

Wo ist das Problem?

Mit Design Thinking Innovationen entwickeln und umsetzen

Bearbeitet von
Markus Blatt, Emmanuel Sauvonnet

2. Auflage 2017. Buch. 233 S. Kartoniert
ISBN 978 3 8006 5318 8
Format (B x L): 24,0 x 19,0 cm

[Wirtschaft > Management > Unternehmensführung](#)

Zu [Inhalts-](#) und [Sachverzeichnis](#)

schnell und portofrei erhältlich bei


DIE FACHBUCHHANDLUNG

Die Online-Fachbuchhandlung [beck-shop.de](#) ist spezialisiert auf Fachbücher, insbesondere Recht, Steuern und Wirtschaft. Im Sortiment finden Sie alle Medien (Bücher, Zeitschriften, CDs, eBooks, etc.) aller Verlage. Ergänzt wird das Programm durch Services wie Neuerscheinungsdienst oder Zusammenstellungen von Büchern zu Sonderpreisen. Der Shop führt mehr als 8 Millionen Produkte.

Mehrheit war davon überzeugt, dass Daten missbraucht werden bzw. Unternehmen Daten weitergeben.

Während das allgemeine Gefährdungspotenzial von allen grundsätzlich erkannt wurde, zeigten sich große Wissensunterschiede hinsichtlich konkreter Gefährdungen. „Digital Natives“ kennen die mit fehlender Privacy einhergehenden potenziellen Gefahren und würden sich einen nach wie vor einfachen Umgang mit dem Internet wünschen, jedoch mit einem zumindest ausreichenden Schutz der persönlichen Daten. Unter den beteiligten Personen mit Kindern herrscht insbesondere in ihrer Funktion als Elternteil ein klarer Konsens, dass Kontrolle über persönliche Daten wünschenswert wäre. Die mangelnde Transparenz dessen, „was im Internet alles so passiert und gemacht wird“, so wie ihr fehlendes technisches Know-how empfanden sie als frustrierend. Die Tatsache, dass die tatsächliche Verwendung von persönlichen Daten nicht nachvollziehbar ist, war Grund genug für einige Teilnehmer, deren Preisgabe bei der Internetnutzung als notwendiges Übel anzusehen.

Die Unternehmensvertreter unterstrichen einhellig den Stellenwert persönlicher Daten für ihr Unternehmen; sie sahen gleichzeitig die Notwendigkeit, mehr Transparenz bei der Daten-Verwendung anzubieten, und für den Fall, dass ihre Unternehmen einen messbaren Nutzen durch die Bereitstellung persönlicher Daten erzielen, die Daten-Besitzer entsprechend zu belohnen. Eine direkte monetäre Belohnung wurde allerdings von allen Unternehmensvertretern abgelehnt. Stattdessen wurde bspw. ein Kupon-System vorgezogen.

Überraschend war, dass alle Teilnehmer auf Basis zahlreicher Anwendungsfälle die Gefahren eines unkontrollierten IoT erkannt haben und sich hierfür eine Lösung wünschten.

Ideen finden

Im Rahmen eines Brainstormings wurde zunächst eine Vielzahl von Ideen generiert. Im Anschluss daran mussten die zahlreichen Lösungsvorschläge gesammelt, geordnet und geclustert werden. Im Ergebnis konnten die drei folgenden Ansätze identifiziert werden:

- Bei Ansatz 1 lag die Hauptstoßrichtung darin, dass datennutzende Unternehmen dem Privacy-Problem einen höheren Stellenwert einräumen und unternehmensintern hierfür Lösungen implementieren sollten. In diesem Zusammenhang wurden zusätzliche Privacy-Mechanismen und -Features vorgestellt und diskutiert.
- Ansatz 2 zielte auf mehr Aufklärung der Nutzer. Hier waren allerdings nur wenige Teilnehmer der Meinung, dass „das Internet sich von allein“ regeln und „Benutzer besser selbst aufpassen“ sollten. Offen blieb bei diesem Ansatz der Selbstregulierung u.a. die Frage, von wem diese Aufklärung initiiert und durchgeführt werden könne und solle, und ob die dargestellten Herausforderungen damit wirklich gelöst werden könnten. Dieser Do-nothing-Ansatz wurde schließlich als nicht-zielführend nicht weiterverfolgt.

