MODERN RE 2023
10. — 12. Oktober 2023 2-tägige Konferenz in Leipzig
summit

Usable Privacy:

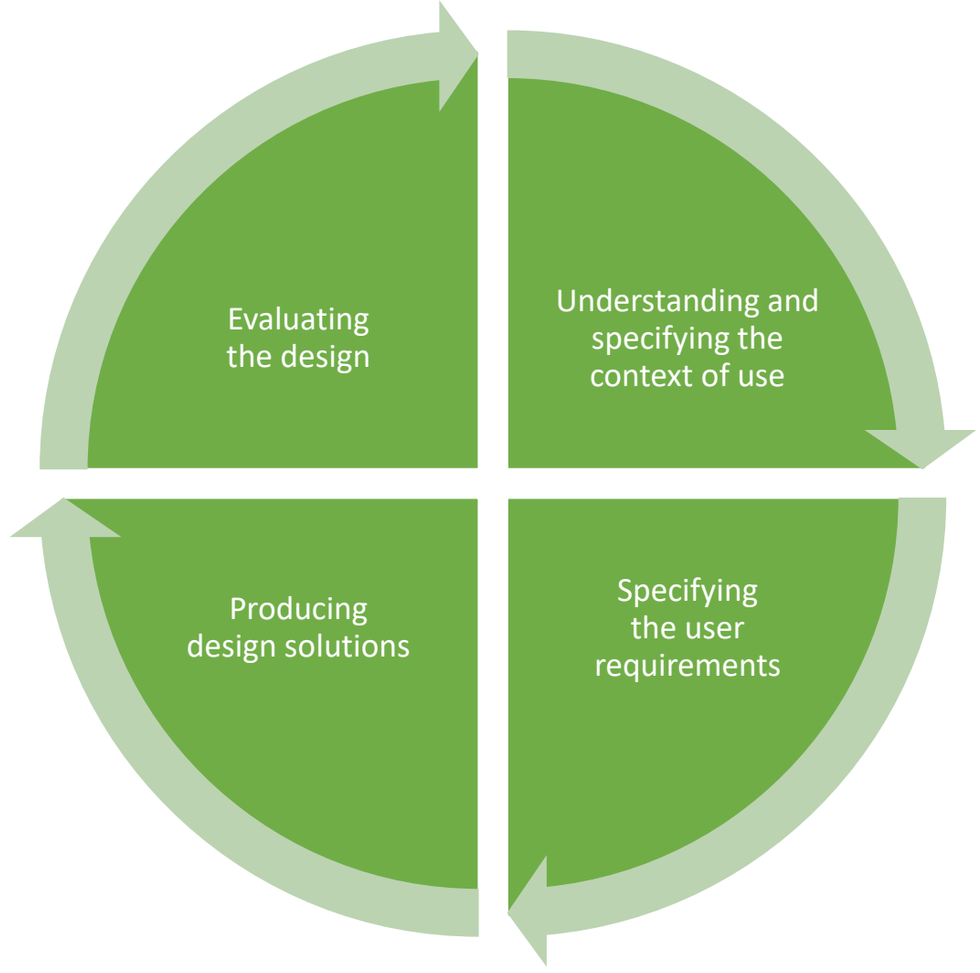
Wie RE-Methoden angepasst werden können, um benutzerfreundlichen Datenschutz zu erreichen

GEFÖRDERT VOM
Bundesministerium für Bildung und Forschung

Hartmut Schmitt
HK Business Solutions

Sven Storck
Fraunhofer IESE

Human-Centered Design-Prozess



Eigene Darstellung basierend auf ISO 9241-210

Benutzergruppenprofile und Privacy-Personas

Benutzergruppenprofile

- Einstellungen, Überzeugungen und Verhaltensweisen der Nutzer*innen
- genaueres Bild derjenigen Stakeholdergruppen, die direkt mit dem System interagieren

- Betroffene Personen – Personen, die personenbezogene Daten verarbeiten
- Nutzer*innen von Privacy & Security Tools[1]
- Nutzer*innen von Internetdiensten[2]

[1]Dupree, Lank & Berry (2018): A case study of using Grounded Analysis as a Requirement Engineering method

[2]Deutschland sicher im Netz (2023): DsiN-Sicherheitsindex 2023

Privacy Personas

- einzelne fiktive Personen
- wichtige Eigenschaften/Details der Benutzergruppe, insbesondere Aspekte des Nutzerverhaltens
- sorgen für besseres Verständnis

- unterschiedliche Datenschutzbedürfnisse der Nutzer*innen
- unterschiedlicher Umgang mit personenbezogenen Daten
- Vorlagen, Beispiele, Workshop-formate, die bei der Erstellung unterstützen[1]

