänger, externe Datenbereinsteller und externe Freunde.

**Zweck 4** **Verpflichtende Weitergabe**

Damit wir die Qualität der bereitgestellten Inhalte oder Funktionen optimieren können, teilen oder verkaufen wir sie mit bzw. an andere Dritte zu Forschungs- oder anderen Zwecken

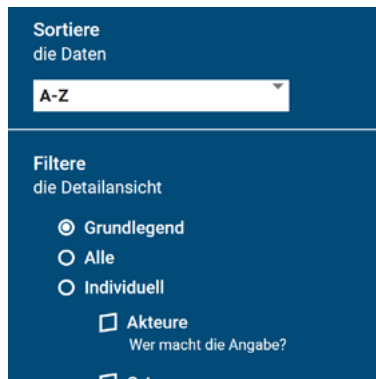
Kontrolle & Widerruf

- Grundlegend verpflichtend
- 🔔 Widerruf nicht möglich.

Um Nutzende auf die besonders sensible Datenverarbeitung im Rahmen der verpflichtenden Datenweitergabe aufmerksam zu machen, bietet die Plattform ein zusätzliches visuelles Element. Ein roter Hinweis am Kopfende der Zweckkarte signalisiert diese Sensibilität.

## FILTERN, SORTIEREN UND SUCHEN

### NUTZENDE KÖNNEN DIE INFORMATIONEN ANHAND IHRES BEDARFS FILTERN, SORTIEREN UND SUCHEN.



Nutzende haben die Möglichkeit, mithilfe von Filterung, Sortierung und Suche die Art und Menge der angezeigten datenschutzrechtlichen Informationen an ihre eigenen Bedürfnisse anzupassen. Gesuchte Details sind dadurch gezielt und schnell auffindbar. Um die Filterinteraktion zu unterstützen, bietet die Plattform drei Schnellauswahlen: die Anzeige der grundlegenden Basisinformationen, die individuelle Auswahl der Filter oder die Anzeige aller verfügbaren Details.



Um Nutzenden einen schnellen und unkomplizierten Zugang zur visuellen Datenschutzerklärung zu ermöglichen, bietet die Plattform eine Filter-Schnellauswahl namens „Grundlegend“. Diese Option zeigt nur die grau hinterlegten Basisinformationen (Name des Zwecks und Kontrolle & Widerruf) an und richtet sich speziell an Nutzende, die digitale Inhalte nicht oft nutzen und einen einfachen Zugang zu wichtigen datenschutzrechtlichen Informationen suchen. Auch Nutzende mit wenig Zeit können so schnell einen grundlegenden Überblick gewinnen.

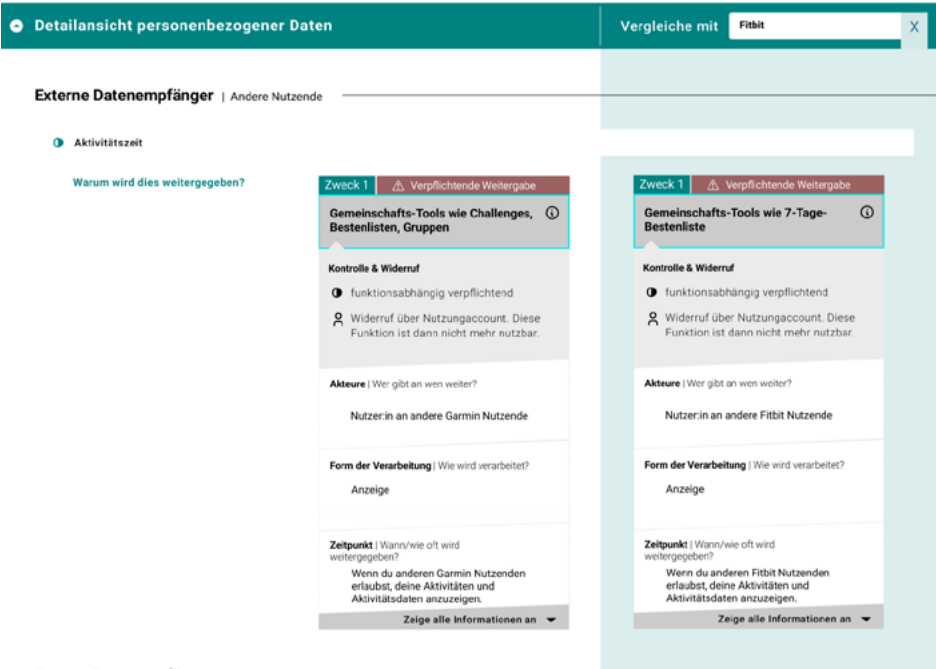
Nutzende haben die Möglichkeit, mithilfe von Filterung, Sortierung und Suche die Art und Menge der angezeigten datenschutzrechtlichen Informationen an ihre eigenen Bedürfnisse anzupassen. Gesuchte Details sind dadurch gezielt und schnell auffindbar. Um die Filterinteraktion zu unterstützen, bietet die Plattform drei Schnellauswahlen: die Anzeige der grundlegenden Basisinformationen, die individuelle Auswahl der Filter oder die Anzeige aller verfügbaren Details.



VERGLEICH

NUTZENDE KÖNNEN VERSCHIEDENE HERSTELLER ANHAND DER ZWECKE DER VERARBEITUNG VERGLEICHEN.

Um die Vergleichbarkeit von Datenschutzerklärungen zu ermöglichen, soll die Plattform als ersten Schritt den Vergleich von Verarbeitungszwecken anbieten. Auf diese Weise können Abweichungen oder Ähnlichkeiten in der Begründung der Datenverarbeitungen erkannt werden.





# PLATTFORM- ENTWICKLUNG – VOM MODELL ZUM TOOL

CONSTANTIN BUSCHHAUS, ARVID BUTTING, STEFFEN HILLEMACHER,  
JUDITH MICHAEL, BERNHARD RUMPE, RWTH AACHEN

## METHODE: MODELLGETRIEBENE ENTWICKLUNG – WAS IST DAS?

Bei der modellgetriebenen Softwareentwicklung steht das Modell im Mittelpunkt, um daraus Teile des Systems zu generieren. Diese Modelle beschreiben z.B. das Domänenwissen, die Struktur, das Verhalten oder graphische Oberflächen eines Programms.

Die Vorteile gegenüber konventioneller Softwareentwicklung bestehen darin, dass Modelle den ganzen Entwicklungsprozess begleiten und wie Software-Code laufend aktuell gehalten werden, da sie als zentrale Artefakte für die Generierung genutzt werden.

Im InviDas-Projekt verwenden wir einen modellgetriebenen Entwicklungsansatz und nutzen den MontiGem Generator zur Entwicklung der Datenschutzlotsin-Plattform. MontiGem ermöglicht die einfache Entwicklung von datenzentrierten Anwendungen.<sup>1</sup> Aus UML/P Klassendiagrammen<sup>2</sup> und Modellen für die Beschreibung von graphischen Nutzer\*innenoberflächen (GUI) werden große Teile der Datenstruktur, der Kommunikation mit der Datenbank, der Zugriffskontrolle und der GUI generiert.

## DATENSCHUTZERKLÄRUNGEN ALS MODELL

Wir haben die Datenschutzerklärungen der sieben größten Hersteller von Smart Wearables (darunter Apple, FitBit und Garmin) auf ihre Gemeinsamkeiten und Unterschiede analysiert, um daraus ein wiederverwendbares Datenmodell für Datenschutzerklärungen zu erhalten.<sup>3</sup> Ein Kritikpunkt hierbei ist, dass nur selten Zusammenhänge zwischen Datenkategorien und den konkreten Daten beschrieben sind und Aussagen über die Verarbeitung der Daten zu generell formuliert sind, um sie als Nutzende tatsächlich nachvollziehen zu können.

Zudem haben wir den rechtlichen Rahmen der Datenschutzgrundverordnung untersucht und gemeinsam mit Rechtsanwält\*innen des assoziierten Partners Planit Legal, die sich auf IT- und Datenschutzrecht spezialisiert haben, unser Modell auf Vollständigkeit überprüft. Im Folgenden beschreiben wir die wichtigsten Klassen des Datenmodells und ihre Funktion in der Plattform.