- Lösungsvorschläge, die sich einer dritten Gruppe zuordnen ließen, stellten eine gesetzgeberische Lösung in den Vordergrund. Hierbei sollten die bereits bestehenden Gesetze zum Schutz der Privatsphäre „modernisiert“ und stärker auf die Gegebenheiten des Internets erweitert werden. Erörtert wurden hierbei stärkere Kontrollen und Strafen bei Missachtung und Verstößen.

Als hilfreich erwies sich für alle Teilnehmer, die Aufgabenstellung zu visualisieren und bspw. den Daten mit Legosteinen von unterschiedlicher Farbe, Form und Größe oder den Datenbeziehungen mit farbigen Fäden eine spielerisch-haptische Dimension zu geben.

Es ist hilfreich, die Aufgabenstellung zu visualisieren, bspw. mit Legosteinen oder farbigen Fäden.

3.5 Wie entwickelt man ein ganz neues Produkt aus Nutzersicht

Alle drei Ansätze wurden aber relativ schnell verworfen. Bei Ansatz 1 wurde als Hauptargument mangelnde Neutralität gesehen, da Unternehmen – innerhalb gesetzlicher Rahmenbedingungen – in erster Linie ihre eigenen Interessen wahrnehmen und erst in zweiter Linie die ihrer Kunden. Bei dem gesetzgeberischen Ansatz wurden insbesondere die vermutlich langsame Umsetzungsgeschwindigkeit und die geografische Limitierung nationalstaatlicher Regulierungen ins Feld geführt. Auf die Diskussion zum aktuellen Stand der europäischen Datenschutzreform (EU-Datenschutz-Grundverordnung) wurde in diesem Zusammenhang nicht intensiver eingegangen.

Iteration des Lösungsansatzes - Privacy als Produkt

Vor diesem Hintergrund wurde ein weiterer Ansatz entwickelt, der den Schutz von Privacy in den Mittelpunkt rückt und als Produkt anbietet, auf dessen Basis Zusatzdienste aufgebaut werden können. Der unter dem Arbeitstitel „PrivacyGuard“ entwickelte Ansatz basiert auf den folgenden Grundprinzipien:

Privacy-Plattform mit Persona- oder Profilmanagement als Kern des Lösungsansatzes

Anvisiert werden zunächst Aufbau und Betrieb einer Plattform für den kontrollierten Austausch persönlicher Daten zwischen Usern und Unternehmen. Auch von IoT-Geräten erhobene Daten, die mit der Außenwelt kommunizieren können, werden durch die Privacy-Plattform erheblich sicherer. Alle von der Plattform angebotenen Dienste basieren auf Privacy. Die Plattform schafft für den jeweiligen User Transparenz und ermöglicht die Ausübung vollständiger Kontrolle über persönliche Daten aus verschiedenen Quellen. Darüber hinaus wird über die Plattform ein

Teil 3: Mit Design Thinking Innovationen entwickeln

fairer (Gegen-)Wert für die Benutzung von Daten ermittelt und dieser für den Fall der Nutzung übertragen.

Über die Dienste hinaus, die Teil der Plattform sind, um Privacy, Kontrolle und Wertermittlung zu gewährleisten, versucht die Plattform nicht, persönliche Daten in eigener Sache zu nutzen, Mehrwertdienste nachzubilden oder anzubieten. Der Kern des Geschäftsmodells besteht darin, dass ein Plattformbetreiber Privacy als Produkt anbietet. Zwei Gestaltungsmodelle können dafür verwendet werden:

Lösung 1: Der Plattformbetreiber stellt als neutrale Instanz sicher, dass bei jeder über seine Plattform stattfindende Kommunikation nur die von einem User freigegebenen persönlichen Daten weitergegeben werden. Die Plattform fungiert damit als Privacy-Betriebssystem, bei dem nur das durchgeht, was aus User-Sicht auch durchgehen soll. Um Privacy-Settings zu respektieren, wird dieser Privacy-Layer für jede Kommunikation über das Internet benutzt.