[1] Groen, E. C. et al.: Achieving usable security and privacy through Human-Centered Design. In: N. Gerber et al. (Eds.): Human Factors in Privacy Research. Springer

Vorname, Name

Alter: x Jahre

Tätigkeit: …

Persönliche Werte:

- Beispieltext

Zitat bzw. Motto

Persönliche/berufliche Situation:

Beispieltext

Persönlichkeit:

introvertiert	extrovertiert
rational	intuitiv
sorgfältig	nachlässig
misstrauisch	vertrauensvoll

Einstellung:

Privatheit	Datenpreisgabe
Vertrauen zum Broker	
Vertrauen zum Provider	
Eigenverantwortlichkeit	
Selbstvertrauen	

Wissen & Fähigkeiten:

- Wissen über Datenschutz
- Verständnis der Konsequenzen
- Verständnis der Risiken
- Wissen über Datenverwendung
- Fähigkeiten Datenschutzmaßnahmen anzuwenden

Gewohnheiten:

- Privatsphäreeinstellungen nutzen
- Datenschutzerklärung lesen
- Consent-Management Tools nutzen

Frank Nußbaum (fatalistische Nutzer:innen)

Alter: 21 Jahre

Tätigkeit: KfZ-Mechatroniker

Persönliche Werte:

- Einfacher Nutzen ist wichtiger als Auseinandersetzung mit Datenschutzeinstellungen.
- Wissen bzgl. Datenschutz ist vorhanden, aber das Vertrauen in die Umsetzung ist nicht gegeben.

„Gefahren gibt es überall, bringt doch eh alles nichts!“

Persönliche/berufliche Situation:

Frank hat nach Abschluss der mittleren Reife eine Ausbildung zum KfZ-Mechatroniker abgeschlossen und arbeitet nun in einer kleinen freien Autowerkstatt. Obwohl sein Beruf viel mit Technik in Form von Sensoren und Regelprogrammen im Kontext von Fahrzeugen zu tun hat, ist er beruflich nicht auf digitale Dienstleister oder Online-Plattformen angewiesen. Die Computer in der Werkstatt dienen in erster Linie dem Auslesen von Fahrzeuginformationen und dem Zugriff auf nicht öffentliche Datenbanken von Herstellern oder Lieferanten.
In seiner Freizeit bastelt er gern an seinem Kleinwagen, den er immer wieder sportlichen Umbauten unterzieht. Um passende Ersatz- und Anbauteile günstig zu erhalten, ist er auf verschiedenen Online-Plattformen angemeldet und durchsucht diese regelmäßig nach entsprechendem Tuning-Zubehör.
In seiner Community ist man generell offen und tauscht sich gerne aus. Damit dies gut möglich ist, hinterlässt er in vielen Profilen auch seine privaten Kontaktdaten. Immerhin ist sein Fachwissen als KfZ-Mechatronik häufig gefragt, während er gleichzeitig mit seinem Wissen über die sportliche Modifikation von Fahrzeugen auch gern in diesen Kreisen öffentlich auftritt.

Persönlichkeitsmerkmale:

introvertiert	extrovertiert
rational	intuitiv
sorgfältig	nachlässig
misstrauisch	vertrauensvoll

Fokus: Einstellung & Verhalten

Auch wenn er in seiner Freizeit regelmäßig digitale Plattformen besucht und nutzt, was konkret mit seinen persönlichen Daten im digitalen Ökosystem geschieht, ist ihm nicht klar. Aber er hat auch kein großes Interesse daran, sich tiefer mit der Thematik auseinanderzusetzen. Für ihn steht der **Nutzen und die Bequemlichkeit im Vordergrund**. Wenn ihm eine Plattform nicht seriös vorkommt oder sein Vertrauen verloren geht, schränkt er die Nutzung lieber ein oder verzichtet gänzlich darauf.

Fokus: Wissen & Fähigkeiten im Datenschutz:

Frank sieht sich selbst als **Amateur im Bereich Datenschutz** und Datensouveränität. Er hört immer wieder von verschiedenen Vorfällen und erhält auch selbst Phishing-Mails. Jedoch tut er diese als „leicht erkennbar“ ab und sieht keinen Grund dafür, sich auf dem Themengebiet neues Wissen anzueignen. Grundlegend geht er davon aus, dass regelmäßige Updates sowie ein Spam-Filter als Vorsorge ausreichend sind. Alles Weitere ist vertane Zeit, da es immer einen Weg gibt, wenn jemand an die Daten will.

