Maik Heidisch, Prof. Dr. Norbert Pohlmann

»Elektronischer Datenbrief – eine aktive informationelle Selbstbestimmung im Internet

Eine klare Übersicht zu haben über eigene persönliche Daten, die bei den Internet-Dienst-Anbietern gespeichert sind, hilft, sich selbstbestimmt im Internet zu bewegen. Der elektronische Datenbrief stellt einen zukunftsweisenden Lösungsvorschlag für die Anbieter von Internet-Diensten dar und zeigt auf, wie eine aktive informationelle Selbstbestimmung im Internet umgesetzt werden kann, die die Wahrung der Grundrechte der Nutzer gewährleistet und damit das Internet vertrauenswürdiger macht!

DER AUTOR

Prof. Dr. (TU NN) **Norbert Pohlmann** ist Informatikprofessor für Verteilte Systeme und Informationssicherheit sowie Leiter des Instituts für Internet-Sicherheit. Im Jahr 2011 erhielt er durch die Zeitschrift UNICUM BERUF die Auszeichnung „Professor des Jahres“ in der Kategorie Ingenieurwissenschaft und Informatik.

DER AUTOR

Maik Heidisch ist studentischer Mitarbeiter am Institut für Internet-Sicherheit und Stipendiat der Stiftung der Deutschen Wirtschaft. Nach seinem Bachelorstudium an der Hochschule Niederrhein in Krefeld studiert er aktuell an der Fachhochschule Gelsenkirchen im Masterstudiengang Internet-Sicherheit.

Soziale Netze wie Facebook, Google+ usw. verdienen ihr Geld vor allem mit Werbung. Die Nutzer zahlen nichts für den Internet-Dienst, geben aber massenhaft persönliche Daten preis, für die der Betreiber sich die Rechte über die AGB geben lässt. Mit diesen persönlichen Daten erstellt der Betreiber eines Internet-Dienstes Nutzerprofile, die für den Verkauf von Waren und Dienstleistungen interessant sind, weil sie passgenaue, individualisierte Werbung ermöglichen. Diese zielgenaue Werbung lassen sich die Betreiber wie z. B. soziale Netzwerke durch das Schalten individualisierter Anzeigen gut bezahlen. Dieses Prinzip „Bezahlen mit persönlichen Daten“ wird auch bei anderen Diensten wie Suchmaschinen, E-Mail-Diensten, Nachrichtendiensten, usw. angewendet. Aber auch im Bereich von E-Commerce wie z. B. Amazon werden persönliche Daten erhoben, gespeichert und ausgewertet, um den Kunden individuelle Angebote machen zu können. In Deutschland gibt es aber das Recht auf informationelle Selbstbestimmung! Dieses Grundrecht gewährleistet die Befugnis des Einzelnen, grundsätzlich selbst über die Preisgabe und Verwendung seiner persönlichen Daten zu bestimmen. Der elektronische Datenbrief ist eine Idee, die aktive informationelle Selbstbestimmung im Internet möglich zu machen.

Forderung, gespeicherte Daten regelmäßig an die Betroffenen zu versenden – Datenbrief

Der Datenbrief ist eine Forderung des Chaos Computer Clubs, der Firmen, Behörden und Institutionen, die personenbezogene Daten erheben, verpflichtet, in regelmäßigen Abständen kostenlose Informationen über die gespeicherten Daten an die Betroffenen zu versenden. Dies umfasst auch „angereicherte Daten“ wie zum Beispiel Profile und Scoring-Werte. Dieser Datenbrief würde die informationelle Selbstbestimmung maßgeblich stärken. Aktuell hat ein Betroffener nach dem Bundesdatenschutzgesetz bereits ein Recht auf Auskunft (vgl. §§ 19, 34 BDSG), jedoch muss dazu bekannt sein, an welchen Stellen Daten über den Betroffenen gespeichert werden. Anschließend muss der Bürger als Bittsteller gegenüber der speichernden Stelle auftreten. Dies wird oft durch eine aufwendige Identifikation mittels einer Kopie des Personalausweises oder des PostIdent-Verfahrens erschwert.

