Erreichen von Usable Privacy durch die Einbindung bewährter RE-Methoden in den Human-Centered-Design-Prozess

Hartmut Schmitt, HK Business Solutions GmbH, hartmut.schmitt@hk-bs.de
Eduard C. Groen, Fraunhofer IESE, eduard.groen@iese.fraunhofer.de

Bei der Entwicklung interaktiver Systeme sind die Nutzer*innen und deren Anforderungen und Bedarfe von zentraler Bedeutung. Ein gängiges Verfahren, um die Nutzer*innen eines interaktiven Systems in den Entwicklungsprozess miteinzubeziehen, ist der in ISO 9241-210 [1] beschriebene menschzentrierte Gestaltungsprozess (*HCD-Prozess*). Die dort definierten Grundsätze und Aktivitäten sind jedoch eher abstrakt gehalten und bieten nur wenig konkrete Anleitung für die Umsetzung, wodurch der HCD-Prozess im Requirements Engineering (RE) häufig keine Anwendung findet. In diesem Beitrag zeigen wir auf, wie der HCD-Prozess mit etablierten RE-Methoden und -Techniken sinnvoll erweitert werden kann und wie es durch diese Kombination gelingt, die Menschen stärker in den Mittelpunkt des Entwicklungsprozesses zu rücken.

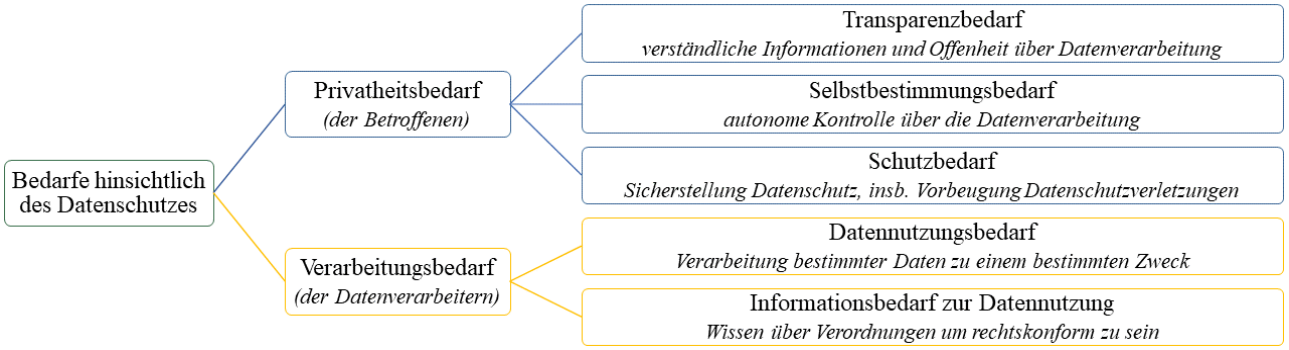
Kontext und Motivation

Eine der derzeit größten Herausforderungen der Softwareentwicklung ist es, ein hohes Maß an Datenschutz zu erreichen und trotzdem die Benutzerfreundlichkeit sicherzustellen [2]. Daher untersuchen wir aktuell die Integration von RE und HCD-Prozess anhand eines Anwendungsbeispiels, in dem Lösungen für den Datenschutz in sogenannten digitalen Ökosystemen entwickelt werden. Wir zeigen, wie mithilfe konkreter Methoden datenschutzbezogene Bedarfe und Anforderungen analysiert und entsprechende Benutzermerkmale gesammelt und in Form von Benutzergruppenprofilen und Privacy-Personas strukturiert werden können [3]. Dadurch ist es möglich, ein tieferes Verständnis für die wichtigsten Nutzergruppen zu gewinnen, die Eigenschaften der Stakeholder in Bezug auf benutzerfreundlichen Datenschutz (Usable Privacy) zu spezifizieren und auf dieser Grundlage benutzerfreundliche Lösungen für den Datenschutz umzusetzen. Eine initiale Ausarbeitung von Teilen dieses Forschungsbeitrags wurde beim Fachgruppentreffen 2019 vorgestellt [4]. Zwischenzeitlich wurden die damals vorgeschlagenen Methoden in der Domäne Beschäftigtendatenschutz erfolgreich angewendet und evaluiert. In diesem Beitrag zeigen wir auf, wie wir die weiterentwickelten Methoden auf das technisch komplexere Umfeld der digitalen Ökosysteme übertragen.

