Privacy by Design am Beispiel einer Plattform zur Unterstützung kollaborativer Reflexion am Arbeitsplatz

Martin Degeling, Jan Nierhoff

Institut für Arbeitswissenschaft
Ruhr-Universität Bochum
Universitätsstr. 150
44801 Bochum
martin.degeling@ruhr-uni-bochum.de
jan.nierhoff@ruhr-uni-bochum.de

Abstract: Der vorliegende Beitrag stellt die Entwicklung und Einführung einer Software zur Unterstützung kollaborativer Reflexion am Arbeitsplatz vor. Dabei wurden schon während früher Entwicklungsphasen Datenschutzfragen viel Raum eingeräumt und im weiteren durch enge Einbindung verschiedener Akteure, etwa durch Workshops und Fragebögen, versucht theoretische Konzepte des Privacy By Design in den agilen Softwareentwicklungsprozess einzubinden.

1 Einleitung

Wesentlicher Bestandteil vieler Anwendungen im Netz ist es heutzutage, Inhalte mit anderen teilen und kommentieren zu können. Etwas zu teilen bedeutet auf der einen Seite sich den Risiken auszusetzen etwas einer anderen Person gegenüber preiszugeben, ohne sicher zu wissen, wie diese mit den Informationen umgehen wird. Gleichzeitig birgt es aber auf der anderen Seite auch die Chance, etwas voneinander zu lernen und gemeinsam Ideen zu entwickeln. Die Vorteile des Austauschs von Erfahrungen gibt es dabei nicht nur im privaten Rahmen, sondern auch am Arbeitsplatz. Dort kann der Austausch von, während der Arbeit gemachten, Erfahrungen zur gemeinsamen Reflexion der Aufgaben genutzt werden und bestenfalls sowohl den Arbeitsprozess als auch das Erleben des Prozesses angenehmer gestalten. Dabei bietet insbesondere der computergestützte Austausch, der über das undokumentierte Gespräch beim Kaffee oder auf dem Büroflur hinausgeht, auch Gefahren - sowohl für Arbeitnehmer/innen als auch für die sie beschäftigenden Organisationen.

Der vorliegende Beitrag beschreibt die Entwicklung einer Software zur Unterstützung kollaborativer Reflexion[1], deren Ziel es ist Angestellten, insbesondere im Gesundheitswesen, Möglichkeiten bereit zu stellen, um Erfahrungen über die Arbeit

[1] Die hier beschriebene Forschung ist Teil des von der Europäischen Kommission im Rahmenprogramm 7 geförderten Projekts „MIRROR“. Weitere Informationen sind unter http://www.mirror-project.eu verfügbar.

auszutauschen und gemeinsam Vorschläge zu erarbeiten mit denen die Arbeit für alle Seiten besser gestaltet werden kann.

Bei der Entwicklung und Einführung der Software wurde besonderer Wert auf den Schutz der informationellen Selbstbestimmung aller Beteiligten und die Sicherheit der durch das System verarbeiteten Daten gelegt, unter anderem, weil diese als besondere Faktoren zur Nutzungsmotivation identifiziert wurden. Der Beitrag beschreibt das Vorgehen bei dem der Fokus auf der Nutzung von Modellen des privacy by design und dem Einsatz von Methoden der partizipativen und agilen Software Entwicklung lag.

Bei der entwickelten Software handelt es sich um eine webbasierte Anwendung, die es Nutzer/innen – im ersten Einsatz Ärztinnen und Ärzte einer Klinik und Pflegekräfte in einem Heim für Demenzkranke – erlaubt Erfahrungen, die sie in Gesprächen mit Angehörigen von Patienten gemacht haben, zu dokumentieren und diese mit anderen zu teilen (Prilla et al., 2012). Über die Unterstützung der gemeinsamen Diskussion und Reflexion erlaubt die Software den Nutzer/innen Erkenntnisse zu abstrahieren, zu dokumentieren und mit den einzelnen Erfahrungsberichten zu verknüpfen. Dabei ist es in dem Prozess von zentraler Bedeutung, dass die Kommunikation nicht ausschließlich in der Anwendung, sondern zusätzlich in Workshops und regelmäßigen Sitzungen stattfindet.