Fokus: Gewohnheiten

Wenn Frank auf digitalen Plattformen bzw. digitalen Ökosystemen unterwegs ist, steht für ihn der **Nutzen klar im Fokus**. Beim Anmelden werden die **Datenschutzbestimmungen schnell abgehakt und übersprungen**, um mit dem neuen Profil aktiv zu werden. Wenn es Einstellmöglichkeiten gibt, werden meist nur die vorgeschlagenen Einstellungen übernommen. Lediglich bei privaten Daten, die für ihn ein größeres Risiko bergen, wie zum Beispiel Bank- bzw. Kontodaten, reagiert er misstrauisch.

Bedarfe hinsichtlich des Datenschutzes

Eine neue Art von Anforderung

- Definition gemäß IREB: „Eine **Benutzeranforderung** ist ein von einem Stakeholder wahrgenommener **Bedarf**.“
  - *Was* soll **die Software** machen? (funktionale Anforderung)
  - *Wie* gut soll **die Software** dies machen? (Qualitätsanforderung)

Wie ist es mit Bedarfen, die sich **nicht auf eine konkrete Software beziehen**, d. h. allgemeingültiger und abstrakter sind?

Bedarfe: anders als andere Anforderungen

- „Usable Privacy“-Aspekte lassen sich schlecht als Anforderung dokumentieren.
  - zu unspezifisch:
    „Das System sollte die Privatheit der Benutzer schützen.“
  - zu lösungsorientiert:
    „Beim Login des Nutzers, sollte das System diese Aktionen durchführen: …“

Bedarfe als Anforderungsart:

Usable-Privacy-Lösungen werden meist entworfen, um abstrakte Bedarfe von Datennutzern & Betroffenen zu erfüllen

Definition: Bedarfe hinsichtlich Datenschutz

„Ein **Bedarf** ist ein **geäußertes Ziel** einer *betroffenen Person* oder eines *Datennutzers* im Hinblick auf die Verarbeitung *personenbezogener Daten*.“

- Bedeutet: Bedarfe können (anders als Anforderungen) nicht direkt in technische oder organisatorische Maßnahmen, Softwarefunktionen bzw. -qualitäten umgesetzt werden.

Wie werden Bedarfe erhoben?

- Workshops für Datennutzer und Betroffene
  - Analyse der wichtigsten Datenklassen (Konkretisierung des Kontextes)
  - Abfrage der Bedarfe durch Leitfragen
- Zeitpunkt
  - Frühe Projektphasen: allgemeine Erhebung, Wiederverwendung existierender Bedarfe
  - Wenn die Projektziele definiert sind: szenarienbasierte Erhebung

Die fünf Datenschutzbedarfe (1/2)

Privatheitsbedarfe *(der Betroffenen)*

Transparenzbedarf: *verständliche Informationen und Offenheit über Datenverarbeitung*

Leitfrage: Was möchten Sie als Betroffener bzgl. der Sammlung, Verarbeitung oder Verwendung dieser Daten wissen?

Selbstbestimmungsbedarf: *autonome Kontrolle über die Datenverarbeitung*

Leitfrage: Welche Bedarfe haben Sie als Betroffener bzgl. Ihrer Selbstbestimmung hinsichtlich ihrer Daten?

Schutzbedarf: *Sicherstellung Datenschutz, insb. Vorbeugung Datenschutzverletzungen*

Leitfrage: Welche Bedarfe haben Sie als Betroffener bzgl. des Schutzes dieser Daten?

Die fünf Datenschutzbedarfe (1/2)

Verarbeitungsbedarfe *(der Datennutzer)*

Datennutzungsbedarf: *Verarbeitung bestimmter Daten zu einem bestimmten Zweck*

Leitfrage: Welche Bedarfe haben Sie als Datennutzer bzgl. der Verarbeitung dieser Daten?

Informationsbedarf zur Datennutzung: *Wissen über Verordnungen, um rechtskonform zu sein*

Leitfrage: Welche Bedarfe haben Sie als Datennutzer bzgl. Informationen zur rechtskonformen Verarbeitung der Daten?

Wie dokumentiert man Bedarfe?

