Sven Wohlgemuth

Privatsphäre durch die Delegation von Rechten

VIEWEG+TEUBNER RESEARCH

Sven Wohlgemuth

Privatsphäre durch die Delegation von Rechten

Mit einem Geleitwort von Prof. Dr. Günter Müller

VIEWEG+TEUBNER RESEARCH

Bibliografische Information der Deutschen Nationalbibliothek
Die Deutsche Nationalbibliothek verzeichnet diese Publikation in der Deutschen Nationalbibliografie; detaillierte bibliografische Daten sind im Internet über <http://dnb.d-nb.de> abrufbar.

Dissertation der Albert-Ludwigs-Universität Freiburg im Breisgau, 2008

1. Auflage 2009

Lektorat: Christel A. Roß

Vieweg+Teubner ist Teil der Fachverlagsgruppe Springer Science+Business Media.
www.viewegteubner.de

Umschlaggestaltung: KünkelLopka Medienentwicklung, Heidelberg
Druck und buchbinderische Verarbeitung: STRAUSS GMBH, Mörlenbach
Gedruckt auf säurefreiem und chlorfrei gebleichtem Papier.
Printed in Germany

ISBN 978-3-8348-0721-2

Geleitwort

Die Landschaft für personalisierte Dienstleistungen in der Internetökonomie befindet sich im Wandel. Aufgrund technologischer Neuheiten der Vernetzung und der dadurch erreichbaren Kostenersparnis werden personalisierte Dienstleistungen auf mehrere Dienstleister aufgeteilt. Neue Dienste entstehen. Die Bonusprogramme des Customer Relationship Management (CRM), die JobCard und die elektronische Gesundheitskarte sind dafür Beispiele. Es stellt sich die Frage, wie Nutzer ihre Privatsphäre und damit ihre informationelle Selbstbestimmung schützen können, wenn ihre persönlichen Daten von den Diensten nicht nur erhoben, sondern auch weitergegeben werden müssen. Gegenwärtig übertragen Nutzer ihre informationelle Selbstbestimmung an diese Dienste, indem sie generell zu deren Datenschutzerklärung einwilligen müssen, möchten sie deren Dienstleistung in Anspruch nehmen. Die Informatik bietet zahlreiche Lösungen zum Schutz der Privatsphäre an. Allerdings beziehen sie sich auf die Erhebung persönlicher Daten und nicht auf deren Nutzung. Um die personalisierten Dienstleistungen zu nutzen und gleichzeitig die informationelle Selbstbestimmung zu bewahren, müssen die informatischen Sicherheitssysteme dem Nutzer auch die Durchsetzung der Regeln zur Nutzung persönlicher Daten ermöglichen. Hierzu leistet die vorliegende Arbeit einen originellen Beitrag, indem sie statt der direkten Datenweitergabe die kontrollierte Delegation von Rechten vorschlägt.

Der Autor stellt zwei neuartige Protokolle zur kontrollierten Delegation von Rechten vor, die eine kontrollierte Weitergabe persönlicher Daten nach den vereinbarten Regeln ermöglichen und eine Erweiterung der Zugriffskontrolle des Identitätsmanagement um Konzepte der Nutzungskontrolle darstellen. Er zeigt am Beispiel des CRM das Problem der Verkettbarkeit der Transaktionen eines Nutzers und folglich der indirekten Datenweitergabe bzw. des Kontrollverlustes über den Zugriff auf persönliche Daten, wenn heutige Sicherheitssysteme zur Delegation von Rechten bzw. zum Schutz der Privatsphäre bei der Nutzung der neuen Dienste eingesetzt werden. Ihr Einsatz verlangt nach einer vertrauenswürdigen dritten Partei. Die Arbeit baut auf existierenden Public-Key Infrastrukturen auf und zeigt damit einen neuen Anwendungsbereich für anonymisierte Credentials, die prinzipiell diese dritte Partei vermeiden können. Anhand einer Implementierung der Protokolle zeigt der Autor deren Machbarkeit und Schutzwirkung. Die Problemstellung darf für sich in Anspruch nehmen zugleich praktisch relevant und wissenschaftlich anspruchsvoll zu sein. Daher wünsche ich der Arbeit die verdiente Aufnahme in Wissenschaft und Industrie.

Prof. Dr. Günter Müller

Vorwort

Die vorliegende Arbeit wurde im Sommersemester 2008 von der Fakultät für Angewandte Wissenschaften der Abert-Ludwigs-Universität Freiburg als Dissertation angenommen. Sie bildet den Abschluss meiner Promotion am Institut für Informatik und Gesellschaft. An dieser Stelle möchte ich mich bei allen bedanken, die zum Gelingen dieser Arbeit beigetragen haben.

An erster Stelle gilt mein herzlichster Dank meinem akademischen Lehrer und Doktorvater Prof. Dr. Günter Müller. Die gewährte akademische Freiheit und seine direkte und offene Art der konstruktiven Kritik haben das Gelingen dieser Arbeit wesentlich gefördert. Zudem möchte ich mich für sein Vertrauen und die damit verbundene Übertragung von verantwortungsvollen und vielfältigen Aufgaben bedanken. Die dabei gewonnen Erfahrungen reichen weit über die Promotion hinaus und haben sich jetzt als äusserst wertvoll erwiesen.

