GEFÖRDERT VOM
Bundesministerium für Bildung und Forschung

Usable Privacy: Geeignete RE-Methoden für benutzerfreundlichen Datenschutz

REConf, 25.04.2023

Hartmut Schmitt
HK Business Solutions

Sven Storck
Fraunhofer IESE

Inhalte

RE-Methoden hinsichtlich Datenschutz

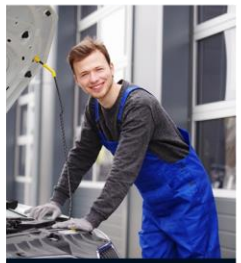
Frank Nußbaum (fatalistische Nutzer:innen)

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. In seiner Freizeit bastelt er gern an seinem Golf, 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.
Was konkret mit seinen persönlichen Daten im digitalen Ökosystem geschieht, ist ihm nicht klar, aber er hat auch kein großes Interesse daran, sich mit den Datenschutzbestimmungen oder -einstellungen vertieft auseinanderzusetzen.
Frank hört zwar immer wieder von Phishing-Vorfällen und hat sich damit beschäftigt, geht aber davon aus, dass regelmäßige Updates sowie ein Spam-Filter ausreichen. Weitere Maßnahmen sind ihm zu aufwendig, da deren Nutzen auch verstärkt angezweifelt werden.
Kommt ihm eine digitale Plattform/ ein digitales Ökosystem zu unsicher vor oder geht sein Vertrauen in die Sicherheit verloren, schränkt er eher die Nutzung ein, anstatt sich vertieft mit Sicherheitsmaßnahmen zu beschäftigen.

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

Privatheitsbedarfe *(der Betroffenen)*

Transparenzbedarf
verständliche Informationen und Offenheit über Datenverarbeitung

Selbstbestimmungsbedarf
autonome Kontrolle über die Datenverarbeitung

Schutzbedarf
Sicherstellung Datenschutz, insb. Vorbeugung Datenschutzverletzungen

Verarbeitungsbedarfe *(der Datenverarbeiter)*

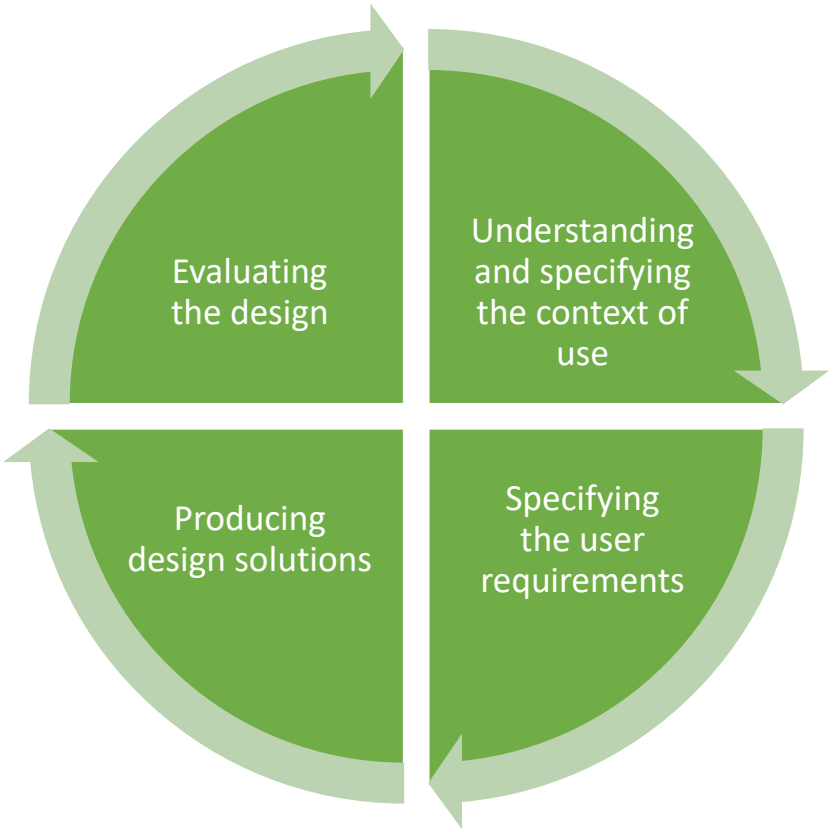
Datennutzungsbedarf
Verarbeitung bestimmter Daten zu einem bestimmten Zweck