Datenschutzbedarfe und -anforderungen

Benutzeranforderungen sind Anforderungen, die Benutzerbedürfnisse ausdrücken [5]. Sie zielen darauf ab, was ein interaktives System können soll (funktionale Anforderungen) bzw. wie gut es dies können soll (Qualitätsanforderungen) [6]. *Bedarfe hinsichtlich des Datenschutzes* sind insofern besonders, als sie sich nicht auf ein bestimmtes Softwaresystem beziehen, sondern eher darauf, was mit personenbezogenen Daten geschieht. Entsprechende Bedarfe formulieren also Wünsche relevanter Stakeholder im Hinblick auf die Verarbeitung personenbezogener Daten und sind oft allgemeiner als funktionale oder Qualitätsanforderungen. Werden solche Datenschutzaspekte in Form herkömmlicher Benutzeranforderungen dokumentiert, sind sie häufig entweder zu unspezifisch (z. B. „Das System muss die Privatsphäre der Benutzer wahren.“) oder sie schränken den Lösungsraum ein, da sie eine bestimmte Variante vorgeben (z. B. „Gesundheitsdaten sollen mittels *Differential Privacy* geschützt werden.“).
Um besser zu verstehen, was die Stakeholder antreibt, schlagen wir eine Ontologie vor, mit der die Bedarfe hinsichtlich des Datenschutzes als eigenständige Anforderungen verwaltet und in logischen Gruppen organisiert werden können (vgl. Abbildung 1). Wir unterscheiden hierbei zwei Stakeholdergruppen: die Betroffenen, deren Daten verarbeitet werden, und die Datenverarbeiter. Diese Unterscheidung erleichtert die Aufdeckung möglicher Interessenkonflikte.

Abbildung 1: Bedarfe hinsichtlich des Datenschutzes



Benutzergruppenprofile und Privacy-Personas

Die Eigenschaften der Nutzer*innen beeinflussen stark den Nutzungskontext eines Systems. Es ist daher sinnvoll, relevante Informationen zu sammeln und zu analysieren, um den Kontext besser verstehen bzw. spezifizieren zu können. Die ISO 9241-210 [1] nennt als Artefakte zur Beschreibung von Benutzermerkmalen „Benutzergruppenprofile“ und „Personas“, konkretisiert diese aber nicht.

Benutzergruppenprofile sind ein probates Mittel, um ein genaueres Bild von Stakeholdergruppen zu zeichnen, die direkt mit dem System interagieren. Dupree et al. [7] teilen die Nutzer*innen von Datenschutzwerkzeugen abhängig von deren Einstellungen, Überzeugungen und Verhaltensweisen in fünf Benutzergruppen ein: *marginally aware*, *fundamentalist*, *struggling amateur*, *technician* und *lazy expert*. Bei Profilen, die stark auf die Nutzung bestimmter Technologien fokussieren, ist zu beachten, dass diese Technologien oft nach einigen Jahren veraltet sind, was dazu führt, dass auch entsprechende Benutzergruppenprofile ihre Relevanz verlieren. In Bezug auf Datenschutz ist zudem zu berücksichtigen, dass es starke kulturelle Unterschiede gibt.

Von den Benutzergruppen sind sogenannte Personas zu unterscheiden. Dies sind einzelne fiktive Personen, die typische Benutzergruppen repräsentieren [8]. Sie werden aus den identifizierten Nutzergruppen abgeleitet, um die wichtigsten Eigenschaften und Details der jeweiligen Nutzergruppe hervorzuheben [9]. Ziel ist es, eine anschaulichere Beschreibung der Nutzer*innen zu erhalten als bei den abstrakten Benutzergruppenprofilen. Grundlage für die Erstellung von Personas können quantitative oder qualitative Datenerhebungen, Befragungen oder teilnehmende Beobachtungen von potenziellen Nutzer*innen sein. Cooper et al. [8] empfehlen, die verschiedenen Aspekte des Nutzerverhaltens als Verhaltensvariablen in den Personas aufzuführen, z. B. Aktivitäten, Einstellungen, Fähigkeiten und Motivationen.