Inhalt des Datenbriefs

Der Datenbrief soll postalisch oder elektronisch übermittelt werden und alle über den Betroffenen gespeicherten Daten sowie deren Ursprung enthalten. Außerdem soll er beinhalten, ob und welche Daten an eine dritte Stelle übermittelt wurden. Der Zweck und die Rechtsgrundlage für die Speicherung und Übermittlung sowie eine Widerspruchs- und Korrekturmöglichkeit sollen ebenfalls inbegriffen sein. Die Unterlassung der Versendung von Datenbriefen soll mit harten Strafen für die verantwortliche Stelle geahndet werden.

Vorteile des Datenbriefs

Die Vorteile des Datenbriefs liegen auf der Hand. Die Verarbeitung eigener persönlicher Daten kann von den Betroffenen besser überblickt

und kontrolliert werden; der regelmäßige Überblick über den gegebenenfalls enormen Umfang der Datenspeicherung sensibilisiert für den weiteren Umgang mit den eigenen Daten. Zudem erhalten die Betroffenen die Möglichkeit, die Richtigkeit der Daten zu überprüfen und gegebenenfalls eine Korrektur und einen Widerspruch zu veranlassen. Da die Rechtsgrundlage für die Speicherung und Übermittlung der Daten in dem Datenbrief angegeben werden muss, müssen die Stellen die Legalität der Datenhaltung überprüfen. Dieser Mehraufwand für das Unternehmen soll die kritische Prüfung der Notwendigkeit der Datenspeicherung bewirken und somit Anhäufungen personenbezogener Daten unattraktiv machen. Liegt eine Notwendigkeit für die Datenspeicherung vor, ist der bürokratische Aufwand laut dem Chaos Computer Club jedoch vertretbar, da dem Datenbrief Reklame, amtliche Mitteilungen, Rechnungen, Vertragsänderungen oder anderen Korrespondenzen beiliegen können.

Kritiker sehen Probleme mit dem Datenbrief

Neben den Vorteilen sehen Kritiker jedoch auch eine Reihe Probleme. So würden speichernde Stellen, denen teilweise keine aktuelle Adresse vorliegt, Datenbriefe, die hochsensible und persönliche Daten enthalten, zum Beispiel an Eltern, Studentenwohnheime, Ex-Lebenspartner usw. senden. Außerdem könnten Dienstleistungsunternehmen den Versand der Datenbriefe übernehmen. Die Daten würden dadurch zusätzlich an einem weiteren Ort zentralisiert verarbeitet. Dies dupliziert die Daten nicht nur, sondern schafft zusätzlich ein potenzielles Angriffsziel. Aktuell speichern größere Stellen die Daten der Betroffenen eventuell in verschiedenen Bereichen. Der Versand der Datenbriefe verlangt die zentrale Zusammenführung und Aufbereitung. Entsprechend aufbereitete Daten haben einen höheren Wert und könnten für andere Zwecke als den Datenhandel genutzt werden, um damit die dafür anfallenden Kosten zu decken. Die anfallenden Kosten könnten auch durch die Beilage von Werbung des eigenen Unternehmens oder Dritter sowie durch Preiserhöhungen kompensiert werden. Der unverschlüsselte elektronische Versand der sensiblen Daten und eventuell nicht sicher vernichtete postalische Datenbriefe stellen zudem ein Sicherheitsrisiko dar.