Die zentrale Klasse des Datenmodells<sup>4</sup> ist die Datenschutzerklärung, die Hersteller in der Plattform basierend auf ihrer originalen Datenschutzerklärung anlegen können. Jede Erklärung beinhaltet ein Datum, ab dem das Original gültig ist, und es ist ein Mindestalter angegeben, ab dem Nutzende der Erklärung rechtsgültig zustimmen können. Zusätzlich bilden vier weitere Klassen die relevanten Konzepte einer

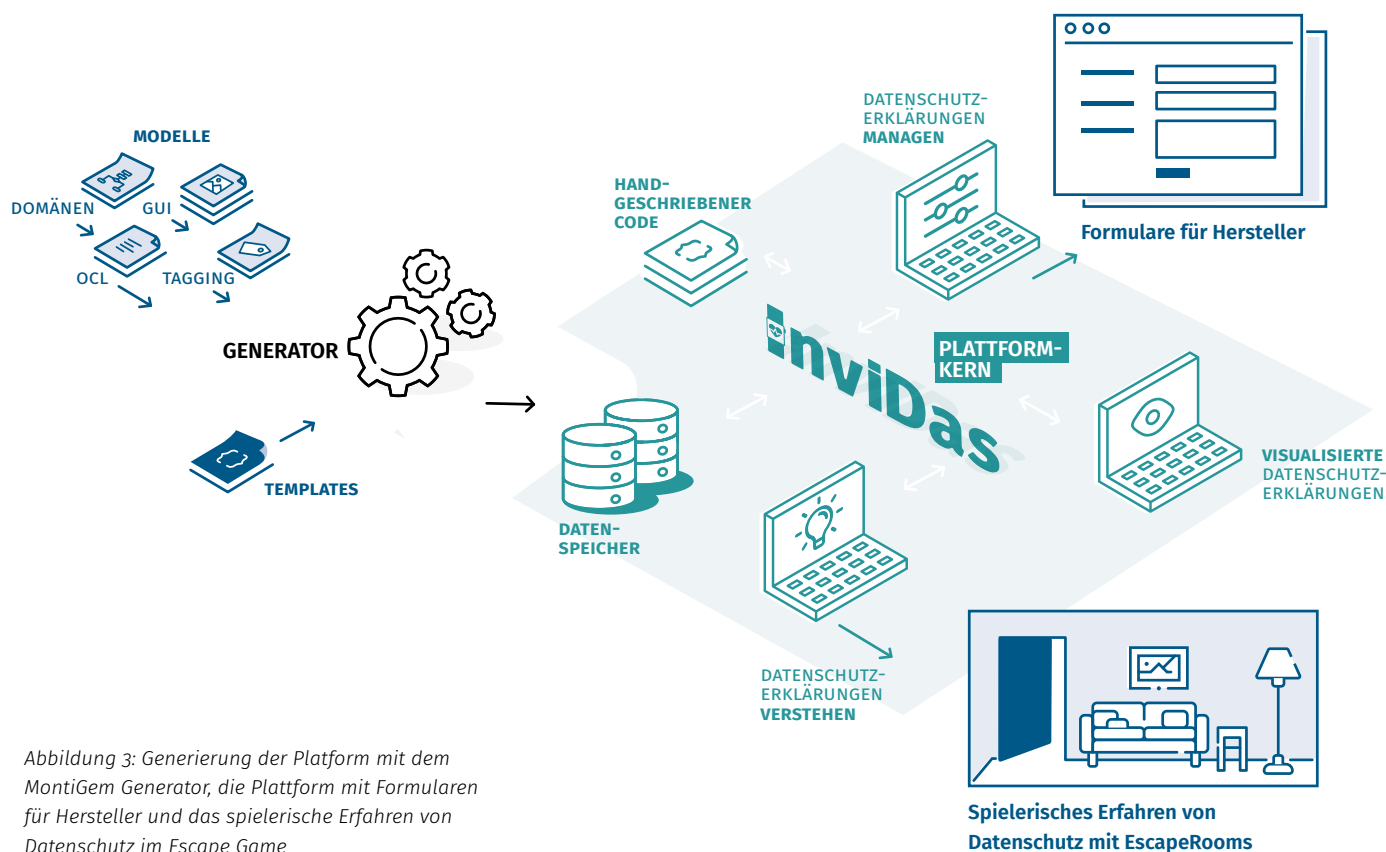


Abbildung 3: Generierung der Plattform mit dem MontiGem Generator, die Plattform mit Formularen für Hersteller und das spielerische Erleben von Datenschutz im Escape Game

Datenschutzerklärung ab: Dateneintrag, Datenkategorie, Datenverarbeitung, und Regionen. Dateneinträge und Datenkategorien liefern Details zu den Daten, die schützenswert sind. Beide haben einen Namen und Dateneinträge können durch Datenkategorien zusammengefasst werden, z.B. die Datenkategorie „Aktivitätsdaten“ mit Dateneinträgen zu den gezählten Schritten und Pulsaufzeichnungen. Regionen geben an, wo die Datenschutzerklärung gültig ist.

Eine Datenverarbeitung wird an einem Ort und durch eine\*n Akteur\*in ausgeführt, wobei Nutzer\*in, Hersteller und externe Datenbereitstellende möglich sind. Für jede Datenverarbeitung wird mindestens ein Zweck angegeben, der sich auf bestimmte Daten bzw. Datenkategorien der Verarbeitung bezieht und eine Rechtsgrundlage besitzen muss. Dem Zweck (1) kann widersprochen werden, ohne den Service des Herstellers zu beschränken, (2) er ist verpflichtend für die Nutzung des Wearables oder (3) er ist verpflichtend, um einen bestimmten Service zu nutzen. Es gibt verschiedene Formen der Datenverarbeitung und es existieren viele Begriffe, die eine ähnliche Bedeutung haben können. Um die Verständlichkeit zu erhöhen und einen Vergleich zu ermöglichen, wurden die Verarbeitungen für das Datenmodell und die Plattform auf drei Arten reduziert, die sich in ihren Charakteristiken unterscheiden und sich deshalb nachvollziehbar beschreiben lassen: die Erhebung bzw. Aufbereitung, die Speicherung und die Weitergabe. Die Erhebung bzw. Aufbereitung beschreibt den Vorgang der Datensammlung und weitere Verarbeitungen, die weder Speicherungen noch Weitergaben sind, darunter fällt z. B. die Analyse. Es wird unterschieden, ob sie einmalig statt-

finden, z. B. beim Erstellen eines Nutzerkontos, kontinuierlich durchgeführt werden oder nur bei einer bestimmten Aktivität der Nutzenden.

Für die Datenspeicherung wird angegeben, wie lange diese andauert, entweder als Zeitspanne oder bis zu einem bestimmten Ereignis. Für die Datenweitergabe ist entscheidend, wer ihre Empfänger\*in ist und in welchem Land die empfangende Instanz sitzt, da dort andere Datenschutzgesetze gelten können.

#### AUFBAU DER PLATTFORM

Die InviDas-Plattform nutzt den MontiGem Generator, um Programmcode für das Backend und Frontend der Anwendung zu generieren. Im Backend ist dies eine Java Anwendung, die das Apache TomEE Framework nutzt, ein Apache HTTP Webserver und eine Postgres Datenbank, in der die Daten der Hersteller eingepflegt werden können, jeweils in eigenen Docker Containern. Im Frontend generieren wir TypeScript und HTML Code in das Angular Framework.

Das Ziel der Plattform ist es, Datenschutzklärungen von Smart Wearables besser verständlich zu machen. Hierfür müssen wir die Datenschutzverantwortlichen der Hersteller motivieren, ihre Datenschutzklärungen in die Plattform einzupflegen, um einen Vergleich zwischen den verschiedenen Anbietern und Erklärungen zu erlauben. Dies ist über Formulare möglich (siehe Abb. 3). Die Plattform verfügt über ein Rechte-Rollen-Konzept, um es Herstellern zu ermöglichen ihre Daten einzupflegen. Zudem können Administrator\*innen Accounts für Hersteller erstellen.