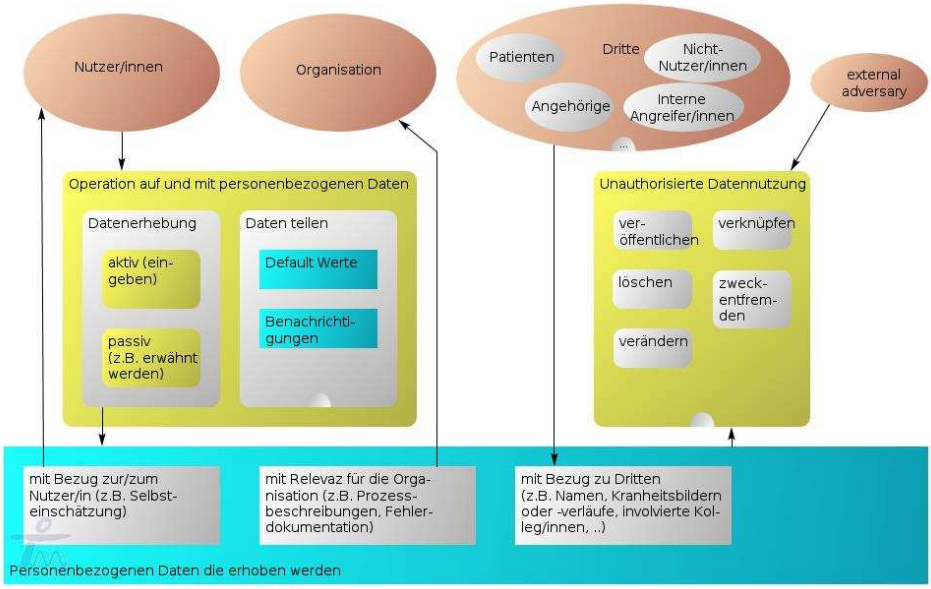

Abbildung 1: Modell der beteiligten Rollen, Aktionen und Datentypen aus Datenschutzsicht

2 Beteiligte Rollen und Risiken

Im Rahmen der Ideen- und Konzeptentwicklung haben sich mehrere Interessensgruppen herauskristallisiert, die auf der einen Seite unterschiedliche Anforderungen an die Software haben und für die auf der anderen Seite eine Abschätzung der Datenschutzrisiken durchgeführt werden muss. Eine Übersicht zeigt Abbildung 1.

Die **Nutzerinnen und Nutzer** sind die im Fokus der Softwareentwicklung stehende Gruppe. Neben den funktionalen Anforderungen bezüglich des konkreten Einsatzes der Software, etwa welche Selbsteinschätzungsfragen am meisten Sinn machen und wie die Software möglichst gut mit den bereits bestehenden Anwendungen zusammen arbeiten kann, stehen bei unterschiedliche Datenschutzfragen im Mittelpunkt. Einerseits, der Schutz vor nicht abgesprochener Leistungs- und Verhaltenskontrolle durch den oder die Vorgesetze/n. Andererseits aber auch die Unterstützung bzw. Abbildung bestehender Vertrauensbeziehungen und Hierarchien die den Schutz vor Missbrauch der Daten durch Kolleg/innen verhindern sollen - positiv formuliert: die Ermöglichung exakt die Kolleg/innen in den Reflexionsprozess einzubeziehen, mit denen er am besten durchgeführt werden kann.

Aus der Sicht der **Organisation** in der die Software eingesetzt werden soll ergaben sich in der Analyse zwei Schwerpunktthemen. Erstens sind die Informationen die die Angestellten zur Reflexion der eigenen Arbeit festhalten aus Sicht der Organisation kritische Unternehmensdaten. Dem lag die Annahme zu Grunde, dass sich die erhobenen Daten auf Vorgänge beziehen die innerhalb der Organisation stattfinden und vor allen Dingen auch – möglicherweise kritische – Missstände innerhalb der Organisation dokumentieren. Obwohl die Software nicht in die Infrastruktur und Geschäftsprozesse eingreifen sollte, war es aus Sicht der Befragten von hoher Wichtigkeit, dass sie das selbe Datensicherheitsniveau erfüllt wie alle anderen Anwendungen im Unternehmen auch. In dem Krankenhaus für den der erste Prototyp entwickelt wurde bestand etwa die Sorge, dass die unerwünschte Veröffentlichung von etwaigem unprofessionellem Verhalten der Ärztinnen und Ärzte, potenzielle Grundlage für Klagen gegen das Krankenhaus sein könnte, z.B. wenn ein Arzt in der Anwendung dokumentiert, sich in einem Angehörigengespräch nicht souverän verhalten zu haben. Kritisch wurde daher auch die Frage vom Einsatz der Software auf mobilen Geräten betrachtet. Insbesondere für eigene Geräte sollten die Anforderungen an den Schutz der Daten auf dem Gerät besonders hoch sein („Bring Your Own Device"-Policies).

