Anforderungen und Rahmenwerk für den betrieblichen Datenschutz

Hartmut Schmitt
HK Business Solutions GmbH, Sulzbach
hartmut.schmitt@hk-bs.de

Svenja Polst
Fraunhofer IESE, Kaiserslautern
svenja.polst@iese.fraunhofer.de

Zusammenfassung

In diesem Beitrag berichten wir über einen Ansatz zur Entwicklung praxistauglicher und rechtskonformer Lösungen für den betrieblichen Datenschutz. Wir geben einen Überblick über unseren agilen RE-Prozess bei der Anforderungserhebung, Modellierung und Lösungskonzeption und berichten über die Besonderheiten, etwa beim Umgang mit gegensätzlichen Stakeholderinteressen und konkurrierenden Qualitätseigenschaften.

Kontext und Motivation

Durch die Digitalisierung haben Unternehmen heute die Möglichkeit, in umfassender Weise Daten ihrer Arbeitsprozesse zu erheben und zu analysieren. Hierbei fallen immer mehr personenbezogene Daten wie Kunden- oder Mitarbeiterdaten an, wodurch die informationelle Selbstbestimmung der Betroffenen gefährdet sein kann. Aktuell haben diese meist weder das Wissen noch die Möglichkeit, die erhobenen Daten, deren Verarbeitung und mögliche Konsequenzen für ihre Privatsphäre zu verstehen, geschweige denn zu kontrollieren. Dem Interesse der Unternehmen, die Potentiale einer umfänglichen Datenanalyse zu nutzen, stehen also die Selbstbestimmungsrechte und mögliche Informationsziele der Betroffenen entgegen.

Die EU-Datenschutzgrundverordnung sorgt seit Mai 2018 dafür, dass der betriebliche Datenschutz strenger reguliert wird. Unternehmen haben erweiterte Informationspflichten gegenüber den Betroffenen, müssen Verarbeitungsverzeichnisse für personenbezogene Daten erstellen und Datenschutzpannen melden. Das Problem: Da die Regeln der DSGVO oft schwammig formuliert sind, wissen viele Unternehmen nicht, wie sie sich genau zu verhalten haben [1]. 74 % der Unternehmen sehen einer aktuellen Bitkom-Studie zufolge Datenschutzanforderungen sogar als größte Hürde beim Einsatz neuer Technologien [2].

Unser Ziel ist es daher, mehr Transparenz bei der Erhebung und Nutzung personenbezogener Daten im Unternehmen zu schaffen und den Betroffenen entsprechende Einstellmöglichkeiten zur Durchsetzung ihrer Interessen zur Verfügung zu stellen; dies erfolgt in Form sog. *Privacy Dashboards*. Hierbei betrachten wir insbesondere den Bereich Mitarbeiterdatenschutz, für den wir einen fairen Interessenausgleich zwischen Arbeitgebern, Arbeitnehmern und Arbeitnehmervertretungen, z. B. Betriebs- und Personalräten, anstreben. Mit diesem Bericht wollen wir andere Initiativen und Projekte in den Bereichen Privatsphäre, RE und betrieblicher Datenschutz an unseren Erkenntnissen teilhaben lassen.

RE-Prozess und Besonderheiten

Für unser Vorhaben [3] haben wir eine iterative Vorgehensweise mit insgesamt sechs halbjährigen Iterationen gewählt. Sämtliche Entwicklungsergebnisse werden im Projektverlauf regelmäßig evaluiert und die zugrundeliegenden Anforderungen werden kontinuierlich aktualisiert, z. B. bei technischen Neuerungen oder Urteilen zur DSGVO. Im Folgenden stellen wir die Besonderheiten und Herausforderungen beim betrieblichen Datenschutz vor und beschreiben, wie wir diese in der Anforderungs- und Konzeptionsphase angegangen haben:

(1) Der Privatsphäreschutz und die Verwendung personenbezogener Daten im beruflichen Kontext stehen in einem Spannungsfeld. Mögliche Konflikte müssen schon in der Anforderungsphase berücksichtigt werden.

(2) Momentan gibt es nur wenig Literatur zur Privatsphäre von Arbeitnehmern, was die Entwicklung entsprechender Privacy Dashboards herausfordernd gestaltet. Potentielle Untergruppen der Stakeholdergruppe „Arbeitnehmer“ müssen identifiziert werden.