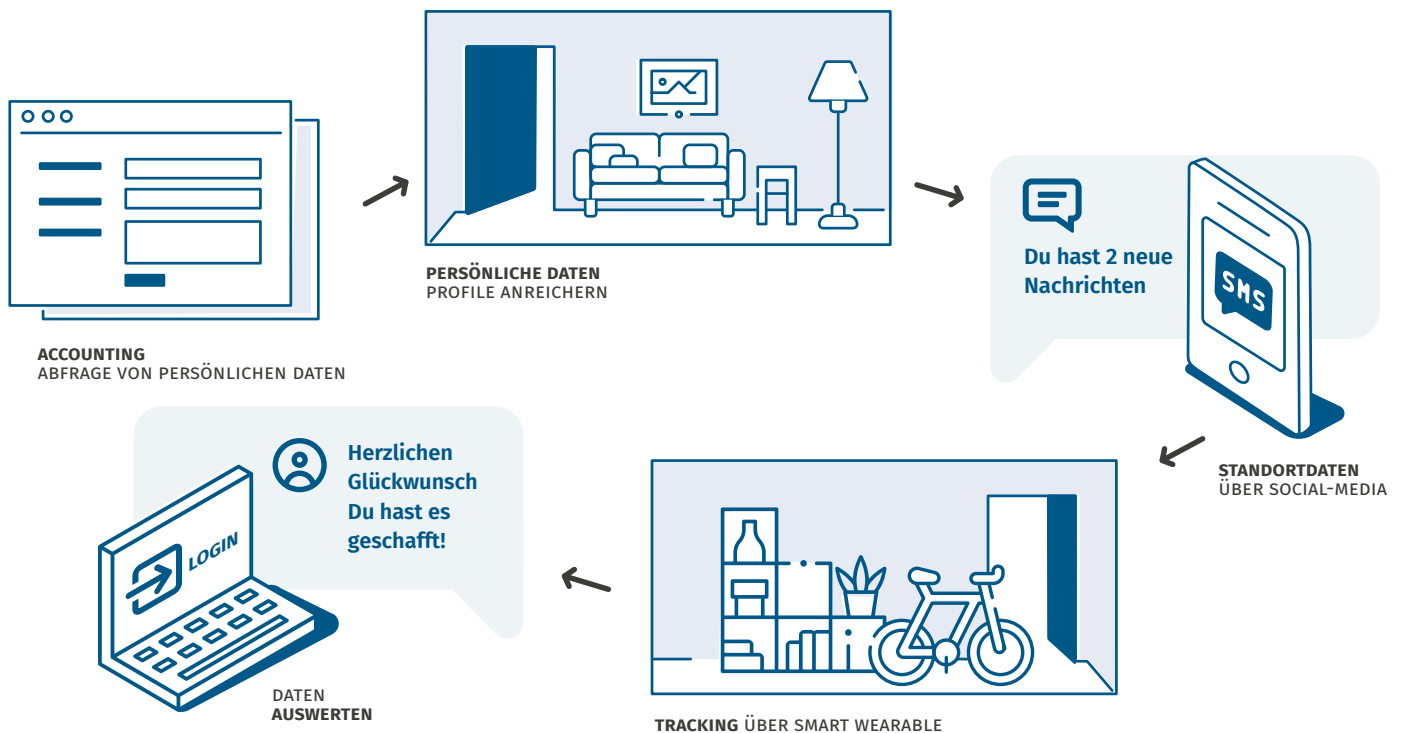


Abbildung 4: Datenschutz im Escape Game spielerisch erfahren

## DATENSCHUTZ GAMIFIZIEREN

Gamifizierung beschreibt die Einbettung von spielerischen Elementen in seriöse Kontexte mit dem Ziel, das Engagement, die Motivation und die Beteiligung zu fördern. Beispiele für solche spielerischen Elemente sind Punktwertungen, Bestenlisten, Abzeichen, Herausforderungen und andere Anreize. Der Ansatz der Gamifizierung basiert auf der Idee, dass Menschen einen intrinsischen Spieltrieb haben und sich an Belohnungen durch Gewinne und Leistungen erfreuen.

Im Projekt wurde das Konzept der Gamifizierung durch ein Escape Game umgesetzt, das den Spielenden den Umgang mit Datenschutz und personenbezogenen Daten näherbringen soll. Diese Lektionen sind in die für den Spielfortschritt erforderlichen Schritte integriert.

Zu Beginn des Spiels wird der\*die Spieler\*in dazu aufgefordert, persönliche Daten anzugeben, deren Angabe eigentlich nicht erforderlich ist und das Spielerlebnis nicht verändert. Dies soll Spielenden vermitteln, dass personenbeziehbare Daten nicht immer vollständig angegeben werden müssen, um spezifische Dienstleistungen zu nutzen.

Das Ziel des Spielverlaufs ist es, den Standort einer Person herauszufinden, um dieser einen Streich zu spielen. Dazu bieten sich den Spieler\*innen im Verlauf des Spiels zwei Möglichkeiten. Einmal über den Social-Media-Status der gesuchten Person sowie über die Trackingfunktion der

Fitnessuhr, die bereits auf der Herstellerseite im Kundenprofil eingeloggt ist. Die Spieler\*innen sollen dabei lernen,

- (1) dass Standortdaten in den falschen Händen missbraucht werden können,
- (2) dass die Ortung über Smart Wearables sehr genau ist und somit ein größeres Missbrauchspotenzial besteht, und
- (3) dass jede Person für den Schutz ihrer Daten mitverantwortlich ist, z.B. wenn es darum geht ein geeignetes Passwort auszuwählen oder zu verhindern, dass anderen Personen durch Unachtsamkeit Zugriff auf die eigenen Daten ermöglicht wird.

<sup>1</sup> <https://www.se-rwth.de/research/MontiGem>

<sup>2</sup> <https://www.mbse.se-rwth.de/book1>

<sup>3</sup> A. Butting, N. Conradie, J. Croll, M. Fehler, C. Gruber, D. Herrmann, A. Mertens, J. Michael, V. Nitsch, S. Nagel, S. Pütz, B. Rumpe, E. Schaueremann, J. Schöning, C. Stellmacher, S. Theis: *Souveräne digitalrechtliche Entscheidungsfindung hinsichtlich der Datenpreisgabe bei der Nutzung von Wearables*. In: *Selbstbestimmung, Privatheit und Datenschutz: Gestaltungsoptionen für einen europäischen Weg*, pp. 489-508, Springer Fachmedien Wiesbaden, Apr. 2022.

<sup>4</sup> *Modeling Privacy Policies of Smart Watches: A Reuseable Generic Data Structure Model*: <https://zenodo.org/record/5898204>



# ETHISCHE BEWERTUNG DER AUSWIRKUNGEN VON WEARABLES AUF DIE AUTONOMIE DER NUTZER\*INNEN

NIEL CONRADIE, SASKIA NAGEL, RWTH AACHEN

Für eine ethische Diskussion um Wearable-Technologien im Allgemeinen und für die spezifischen Ziele des InviDas-Projektes, die digitale Souveränität der Nutzer\*innen von Wearables zu fördern, untersuchen wir die Auswirkungen von Wearables auf die Autonomie - und insbesondere die Entscheidungsautonomie - dieser Nutzer\*innen. In Anlehnung an die einflussreiche Ansicht von Luciano Floridi (2020) ver-

stehen wir digitale Souveränität als legitime Kontrolle über das Digitale. Darüber hinaus argumentieren wir, dass diese Kontrolle im Falle individueller digitaler Souveränität am besten als Autonomie oder Selbstbestimmung in Bezug auf die digitalen Dimensionen des eigenen Lebens zu verstehen ist (Conradie und Nagel 2022). Um zu untersuchen, wie diese Autonomie durch Wearables beeinträchtigt werden könnte,

haben wir zunächst einen konzeptionellen Überblick über die allgemeine ethische Diskussion um Wearables erstellt, in dem wir moralische Kalküle identifiziert haben, die Entwickler\*innen, Anbieter und Nutzer\*innen solcher Technologien berücksichtigen müssen. Für jedes dieser Kalküle gibt es sowohl moralische Chancen als auch moralische Herausforderungen zu berücksichtigen. Obwohl jedes dieser Kalküle eine eigene ausführliche Diskussion um Abwägungsprozesse zu verschiedenen moralischen Werten, z.B. zu Gerechtigkeit und Wohlergehen, verdient, die wir an anderer Stelle vorgelegt haben (siehe Conradie und Nagel 2022), liegt unser besonderes Augenmerk hier darauf, wie sich diese Technologien auf die Autonomie der Nutzer\*innen auswirken können.

Unsere Fähigkeit, unsere eigenen Entscheidungen zu treffen ist uns wichtig. Diese Selbstbestimmung über unsere Entscheidungen nennen wir Entscheidungsautonomie. Sie ist der moralische Wert, den wir im Folgenden als zentral betrachten werden. Wearables verfügen über drei Eigenschaften, die ihren potenziellen Einfluss auf die Entscheidungsfindung verstärken. Ihre unmittelbare Präsenz am Körper der Nutzer\*innen (Nähe) in Verbindung mit ihrer leichten Zugänglichkeit und Nutzung (Bequemlichkeit) und ihrer Allgegenwart (Ubiquität) machen sie zu idealen Einfallstoren für Eingriffe, die die Autonomie der Nutzer\*innen beeinflussen (Conradie et al. 2022). Wichtig zu bemerken ist, dass wir alle drei Eigenschaften von Wearables erwarten oder sie sogar fordern: Es sind Eigenschaften, die ein exzellentes Wearable haben sollte. Das Fehlen einer dieser Eigenschaften wäre ein Defizit des betreffenden Wearables. Daher können wir davon ausgehen, dass Entwickler\*innen und Anbieter bestrebt sind, genau diese Qualitäten zu liefern. Gerade diese Eigenschaften ermöglichen die moralisch wünschenswerten und moralisch nicht wünschenswerten Möglichkeiten und können daher nicht „wegdesignt“ werden, sondern müssen für jeden einzelnen Fall ausgehandelt werden. Wenn wir die Vorteile wollen, die diese Technologien zweifellos bringen können, müssen wir die Herausforderungen, mit denen sie untrennbar verbunden sind, akzeptieren und uns ernsthaft damit auseinandersetzen. Studien mit Smartphones (die zwar keine Wearables im engeren Sinne sind, aber viele relevante Eigenschaften mit Wearables teilen) haben gezeigt, dass ein Gerät, das sich in unmittelbarer Nähe des\*der Nutzens befindet und für ihn\*sie leicht zugänglich ist, schnell zu einem fast unhinterfragten Teil der täglichen Aktivitäten und Entscheidungen einer Person werden kann (Hamilton und Yao 2018; zur Reflektion siehe Reiner und Nagel 2017). Ein weiterer Hinweis für die Nähe und Allgegenwärtigkeit von Wearables ist, dass sie sehr persönliche und intime Daten sammeln, einschließlich Gesundheits-, Bewegungs- und

Standortdaten. Dies ermöglicht eine Vielzahl nützlicher Eingriffe zur Verbesserung des Lebens einer Person, u.a. auch zur Förderung ihrer Autonomie, weckt jedoch Bedenken hinsichtlich möglicher Verletzungen der Privatsphäre und der Aussicht, dass diese Daten missbraucht werden können, um die Autonomie der Person zu untergraben.