Meinung der Politik zum Datenbrief

Der Datenbrief wurde Anfang 2010 auch in der Politik diskutiert. So zeigten sich zum Beispiel der damalige Bundesinnenminister Thomas de Maizière und die Bundesjustizministerin Sabine Leutheusser-Schnarrenberger Anfang März 2010 aufgeschlossen gegenüber der Idee. Auch Bundesdatenschutzbeauftragter Peter Schaar bezeichnete den Datenbrief bereits im Januar 2010 als sinnvoll. Im Mai 2010 relativierten die Bundesjustizministerin Sabine Leutheusser-Schnarrenberger und der Bundesdatenschutzbeauftragte Peter Schaar jedoch ihre Meinung, da es unter praktischen Gesichtspunkten „riesige Probleme“ gebe. Das Anliegen sei „absolut unterstützenswert“, aber „noch nicht ganz zu Ende gedacht“.

Elektronischer Datenbrief – ein zukunftsweisender Lösungsvorschlag

Mit dem elektronischen Datenbrief stellt das Institut für Internet-Sicherheit einen zukunftsweisenden Lösungsvorschlag, wie eine aktive informationelle Selbstbestimmung im Internet umgesetzt werden könnte, für die Anbieter von Internet-Diensten vor. Der Großteil der Kritik am Konzept des Datenbriefes konzentriert sich auf die Art der Zustellung, speziell auf das Problem der Fehladressierung und des damit verbundenen Missbrauchspotenzials. Der elektronische Datenbrief verpflichtet daher Firmen, Behörden und Institutionen, die personenbezogene Daten erheben und Anbieter eines Internet-Dienstes sind, den Betroffenen die Informationen über die gespeicherten Daten jederzeit kostenlos über einen standardisierten Elektronischen-Datenbrief-Dienst zur Verfügung zu stellen. Dieser Elektronische-Datenbrief-Dienst muss in den bestehenden Internet-Dienst integriert sein, damit der Zugriff mit den gleichen Zugangsdaten möglich ist.

Datenerfassungen ohne aktives Konto

Anbieter, die personenbezogene Daten erfassen, obwohl von dem Betroffenen nie aktiv ein Konto bei der erfassenden Stelle angelegt wurde, müssen zudem verpflichtet werden, den Betroffenen über den der Stelle bekannten Kommunikationsweg über die Erfassung zu informieren, sobald pseudonymisierte Daten und der Betroffene miteinander verbunden werden können. In dieser Benachrichtigung muss die Adresse des Internet-Dienstes angegeben sein, damit der Betroffene nach einer Identifikation dort Zugangsdaten anlegen kann. Durch die Identifikation besteht bei einer Fehladressierung kein Missbrauchspotenzial. Liegt der erfassenden Stelle keine Kommunikationsmöglichkeit vor, muss die Auflösung der Pseudonymisierung unzulässig und somit rechtswidrig sein. Diese Regelung betrifft zum Beispiel das pseudonymisierte Sammeln von Informationen mittels Cookies.

Regelmäßige Benachrichtigungen

Zudem muss eine regelmäßige Benachrichtigung der Betroffenen über die weitere Speicherung der personenbezogenen Daten erfolgen. Da dies automatisch und elektronisch über den Internet-Dienst initiiert werden kann, bedeutet dies keinen Mehraufwand für die speichernden Stellen. Die Betroffenen werden jedoch erinnert, die gespeicherten Daten wiederholt zu überprüfen.

Standardisierung des Elektronischen-Datenbrief-Dienstes

Es muss sich um einen standardisierten Elektronischen-Datenbrief-Dienst handeln, damit ein einheitlicher, einfacher und sicherer Zugriff gewährleistet wird. Die einheitliche und einfache Bedienung ermöglicht eine schnelle Akzeptanz und Einarbeitung durch die Bürger. Außerdem unterstützt ein standardisierter Elektronischer-Datenbrief-Dienst eine sichere Umsetzung der Integration in die jeweiligen Internet-Dienste. Dies impliziert zum Beispiel die Verwendung von SSL und den Schutz gegen Angriffe auf die Datenbank. Zusätzlich muss in den Elektronischen-Datenbrief-Dienst jedes Internet-Dienstes eine nutzbare Schnittstelle eingebaut sein, über die die personenbezogenen Daten mittels einer Elektronischen-Datenbrief-Anwendung abgerufen und dadurch mit den Daten anderer erfassenden Stellen zusammengeführt werden können. Dies bietet erfahreneren Benutzern eine globale Sichtweise auf die gesammelten Daten und die Möglichkeit, zeitnah per Push-Verfahren über Änderungen informiert zu werden.