Die letzte Gruppe die aus einer Datenschutzperspektive von der Software betroffen ist, sind **Dritte** über die etwas festgehalten wird. Im Falle des Krankenhauses also Patienten und deren Angehörige. Es sollte möglichst sichergestellt werden, dass keine personenbezogenen Daten über diese in der Software festgehalten werden. Im Falle personenbeziehbarer Informationen müssen diese pseudonymisiert werden.

3 Anforderungen an die Software

3.1 Allgemeine Anforderungen

Um die informationelle Selbstbestimmung der Nutzer/innen möglichst gut zu schützen wurde die Anwendung nach den Prinzipien des privacy by design gestaltet. Ähnlich wie bei Fragen der Datensicherheit kann so verhindert werden, dass eine datenschutzfreundliche Systemgestaltung erst am Ende eines Entwicklungsprozesses diskutiert wird (vgl. [Si05]) und wichtige Designentscheidungen nicht mehr umkehrbar sind. In der Literatur werden Richtlinien für privacy by design meist auf einer abstrakteren Ebene beschrieben (vgl. etwa [Ca09],[La01],[Sch10]). Sie enthalten vor allem Vorschläge, die auf der einen Seite den/die Nutzer/in und seine/ihre Informationelle Selbstbestimmung in den Fokus rücken, etwa durch die Betonung von Freiwilligkeit, der Notwendigkeit explizierter Einwilligung und der Durchsetzung von Betroffenenrechten (vgl. auch [Bi07]) wie das Recht auf Auskunft über die gespeicherten Daten. Auf der anderen Seite legen sie besonderen Wert darauf, dass die Prinzipien möglichst früh in den Software-Entwicklungsprozessen berücksichtigt werden. Wie genau das geschehen kann bleibt allerdings im Detail unklar (vgl. dazu [Sp09] und Ansätze von [Gü10], [Gü11]). Aus den verschiedenen verfügbaren Ansätzen hat sich für unsere Entwicklung dabei ein Mix als produktiv und umsetzbar herausgestellt. Die folgenden Prinzipien wurden beim Systemdesign betrachtet:

1. Daten Minimierung: Welche Informationen sind tatsächlich notwendig: Eine Entscheidung die gerade in agilen Entwicklungsprozessen schwierig zu beantworten ist. Das schließt mit ein, dass bei einem (Forschungs-)prototypen zu Beginn nicht klar ist, welche Informationen notwendig und nützlich sind um kollaborative Reflexion zu unterstützen

2. Informierte Einwilligung: Insbesondere am Arbeitsplatz ist die informierte und freiwillige Einwilligung schwierig zu erreichen (vgl. dazu neben anderen [Be11], [Cl05]). Uns war es wichtig, dass an möglichst vielen Stellen eine Einwilligung (explizit wie implizit) notwendig ist. Etwa bei der Registrierung aber auch bei einzelnen Prozessschritten.

3. Privacy by default: Auch bei auf Kollaboration ausgelegten Anwendungen sollten personenbezogene Informationen standardmäßig nicht geteilt werden.

4. Awareness und Transparenz: Ziel muss es sein, den Nutzer/innen möglichst transparent zu machen welche Informationen wo für wen verfügbar sind. Hier sind Abwägungen gegenüber einfacher Handhabung und Übersichtlichkeit notwendig.

5. Anonymität und Pseudonymität: Um auch Kritik, die für einen Reflexionsprozess sehr produktiv sein kann [Wo08] zu erlauben sollte die Nutzung der Anwendung zumindest pseudonym und gegebenenfalls anonym

möglich sein. Insbesondere Informationen über unbeteiligte Dritte sollten anonymisiert werden.

6. Löschung: Beim Design der Anwendung aber auch Datenhaltung sollte sichergestellt werden, dass ein Löschen möglich ist, ohne z.B. Datenstrukturen durch gelöscht Abhängigkeiten zu zerstören.

3.2 Erhebung spezifischer Anforderungen

Im Rahmen eines Privacy Impact Assessments (PIA) wurde bereits vor Start der Entwicklung der Anwendung eine Umfragen-basierte Studie mit den potentiellen Nutzern/innen durchgeführt (vgl. [De11]). Die Vorabbefragung hatte zwei Ziele: Erstens sollte ein Überblick über die Aufmerksamkeit für Datenschutzprobleme bei den potentiellen Nutzer/innen erhoben werden. Dabei war der Unterschied zwischen generellen Bedenken und den Folgen für das tatsächliche Handeln von besonderem Interesse. Zweitens sollte erhoben werden in wie weit die Teilnehmer/innen ihren Organisationen und Kollegen vertrauen und bereit sind personenbezogene Daten diesen anzuvertrauen. Da der Arbeitskontext noch die zusätzliche Komponente des Abhängigkeitsverhältnisses zwischen Arbeitnehmer/innen und Arbeitgeber/innen beinhaltet war das Ziel der Befragung möglichst früh auf mögliche Probleme, die letztlich auch zu einer geringen Akzeptanz führen könnten, aufmerksam zu werden.