Sogenannte *Privacy-Personas* sollten dementsprechend den unterschiedlichen Umgang mit personenbezogenen Daten und die unterschiedlichen Datenschutzbedürfnisse der Nutzer*innen hervorheben. Mithilfe dieser Angaben kann sich das Design- und Entwicklungsteam besser in die Rolle der Nutzer*innen hineinversetzen. Es kann deren Bedürfnisse besser verstehen und verschiedene Nutzungsszenarien aus deren Sicht durchspielen. Dadurch ist es einfacher, die richtigen Designentscheidungen zu treffen, auch bei der Gestaltung von Datenschutzfunktionen [10].

Verschiedene Projekte im Bereich Datenschutz [11] haben Vorlagen und Beispiele für Privacy-Personas entwickelt, die es ermöglichen, Forschungsdaten systematisch auszuwerten und die gesammelten Erkenntnisse strukturiert und übersichtlich zusammenzufassen, sodass im weiteren Entwicklungsprozess darauf zurückgegriffen werden kann.

Fazit

Mit den hier vorgestellten RE-Methoden kann der HCD-Prozess erweitert werden, um sicherzustellen, dass Usable Privacy in einem System korrekt implementiert wird [3]. Die Methoden lassen sich unserer Erfahrung nach sehr gut in die Aktivitäten des HCD-Prozesses integrieren. Der damit verbundene Aufwand ist überschaubar und gerechtfertigt, da er zu besserem Datenschutz unter Erhalt der Benutzerfreundlichkeit führt. So leistet der systematische Einsatz dieser RE-Methoden einen positiven Beitrag zur Gesamtqualität eines Systems, und zwar nicht nur in Bezug auf Einschränkungen (z. B. bessere Gewährleistung der Einhaltung von Datenschutzbestimmungen), sondern auch in Bezug auf die Systemqualität (z. B., weil Sicherheitsaspekte eingehender analysiert wurden) und die Qualität der Nutzung (z. B. größeres Vertrauen in das System). Selbstverständlich sind die vorgestellten Methoden nicht die einzigen RE-Methoden, die als sinnvolle Erweiterungen oder Konkretisierungen des HCD-Prozesses in Frage kommen. Da wir sie im beschriebenen Kontext – Datenschutz in digitalen Ökosystemen – jedoch als zielführende Ergänzungen empfunden haben, ermutigen wir die Leser*innen, diese Methoden selbst auszuprobieren und eigene Erfahrungen mit uns zu teilen.

Das Projekt D’accord, in dem diese Arbeit entstand, wird vom Bundesministerium für Bildung und Forschung gefördert (FKZ: 16KIS1506K, 16KIS1507).

Literatur

[1] ISO (2019): Standard ISO 9241-210:2019(E), Ergonomics of human-system interaction – Part 210: Human-centred design for interactive systems. ISO.

[2] Deininger, T. & Dittrich, N. (2021): Softwareentwicklung und Datenschutz – wie passt das zusammen? https://heise.de/-6155870

[3] 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.

[4] Schmitt, H. & Polst, S. (2019): Anforderungen und Rahmenwerk für den betrieblichen Datenschutz. SW-Trends 40(1), pp. 9–10.

[5] Glinz, M. (2017): A glossary of Requirements Engineering terminology. https://www.ireb.org/en/cpre/cpre-glossary/

[6] Glinz, M. (2007): On non-functional requirements. In: Proc. of RE, pp. 21–26.

[7] Dupree, J.-L., Lank, E., & Berry, D. M. (2018): A case study of using Grounded Analysis as a Requirement Engineering method. Sci. Comput. Program., 152, pp. 1–37.

[8] Cooper, A., Reimann, R., & Cronin, D. (2012): About face 3: The essentials of Interaction Design. Wiley.

[9] Harley, A. (2015): Personas make users memorable for product team members. https://www.nngroup.com/articles/persona/

[10] AK Usable Security & Privacy (2019): Nutzerzentrierter Schutz sensibler Daten. Fachschrift. German UPA e.V.

[11] https://www.trusd-projekt.de/, https://daccord-projekt.de/