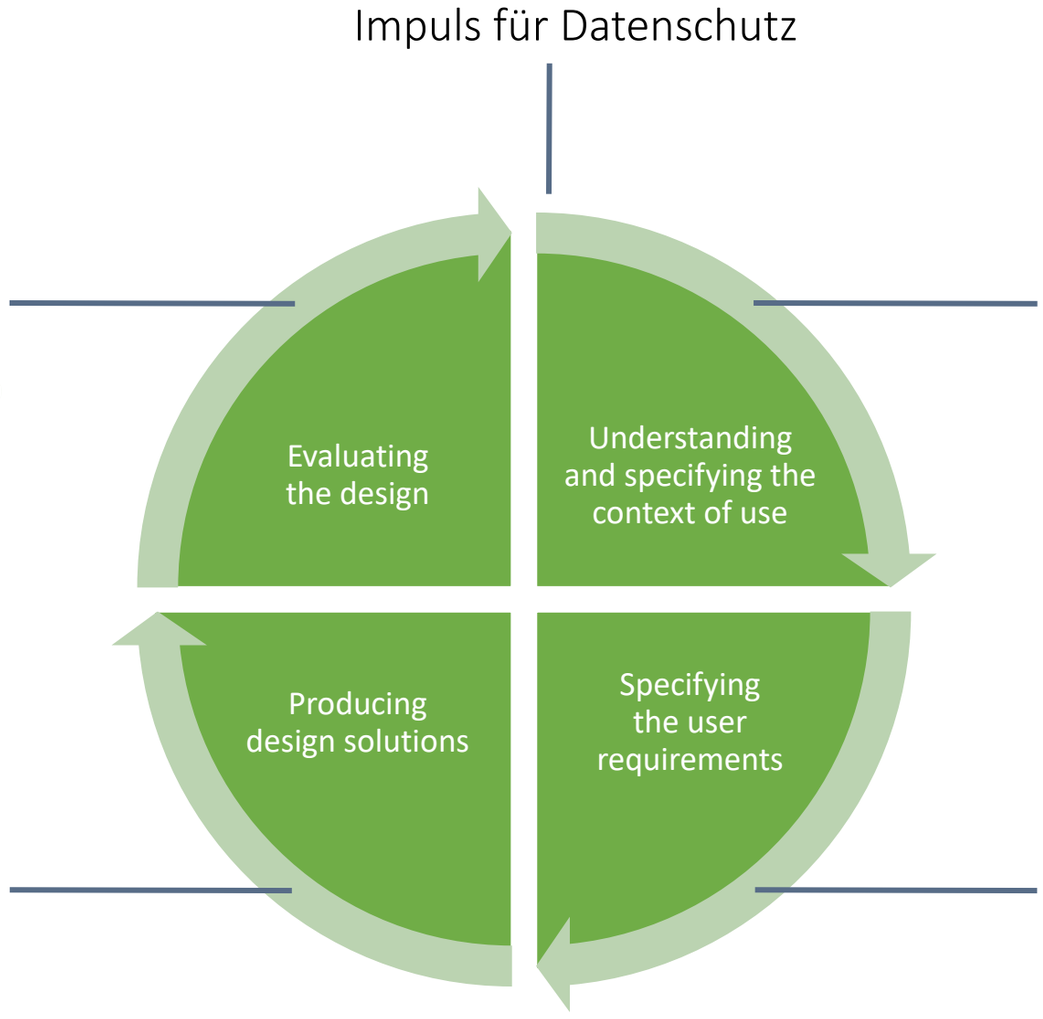
Notationsschablone für Wünsche, Erwartungen der Benutzergruppen:

„Als <Benutzergruppe> möchte ich <Bedarf>, damit <Begründung>.“

Wie analysiert man Bedarfe?

- Priorisierung nach Projektrelevanz
- Juristische Bewertungen steigern die Rechtsgültigkeit, insbesondere bei sich widersprechenden Bedarfe.
- Abgleich mit den erhobenen Benutzer-/Systemanforderungen steigert Effektivität der Datenschutzmaßnahmen.
  - Sicherstellung der Bedarfe der Stakeholder

RE und Datenschutz im Human-Centered Design



- Zu verarbeitende personenbezogene Daten auswählen
- Qualitätsmodell verwenden, z. B. Datenschutz als Qualitätsmerkmal[1]
- Relevante Stakeholdereigenschaften sammeln und dokumentieren

[1]Schmitt & Groen (2021): Qualitätsmodell zur Förderung des Beschäftigtendatenschutzes

- Bedarfe erheben
- Datenschutzanforderungen, Ziele und Aufgaben ableiten
- Personas ergänzen

- Entwurfsentscheidungen basieren auf Bedarfen
- Best Practices einhalten Benutzergruppen berücksichtigen

- User-Tests durchführen
- Compliance sicherstellen
- Bedarfserfüllung prüfen
- Anwendungsszenarien pro Persona prüfen