(3) Unternehmen unterscheiden sich hinsichtlich der Branche, Fähigkeiten der Mitarbeiter und der Möglichkeiten, ein Privacy Dashboard in ihre Systemlandschaft zu integrieren. Wir wollen daher eine Grundlage für die Entwicklung von Privacy Dashboards schaffen, die für viele Unternehmen nützlich ist, aber über die bloße Dokumentation von Anforderungen hinausgeht.

Der Fokus unseres Berichts liegt auf dem Umgang mit widersprüchlichen Bedürfnissen im RE-Prozess (vgl. *Bedarfskategorien* und *Qualitätsmodell*), dem Vorgehen, um Arbeitnehmer besser zu verstehen (*vgl. Mentales Modell)*, und der Aufarbeitung von Ergebnissen für Unternehmen *(vgl. Modellierungsrahmenwerk)*.

Bedarfskategorien

Als Grundlage für die Erhebung und Dokumentation der Stakeholderbedürfnisse und -anforderungen haben wir ein *Anforderungsmodell* entwickelt, das es uns erlaubt, potentielle Spannungen und Konflikte herauszuarbeiten. Es unterscheidet folgende Bedarfskategorien:

Ein *Selbstbestimmungsbedarf* beschreibt einen Bedarf bzw. Wunsch einer Person nach eigenem Einfluss auf die Verwendung eigener Daten.

Ein *Transparenzbedarf* beschreibt einen Bedarf bzw. Wunsch einer Person nach Informationen über die Verwendung ihrer personenbezogenen Daten.

Ein *Schutzbedarf* beschreibt einen Bedarf bzw. Wunsch einer Person nach Schutz ihrer Privatsphäre.

Ein *Datennutzungsbedarf* beschreibt einen Bedarf bzw. Wunsch einer Person nach dem Zugriff auf Informationen über bestimmte Abläufe oder Sachverhalte. Die Datennutzungsbedarfe stehen in Konflikt mit Schutzbedarfen.

Eine *Benutzeranforderung* beschreibt eine Rahmenbedingung oder einen Bedarf bzw. Wunsch eines Stakeholders hinsichtlich der Bedienung oder Funktionalität des Dashboards.

Weitere Anforderungen, die im betrieblichen Kontext eine Rolle spielen, sind *Einführungsanforderungen* (z. B. Schulungsbedarf) und *Supportanforderungen* (z. B. Verfügbarkeit von Ansprechpartnern). Für jede Bedarfs- bzw. Anforderungskategorie haben wir entsprechende Fragen formuliert, z. B. „Welche meiner personenbezogenen Daten halte ich bei meiner Arbeit generell für schützenswert?“, und in Workshops mit Stakeholdern bearbeitet. Anschließend haben wir zu jedem Datennutzungsbedarf die konfliktiven Schutzbedarfe erhoben und somit eine gute Basis geschaffen, um diese Konflikte in den folgenden Arbeiten anzugehen.

Qualitätsmodell

Bei der Entwicklung betrieblicher Privacy Dashboards sind unterschiedliche Qualitätseigenschaften von Bedeutung, die wir in einem *Qualitätsmodell* dokumentiert haben. Diese Eigenschaften können sich auf die Produktqualität beziehen (z. B. Zuverlässigkeit), aber auch auf die Nutzungsqualität (z. B. Zufriedenheit), die Prozessqualität (z. B. Prozesskonformität) oder die Strukturqualität (z. B. Bewusstsein der Mitarbeiter). Als Grundlage unseres Qualitätsmodells dienten die ISO-Normen 9001, 9241 und 25010, das Modell Gokyo Ri [5] sowie das Standard-Datenschutzmodell [6].