Bei Herrn Prof. Dr. Gerhard Schneider möchte ich mich für die Übernahme des Zweitgutachtens unter der engen zeitlichen Restriktion bedanken. Für die finanzielle Förderung meiner Arbeit im Rahmen des Schwerpunktprogramms *Sicherheit in der Informations- und Kommunikationstechnik* bzw. des Network of Excellence *Future of Identity in the Information Society (FIDIS)* danke ich der Deutschen Forschungsgemeinschaft und der Europäischen Kommission.

Von den Kolleginnen und Kollegen der Abteilung Telematik des Instituts für Informatik und Gesellschaft habe ich große Unterstützung erhalten. Dafür möchte ich mich bei Ihnen herzlich bedanken. Insbesondere die intensiven Diskussionen mit Frau Maike Gilliot, Herrn Dr. Stefan Sackmann, Herrn Dr. Jens Strüker, Herrn Dr. Adolf Hohl, Herrn Dr. Moritz Strasser und Herrn Sebastian Höhn waren sehr wertvoll. Frau Julia Bär danke ich für Ihre stete Hilfsbereitschaft und Prüfung meiner englischsprachigen Texte.

Einen großen Dank gebührt auch meinen Freunden Herrn Wolfgang Kimmig, Herrn Andreas Künze und Herrn Kai Pleger. Vor allem im letzten Jahr der Promotion gab mir die gemeinsame Zeit beim Tennisspiel die erforderliche Kraft.

Ein besonders großes und herzliches Dankeschön gebührt meiner Mutter, die mich während meiner gesamten Ausbildungszeit uneingeschränkt unterstützt hat. Ohne ihre Unterstützung wäre mein persönlicher und beruflicher Werdegang nicht möglich gewesen. Es ist mir daher eine große Freude, ihr diese Arbeit zu widmen.

Sven Wohlgemuth

Inhaltsverzeichnis

1 Privatsphäre: Eine Frage des Vertrauens?

Allein im deutschen Wirtschaftsraum erheben 65,2% der Unternehmen persönliche Daten ihrer Nutzer, und über die Hälfte dieser Unternehmen planen diese Erhebung auszuweiten [SS05]. Die Unternehmen erreichen damit eine personalisierte Ansprache (57,0%), die Individualisierung von Verkaufsgesprächen (53,8%) und die individuelle Anpassung ihrer Produkte bzw. Dienstleistungen (47,4%). Ferner vernetzen sich Unternehmen über das Internet, um Kosten zu senken und externe Dienstleistungen in die eigenen Geschäftsprozesse zu integrieren. Damit entstehen neue technische Datendienste, welche die erhobenen Daten verwalten, sie an andere Dienste weitergeben und ggf. selbst personalisierte Dienstleistungen anbieten. So nehmen Diensteanbieter nicht nur die Rolle eines Datenkonsumenten sondern auch die eines Datenanbieters ein. Sie können Profile über Nutzer erstellen, zu denen sie Daten erhoben oder von einem Datendienst erhalten haben. Die Anwendungsfälle der Erhebung persönlicher Daten und ihrer Weitergabe unterscheiden sich zudem in der Kommunikationsbeziehung eines Nutzers. Bei der erstmaligen Erhebung persönlicher Daten kommuniziert ein Nutzer direkt mit dem Datenkonsumenten. Der Informationsfluss der Daten erfolgt in einer 1:1 Beziehung. Bei der Weitergabe persönlicher Daten erhält der Datenkonsument die Daten nicht direkt vom Nutzer, sondern der Datendienst gibt die Daten als Datenanbieter weiter. Es besteht eine 1:n Beziehung. Beispiele für Anwendungen dieser Art eines Informationssystems sind Kundenbindungsprogramme (Customer Relationship Management - CRM) [Lau04], behördliche Dienstleistungen unter Verwendung der Bügerkarte bzw. JobCard [SH04] und medizinische Dienstleistungen unter Verwendung der Gesundheitskarte und der elektronischen Patientenakte [Bun04]. Die Abbildung 1.1 stellt dieses Modell der Datenerhebung und Weitergabe in Anlehnung an [PHB06] dar.

1.1 Alles oder nichts

Die europäischen Datenschutzdirektiven [Eur95, Eur02], das „Volkszählungsurteil“ des Bundesverfassungsgerichts [Bun83] und die nationalen Datenschutzgesetze [Bun97, Bun01] fordern die informationelle Selbstbestimmung, d.h. für eine Erhebung und Weitergabe persönlicher Daten ist eine zweckbezogene Einwilli-