142

beck-shop.de
DIE FACHBUCHHANDLUNG

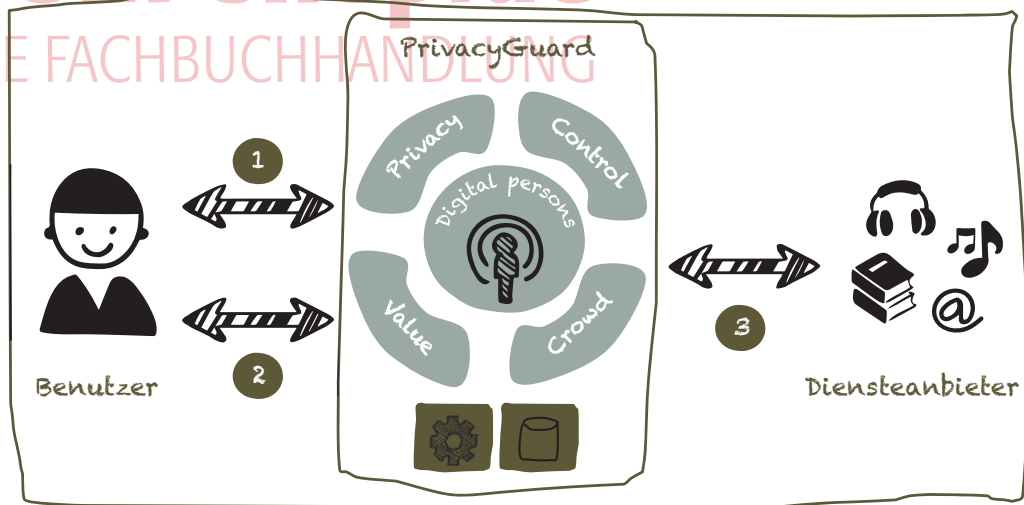


Abbildung 34: Privacy als Produkt – Lösung 1

3.5 Wie entwickelt man ein ganz neues Produkt aus Nutzersicht

Lösung 2: Diensteanbieter erfahren User-Einstellungen über eine Abfrage bei der Privacy-Plattform. Die Plattform antwortet mit angefragten und freigegebenen Daten zusammen mit einem Zertifikat. Der Diensteanbieter kann dann dem User auf seine Bedürfnisse zugeschnittene Dienste anbieten.

Einnahmemöglichkeiten bestehen für einen Plattform-Betreiber bei privaten Usern (bspw. mit einem geringen monatlichen Pauschalbetrag) sowie bei Unternehmen, die auf gezielt freigegebene, persönliche User-Daten zugreifen möchten. Der gebotene Gegenwert für die Bereitstellung dieser Userdaten wird vom Unternehmen bestimmt.

In ihrer einfachsten Ausprägung administriert und kontrolliert die Privacy-Plattform persönliche Daten und hält User-bezogene Privacy-Einstellungen bereit. Der Benutzer gibt seine Privacy-Einstellungen zu den von ihm benutzten Diensten ein; ein Online-Diensteanbieter fragt diese ab, um sie verwenden zu können.