Ein anderer entscheidender Faktor zur Bewertung von Wearables ist die Eigenschaft solcher Systeme, die wir als intelligente Wearables bezeichnen können, den Benutzer\*innen kognitive Entlastung zu erleichtern (Conradie und Nagel 2022). Unter kognitiver Entlastung versteht man die Übertragung der Kontrolle über die Durchführung einer kognitiven Aufgabe oder über das Treffen einer Entscheidung an ein Gerät oder System. Diese Möglichkeit besteht, wenn das Wearable in der Lage ist, Daten zu sammeln und algorithmisch so zu verarbeiten, dass es zielgerichtete und (bisweilen) korrigierende Ergebnisse erzeugen kann. Eine solche Übertragung von Kontrolle kann die - vielleicht überraschende - Folge haben, dass der\*die Nutzer\*in insgesamt mehr Kontrolle über das Erreichen der eigenen Ziele hat (Kohler et al. 2014; Carter 2018). Um dies zu veranschaulichen, betrachten wir das Beispiel eines Tennisspielers, der daran arbeitet, bestimmte Aspekte seines Spiels zur Gewohnheit und schließlich zum Reflex zu machen. Er zielt darauf ab, die Kontrolle über diese Aspekte an seine automatischen Reaktionen abzugeben, um sein übergeordnetes Ziel besser erreichen zu können: den Sieg im Tennisspiel. Als weitere Beispiele, die Wearables involvieren, dient die Berechnung eines optimalen Trainingsplans, die an ein Fitness-Wearable delegiert wird oder die Suche nach dem nächstgelegenen passenden Restaurant über eine Smartwatch. Ausschlaggebend für die in InviDas zentralen Überlegungen zum Datenschutz und zur Datensouveränität ist, dass intelligente Wearables diese kognitive Entlastung, die Nutzende sich wünschen und die sie unterstützen, nur erreichen können, wenn sie in der Lage sind, relevante Daten zu sammeln und zu verarbeiten.

#### MORALISCHE CHANCEN UND BEDENKEN

Wearables können die Entscheidungsautonomie auf vier allgemeine Arten fördern: (1) die Freisetzung kognitiver Kapazitäten, (2) die Bereitstellung von Informationen, (3) die Erweiterung des Handlungsspielraums und (4) das „Nudging“ zu unseren selbstgesetzten Zielen. Die Freisetzung kognitiver Kapazitäten ist selbsterklärend: Durch die Erleichterung der kognitiven Entlastung ermöglicht das Wearable den Nutzenden, sich auf die Tätigkeiten zu konzentrieren, die sie für wertvoller halten, und erhöht die Wahrscheinlichkeit, dass Nutzende Gründe erkennen können, die sie sonst übersehen hätten und, dass sie in der Lage sind, ihre Ziele zu erreichen.

(2) bezieht sich auf die Bereitstellung von Informationen, die sonst nicht zur Verfügung stehen (z.B. genaue Angaben zur Herzfrequenz beim Intervalltraining), so dass Nutzende Überlegungen, die für ihre Ziele relevant sind, besser erkennen können. Mit (3) „Erweiterung des Handlungsspielraums“ ist hier gemeint, dass das Wearable Optionen direkt ermöglicht, die vorher nicht verfügbar waren. Offensichtliche Beispiele hierfür sind Wearables, die zur Unterstützung von Menschen mit eingeschränkter Autonomie eingesetzt werden. Ein gutes Beispiel hierfür ist der Fall von Simon Wheatcroft, einem Langstreckenläufer, der erblindet ist. Er verwendet ein von der Firma WearWorks entwickeltes Wearable, das mit einem GPS-System verbunden ist und über mehrere am Körper getragene Sensoren verfügt, die Bewegungs- und Annäherungsdaten sammeln, die dann verarbeitet werden, um Simon Wheatcroft (oder jedem\* jeder anderen Nutzer\*in) durch haptische Hinweise Orientierung zu geben (Sisson 2017). Dieses Beispiel unterstreicht auch, dass die Auswirkungen, die sowohl moralisch wertvoll als auch nachteilig sein können, für besonders schutzbedürftige Personen wie Menschen mit Behinderungen, Kinder oder ältere Erwachsene besonders bedeutsam sein können (Conradie et al. 2022). Für eine Diskussion von (4) muss zunächst geklärt werden, was unter „Nudging“ zu verstehen ist. Einem\*einer Akteur\*in X in Bezug auf eine Entscheidung Y einen „Schub“ zu geben, bedeutet, die für Y relevante Entscheidungsarchitektur von X so zu verändern, dass eine bevorzugte Wahl gefördert wird, ohne dass Optionen vom Tisch genommen oder neue, z.B. finanzielle Anreize eingeführt werden (Thaler und Sunstein 2009; Felsen, Castelo und Reiner 2013; Moles 2015; Levy 2017). Die Idee hinter einem Nudge ist, dass der\*die Betroffene seine volle Autonomie bei der Entscheidungsfindung behält. Gleichzeitig aber erhöht das Nudging die Wahrscheinlichkeit, dass der\*die Betroffene die vom Nudger intendierte Wahl trifft, die immer auch im angenommenen Interesse der Person sein sollte, die geschubst wird, dem Nudge. Nudges können zur Förderung des Wohlergehens oder zur Unterstützung der Autonomie des Nudgees eingesetzt werden. Solche Nudges können besonders effektiv sein, wenn sie durch Wearables angewendet werden, aufgrund der Eigenschaften der Nähe und der Ubiquität. Eine Smart-Watch, die die Fitnessdaten eines Benutzers oder einer Benutzerin beim Joggen aufzeichnet und anhand dieser Daten vorschlägt, wann der\*die Benutzer\*in eine Pause einlegen sollte, ist ein einfaches Beispiel für ein Wearable, das einen Nudge einsetzt, um den\*die Benutzer\*in davor zu bewahren, sich zu überanstrengen oder eine Krankheit zu verschlimmern. Hier handelt es sich eindeutig um einen Fall, in dem der Stupser dem Wohlbefinden dient, ohne die Autonomie des Nutzers oder der Nutzerin zu verlet-

zen. Aber Nudges können auch besser als autonomie-neutral sein. Sie können in einigen Fällen die Fähigkeit eines Akteurs zur Selbstbestimmung aktiv stärken (Levy 2017). Nehmen wir an, eine Raucherin will ihre Sucht überwinden und kauft zu diesem Zweck ein Gesundheitsgerät, das Nutzende an die Gefahren des Rauchens erinnert und die Warnung vielleicht mit abschreckenden Bildern untermalt, wenn es erkennt, dass die Nutzende raucht. Das Gerät dient dazu, die Autonomie der betreffenden Person zu unterstützen, indem es den Versuch unterstützt, mit dem Rauchen aufzuhören.

Betrachten wir nun die moralischen Herausforderungen oder Risiken: (1) das Risiko der Überauswahl und der Informationsüberflutung, (2) das Risiko Fähigkeiten zu verlieren und abhängig zu werden und (3) die Möglichkeit des „sludging“ und „overnudging“. Die Überauswahl in (1) bezieht sich auf eine Situation, in der die Bereitstellung von vielen Optionen dazu führt, dass Akteur\*innen weniger in der Lage sind, die Option zu wählen, die tatsächlich am besten zu den eigenen Zielen passt. Eine Informationsüberlastung liegt dann vor, wenn die Bereitstellung von zu vielen unnötigen Informationen den gleichen Effekt hat. Es ist daher von entscheidender Bedeutung, dass Designer\*innen von Wearables eine Auswahl relevanter Optionen auf benutzerfreundliche Weise bereitstellen sollten. Außerdem sollten - was für die Arbeit von InviDas direkt relevant ist - Benutzervereinbarungen (eine Umgebung, in der es schnell zu Informationsüberlastung kommt) mehr auf Erklärbarkeit und Benutzerfreundlichkeit als auf reine Transparenz oder die Bereitstellung maximaler Details ausgerichtet sein.