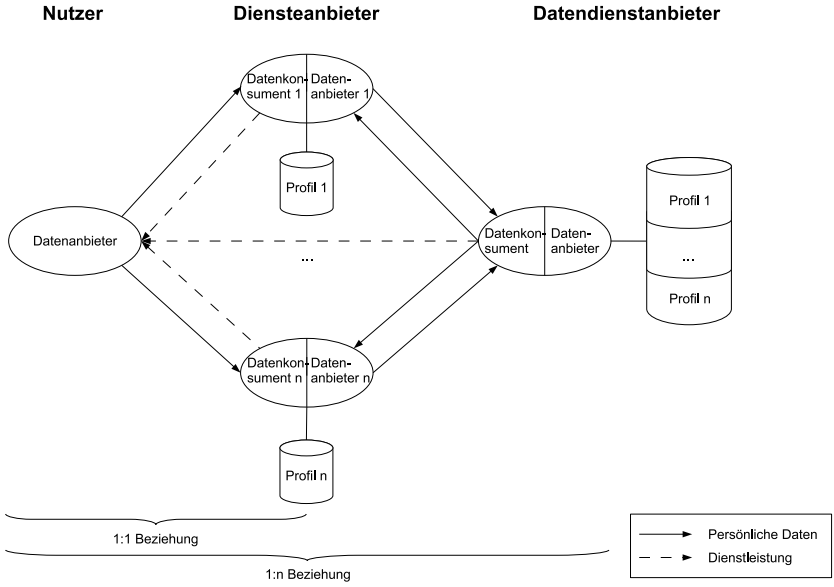

Abbildung 1.1: Modell der Erhebung und Weitergabe persönlicher Daten in Anlehnung an [PHB06].

gung des betroffenen Nutzers nötig. In der Praxis müssen Nutzer den Diensteanbietern vertrauen, dass sie persönliche Daten nach den vereinbarten Datenschutzregeln erheben sowie weitergeben und es zu keinem Missbrauch dieser Daten kommt. In der Praxis willigen Nutzer generell zu allen Regeln einer Datenschutzerklärung ein bzw. lehnen alle Regeln durch den Widerruf ihrer Einwilligung ab. Eine Einwilligung zu einer Datenweitergabe im Einzelfall und somit zu einer bestimmten Profilbildung ist nicht möglich. Nutzer müssen die allgemeinen Geschäftsbedingungen akzeptieren und geben den Diensteanbietern damit eine Vollmacht für die Nutzung ihrer Daten. Auch mit technischen Mitteln können Nutzer die vereinbarten Regeln nicht durchsetzen. Mit den existierenden technischen Sicherheitswerkzeugen zum Schutz der Privatsphäre können sie sich sich zwar vor einer unerwünschten Profilbildung bei der Erhebung ihrer Daten schützen. Im Fall der Weitergabe persönlicher Daten bieten sie jedoch keinen Schutz, so dass Nutzer weiterhin den Diensteanbietern vertrauen müssen. Auf der anderen Seite ist einem Nutzer jede seiner Transaktionen eindeutig von den Diensteanbietern zurechenbar. Das aktuelle, einseitige Vertrauensmodell zeigt die Abbildung 1.2.

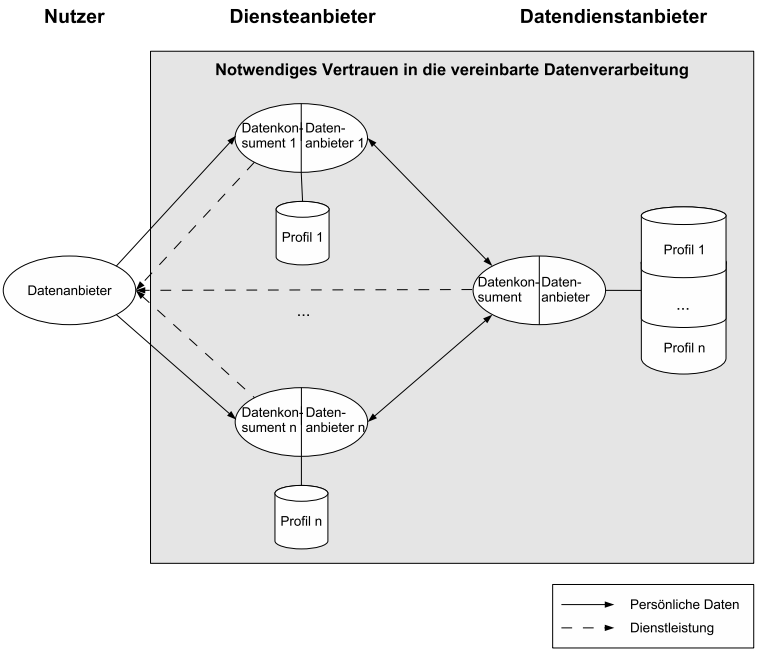

Abbildung 1.2: Das aktuelle, einseitige Vertrauensmodell zum Erhalt der informationellen Selbstbestimmung.

Technisch gesehen entspricht die Einwilligung eines Nutzers einem transaktionsbezogenen Zugriffsrecht auf seine Daten. Die Delegation eines Rechts für den Zugriff auf persönliche Daten wird durch die Delegation von Berechtigungsnachweisen erreicht. Sprachen zur Formulierung von Datenschutzregeln, wie z.B. P3P [CLM+02] und EPAL [AHK+03a], unterstützen zwar Regeln zur Datenerhebung bzw- Nutzung und deren Delegation, jedoch fehlt ein technischer Mechanismus mit dem Nutzer die Bedingungen und Obligationen durchsetzen oder ihre Einhaltung kontrollieren können. Identitätsmanagementsysteme, wie Shibboleth [CEH+05], Liberty Alliance [CHKT05], der Freiburger iManager [WJGtM+04] und IBM idemix [CH02], ermöglichen zwar eine kontrollierte Herausgabe von persönlichen Daten und schützen so vor einer unerwünschten Profilbildung; jedoch unterstützen sie keine transaktionsbezogene Delegation von Rechten. Deren Alles-oder-Nichts Prinzip erfordert a priori die Aufgabe aller Rechte an den Daten. Technische Werkzeuge für eine Delegation von Rechten, wie z.B. Kerberos

[KN93] und SPKI [EFL+99], ermöglichen eine transaktionsbezogene Delegation. Jedoch können die beteiligten Dienste die Transaktionen des Nutzers anhand der statischen Merkmale der Berechtigungsausweise verketten und somit Profile über Nutzer anlegen. Dies stellt einen Regelverstoß dar.