Die Fragebogenstudie wurde mit 134 Teilnehmer/innen in fünf unterschiedlichen Organisationen durchgeführt, von denen zwei[2] später auch die hier vorgestellte Anwendung nutzen. Der Fragebogen enthielt insgesamt 27 Fragen die sich auf die oben beschriebenen Themenfelder bezogen. Zu den Ergebnissen zählte, dass insbesondere in den Organisationen die im Gesundheitswesen angesiedelt sind ein sehr hohes Bewusstsein für und Sorge um Datenschutzfragen existierte. Gleichzeitig war ein gutes Vertrauensklima zwischen den Teilnehmer/innen und ihren Kolleg/innen bzw. den Arbeitgeber/innen und Vorgesetzen feststellbar. Für das weitere Vorgehen war dies auch deshalb relevant, weil die Studie einen Zusammenhang zwischen dem Vertrauen gegenüber Kolleg/innen und der Bereitschaft persönliche Informationen mit ihnen zu teilen, nachweisen konnte. Zudem war eine der größten Sorgen der Teilnehmer/innen, dass die Informationen, die Sie in das System eintragen, von den Arbeitgeber/innen missbraucht werden könnten (unauthorized secondary use).

Auch wenn das Vertrauen unter den Kolleg/innen und in die Arbeitgeber/innen nachweisbar gut ist, ist es notwendig die Ergebnisse in Anforderungen an die Software zu übersetzen. Insbesondere da Vertrauen in Beziehungen einen dynamischen Charakter hat und die Sorge um Missbrauchspotential groß ist, wurde bei der Entwicklung der Anwendung Wert auf die folgenden Punkte gelegt:

- Die Daten sollten nachweisbar vor dem unautorisierten Zugriff durch den/die Arbeitgeber/in und Vorgesetze geschützt sein. Dies macht den Einsatz von Verfahren aus der **Datensicherheit** notwendig.

[2] Von den zwei Organisationen haben 110 (79 und 31) Personen an der Umfrage teilgenommen.

- **Transparenz**maßnahmen sollten sicherstellen, dass die Nutzer/innen nachvollziehen können wer Zugriff auf die von ihnen hinterlegten Informationen hat. Ziel dieser Maßnahmen sollte es auch sein, dass Vertrauen in die Anwendung zu erhöhen.

- Da die persönliche Sorge um die eigenen Daten zwischen den einzelnen Fragebogenteilnehmer/innen stark schwankte sollte die Anwendung in hohem Maße **anpassbar** sein.

Nach der Papier-basierten Vorabbefragung wurde die Software von der Idee bis zu den Prototypen in einem iterativen Verfahren entwickelt und regelmäßig mit den Nutzer/innen diskutiert. In drei Workshops mit Nutzer/innen wurden erst Ideen und dann Prototypen entwickelt und evaluiert, um daraus Anforderungen an die Software abzuleiten. Entsprechend des auch explorativ angelegten Forschungsprojekts, das den Rahmen für die Entwicklung bildet, wurde ein agiler Ansatz bei der Softwareentwicklung gewählt, bei der die Anforderungen in regelmäßigen Abständen neu priorisiert wurden, statt einem festen Pflichtenheft zu folgen

Zusätzlich wurden Gespräch unter anderem mit dem Betriebsrat, dem Datenschutzbeauftragten der Klinik und der für Datensicherheit zuständigen IT-Abteilung geführt um alle in Abschnitt 1 beschriebenen Rollen und Risiken diskutieren zu können. Hierbei wurde Konsens über den Nutzen und die Rechtmäßigkeit der Anwendung erzielt.

4 Entwicklungsprozess der Software

Die TalkReflect App (siehe Abbildung 2) hat im Wesentlichen drei Aufgaben. Den Nutzer/innen zu ermöglichen Gespräche, die sie geführt haben, zu dokumentieren, diese Dokumentationen zu teilen und zu diskutieren und Ergebnisse in Relationen zu gemachten Dokumentationen festzuhalten. Die Dokumentationen bestehen dabei aus mehreren Teilen: Einer Verlaufsdokumentation, wie sie auch regulär für Gespräche angefertigt wird, einer eigenen Einschätzung der Situation und kurzen Einschätzungsfragen die auf einer Skala von 1-10 beantwortet werden können. Diese Fragen lauten z.B. “Wie haben Sie sich in der Situation gefühlt?”, “Wie hat sich Ihr gegenüber vermutlich gefühlt?” und “Werden Sie das Gespräch mit 'nach Hause nehmen'?”.