Da es verständliche rechtliche Bedenken auf Seiten der Entwickler\*innen und Anbieter dieser Technologien gibt, können die rechtlichen Details einer solchen Vereinbarung nicht umgangen oder dem Ermessen des Nutzers überlassen werden. Obwohl es für die Verfasser\*innen dieser Vereinbarungen moralische Gründe gibt, sich um Erklärbarkeit zu bemühen, wird dies verständlicherweise nicht ihr einziges Anliegen sein. Es liegt auch in der moralischen Pflicht der Nutzenden, sich über die rechtlichen Einzelheiten der Vereinbarung, die sie eingehen, zu informieren. Zu (2): Eine Möglichkeit, wie die kognitive Entlastung moralisch besorgniserregend sein kann, besteht darin, dass ein\*e Nutzer\*in zu sehr von einem Gerät abhängig wird, so dass seine\*ihre eigenen Fähigkeiten und Entscheidungsmöglichkeiten bis zu einem Punkt verkümmern, an dem seine\*ihre Autonomie bedroht ist. Dies wird oft als „De-Skilling“ bezeichnet (Vallor 2015). Am wahrscheinlichsten ist dies in Situationen, in denen die Nutzung der Technologie unreflektiert oder zur Gewohnheit wird - genau die Gefahr, die durch die Eigenschaften der tragbaren Technologien entsteht, unmittelbar, allgegenwärtig

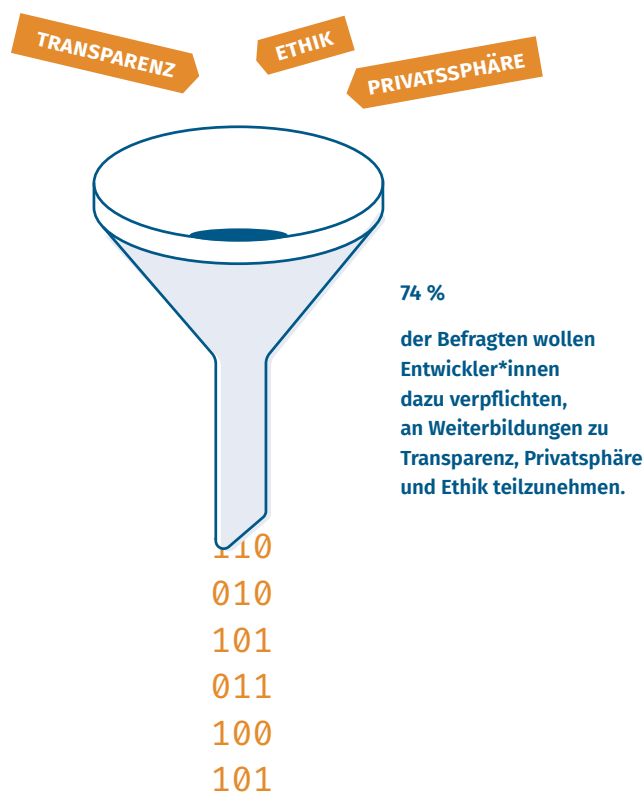


Abbildung 5: Basis: alle Befragten (n = 2000). Angaben in Prozent.  
Frage Q19: Inwiefern stimmen Sie der folgenden Aussage zu?  
Entwickler\*innen von digitalen Technologien sollten verpflichtet sein,  
Kurse und Weiterbildungen zu Transparenz, Privatsphäre und Ethik zu  
absolvieren. © Ipsos | Digital Autonomy Hub<sup>1</sup>

tig und bequem zu sein. Das soll jedoch nicht heißen, dass alle Abhängigkeiten, die sich aus der kognitiven Entlastung ergeben, besorgniserregend sind: Die Abhängigkeit von der Navigationstechnologie ist eine Bereicherung für die Autonomie vieler Menschen, und da diese Systeme (meistens!) ausreichend zuverlässig sind, können wir davon ausgehen, dass sie autonomiefördernd sind. Die wichtigste Erkenntnis ist, dass die Entwickler\*innen von Technologien, die die kognitive Entlastung erleichtern können, gründlich prüfen müssen, ob sie möglicherweise oder sogar wahrscheinlich zu Abhängigkeiten führen. Wenn dies der Fall ist, ist es wichtig, dass die Zuverlässigkeit der Technologie von höchster Qualität ist. Aber selbst, wenn die Zuverlässigkeit kein Problem darstellt, gibt es immer noch einige Abhängigkeiten, die die Entscheidungsautonomie beeinträchtigen können. Wenn

die Abhängigkeit direkt oder indirekt dazu führt, dass eine für die Entscheidungsfindung notwendige Fähigkeit eingeschränkt wird oder verloren geht, haben wir gute Gründe, die Technologie, die diese Abhängigkeit hervorruft, zu überdenken oder sogar abzulehnen.

Und schließlich folgt noch Punkt (3): Der gängigen Konvention folgend, bezeichnen wir Eingriffe, die einen Akteur gegen seine Interessen stupsen, als „Sludges“ (Thaler 2018). Diese Art von Eingriffen kann viele Formen annehmen, wird aber in der Regel mit dem Ziel eingesetzt, den wirtschaftlichen Gewinn auf Kosten der Nutzer\*innen zu steigern. Die Platzierung von teuren, aber ungesunden Süßigkeiten am Ausgang eines Supermarkts ist ein Beispiel für eine Maßnahme, die als Sludge fungieren kann und Kund\*innen zum Kauf dieser Produkte veranlasst, auch wenn dies ihren begründeten Interessen und autonomen Zielen zuwiderläuft. Die Bekämpfung von „Sludges“ lässt sich oft am besten dadurch erreichen, dass die Verbraucher\*innen über ihr Vorhandensein und die Gefahr, die sie darstellen, informiert werden. Das Bewusstsein von einem Nudge oder Sludge ist zwar keine Garantie dafür, kann aber viel dazu beitragen, dass die Menschen sich gegen die möglichen Auswirkungen auf ihre Entscheidungen wehren. Abgesehen von „Sludges“ gibt es zwei weitere Möglichkeiten, wie Nudges die Autonomie untergraben können. Erstens können sich unsere Ziele und Werte oft als sehr endogen erweisen, so dass wir anfällig dafür sind, von unserer eigenen authentischen Selbstbestimmung weggestupst zu werden. Dies gilt vor allem dann, wenn Nudges unter Umgehung unserer deliberativen Fähigkeiten funktionieren (Grüne-Yanoff 2012). Zweitens kann Nudging dazu dienen, die Entwicklung der für die Autonomie notwendigen Fähigkeiten zu verhindern oder zu beeinträchtigen, indem einem Akteur bestimmte unersetzliche Lernerfahrungen genommen werden (Blöser et al. 2010; Niker et al. 2021). Dies kann selbst dann eintreten, wenn der\*die Stupsende die besten Absichten hat, und wird noch verschärft, wenn der\*die Nudgee das Ziel vieler konzertierter Stupsen ist, oder wenn die Quelle des Stupsers unreflektiert in die Entscheidungsfindung der Nudgees integriert wird. Wearables laufen Gefahr, durch ihre Nähe, Allgegenwärtigkeit und Bequemlichkeit genau dies zu bewirken. Eine der besten und einfachsten Möglichkeiten, dieses Risiko zu bekämpfen, besteht darin, die Nutzer\*innen darüber zu informieren, wie sie angestupst werden - oder wie sie angestupst werden könnten. Dies kann wahrscheinlich die Wirksamkeit zumindest einiger Nudges verringern, die oft am besten funktionieren, wenn sie unmerklich bleiben. Diesen Preis sollte man bereit sein zu zahlen, auf der Suche nach einem angemessenen Gleichgewicht, insbesondere in einem kommerziellen Kontext.