1.2 Erweiterung des Vertrauensmodells

Das Ziel ist die Realisierung eines Vertrauensmodells, in dem Nutzer ausschließlich dem Anbieter von persönlichen Daten bei der Erhebung und Weitergabe persönlicher Daten vertrauen und gleichzeitig die Zurechenbarkeit der Transaktionen der Nutzer gegeben ist. Dazu wird das Identitätsmanagementsystem namens DREISAM vorgestellt, mit dem Nutzer die vereinbarten Regeln zur Datenerhebung und Weitergabe bei der Nutzung von Dienstleistungen mit einem Datendienst durchsetzen und und ihre Einhaltung kontrollieren können. Die Abbildung 1.3 zeigt dieses Vertrauensmodell und den Ansatz von DREISAM.

1.3 Die Vorgehensweise

Mit dem Kapitel 2 wird die Delegation von Zugriffsrechten für persönliche Daten und ihre Weitergabe als Ansatz für den Erhalt der informationellen Selbstbestimmung eingeführt. Zu Beginn werden die rechtlichen Anforderungen der informationellen Selbstbestimmung für die Erhebung und die Weitergabe persönlicher Daten genannt. Während die rechtlichen Anforderungen nach dem Verständnis von *Privacy* sich nicht auf die Weitergabe persönlicher Daten beziehen, fordern sie nach dem Verständnis der *Privatsphäre* u.a. die Einwilligung des Nutzers für eine Weitergabe. Am Beispiel des *Customer Relationship Management (CRM)* wird das aktuelle, einseitige Vertrauensmodell für die Einhaltung der rechtlichen Anforderungen nachgewiesen und damit der Begriff des einseitigen CRM eingeführt. Anhand des Fallbeispiels werden Angriffe mit dem Ziel des Missbrauchs persönlicher Daten, in diesem Fall mit dem Ziel einer unerwünschten Datenerhebung und deren Weitergabe, gezeigt. Anstatt persönliche Daten weiterzugeben wird der Ansatz der Delegation von Rechten und deren Nutzung nach den vereinbarten Regeln vorgeschlagen. Damit soll eine Verbesserung des Vertrauensmodells zugunsten der Nutzer erreicht werden. Mit den Anforderungen an dieses mehrseitige CRM mit der Delegation von Rechten und dessen Vergleich mit dem einseitigen CRM schließt das Kapitel 2 ab.

Im Kapitel 3 wird gezeigt, dass auch der Stand der Forschung und Industrie das einseitige Vertrauensmodell zum Erhalt der informationellen Selbstbestimmung

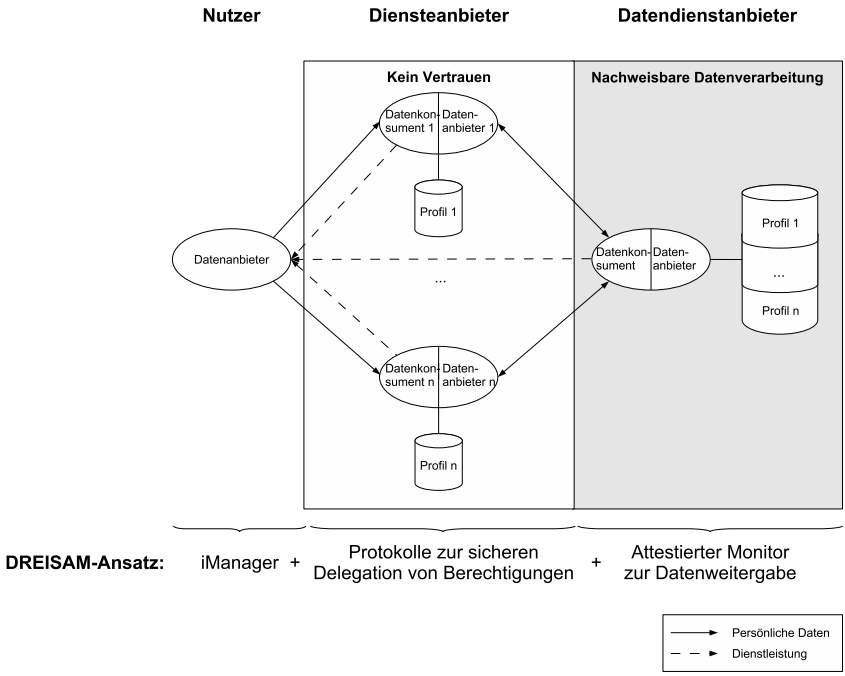

Abbildung 1.3: Das Vertrauensmodell, welches mit dem geforderten Identitätsmanagementsystem DREISAM realisiert werden soll.