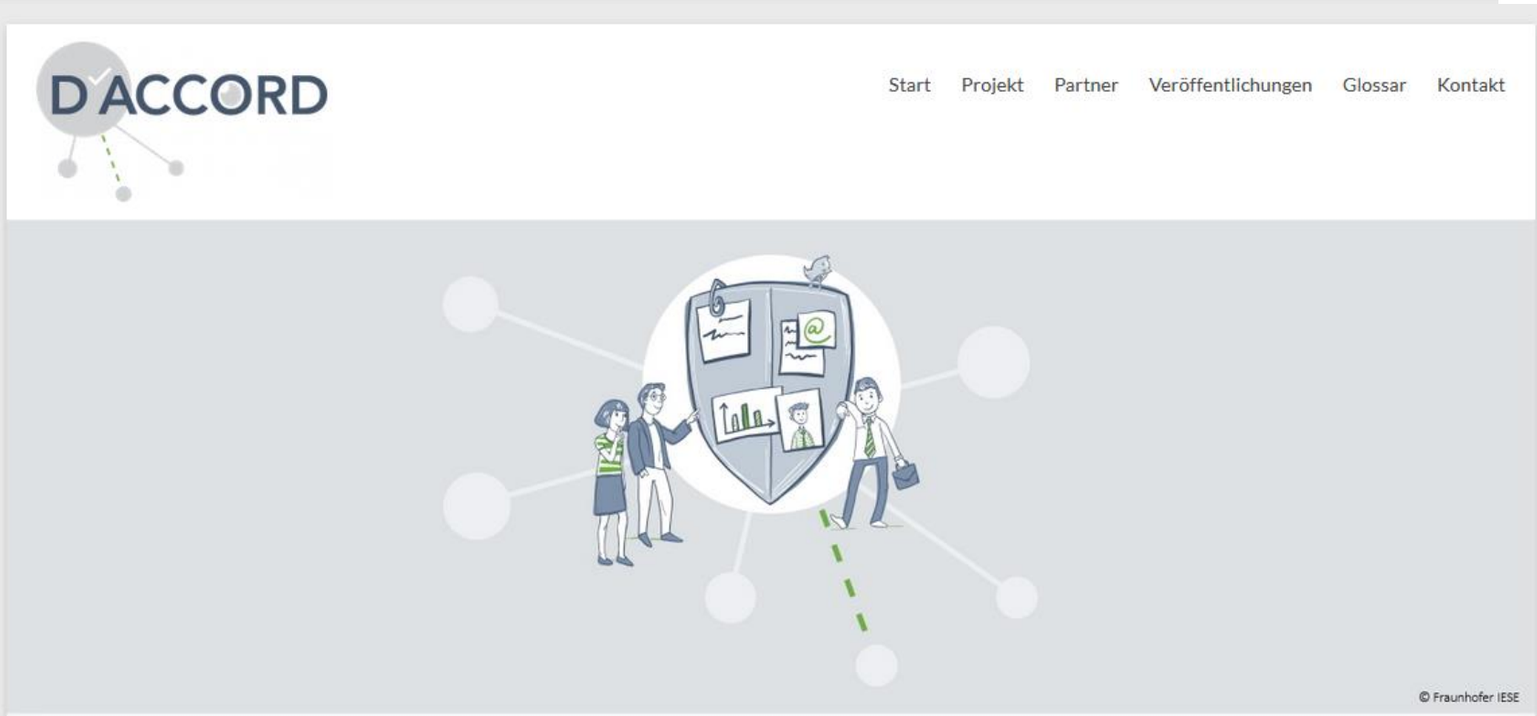
Eigene Darstellung basierend auf ISO 9241-210

Fazit

Fazit

- Ergebnisse gut geeignet für Anwendung im agilen Kontext.
- Die Einbettung der RE-Methoden im Human-Centered Design stellt die korrekte Implementierung von „Usable Privacy“ sicher.
- Besserer Datenschutz unter Erhalt der Benutzerfreundlichkeit …
  - erfüllt die **Randbedingung** der Einhaltung von Datenschutzbestimmungen.
  - steigert die **Systemqualität**, u. a. durch eingehendere Analyse der Sicherheit.
  - steigert die **Nutzungsqualität**, u. a. Vertrauen in das System.
- Weiterführende Informationen zu diesem Thema finden Sie in unserem Buchkapitel in „Human Factors in Privacy Research“.

Vielen Dank für Ihre Aufmerksamkeit



Hartmut Schmitt

HK Business Solutions GmbH

Hartmut.Schmitt@hk-bs.de

Sven Storck

Fraunhofer IESE

Sven.Storck@iese.fraunhofer.de

GEFÖRDERT VOM

Bundesministerium für Bildung und Forschung

Förderkennzeichen
16KIS1506K (HK Business Solutions GmbH)
16KIS1507 (Fraunhofer IESE)