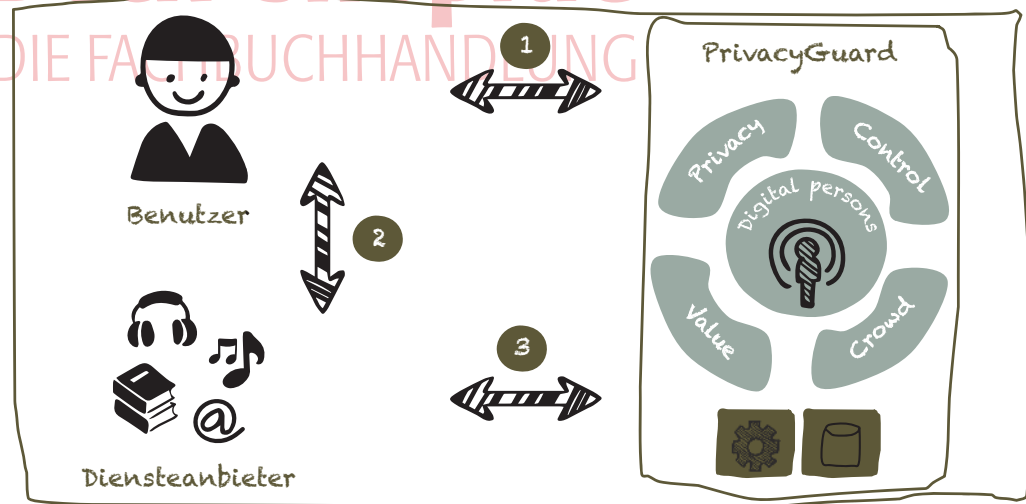


Abbildung 35: Privacy als Produkt – Lösung 2

Teil 3: Mit Design Thinking Innovationen entwickeln

Idealerweise speichert die Plattform nicht nur Privacy-Einstellungen, sondern auch User-Profile, die die vom Benutzer eingestellten Präferenzen wiedergeben. Über diese Präferenzeinstellungen können User ihre Vorlieben eingeben und selbst bestimmen, wer wann und für welchen Gegenwert ihre Daten benutzen darf. So würde bspw. ein Hotelsuchdienst, der ein passendes Hotel für einen Interessenten finden möchte, erfahren, dass dieser Golf spielt, und ihm – und zwar auf seiner Einwilligung basierend – u.a. ein Hotel am Golfplatz anbieten.

Da Privacy-Einstellungen in hohem Maße subjektiv sind, könnten die über die Plattform angebotenen Dienste intelligente Mechanismen zur Verfügung stellen, um einem User eine auf seine individuellen Bedürfnisse zugeschnittene Privacy-Einstellung anzubieten. Hierzu zählt auch das „Recht auf Vergessen“, wobei User-Daten unwiderruflich gelöscht werden können.

144

beck-shop.de
DIE FACHBUCHHANDLUNG

Über diese Grundprinzipien hinaus wurde hervorgehoben, dass die Benutzung von persönlichen Daten kontextbezogen ist. Die Plattform sollte also Privacy-Einstellungen im Sinne des aktuellen Kontextes zur Verfügung stellen. So würden bspw. Daten über Hobbies mit Gleichgesinnten geteilt werden, nicht aber mit Unternehmen, die hobby-spezifische Produkte verkaufen. Oft wissen Internet-Nutzer selbst nicht genau, welche Daten oder Informationen für sie relevant sind, oder sie sind sich dessen nicht bewusst. Relevanz und Kontext dienen dazu, das Web semantisch (eindeutig) zu machen. Im Kontext eines Anglerforums wird mit „Bach“ wahrscheinlich der kleinere Bruder des Flusses gemeint sein; bei der Suche nach einem Konzert wahrscheinlich der Komponist. Relevanz dient auch dazu, offensichtliche sowie nicht-offensichtliche Beziehungen herauszufinden.

Relevanz, Kontext und Insight als Ergänzungsbausteine

Die Plattform kann den Wert und die Einsatzmöglichkeiten der Privacy-Einstellungen erweitern, indem Funktionalitäten wie Relevanz, Kontext und „Insight“ in die beabsichtigte Verwendung der Daten einbezogen und berücksichtigt werden. Diese Funktionalitäten wären gleichzeitig die Grundlage für Unternehmen, Produkte und Dienstleistungen mit einer signifikant höheren Treffer- und damit Verkaufswahrscheinlichkeit vermarkten zu können. Der Kern der Lösung wird somit durch die Erfüllung der Privacy-Bedürfnisse des Kunden gebildet, entfaltet jedoch für ein weiterreichendes Geschäftsmodell seine volle Wirkung erst durch die Integration der Funktionalitäten Relevanz, Kontext und Insight. Diese Funktionalitäten wären deshalb Ergänzungsbausteine, um mit der skizzierten Privacy-Plattform eine ganzheitliche Lösung entwickeln zu können. Wie in der nachfolgenden Übersicht dargestellt, leiten sich daraus zahlreiche Use Cases ab.