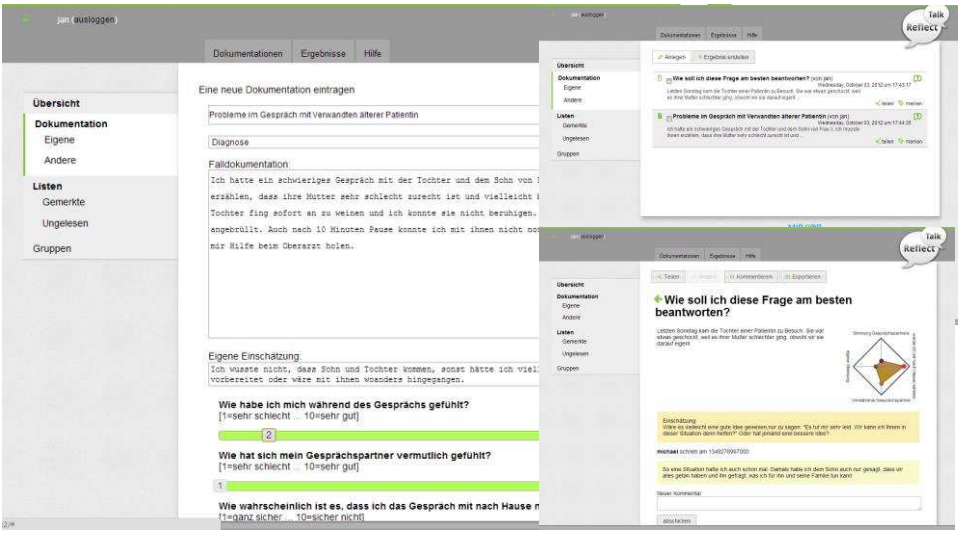

Abbildung 2: Screenshot der Anwendung. Links: Dokumentation eines Gesprächs. Rechts oben: Listenübersicht über dokumentierte Gespräche für die Zugriff besteht. Rechts unten: Ansicht eines selbst dokumentierten Gesprächs

4.1 Umsetzung des Privacy-By-Design

Zurückgreifend auf die in Abschnitt 3 erhobenen Anforderungen wurde folgende Maßnahmen umgesetzt.

Daten Minimierung

Da zu Beginn nicht klar war, welche Informationen zur Unterstützung des Reflexionsprozesses am hilfreichsten sind und zudem ein wesentlicher Teil der Eingabefelder als Freitextfelder implementiert wurden, war eine Minimierung schwierig. Stattdessen wurde, etwa bei der Registrierung, auf optionale Felder gesetzt. Einzig ein Login-Name und ein Passwort sind bei der Registrierung verpflichtend auszufüllen. Innerhalb der Anwendung sind die Eingabefelder mehrfach verändert, erweitert und reduziert worden, vor allem mit Hinblick auf die Unterstützung von Reflexion die die Erhebung von Kontextinformationen vorrausetzt. Hier wurde ein Templatingsystem benutzt um für die unterschiedlichen Anwendungsfälle speziell reduzierte Ansichten zur Verfügung stellen zu können.

Einwilligung

Explizite, informierte Einwilligung für jeden einzelnen Schritt zu fordern war nicht im Sinne der Nutzungsfreundlichkeit. Stattdessen wurde eine explizite, papierbasierte Einwilligung während der Einführung der Software eingeholt, bei der die Nutzer/innen auch über den Zweck und Widerspruchsmöglichkeiten aufgeklärt wurden. Allerdings

besteht bei diesem Vorgehen die Gefahr, dass potentielle Nutzer/innen sich genötigt sehen einzuwilligen, u.a. da auch häufig ein/e Vorgesetze/r bei der Einführung anwesend war. Auf der anderen Seite verpflichtet die Einwilligung nicht zur Nutzung der Anwendung im Nachgang, auch darüber wurden die Teilnehmer/innen informiert. Innerhalb der Anwendung selbst wurde eher auf das Prinzip der impliziten Einwilligung gesetzt. Durch das umgesetzte Privacy-By-Default sind stets explizite Aktionen notwendig um Daten öffentlich zu machen, z.B. um Beiträge für andere freizugeben. Die Standardeinstellung sieht vor, dass ein Eintrag nur für den oder die Autor/in sichtbar ist. Die Anforderung von Seiten eines Vorgesetzen, eine Art Management-Account einzurichten, der alle Einträge automatisch lesen könne, wurde nicht umgesetzt. Das Berechtigungskonzept sieht keine Hierarchien vor.