## DATENSCHUTZ UND DATENSOUVERÄNITÄT

Wearables sind aufgrund ihrer Nähe, ihrer Ubiquität und ihrer Tendenz zu einer unreflektierten Nutzung in einer besonderen Position, um hochsensible und intime Daten ihrer Nutzer\*innen zu sammeln, vor allem Standortdaten und Gesundheitsdaten. In Anbetracht der technologischen Grenzen ist es unvermeidlich, dass beispielsweise eine Fitnessuhr die gesammelten Daten zur Verarbeitung an ein größeres Netzwerk weitergeben muss, wenn sie die volle intelligente Funktionalität bieten soll. Die physische Uhr allein kann die erforderlichen Rechenleistungen nicht erfüllen. Dies bringt die Nutzer\*innen in eine Lage, in der die Nutzung der Technologie voraussetzt, dass Fakten über Bewegungen, Herzfrequenz und deren Erhöhung bei sportlicher Betätigung, Schlafzyklus und vieles mehr durch mangelnden Datenschutz des verarbeitenden Netzwerks gefährdet sein könnten. Derzeit handelt es sich dabei hauptsächlich um Daten über körperliche Gesundheit, aber es befinden sich Sensortechnologien in Entwicklung, die auch Daten über die geistige Gesundheit eines Nutzers sammeln können (Abdullah und Choudhury 2018). Das bringt uns zu der Bedrohung, die Wearables für die Privatsphäre darstellen können. Obwohl hier als separates moralisches Thema behandelt, sind Fragen um die Privatsphäre immer auch eng mit Fragen um die Verletzung von Autonomie verbunden. Im Allgemeinen finden wir Verletzungen der Privatsphäre problematisch, weil solche dazu führen können, dass (a) jene erlangten Daten dazu verwendet werden, uns oder andere auszunutzen bzw. zu manipulieren, oder (b) die Daten direkt dazu verwendet werden, unser Wohlergehen zu beeinträchtigen (z. B. durch Identitätsdiebstahl oder als ein Opfer von Stalking). Nehmen wir als Beispiel für (a) eine Fitnessuhr, die die Funktion besitzt, den Nutzenden auf der Grundlage der über sie gesammelten Daten Joggingrouten zu erstellen. Wenn die Entwickler\*innen dazu bereit wären, könnte dieses System dazu verwendet werden, die Nutzer\*innen regelmäßig auf Strecken zu führen, an welchen Werbung installiert ist oder gar Geschäfte gelegen sind, die die Nutzer\*innen in ihren Interessen an die der Entwickler\*innen anpassen, ohne dass den Nutzer\*innen dies bewusst gemacht wird. In Bezug auf (b) ist die Bedrohung durch Datenschutzverletzungen bei der Art von intimen medizinischen Daten, die von privaten medizinischen Wearables gesammelt werden, nur allzu offensichtlich. Daher sollte jedes legitime System der digitalen Souveränität die Kontrolle über das Digitale so verteilen, dass die Risiken von Datenschutzverletzungen vermieden werden. Diese Bedingung wird oft durch folgenden Lösungsvorschlag eingelöst: Bedenken hinsichtlich des Schutzes der Privatsphäre können - teilweise oder ganz - ausgeräumt werden, sofern eine an-

gemessene Verteilung der Kontrolle über die Daten und die Systeme, die diese Daten verarbeiten, erreicht werden kann. Die rechtlichen und sozialen Mechanismen, durch die diese Verteilung (zumindest normativ) festgelegt wird, konzentrieren sich weitgehend auf die Benutzervereinbarungen, die mit der Technologie einhergehen. Diese Vereinbarungen sollten grundsätzlich die Grenzen der Kontrolle für Nutzer\*innen, Entwickler\*innen und Anbieter abstecken.

## DIE ROLLE DES INVIDAS-Projekts: FÖRDERUNG DER AUTONOMIE DURCH ERKLÄRBARKEIT

In Anbetracht unserer Untersuchung des Verhältnisses zwischen Wearable-Technologien und individueller digitaler Souveränität, die wir als untrennbar von Überlegungen zur Autonomie betrachten, kann die ethische Rolle des Invidas-Projekts so bestimmt werden: sie soll für eine bessere Erklärbarkeit der Benutzervereinbarungen sorgen, welche die Grenzen der Kontrolle über das Digitale zwischen den verschiedenen beteiligten Parteien festlegen. Dadurch erhält der\*die Nutzer\*in mehr Kontrolle über die Ausgestaltung der Kontrolle selbst. Indem sie den Inhalt dieser Vereinbarungen spielerisch oder auf andere Weise erklärbar und nutzbar macht, erhöht die Datenschutzlotsin-Plattform die Wahrscheinlichkeit einerseits, dass Informationen bereitgestellt werden können, ohne dass eine Überauswahl droht, und andererseits, dass kognitive Kapazitäten freigesetzt werden können, während gleichzeitig die Risiken des De-Skilling und erhöhter Abhängigkeit verringert werden. Indem den Nutzer\*innen mehr Einblick in die Art und Weise gegeben wird, wie diese Technologien ihre Nutzer\*innen beeinflussen können, lassen sich zudem Sludges und übermäßiger Nudging-Einfluss vermeiden. Und letztlich stellt die Erklärbarkeit der Nutzervereinbarung ein mögliches Bollwerk gegen Verletzungen der Privatsphäre verschiedener Art dar, indem sie dem\*der Nutzer\*in ein größeres Bewusstsein dafür vermittelt, welche Daten zu welchem Zweck gesammelt werden oder werden können und das genau auf eine solche Art und Weise, die die Nutzer\*innen verstehen und nutzen können – was ihnen wiederum mehr Kontrolle und Wissen, die Bausteine für Autonomie, an die Hand gibt.

<sup>1</sup> Mensch und Technik in Interaktion. Wie gelingt individuelle digitale Souveränität?, *Gesellschaft für Informatik | Digital Autonomy Hub*, 2021, <https://digitalautonomy.net/studie>





Ob Smartwatch oder Datenbrille: Je intelligenter Wearables werden, desto größer ist die Rolle, die sie für unsere Lebens- und Arbeitswelt – und zum Teil auch für unser Verhalten – spielen können. Die Aachener Diskussionsplattform DenkfabrikEthik und InviDas luden im Juni 2022 zu „Digital Autonomy + Smart Wearables“ ins Einstein Center Digital Future nach Berlin und zur Onlineteilnahme ein um das Thema aus den Perspektiven der Technikethik, des Datenschutzes und der Designforschung zu beleuchten.

Unterstützt wurde die Veranstaltung vom Weizenbaum-Institut für die vernetzte Gesellschaft und dem Einstein Center Digital Future.

VON OBEN NACH UNTEN Saskia Nagel (RWTH Aachen), Rebecca Caldwell (Garmin), Florian Conradi und Michelle Christensen (Weizenbaum-Institut)





Aufzeichnungen der Talks und der Podiumsdiskussion sind auf <https://invidas.gi.de/denkfabrethik> zu finden.

RECHTS Tobi Müller (Moderation) und Elisabeth Schauermann (Gesellschaft für Informatik)



VON LINKS NACH RECHTS: Tobi Müller (Moderation), Rebecca Caldwell (Garmin), Michelle Christensen (Weizenbaum-Institut), Saskia Nagel (RWTH Aachen), Gesche Joost (Universität der Künste Berlin/Weizenbaum-Institut)

# SICHERE UND DATENSCHUTZ- FREUNDLICHE UMSETZUNG DER PLATTFORM

RALF GUNDELACH, DOMINIK HERRMANN, OTTO-FRIEDRICH-UNIVERSITÄT BAMBERG

## **BENUTZBARKEIT VERSUS SICHERHEIT**

Eine der größten sicherheitstechnischen Herausforderungen bei der Entwicklung der InviDas-Plattform bestand darin, die richtige Balance zwischen Benutzerfreundlichkeit und Sicherheit zu finden. Dieser „Usability Security Tradeoff“ betrifft grundsätzlich alle Anwendungssysteme.

Einerseits ist ein hohes Maß an Sicherheit erforderlich, um vertrauliche Daten zu schützen und unbefugten Zugriff zu verhindern. Andererseits müssen die Systeme benutzerfreundlich und einfach zu bedienen sein, damit die Anwenderinnen und Anwender nicht durch komplizierte Sicherheitsmechanismen verwirrt oder frustriert werden.

Ein häufig zitiertes Beispiel für diesen Kompromiss betrifft die Passwortsicherheit. In der InviDas-Plattform wurden für den Herstellerlogin Passwörter zur Authentifizierung gewählt, da diese nach dem aktuellen Erkenntnisstand den besten Kompromiss zwischen Benutzbarkeit,

Sicherheit und Betriebbarkeit (sowohl hinsichtlich der Einrichtung als auch des laufenden Betriebs eines Authentifizierungsmechanismus auf Server- und Benutzer\*innen-seite) darstellen. Auf strenge Passwortrichtlinien wird im Interesse der besseren Benutzbarkeit verzichtet, da diese dazu führen können, dass Anwenderinnen und Anwender frustriert sind und von der Nutzung komplett absehen.