bei der Delegation von Rechten realisiert. Der Nachweis erfolgt durch die Anwendung der entsprechenden Systeme bzw. deren Protokolle für CRM und der sich daraus ergebenden Möglichkeiten der Diensteanbieter zu einem Regelverstoß und damit zu einer unerwünschten Datenerhebung bzw. Datenweitergabe. Es zeigt sich, dass der Freiburger Identitätsmanager iManager und das anonymisierte Credentialsystem IBM idemix nach [CL01] und mit den Erweiterungen nach [CL02] in Kombination mit dem Delegationsmechanismus nach [Neu93] sich als Ausgangspunkt für das geforderte Identitätsmanagementsystem DREISAM eignen. Jedoch verliert ein Nutzer bei der Nutzung anonymisierter Credentials für die Delegation von Rechten aufgrund der zwingenden Weitergabe seines kryptographischen Schlüssels die Kontrolle über den Zugriff auf seine Daten. Die Regeln für den Datenzugriff sind somit weder durchsetzbar noch kontrollierbar. Das Kapitel schließt mit einer Diskussion der Lösungsansätze für die Einhaltung der vereinbarten Regeln ab, die sich auf den Zeitpunkt der Nutzung der delegierten Rechte,

d.h. vor, während und nach einer Zugriffsanfrage, beziehen.

Die vorgeschlagene Lösung, das Identitätsmanagementsystem DREISAM, stellt das Kapitel 4 vor. Zu Beginn werden die erforderlichen Protokolle zur Delegation von Rechten und deren Widerruf in Form von Credentials vorgestellt. Die Protokolle sollen das technische Problem lösen, dass Nutzer bei der Weitergabe von anonymisierten Credentials die Kontrolle über ihren zugehörigen geheimen kryptographischen Schlüssel verlieren. Der Systementwurf von DREISAM spezifiziert dessen Teil-Systeme und Protokolle. Ein attestierter Monitor wird für die Überwachung der Zugriffsentscheidungen des Datendienstes entsprechend den delegierten Rechten und Regeln eingesetzt. Abschließend wird die Funktionsweise von DREISAM anhand dessen Implementierung für das Fallbeispiel CRM veranschaulicht.

Das Kapitel 5 zeigt die Schutzwirkung von DREISAM. Es erbringt den Nachweis, dass DREISAM einen Schutz vor den Gefährdungen bietet, die im Baustein *Datenschutz* des IT-Grundschutz-Katalogs des Bundesamts für Sicherheit in der Informationstechnik aufgeführt sind. Zur Bewertung werden aus diesen Bedrohungen Angriffe mit dem Ziel einer unerwünschten Erhebung und Weitergabe persönlicher Daten abgeleitet. Die identifizierten Angriffsfälle werden auf DREISAM ausgeführt. Zudem wird die Schutzwirkung von DREISAM anhand dessen Implementierung für das Fallbeispiel CRM veranschaulicht.

Das Kapitel 6 schließt die Arbeit mit der Einschätzung der Potentiale für DREISAM ab. Es wird dessen Anwendung von für kartenbasierte behördliche und medizinische Dienstleistungen sowie für die Weitergabe elektronischer Dokumente und deren kontrollierte Nutzung im Rahmen des Digital Rights Managements skizziert.

2 Delegation von Rechten am Beispiel CRM

Nach der informationellen Selbstbestimmung soll der Einzelne selbst über die Herausgabe und Weitergabe seiner Daten bestimmen können [Wes67, Bun83]. Das Ziel von Kapitel 2 ist es, die Anforderungen für die Delegation von Rechten für den Zugriff auf persönliche Daten abzuleiten, mit der die informationelle Selbstbestimmung bei der Erhebung und Weitergabe von persönlichen Daten erhalten bleiben soll. Dazu werden im Abschnitt 2.1 die rechtlichen Anforderungen der informationellen Selbstbestimmung aufgeführt. Am Beispiel des Customer Relationship Management (CRM) wird in Abschnitt 2.2 das real angewendete Vertrauensmodell identifiziert. Eine Bedrohungsanalyse zeigt daraufhin mögliche Verletzungen der informationellen Selbstbestimmung und die Einseitigkeit von CRM in der Praxis. Aus der Bedrohungsanalyse ergibt sich die Forderung nach einen Zugriffskontrollmechanismus, der Nutzer vor den identifizierten Verletzungen schützen soll und dazu ein mehrseitiges CRM zum Ziel hat. Da sich sowohl die erstmalige Erhebung als auch die Weitergabe persönlicher Daten auf deren Zugriff beziehen, stellt der Abschnitt 2.3 das Modell für die erforderliche Zugriffskontrolle mit der Delegation von Rechten vor. Der Abschnitt 2.4 stellt mit dem Vergleich zwischen dem einseitigen und dem mehrseitigen CRM den Beitrag des vorgeschlagenen Zugriffskontrollmechanismus und damit das Ergebnis dieses Kapitels dar.