Die Plattformfunktionalitäten werden durch Application Programming Interfaces (APIs) der Außenwelt zugänglich gemacht. Mithilfe der APIs können Dienste bereichert oder neu gebaut und angeboten werden, die dem User Privacy, Kontrolle und einen Gegenwert garantieren. Als Platzgründen wird hier auf die erarbeiteten Use Cases sowie entsprechende Business Case-Analysen nicht näher eingegangen.

In der nachfolgenden Architektur-Skizze ist der Aufbau der Plattform mit seinen Hauptfunktionalitäten dargestellt.

Teil 3: Mit Design Thinking Innovationen entwickeln

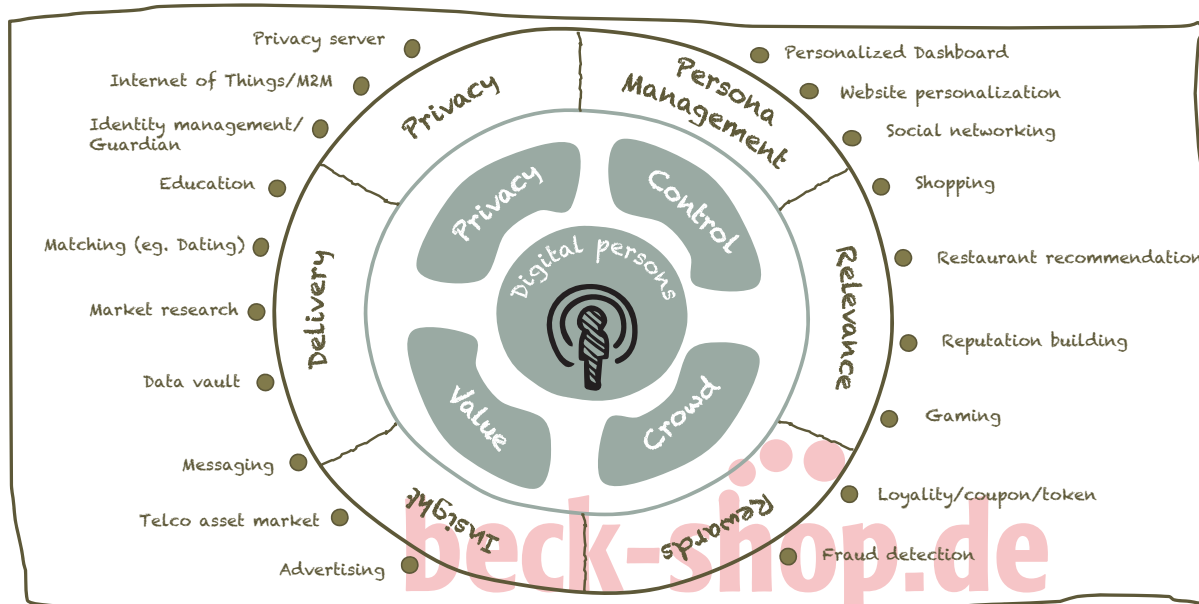


Abbildung 36:
Privacy-Plattform
mit Use Cases

Privacy – das vollständige Management der Privacy eines Users: welche Daten wann zu welchem Preis geteilt werden dürfen.

Persona Management – Persona- oder Profil-Management ist der Kern der Plattform. Präferenzen können hier verwaltet, Pro le durch intelligente Systeme automatisch angepasst und bereichert werden.

Relevanz – diese Funktionalität ermöglicht es, Verbindungen zwischen Daten, Menschen, Communities, Dingen, Diensten und Präferenzen herauszufinden. Mithilfe von Relevanz können User und Unternehmen noch gezielter als bisher Dienste nutzen und anbieten. Damit kann die Plattform ein tiefergehendes Verständnis für die Wünsche der User und