Eine verbreitete Strategie besteht darin, Passwörter auf mehreren Seiten wiederzuverwenden, was im Falle eines Datenlecks zur Kompromittierung mehrerer Accounts führen kann. Unabhängig davon sind strenge Vorgaben hinsichtlich der Anzahl von Großbuchstaben, Ziffern und Sonderzeichen wenig effektiv. Viele Nutzerinnen und Nutzer minimieren den Aufwand für die Passwortwahl. Sie erzeugen Passwörter, die den Anforderungen gerade noch genügen, jedoch unsicher sind. Diese Erkenntnisse sind seit mehr als zwanzig Jahren bekannt, haben aber

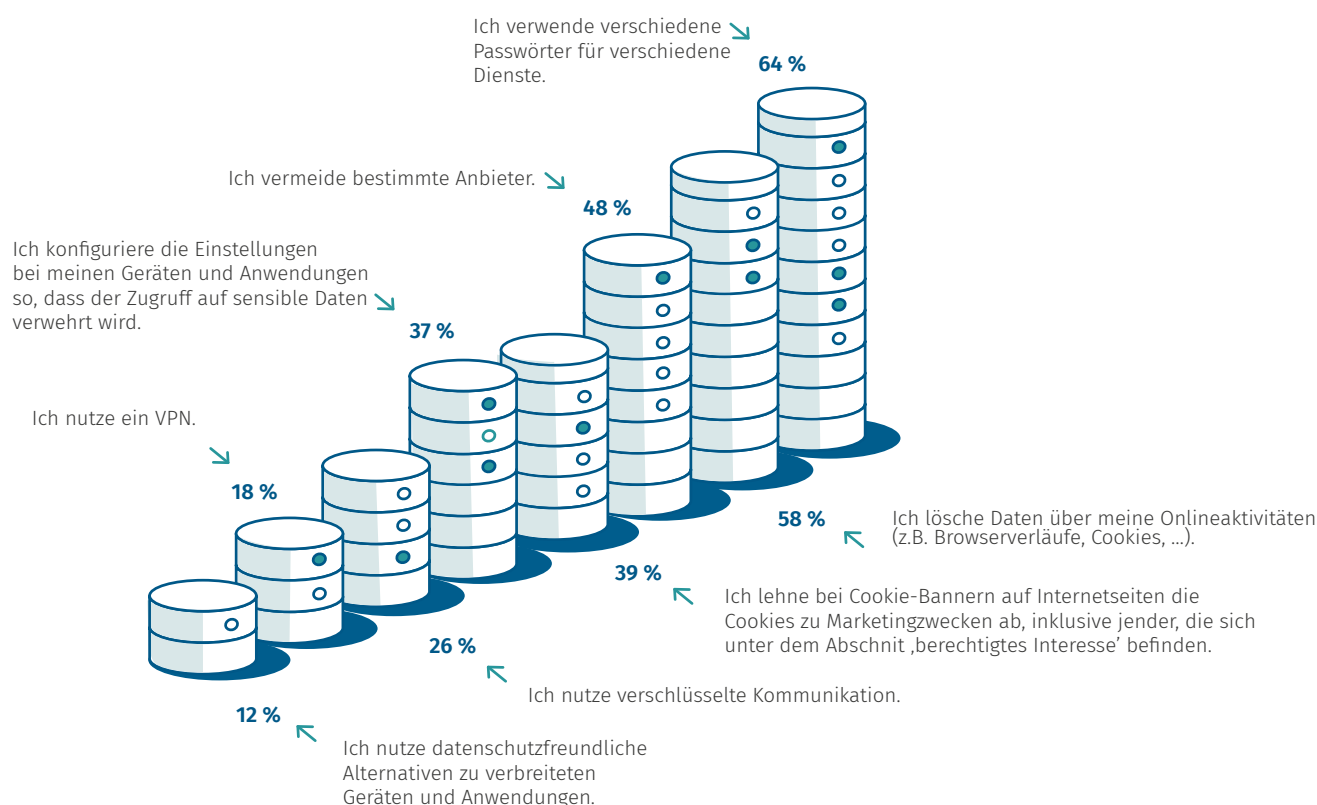


Abbildung 6: Basis: Befragte, die Maßnahmen zum Schutz ihrer Daten umsetzen (n = 1960). Angaben in Prozent.  
Frage Q15: Welche Maßnahmen treffen Sie, um Ihre Daten zu schützen? © Ipsos | Digital Autonomy Hub¹

erst vor einigen Jahren Eingang in die gängigen Standards des NIST (National Institute of Standards and Technology, USA) und des BSI (Bundesamt für Sicherheit in der Informationstechnik, Deutschland) gefunden.

Für eine Anbindung von Garmin Wearables an die InviDas-Plattform, die für die Zukunft geplant ist, wurde der Standard OAuth gewählt. Dieses Verfahren bietet sich an, da Nutzer\*innen, die auf die Daten ihres Wearables zugreifen möchten, in der Regel bereits einen Account bei Garmin besitzen. Durch eine OAuth-basierte Anmeldung werden auf der InviDas-Plattform keine zusätzlichen Zugangsdaten benötigt und es kann auf die bei Garmin bereits vorhandenen Sicherheitsmechanismen zurückgegriffen werden. Dadurch sind die Hürden für die Nutzung der InviDas-Plattform niedrig und der Anteil der sicherheitskritischen Programmlogik auf der Plattform bleibt klein.

### VERSCHLÜSSELUNG, AUTORISIERUNGSKONZEPT, GRANULARITÄT UND ANONYMISIERUNG

Die Softwareentwicklung und Sicherheitsbewertung der InviDas-Plattform erfolgte anhand gängiger Sicherheitsstandards und -empfehlungen, die in einem Leitfaden mit Checklisten zusammengeführt wurden. Dabei wurden verbreitete sicherheitstechnische Fallstricke berücksichtigt, etwa die Auswahl sicherer Algorithmen für die Verschlüsselung und die korrekte Verwendung von Zufallszahlen für deren Initialisierung.

Die Verwendung von Standardbibliotheken schützt nicht unbedingt vor Fehlern, da deren Dokumentation oft nur Beispiele für einfache Problemstellungen enthält. Anhand der Beispiele wird zwar klar, wie eine Bibliothek grundsätzlich zu verwenden ist; es ist aber nicht ausgeschlossen, dass bei der Integration in ein Projekt Implementierungsfehler geschehen.

Ein weiteres Problemfeld ist die korrekte Vergabe von Berechtigungen und deren Einhaltung. Das Framework, auf dem die InviDas-Plattform basiert, verwendet dazu ein RBAC-Konzept, also „Role-Based Access Control“. Mittels RBAC werden Anwenderinnen und Anwendern je nach zugewiesener Rolle vordefinierte Rechte zugewiesen. Die Zuweisung erfolgt durch Annotation an den jeweiligen API-Endpunkten. Damit wird einerseits sichergestellt, dass es keine Inkonsistenzen bei der Definition der Berechtigungen gibt, andererseits erfolgt eine Dokumentation des Zugriffskonzepts an Ort und Stelle.

Im Rahmen einer Literaturrecherche wurde untersucht, welche Daten Wearables erfassen und welche Rückschlüsse daraus auf die Person gezogen werden können. Häufig verbauten Sensoren wie Schrittzähler, Gyroskope und Beschleunigungssensoren erlauben unter bestimmten Umständen Rückschlüsse auf die Gewohnheiten einer Person. Studien haben zudem gezeigt, dass sich viele Nutzerinnen und Nutzer dieser Tatsache nicht bewusst sind und eine falsche Vorstellung davon haben, welche Daten ihr Wearable sammelt und welche Informationen sich daraus über sie ableiten lassen. Unter diesem Gesichtspunkt stellt sich die Frage, inwiefern eine informierte Einwilligung im Sinne der DSGVO überhaupt möglich ist, wenn den Nutzerinnen und Nutzern offensichtlich nicht klar ist, wozu genau sie ihre Einwilligung geben.

Die Datenschutzlotsin kann diese Lücke schließen, indem sie den Nutzerinnen und Nutzern klar und ansprechend aufzeigt, welche Daten zu welchem Zweck erhoben werden. Darüber hinaus wurden Überlegungen angestellt, wie bestimmte Daten genutzt werden können ohne die Privatsphäre der Wearable-Nutzerinnen und -Nutzer zu verletzen.

Ein gängiges Verfahren zum Schutz von Individuen ist das Konzept der k-Anonymität. Dabei werden so viele Attribute eines Datensatzes entfernt oder verallgemeinert (z.B. durch Angabe einer Spanne statt des tatsächlichen Alters einer Person), dass es noch  $k-1$  andere Einträge im Datensatz mit den gleichen Attributwerten gibt. Dadurch ist es nicht mehr möglich einen Eintrag direkt einer Person zuzuordnen, wenn der Datensatz z.B. für Forschungszwecke veröffentlicht wird.

Eine noch höhere Sicherheit kann durch Systeme erreicht werden, die das Konzept der „Differential Privacy“ umsetzen. Eine mögliche Implementation dieses Konzepts sieht vor, die sensiblen Daten nicht als Datensatz herauszugeben, sondern nur über eine Schnittstelle, bei deren Abfrage jeweils ein Zufallswert hinzuaddiert wird. Damit können die Daten zwar noch für statistische Auswertungen verwendet werden, Rückschlüsse auf eine Person sind aber – bei ausreichend starkem Rauschen – nicht mehr möglich.

## KOMPLEXITÄT ALS BEDROHUNG

Eine wichtige Erkenntnis im „Security Engineering“ besteht darin, dass eine hohe Komplexität von Systemen deren Sicherheit gefährdet. Komplexität erhöht die Anzahl der Fehlerquellen und erschwert es, das Gesamtsystem zu verstehen und sicherheitsrelevante Schwachstellen in einem System zu erkennen und zu beheben.