2.1 Rechtliche Anforderungen der informationellen Selbstbestimmung

Unter dem Begriff *Privacy* wurde 1967 die informationelle Selbstbestimmung von Alan F. Westin gefordert: „*Privacy is the claim of individuals, groups, or institutions to determine for themselves when, how, and to what extend information about them is communicated to others*“ [Wes67]. Damit soll es einem Einzelnen möglich sein, selbst über den Zeitpunkt, die Art und den Umfang der Erhebung und Weitergabe persönlicher Daten zu bestimmen. In Deutschland hat das Bundesverfassungsgericht im Jahr 1983 die informationelle Selbstbestimmung als ein Grundrecht des Einzelnen erklärt. Nach dem sogenannten „Volkszählungsurteil“ umfasst die informationelle Selbstbestimmung den „*Schutz des Einzelnen*

gegen eine unbegrenzte Erhebung, Speicherung, Verwendung und Weitergabe persönlicher Daten [...] Das Grundrecht gewährleistet die Befugnis des Einzelnen, grundsätzlich selbst über die Preisgabe und Verwendung seiner persönlichen Daten zu bestimmen“ [Bun83]. Das Urteil schränkt das Recht auf informationelle Selbstbestimmung jedoch ein, falls daran das Allgemeininteresse überwiegt.

2.1.1 Privacy

Der Begriff *Privacy* ist im US-amerikanischen Raum zusätzlich zur Forderung von Alan F. Westin auch von Samuel D. Warren und Lous D. Brandeis durch „*the right to be let alone*“ [WB90] geprägt. Letztere fordern für den Einzelnen das Recht sich zurückziehen zu dürfen und keine Daten über sich zu veröffentlichen. Gesetzlich geregelt ist der Schutz persönlicher Daten allerdings nur für bestimmte Anwendungsbereiche [Hen99, Lan05]. Das *United States Department for Health Education and Welfare* definiert zwar unter dem Begriff *Fair Information Practices* Mindestprinzipien für den Schutz von Patientendaten, allerdings ist deren Einhaltung nicht rechtlich vorgeschrieben [Smi93]. Dies ist hingegen nach dem *US Privacy Act* [Uni74] für behördliche Dienstleistungen der Fall. Für den wirtschaftlichen Bereich wurden die Mindestprinzipien von der *Organization for Economic Cooperation and Development (OECD)* als Richtlinien standardisiert [Org80]. Es handelt sich um die folgenden Prinzipien:

- **Eingeschränkte Profilbildung (*Collection Limitation Principle*):** Der Umfang des erstellten Profils sollte zu dessen Verwendungszweck angemessen sein. Die Datenerhebung sollte mit legalen Mitteln und mit dem Wissen oder dem Einverständnis der betroffenen Person erfolgen.

- **Qualität der erhobenen Daten (*Data Quality Principle*):** Die erhobenen Daten sollten für den Zweck relevant und notwendig sein. Weiterhin sollten sie korrekt, vollständig und aktuell sein.

- **Angabe des Verwendungszweckes (*Purpose Specification Principle*):** Der Zweck der Erhebung persönlicher Daten soll spätestens zum Zeitpunkt der Datenerhebung angegeben werden. Ändert sich der Verwendungszweck, so soll diese Änderung ebenfalls angegeben werden. Zusätzlich soll die weitere Nutzung der erhobenen Daten zur Erfüllung dieses Zweckes oder äquivalenter Zwecke beschränkt werden.[1]

[1] Neue Verwendungszwecke sollen nicht willkürlich eingeführt werden und zu dem bereits angegebenen Verwendungszweck kompatibel sein. Wenn erhobene Daten nicht mehr für den angegebenen Zweck benötigt werden, so sollen sie entweder gelöscht oder anonymisiert werden, sofern dies machbar ist.

- **Eingeschränkte Nutzung der erhobenen Daten (*Use Limitation Principle*):** Persönliche Daten dürfen nicht für andere Zwecke als unter den angegebenen Verwendungszwecken veröffentlicht, zur Verfügung gestellt oder auf andere Weisen genutzt werden. Eine Ausnahme besteht dann, wenn der Eigentümer dieser Daten dem Zweck zugestimmt hat oder ein richterlicher Erlass besteht.

- **Verwendung angemessener Sicherheitsmaßnahmen (*Security Safeguards Principle*):** Persönliche Daten sollen durch angemessene Sicherheitsmaßnahmen vor unbeabsichtigten Verlust und gegen unerlaubten Zugriff, Vernichtung, Nutzung, Änderung und Veröffentlichung geschützt werden.

- **Offene Profilbildung (*Openness Principle*):** Es sollte eine allgemeine Politik der Offenheit bestehen, die Auskunft über die Entwicklungen, Praktiken und Richtlinien der Organisation mit Bezug zu den von ihr erhobenen persönlichen Daten gibt. Es sollten dem Einzelnen Mittel zur Verfügung stehen, mit denen er die Existenz und die Motivation zur Datenerhebung, die wesentlichen Verwendungszwecke der erhobenen Daten und den Datenschutzbeauftragten dieser Organisation ermitteln kann.