Ziel des Gesamtprozesses war es möglichst wenig explizite Informationen über unbeteiligte Dritte wie Patienten im System vorzuhalten, da von diesen keine explizite Einwilligung erfragt werden kann. Bei Einführungsworkshops wurde regelmäßig darauf hingewiesen. Da die Anwendung aber zur Dokumentation etwa von Gesprächen Freitextfelder vorsieht, lässt sich dies nur schwierig kontrollieren und die Verantwortung liegt vor allem bei den Nutzer/innen. Zur Unterstützung wurden aber Hinweise neben den Eingabefeldern hinzugefügt, die während der Eingabe auf diese Regel hinweisen. Technische Lösungen, wie etwa die automatische Suche nach Namen mittels computerlinguistischer Analysen, wurden aufgrund der hohen Implementierungskomplexität verworfen.

Default Einstellungen

Entgegen erster Ideen gibt es keine Standardeinstellungen mit wem eine Dokumentation geteilt wird. Diese Standard-Einstellungen sind auch nicht von Nutzer/innen selbst änderbar. Stattdessen muss für jeden einzelnen Fall nach dem Speichern separat der 'Teilen' Dialog aufgerufen werden, um etwas für andere freizugeben. Dabei kann entweder mit einzelnen anderen Nutzer/innen geteilt werden oder mit der gesamten Gruppe. Nicht umgesetzt wurde der Default-Wert, dass Beiträge nur anonym gespeichert und explizit der eigenen Person zugeordnet werden müssen. Stattdessen kann beim Speichern jedes Beitrags zwischen anonym und personenbezogen gewählt werden. Diese kann auch im Nachhinein geändert werden.

Die Anwendung erlaubt es nur die Textteile von Dokumentationen zu teilen. Die Selbsteinschätzungen, die den emotionalen Zustand der Nutzer/innen zum Zeitpunkt des Gesprächs festhalten sollen, sind nicht Teil der Dokumentationen und für andere, auch nach dem Teilen nicht einsehbar. Die Entscheidung wurde damit begründen, dass erhebliches Kontextwissen notwendig ist, um die auf einen Zahlenwert reduzierte Information etwa über die eigene Gefühlslage, bewerten zu können. Stattdessen sind sie eher als Erinnerungsanker für diejenigen gedacht, die die Anwendung nutzen und sich nach einiger Zeit an einen Fall zurückerinnern wollen und gegebenenfalls dann auch zu einer anderen Einschätzung kommen können.

Awareness und Transparenz

Sowohl in der Einzelansicht einer Dokumentation als auch in der Übersicht ist ständig sichtbar wer, bzw. wie viele Nutzer/innen auf eine Dokumentation zugreifen können. Unter der Dokumentation selbst sind die Nutzer/innen namentlich oder mit Pseudonym aufgeführt. Innerhalb der Anwendung gibt es außerdem mehrere Listenansichten welche unter anderem die von dem/der Nutzer/in selbst angefertigten Dokumentationen auflisten, so dass sich leicht herausfinden lässt wie viele Informationen im System hinterlegt sind. Über die technischen Rahmenbedingungen, wie den Speichort, werden die Nutzer/innen während der Einführung hingewiesen ebenso auf die Möglichkeiten genauere Nachfragen an den Support zu richten.

Anonyme und Pseudonyme Nutzung

Es steht den Nutzer/innen frei sich mit einem Pseudonym zu registrieren. Notwendige Daten zur Registrierung sind nur ein Benutzer/innenname ein Passwort und ein Registrierungsschlüssel, der für die Zuordnung des Accounts zu einer Organisation notwendig ist.

Im Laufe der Entwicklung gab es auch den Wunsch Kommentare und Dokumentationen anonym speichern zu können. Das ist möglich, aber natürlich lässt sich gerade in kleinen Gruppen anhand der Sprache oft der oder die Autor/in identifizieren. Wobei sich andererseits im Krankenhauskontext, insbesondere bei der Beschreibung von Fällen, ein sehr ähnlicher Sprachduktus herausbildet was eine Zuordnung erschwert. Nichtsdestotrotz lässt sich Anonymität so nicht sicherstellen.