Informationsbedarf zur Datennutzung
Wissen über Verordnungen, um rechtskonform zu sein

Einbettung im Human-Centred Design-Prozess

Benutzergruppenprofile und Privacy-Personas

Human-Centered Design-Prozess



Eigene Darstellung basierend auf ISO 9241-210

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 (2022): DsiN-Sicherheitsindex 2022

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. (im Druck). 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. In seiner Freizeit bastelt er gern an seinem Golf, 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.
Was konkret mit seinen persönlichen Daten im digitalen Ökosystem geschieht, ist ihm nicht klar, aber er hat auch kein großes Interesse daran, sich mit den Datenschutzbestimmungen oder -einstellungen vertieft auseinanderzusetzen.
Frank hört zwar immer wieder von Phishing-Vorfällen und hat sich damit beschäftigt, geht aber davon aus, dass regelmäßige Updates sowie ein Spam-Filter ausreichen. Weitere Maßnahmen sind ihm zu aufwendig, da deren Nutzen auch verstärkt angezweifelt werden.
Kommt ihm eine digitale Plattform/ ein digitales Ökosystem zu unsicher vor oder geht sein Vertrauen in die Sicherheit verloren, schränkt er eher die Nutzung ein, anstatt sich vertieft mit Sicherheitsmaßnahmen zu beschäftigen.

Wissen & Fähigkeiten:

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

Persönlichkeit:

introvertiert	extrovertiert
rational	intuitiv
sorgfältig	nachlässig
misstrauisch	vertrauensvoll

Einstellung:

Privatheit — Datenpreisgabe

- Vertrauen zum Broker
- Vertrauen zum Provider
- Eigenverantwortlichkeit
- Selbstvertrauen

Gewohnheiten:

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

Bedarfe hinsichtlich Datenschutz

Eine neue Art von Anforderung

- Definition gemäß IREB: „Eine **Benutzeranforderung** ist ein von einem Stakeholder wahrgenommener **Bedarf**.“
  - Bezieht sich auf **eine konkrete** Softwarelösung
    - *Was* soll das System machen? (funktionale Anforderung)
    - *Wie* gut soll das System dies machen? (Qualitätsanforderung)

➢ Wie ist es mit Bedarfen, die sich **nicht auf ein konkretes Softwaresystem beziehen**, d. h. allgemeingültiger und abstrakter sind?

Bedarfe: anders als andere Anforderungen

- Aspekte der „Usable Privacy“ lassen sich nicht gut als Anforderung dokumentieren;
  - entweder zu unspezifisch: „Das System sollte die Privatheit der Benutzer schützen“ (gilt auch für Notationen wie Soft-Goal-Modeling)
  - oder bereits zu lösungsorientiert: „Wenn der Benutzer sich einloggt, sollte das System folgende Aktionen durchführen: …“

➢ Usable-Privacy-Lösungen werden meist entworfen, um die Bedarfe von Datennutzern & Betroffenen zu erfüllen → Bedarfe als Anforderungsart

Definition: Bedarfe hinsichtlich Datenschutz

- „Ein **Bedarf** ist ein **geäußertes Ziel** einer *betroffenen Person* oder eines *Datennutzers* im Hinblick auf die Verarbeitung *personenbezogener Daten*“ (gemäß D‘accord-Glossar)
  - Dies heißt: Bedarfe können (anders als Anforderungen) nicht direkt in technische oder organisatorische Maßnahmen, Softwarefunktionen bzw. -qualitäten umgesetzt werden.