- **Individuelle Beteiligung der betroffenen Personen (*Individual Participation Principle*):** Ein Einzelner sollte das Recht haben,
  - von einem Datenschutzbeauftragten einer Organisation zu erfahren, ob und ggf. welche persönliche Daten von der Organisation über ihn erhoben wurden,
  - innerhalb einer angemessen Zeit, evtl. zu einer nicht übertriebenen Gebühr, auf eine angemessene Art und Weise und in einer für ihn verständlichen Form über die erhobenen Daten in Kenntnis gesetzt zu werden,
  - eine Begründung zu erhalten, wenn eine der obigen beiden Anfragen abgelehnt wurde, und eine solche Ablehnung juristisch anfechten zu können und
  - eine Datenerhebung juristisch anzufechten und, falls die Anfechtung erfolgreich gewesen ist, die Löschung, Richtigstellung, Vervollständigung oder Änderung des Profils anzuordnen.

- **Haftungsumfang (*Accountability Principle*)**: Ein Datenschutzbeauftragter sollte für die Einhaltung der Mittel, mit denen diese Prinzipien befolgt werden, haften.

Allein die Prinzipien der eingeschränkten Profilbildung und der eingeschränkten Nutzung der erhobenen Daten haben einen Zusammenhang mit der informationellen Selbstbestimmung. Das erste Prinzip fordert eine zweckbezogene Profilbildung und das Einverständnis des betroffenen Nutzers zur Profilbildung; das zweite Prinzip fordert, dass die erhobenen Daten nur für den vorher angegebenen Zweck genutzt und weitergegeben werden sollen.

Sofern die Verarbeitung persönlicher Daten nicht durch ein branchenspezifisches Gesetz reguliert ist, können Diensteanbieter frei über die erhobenen Daten verfügen. Dies widerspricht jedoch der Definition der informationellen Selbstbestimmung nach Westin. Nutzer haben keine rechtliche Möglichkeit, mit der sie die Weitergabe ihrer Daten bestimmen. So können Profile entgegen den Interessen der betroffenen Nutzer erstellt werden, ohne dass gegen rechtliche Anforderungen verstoßen wird. Die Forderung der informationellen Selbstbestimmung ist verletzt und folglich haben Nutzer keine *Privacy* mehr.

2.1.2 Privatsphäre

Nach den Datenschutzdirektiven der Europäischen Union zum Schutz von Personen bei der Verarbeitung persönlicher Daten [Eur95, Eur02] und deren Umsetzung durch nationale Gesetze, z.B. dem Teledienstedatenschutzgesetz [Bun97] und dem Bundesdatenschutzgesetz [Bun03], ist die *Privatsphäre* und damit die informationelle Selbstbestimmung gewährleistet, wenn ihre Mindestprinzipien befolgt werden. Die Mindestprinzipien regulieren die Erhebung, Verwendung, Speicherung und Weitergabe persönlicher Daten für öffentliche und private Organisationen und müssen vor Beginn einer Datenverarbeitung erfüllt sein. Sie definieren den vertraulichen und zurechenbaren Rahmen in dem persönliche Daten in den Mitgliedstaaten der Europäischen Union verarbeitet werden dürfen und die bei ihrer Weitergabe an Organisationen ausserhalb der Mitgliedstaaten eingehalten werden müssen. Der Rahmen der Datenverarbeitung wird mit dessen Zweckbezug, der Forderung nach dem minimalen Umfang der Datenerhebung und -weitergabe gemäß dem Verwendungszweck, der Identität des Datenverarbeiters und im Falle einer Weitergabe persönlicher Daten mit der Angabe der Empfänger definiert. Zum Schutz vor u.a. einem unbefugten Zugriff werden technische und organisatorische Maßnahmen, wie z.B. der Einsatz einer Zugriffskontrolle, vorgeschrieben.

Die informationelle Selbstbestimmung wird dadurch gewährleistet, dass eine Verarbeitung persönlicher Daten nur dann zulässig ist, wenn der betroffene Nutzer dazu eingewilligt hat oder eine Rechtsvorschrift die Verarbeitung erlaubt. Die Einwilligung eines Nutzers bezieht sich somit auch auf die Weitergabe persönlicher Daten und ist vor Beginn der Datenverarbeitung einzuholen. Die Einwilligung ist

neben der schriftlichen auch in elektronischer Form möglich [Bun97] und kann von dem Nutzer widerrufen werden. Sollen persönliche Daten für eine Personalisierung von Dienstleistungen und für Zwecke der Werbung und Marktforschung verarbeitet werden, so muss wiederum die Einwilligung des Nutzers vorliegen und die Daten sind zu anonymisieren bzw. pseudonymisieren [Bun97]. Auch der Umfang der zu verarbeitenden Daten wird geregelt. Das Bundesdatenschutzgesetz gibt vor, dass "*die Gestaltung und Auswahl von Datenverarbeitungssystemen sich an dem Ziel auszurichten haben, keine oder so wenig persönliche Daten wie möglich zu erheben, zu verarbeiten oder zu nutzen. Insbesondere ist von den Möglichkeiten der Anonymisierung und Pseudonymisierung Gebrauch zu machen*" (Prinzip der Datenvermeidung und Datensparsamkeit) [Bun03]. Zusätzlich haben Nutzer das Recht auf Berichtigung, Löschung und Sperrung ihrer gespeicherten Daten.