Nicht-autorisierte Zweitnutzung

Auf organisatorischer Ebene wurden mehrere Maßnahmen ergriffen, um dem Problem der nicht-autorisierten Zweitnutzung (unauthorized secondary use) zu begegnen, was in der Vorabstudie als größte Sorge der Nutzer/innen identifiziert wurde. Die oben beschriebenen Transparenz, Awareness und Anonymitätsfunktionen tragen dazu bei, dass eine ungewollte Preisgabe von Informationen an Dritte, wie etwa dem/r Oberarzt/ärztin, innerhalb der Anwendung vorgebeugt wird. Zudem ist es möglich eine einmal getätigte Freigabe rückgängig zu machen und so den Zugriff für Dritte auch im Nachgang einzuschränken. Maßnahmen zur Zweckbindung der Daten sind vor allem auf organisatorischer Ebene installiert. Die Vereinbarung mit dem Betriebsrat besagt etwa, dass die Daten ausschließlich zur Fortbildungszwecken verwendet werden dürfen. Zudem sieht das Gruppenkonzept vor, dass die Freigabe von Daten zuerst innerhalb der Station einem kleinen Kreis von Personen zugängig gemacht wird.

Auf der Ebene der Infrastruktur wurde das Hosting vom Forschungspartner übernommen, um zu verhindern, dass sich auf Grund interner Machtverhältnisse etwa Administratoren Zugang zu den Datenbanken verschaffen.

Nichtdestotrotz bestehen weitere Szenarien der nichtautorisierten Zweckentfremdung, etwa durch rauskopieren von Texten aus dem Browser in andere Anwendungen oder Einsichtnahme in Fällen in denen sich ein/e Benutzer/in nicht ausgeloggt hat.

5 Erfahrungen

Die TalkReflect App befindet sich in einer frühen Phase der Langzeitevaluation. Zusätzliche Anforderungen werden nur noch im geringen Maße umgesetzt. Zuvor wurde sie in zwei unterschiedlichen Anwendungskontexten (Klinik und Pflegeheim) insgesamt 8 Wochen testweise eingesetzt und evaluiert. Die Anwendungsgruppen bestanden aus jeweils ca. 10 Personen die auf einer Station bzw. in demselben Heim beschäftigt waren.

Datenschutz-Features sind nur bei einer kleinen Zahl von Fällen merkbar relevant

Wie auch schon die Vorabuntersuchung vermuten ließ, gibt es keinen direkten Zusammenhang zwischen den vorab geäußerten Datenschutzbedenken und der Nutzung von Datenschutzfreundlichen Funktionen wie dem anonymen veröffentlichen von Kommentaren oder den Möglichkeiten für jeden Beitrag spezielle Leseberechtigungen zu vergeben. Während sich in der Befragung ein durchschnittlich recht hoher "Privacy Concern", insbesondere in der Klinik, ermitteln ließ, schlägt sich das in der Nutzung nicht sichtbar nieder. In der Regel registrieren sich die Nutzer/innen mit ihrem Namen oder einem leicht zuzuordnenden Kürzel, Beiträge werden nicht-anonym verfasst und meist mit allen anderen Nutzer/innen geteilt. Nichtsdestotrotz wurde in den Feedbacks betont, dass es den Nutzer/innen wichtig ist, dass die Funktionen zur Verfügung stehen. Statistische Auswertungen zur Nutzung der Funktionen sind allerdings erst nach Abschluss des Langzeittest möglich. Bisher wurde die Anwendung vor allem in kleinen Gruppen genutzt, in denen alle Nutzer/innen sich persönlich bekannt sind. Die Notwendigkeit von Funktionen, wie dem anonymen Veröffentlichen von Nachrichten, ergibt sich in der Regel auch nicht in der Breite, sondern zeigt sich vor allem in – wesentlich selteneren – kritischen Situationen.

Usability vs. Datenschutz

Bereits nach den ersten Tests hat sich gezeigt, dass es eine – fast schon klassische - Diskrepanz zwischen den Anforderungen einer komfortablen Nutzung und dem Einsatz möglichst Datenschutzfreundlicher Funktionen gibt. So gab es schon nach kurzer Zeit von Seiten der Nutzer/innen den Wunsch, dass es möglich sein müsse unkompliziert einen Beitrag sofort mit allen anderen Nutzer/innen zu teilen, statt alle einzeln auszuwählen. Mit der Einführung einer Gruppenverwaltung entstanden aber weitere Fragen wie etwa, ob alle Beiträge die für eine Gruppe sichtbar sind, auch denjenigen zugänglich sein sollten, die später der Gruppe hinzugefügt werden.