➢ Bedarfe wurden in mehreren größeren Projekten erfolgreich angewandt

Wie werden Bedarfe erhoben?

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

Die fünf Bedarfe hinsichtlich Datenschutz (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 Bedarfe hinsichtlich Datenschutz (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 und analysiert man Bedarfe?

- **Dokumentation** mithilfe einer einfachen **Notationsart** für die Wünsche, Erwartungen bzgl. Ansichten der Benutzergruppen:
  „Als *<Benutzergruppe>* möchte ich *<Bedarf>*, damit *<Begründung>*.“
- **Priorisierung** nach Projektrelevanz
- **Analyse** sowie **Verhandlung** in zwei Schritten:
  - Eine **juristische Bewertung** steigert die **Rechtsgültigkeit** durch die Aufdeckung und Schlichtung sich widersprechender Bedarfe.
  - Ein **Abgleich** mit den erhobenen bzw. definierten Benutzer- und Systemanforderungen steigert die **Effektivität** der Datenschutzmaßnahmen, da die Bedarfe/Erwartungen relevanter Stakeholder sichergestellt werden.

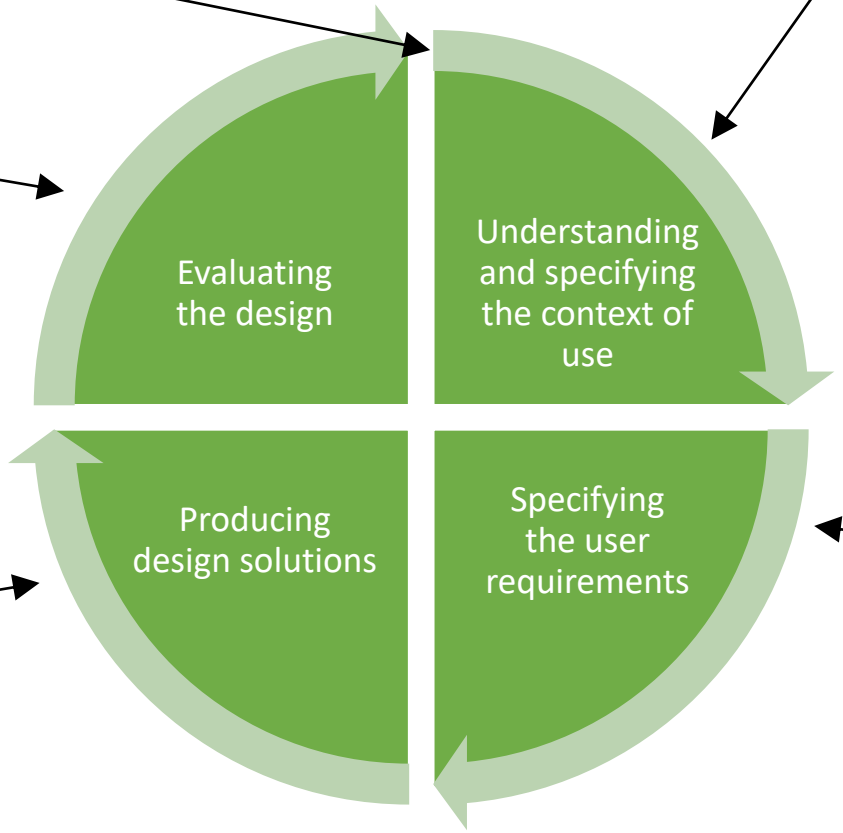
RE und Datenschutz im Human-Centered Design

Impuls für Datenschutz

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

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



Entwurfsentscheidungen basieren auf Bedarfen
Best Practices einhalten
Benutzergruppen berücksichtigen

Bedarfe erheben
Datenschutzanforderungen, Ziele und Aufgaben ableiten
Personas ergänzen