Unser besonderes Augenmerk gilt konkurrierenden Qualitätseigenschaften, also Beziehungen, bei denen die Verbesserung der einen Eigenschaft eine Verschlechterung der anderen Eigenschaft nach sich zieht [4]. Beispielsweise sind sechs Datenschutz-Schutzziele, die wir aus dem Standard-Datenschutzmodell übernommen haben, als Dual-Achsen mit jeweils komplementären Schutzzielen angelegt: Verfügbarkeit–Vertraulichkeit, Integrität–Intervenierbarkeit und Transparenz–Nichtverkettung. Hierbei können die beiden Ziele auf einer Achse nicht gleichzeitig maximiert werden, ohne dass es zu Widersprüchen bzw. Konflikten kommt. Ein Beispiel: Der maximalen Verfügbarkeit (personenbezogene Daten können immer wie vorgesehen genutzt werden) steht die maximale Vertraulichkeit (nur Befugte dürfen in zulässiger Weise auf die personenbezogenen Daten zugreifen) im Wege.

Mentales Modell

Um das Dashboard möglichst gut an den Vorstellungen der Endnutzer auszurichten, haben wir das *mentale Modell* von Arbeitnehmern hinsichtlich ihrer Privatsphäre untersucht. Fragestellungen waren hierbei z. B., was Arbeitnehmer unter personenbezogenen Daten verstehen und ob bzw. wie sie sich in ihrem mentalen Modell unterscheiden. Es wurde ein Expertenmodell entwickelt, das auf Literatur zu Privatsphäre im privaten Kontext sowie Expertenmeinungen basiert; dieses wurde in Interviews validiert, angepasst und es wurden Anforderungen abgeleitet, die z. B. die Verwendung von Bezeichnungen in der Benutzeroberfläche des Dashboards betreffen. Zudem flossen die Erkenntnisse in die Entwicklung von Personas ein.

Modellierungsrahmenwerk

Unsere Ergebnisse sollen Unternehmen eine Entscheidungs- und Arbeitsgrundlage bieten, um ihr eigenes Privacy Dashboard zu entwickeln. Wir haben die Ergebnisse – Rahmenbedingungen, Konzepte und Modelle sowie deren Zusammenhänge mit Bedarfen und Anforderungen – in einem *Modellierungsrahmenwerk* zusammengefasst. In dem Rahmenwerk ist zudem ein Stufenkonzept enthalten, das bei der schrittweisen Einführung von Privacy Dashboards unterstützt – angefangen beim reinen Informationspanel bis hin zur Transparentmachung von Datenfluss-Manipulationen in Echtzeit. Konkrete Ausgestaltungen, die z. B. das Grafikdesign betreffen, sind nicht Teil des Rahmenwerks, da sie stark von den individuellen Wünschen und Corporate-Design-Vorgaben eines Unternehmens abhängen.

Fazit

Unternehmen haben mit dem Rahmenwerk die Möglichkeit, die oben beschriebenen Konflikte entsprechend ihren individuellen Anforderungen aufzulösen und konkurrierende Beziehungen zwischen Qualitätseigenschaften auszutarieren; sie können im Rahmen der gesetzlichen Vorgaben und ähnlicher Randbedingungen also jeweils einen Trade-off finden, der gut zur eigenen Organisation passt. Die Nutzer wiederum haben innerhalb ihrer persönlichen Privacy Dashboards Einstellmöglichkeiten, mit denen sie ihre individuellen Anforderungen und Bedürfnisse ausdrücken können (z. B. maximale Vertraulichkeit der personenbezogenen Daten).

Das Projekt TrUSD, in dessen Rahmen diese Arbeit entstand, wird vom Bundesministerium für Bildung und Forschung gefördert (FKZ: 16KIS0896K, 16KIS0898).

Referenzen

[1] Martin-Jung, H. (2019). Das verflixte erste Jahr. Süddeutsche Zeitung vom 25.05.2019

[2] IT-Sicherheit (2019). Bitkom zieht gemischte Jahresbilanz zur DS-GVO. https://www.itsicherheit-online.com/blog/detail/sCategory/222/blogArticle/3130

[3] TrUSD – Transparente und selbstbestimmte Ausgestaltung der Datennutzung im Unternehmen. https://www.trusd-projekt.de/

[4] Ernest Wallmüller, E. (2002). Qualitätsmodelle im Software Engineering. In: MQ - Management und Qualität 2002(9). Galledia Verlag, Berneck.

[5] Messung und Bewertung von Prozessqualität mit Gokyo Ri. http://www.kneuper.de/GokyoRi/

[6] Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder (2018). Das Standard-Datenschutzmodell.