Um die Einhaltung der Mindestprinzipien zu überprüfen und ggf. Haftungsfragen zu klären, können Diensteanbieter sowohl von Nutzern als auch von einer Kontrollstelle oder einem Datenschutzbeauftragten kontrolliert werden. Mit einer Datenverarbeitung wird ein Datenverarbeiter in Verbindung gebracht, der für die Verarbeitung persönlicher Daten nach den Schutzprinzipien der Datenschutzdirektive verantwortlich ist. Er haftet im Falle einer Verarbeitung entgegen den rechtlichen Anforderungen, so dass von ihm Schadensersatz verlangt werden kann [Eur95]. Verantwortliche Diensteanbieter haben ihre Datenverarbeitung einer Kontrollstelle zu melden. Die Meldung beinhaltet die Identität des Diensteanbieters, die Zweckbestimmung der Datenverarbeitung, die betroffenen Personengruppen, im Fall einer Datenweitergabe die Empfänger der Daten, ob eine Datenweitergabe in Drittländer vorgesehen ist und die Angabe der eingesetzten Sicherheitsmaßnahmen. Dem Nutzer wird zur Kontrolle ein Auskunfts- und Widerrufsrecht eingeräumt. Mit dem Auskunftsrecht hat der Nutzer die Möglichkeit eine Auskunft über die Existenz einer Datenerhebung und ggf. deren Umfang und Zweckbestimmung, über die Empfänger der Daten, über die Ausarbeitungslogik der Datenverarbeitung und über eine Änderung, Löschung oder Sperrung seiner Daten zu erhalten. Ferner kann sich ein Nutzer an eine Kontrollstelle wenden und eine Kontrolle beantragen.

2.2 Einseitiges CRM

Eine Verarbeitung persönlicher Daten und die damit einhergehende auf Nutzer abgestimmte Ausrichtung der Geschäftsprozesse eines Unternehmens wird unter dem Begriff Customer Relationship Management (CRM) zusammengefasst. Mit dem Einsatz von CRM-Systemen zielt ein Unternehmen nach [BS05] auf

- eine Minimierung der Investitionskosten für die Suche nach Nutzern,

- eine Maximierung des Verkaufs eigener Produkt- und Dienstleistungen und
- eine möglichst langfristige Bindung der Nutzer an das Unternehmen.

Eine Ausprägung von CRM sind Kundenbindungsprogramme , wie z.B. *Payback*[2]. Persönliche Daten der Nutzer eines Kundenbindungsprogramms werden für personalisierte Dienstleistungen und Angebote erhoben und zentral von einem Datendienst gespeichert. Als Gegenleistung erhalten Nutzer Bonuspunkte, die sie entweder gegen Güter oder Geldbeträge eintauschen können. Die Akteure und Kommunikationsbeziehungen der Nutzer in einem Kundenbindungsprogramm sind dadurch bestimmt, ob das Programm ein Partnerprogramm betreibt und der Programmbetreiber den Partnerunternehmen seine Dienstleistungen anbietet. Der Programmbetreiber übernimmt die Verwaltung der erhobenen persönlichen Daten, die Organisation und Durchführung von Werbekampagnen und ggf. die finanzielle Abrechnung mit den Nutzern [Lau04]. Als zusätzliche Dienstleistung des Programmbetreibers gegenüber seinen Partnerunternehmen kann er aus seinem Datenbestand potentielle Kunden für ein bestimmtes Produkt bzw. bestimmte Dienstleistung identifizieren. Dies bietet sich für den Programmbetreiber als eine zusätzliche Einnahmequelle an. In dem Szenario dieser Arbeit entspricht ein Programmbetreiber dem Anbieter des Datendienstes und Partnerunternehmen sind die gewöhnlichen Diensteanbieter. Die Dienstleistung der Programmbetreiber wird in die Geschäftsprozesse ihrer Partnerunternehmen eingebunden. So stellt bspw. der Betreiber von *Payback* seine Funktionalität in Form eines autonomen Dienstes zur Verfügung, der in eine eine Service-Orientierte Architektur integriert wird.[3]

Während in den fünfziger und sechziger Jahren die Beteiligung an einem Kundenbindungsprogramm durch Rabatthefte implementiert wurde, nehmen Nutzer nun mittels einer Kundenkarte teil. Kundenkarten werden entweder vom Programmbetreiber oder von einem seiner Partnerunternehmen ausgestellt. Die erste Kundenkarte Deutschlands wurde 1959 von dem Unternehmen E. Breuninger GmbH & Co mit der *Breuninger Card* eingeführt. Ihre Funktionalität bezog sich auf eine bargeldlose Bezahlung und monatliche Sammelrechnung. Zum gegenwärtigen Zeitpunkt bietet sie neben einen Rabatt auf eigene Waren auch Rabatte auf Waren und Dienstleistungen von Partnerunternehmen an. Die Deutsche Lufthansa AG führte 1993 das Vielfliegerprogramm *Miles & More* ein, das ein Kundenbindungsprogramm mit branchenübergreifenden Partnerunternehmen und ein Kreditkartensystem mit der *Miles & More Credit Card* realisiert. Nutzer sammeln Bonuspunkte

[2] http://www.payback.de
[3] http://www.loyaltypartner.com