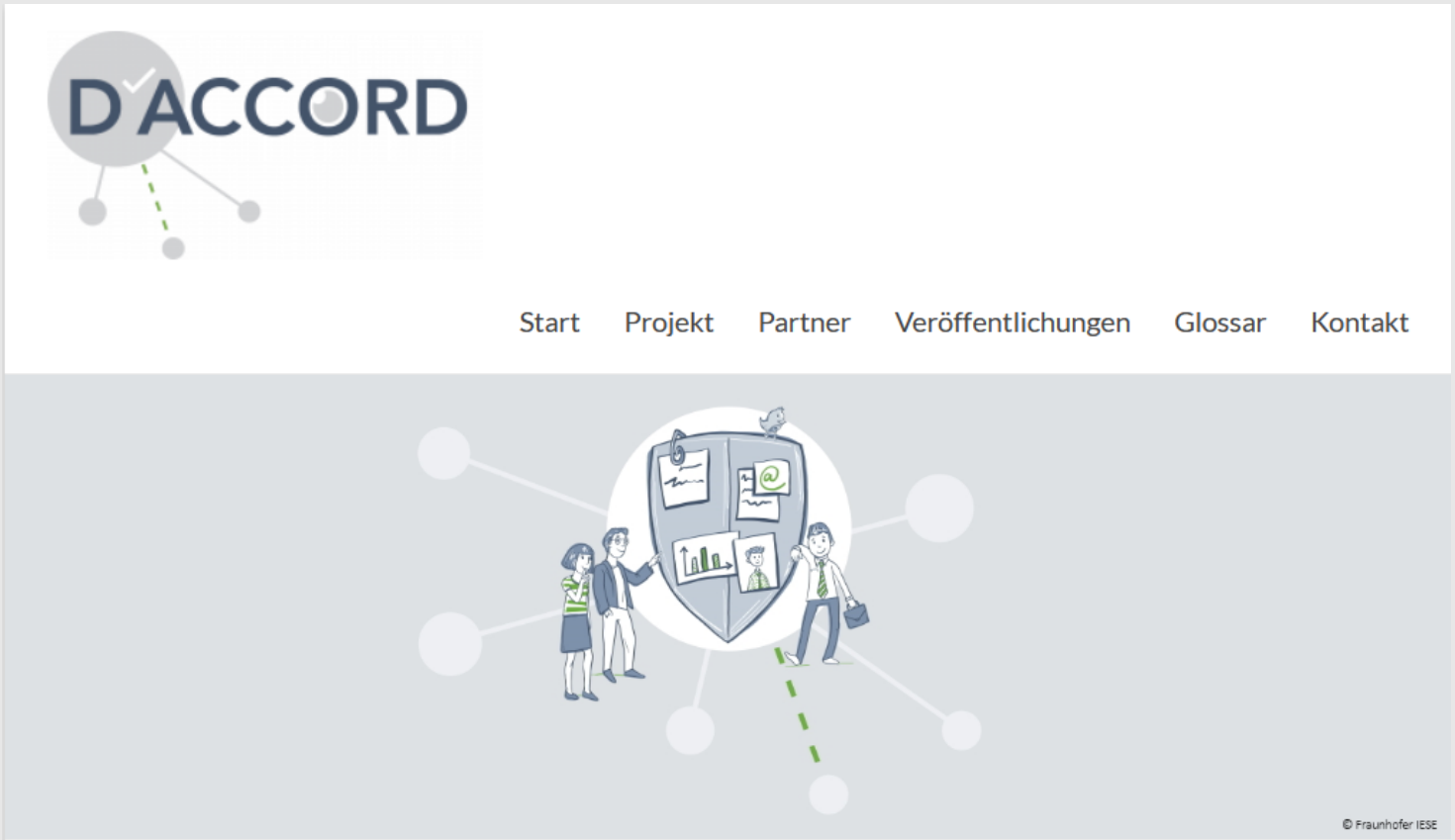
Eigene Darstellung basierend auf ISO 9241-210

Fazit

Fazit

- 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“ (06/2023, Springer).

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)