Die InviDas-Plattform adressiert dieses Problem, indem sie lediglich eine minimale REST-API zur Verfügung stellt. Die klar strukturierte Software-Architektur und die Verwendung eines verbreiteten Frontend-Frameworks (Angular) und gängiger JWT-basierter Authentifizierungsmechanismen reduzieren die Angriffsfläche und machen es den Betreibenden der Plattform leichter, die einzelnen Komponenten aktuell zu halten.

## FAZIT

Bei der Entwicklung der InviDas-Plattform wurde das Ziel verfolgt, einen guten Kompromiss aus Benutzerfreundlichkeit und Informationssicherheit umzusetzen. Hierzu wurde ein Sicherheitskonzept bestehend aus Empfehlungen und Checklisten für Sicherheits- und Datenschutzaspekte entwickelt. Wird die Plattform zukünftig so erweitert, dass dort auch Daten von Wearables durch Nutzende erfasst und verarbeitet werden, müssen die Überlegungen zum angemessenen Schutz personenbezogener Daten mittels Anonymisierung weiterverfolgt werden.

---

<sup>1</sup> Mensch und Technik in Interaktion. Wie gelingt individuelle digitale Souveränität?, *Gesellschaft für Informatik | Digital Autonomy Hub*, 2021, <https://digitalautonomy.net/studie>



# DER WERT VON TRANSPARENTEM DATENSCHUTZ

MANUEL FEHLER, JOHANNES ANGENVOORT, GARMIN WÜRZBURG GMBH

Für Garmin ist der Schutz der Privatsphäre und der Kundendaten von höchster Bedeutung. Als Verarbeiter von personenbezogenen Daten, insbesondere sensibler Daten wie geografischer Position oder Gesundheitsdaten und Körpermetriken, hat Garmin ein effektives Datenschutzprogramm implementiert. Herausfordernd ist es jedoch, die komplexe europäische Datenschutzgrundverordnung sowie die Art der Verarbeitung von Kundendaten – insbesondere im Bereich der Analyse von Fitnessparametern – einfach und verständlich darzustellen. Um hier neue Ansätze zu verfolgen, hat sich Garmin an dem Verbundprojekt InviDas beteiligt.

Das InviDas-Projekt bestätigt, dass Endverbraucher\*innen eine solche klare und leicht verständliche Erklärung des Datenschutzes benötigen, da die Zustimmung zur Datennutzung oftmals für Verunsicherung sorgt. Durch die einfache Vermittlung dieser komplexen Zusammenhänge können eventuelle Bedenken beseitigt werden und letztlich ein höheres Maß an Akzeptanz in der Nutzung der Garmin Geräte erlangt werden.

Auch im Umgang mit B2B-Partnern und Aufsichtsbehörden bringt dieser Ansatz Vorteile mit sich, da die Transparenz bezüglich Privatsphäre und Datenschutz eine schnellere Realisierung neuer Geschäftsmodelle wie auch das schnelle Beantworten von Datenschutzanfragen ermöglicht.

Die lückenlose und barrierefreie Integration von Datenschutz-Serviceportalen wie InviDas in das Gesamtsystem ist dabei für Garmin essenziell. Typische Garmin Kund\*innen bewegen sich häufig zwischen ein oder mehreren Geräten – der Garmin App auf dem Smartphone und Funktionalitäten im Garmin Web Portal. InviDas bietet ein „Privacy by Design“-System und damit die Basis, ein Portal bzw. eine Komponente in ein bestehendes Ökosystem einzubetten. Geboten werden verschiedene Möglichkeiten zur Darstellung von komplexen Zusammenhängen. Von Garmin wird das System als wichtiger Baustein zur ständigen Entwicklung und Verbesserung der eigenen Produkte gesehen.

Nutzer\*innen bietet diese Ansicht von Beginn an bzw. bereits vor dem Erwerb des Produkts eine klare Übersicht über die Datenhoheit. Die Art und der Umfang der Datenverarbeitung werden transparent abgebildet, wie auch die Maßnahmen, die ergriffen werden, um diese Daten zu schützen. Aufgrund verschiedener Präferenzen und Erwartungen der Nutzer\*innen bezüglich der Darstellung komplexer Sachverhalte ist eine entsprechende Skalierbarkeit des Systems notwendig, um eine Vielzahl unterschiedlicher Nutzeransprüche gleichermaßen zu adressieren.

#### **ANFORDERUNGEN AN DAS INVIDAS-SYSTEM**

Um letztlich sowohl für Endkonsument\*innen als auch Firmen in der Nutzung zu überzeugen, sieht Garmin die folgenden Punkte als Anforderungen an das InviDas-System:

Das aus Sicht von Garmin wichtigste Ziel von InviDas im Hinblick auf Endkund\*innen besteht darin, die Komplexität von Datenschutzvereinbarungen deutlich zu reduzieren und so zu ermöglichen, dass sich auch rechtliche Laien in einem ausreichend begrenztem zeitlichen und inhaltlichen Rahmen mit einer Datenschutzerklärung auseinandersetzen. Das fertige InviDas-System muss daher als wertvolle und zeitsparende Alternative zur klassischen Datenschutzvereinbarung wahrgenommen werden und einen Mittelweg zwischen „zeitaufwändigem, genauem Lesen einer Datenschutzvereinbarung“ und „Überspringen der Datenschutzvereinbarung“ darstellen. Es ist zu erwarten, dass InviDas akzeptiert wird, wenn Endkund\*innen durch die Plattform ein potenziell vorhandenes Misstrauensgefühl aufgrund fehlenden Verständnisses der Datenschutzsituation in Verständnis und das Begreifen der Datenschutzsituation umwandeln können. Wird das Ziel der leichten inhaltlichen Verständlichkeit von Datenschutzerklärungen erreicht, so wird ein einfacher und schneller Vergleich verschiedener Hersteller bzgl. ihrer Datenschutzerklärungen ermöglicht. Kund\*innen fühlen sich so zu einer informierten Kaufentscheidung befugt und folglich wird das Vertrauen in das Produkt gestärkt.

Aus Firmensicht bietet InviDas, vor allem den Unternehmen, die als erste am System teilnehmen, die Chance, sich durch kundenfreundlichen Datenschutz von der Konkurrenz zu differenzieren und dadurch einen Wettbewerbsvorteil zu erlangen. Wird in InviDas auch mittel- und langfristig ein signifikanter Zugewinn an Transparenz beim Datenschutz gesehen und Produkte/Hersteller bevorzugt, die auf InviDas verfügbar sind, würde die Nicht-Teilnahme an der Plattform einen Geschäftsnachteil für Firmen darstellen. Entscheidend ist jedoch, dass der Aufwand und die Kosten für Firmen bei der Teilnahme an InviDas angemessen sind und in einem guten Verhältnis zum wirtschaftlichen Nutzen stehen.

#### **POTENZIELLE NUTZUNG BEI GARMIN – AUSBLICK**

Wird sich die Weiterentwicklung und Auswertung des InviDas-Ansatzes als erfolgsversprechend zeigen, wird Garmin das System oder Teile davon in sein Ökosystem integrieren. Vorrangig geht es darum, den Kund\*innen das Thema Datenschutz und Privatsphäre so transparent und umfassend wie möglich nahezubringen und nicht darum, unmittelbar höhere Umsätze zu erzielen. Eine wirtschaftliche Einordnung ist daher nur allenfalls indirekt möglich. Zwar ist davon auszugehen, dass Konsument\*innen mit starkem Vorbehalt gegenüber der Verarbeitung ihrer sensiblen Daten durch den InviDas-Ansatz eingefangen werden können, wie viel Prozent Produkte dadurch mehr verkauft werden würden, kann jedoch nur schwer prognostiziert werden. Viel mehr sieht es Garmin als selbstverständliche Verpflichtung an, seine Produkte ständig weiterzuentwickeln und damit einhergehend auch die gesamte Customer Journey zu optimieren. Hierfür würde InviDas mit der verständlichen Darstellung komplexer Datenschutzvereinbarungen einen wichtigen Beitrag leisten.

GEFÖRDERT VON



Bundesministerium  
für Bildung  
und Forschung

INVIDAS IST TEIL DES DIGITAL AUTONOMY HUB

Das Kompetenzzentrum Digital Autonomy Hub koordiniert ein Netzwerk von Forschungsprojekten. Das gemeinsame Ziel ist es, die individuelle digitale Souveränität zu stärken und allen Menschen einen reflektierten und selbstbestimmten Umgang mit ihren Daten zu ermöglichen.



Digital  
Autonomy Hub

PARTNER



GESELLSCHAFT  
FÜR INFORMATIK



stiftung  
digitale  
chancen

GARMIN®

Otto-Friedrich-Universität Bamberg



Universität Bremen



RWTH AACHEN  
UNIVERSITY



Institut für  
Arbeitswissenschaft

RWTH AACHEN  
UNIVERSITY



RWTH AACHEN  
UNIVERSITY

---

INVIDAS — INTERAKTIVE, VISUELLE DATENRÄUME  
ZUR SOUVERÄNEN, DATENSCHUTZRECHTLICHEN  
ENTSCHEIDUNGSFINDUNG