Priorität von Datenschutzanforderungen sinkt im Laufe des Projekts

Weitere Probleme betreffen nicht nur die technische Umsetzbarkeit sondern auch die Frage nach der Organisation des Entwicklungsprozesses. Während einige Entscheidungen, wie die Clientseitige Verschlüsselung auf Grund der hohen Komplexität und des hohen Anfangsaufwands, schon früh verworfen wurde, stehen weitere Anforderungen an die Datensicherheit noch aus. Einen besseren Schutz der Infrastruktur und Sicherstellung der Verfügbarkeit auf der Ebene von Servern und Backups ist noch genauso umzusetzen wie Funktionen in der Anwendung, die etwa das nachweisbare Löschen von Einträgen ermöglichen. Allerdings verschiebt sich innerhalb der Entwicklungszyklen die Priorität von datenschutz- und datensicherheitsfreundlichen Anforderungen immer weiter zugunsten von erweiterten Nutzungsfunktionen und einfacheren Bedienkonzepten

6 Zusammenfassung

Der vorliegende Beitrag beschreibt die Entwicklung einer webbasierten Anwendung zur Unterstützung kollaborativer Reflexion am Arbeitsplatz. Da die Idee des gemeinsamen Lernens durch Reflexion vorrausetzt, dass die Nutzer/innen Inhalte miteinander teilen, war die Berücksichtigung verschiedener Perspektiven bei der Entwicklung von zentraler Bedeutung. Dabei wurde auf bekannte Prinzipien des Privacy By Design zurückgegriffen, um möglichst frühe Anforderungen zu entwickeln und umzusetzen, die die informationelle Selbstbestimmung der Nutzer/innen unterstützen.

Der Schwerpunkt der Entwicklung lag dabei auf der Umsetzung von sechs abstrakten Anforderungen die aus der Literatur, sowie einer Nutzer/innen-Befragung hergeleitet wurden. Dabei zeigte sich in der Abschlussevaluation, dass Privacy By Design alltagstauglich ist, und gerade in einem agil durchgeführten Projekt dazu führt, dass Datenschutzrelevante Anforderungen früh umgesetzt werden müssen, da ihre Umsetzung später merklich komplexer und gleichzeitig niedriger priorisiert sein kann.

Literaturverzeichnis

[Be07] Beisenherz, G., Tinnefeld, M.-T., 2011. Aspekte der Einwilligung. Datenschutz Datensicherheit - Dud 35, 110–115.

[Bi07] Bizer, J., 2007. Sieben goldene Regeln des Datenschutzes. Datenschutz Datensicherheit 31, 350–356.

[Ca09] Cavoukian, A., 2009. Privacy by Design - The 7 Foundational Principles.

[Cl05] Clarke, S., 2005. Informed Consent and Electronic Monitoring in the Workplace, in: Electronic Monitoring In The Workplace: Controversies And Solutions. p. 227.

[De11] Degeling, M., Ackema, R., 2011. D9.1 User studies on privacy needs, privacy model and privacy guidelines (MIRROR Project Deliverable No. D9.3).

[Gü10] Gürses, F.S., 2010. Multilateral Privacy Requirements Analysis in Online Social Network Services. K.U. Leuven, Heverlee.

[Gü11] Gürses, F.S., Troncoso, C., Diaz, C., 2011. Engineering Privacy by Design. Comput. Priv. Data Prot.

[La01] Langheinrich, M., 2001. Privacy by Design — Principles of Privacy-Aware Ubiquitous Systems, in: Ubicomp 2001: Ubiquitous Computing, Lecture Notes In Computer Science. Springer Berlin / Heidelberg, pp. 273–291.

[Pr12] Prilla, M., Degeling, M., Herrmann, T., 2012. Collaborative Reflection at Work: Supporting Informal Learning at a Healthcare Workplace, in: Proceedings of the ACM International Conference on Supporting Group (GROUP 2012).

[Sch10] Schaar, P., 2010. Privacy by Design. Identity Inf. Soc. 3, 267–274

[Si05] Siponen, M., Baskerville, R., Kuivalainen, T. 2005: Integrating Security into Agile Development Methods. Proceedings of the 38th Annual Hawaii International Conference on System Sciences, 2005. HICSS '05.

[Sp09] Spiekermann, S., Cranor, L.F., 2009. Engineering Privacy. Ieee Trans. Softw. Eng. 35, 67–82.

[Wo08] Van Woerkom, M., Croon, M., 2008. Operationalising critically reflective work behaviour. Pers. Rev. 37, 317–331.