Inhalt des elektronischen Datenbriefs

Jeder Internet-Dienst muss analog zum Datenbrief alle über den Betroffenen gespeicherten Daten sowie deren Ursprung enthalten und auch zeigen, ob und welche Daten an eine dritte Stelle übermittelt wurden. Zudem müssen der Zweck und die Rechtsgrundlage für die Speicherung und Übermittlung und eine Widerspruchs- und Korrekturmöglichkeit enthalten sein. Die Widerspruchs- und Korrekturmöglichkeit impliziert ebenfalls, auch alle nicht für den ordnungsgemäßen Betrieb des Internet-Dienstes erforderlichen Daten, wie zum Beispiel für Werbezwecke angereicherten Daten, komplett löschen zu können.

Umdenken im Geschäftsmodell nötig

Erfolgt die (Teil-)Finanzierung des Internet-Dienstes durch die Einnahmen der personalisierten Werbung, kann die komplette Löschung der für die Werbezecke gespeicherten Daten jedoch auch eine automatische Umwandlung in ein kostenpflichtiges Profil bedeuten. Somit bestünde zum Beispiel bei sozialen Netzwerken die Möglichkeit, auf die personalisierte Werbung zu verzichten. Die Nutzung der sozialen Netzwerke könnte dadurch jedoch auch kostenpflichtig werden, da nicht personalisierte Werbung geringere Einnahmen impliziert. Dies muss jedoch nicht erforderlich sein, wie die VZ-Netzwerke zeigen. Dort ist die personalisierte Werbung kostenlos abschaltbar. Das passende Geschäftsmodell muss von jedem Internet-Dienst-Anbieter gefunden werden.

Vorteile des elektronischen Datenbriefs

Der elektronische Datenbrief teilt die Vorteile des Datenbriefs. Die Verarbeitung eigener persönlicher Daten kann von den Betroffenen durch den Elektronischen-Datenbrief-Dienst jedes Internet-Dienstes und die darin enthaltene standardisierte Schnittstelle jederzeit überblickt und kontrolliert werden. Durch die regelmäßige Benachrichtigung über die weitere Speicherung der personenbezogenen Daten werden die Betroffenen zudem zyklisch mit der Datenspeicherung konfrontiert und dadurch für den weiteren Umgang mit den eigenen Daten sensibilisiert. Zudem wird die Möglichkeit geboten, die Richtigkeit der Daten zu überprüfen und gegebenenfalls eine Korrektur und einen Widerspruch zu veranlassen. Korrigiert der Betroffene angereicherte Daten, entsteht ein Nutzen für den Internet-Dienst-Anbieter, weil die individuelle Werbung besser wird. Da die Rechtsgrundlage für die Speicherung und Übermittlung der Daten in dem elektronischen Datenbrief angegeben werden muss, sind die Stellen verpflichtet, die Legalität der Datenhaltung zu überprüfen. Der mit der Prüfung der Rechtsgrundlage verbundene Mehraufwand für das Unternehmen soll auch hier die kritische Prüfung der Notwendigkeit der Datenspeicherung bewirken und somit Anhäufungen personenbezogener Daten unattraktiv machen.

Lösung der Probleme des Datenbriefes

Der elektronische Datenbrief löst die Probleme des Datenbriefes wie folgt: Durch die Nutzung der gleichen Zugangsdaten wie für den Internet-Dienst und die erforderliche Identifizierung nach dem Erhalt einer Benachrichtigung über die Erfassung besteht bei einer Fehladressierung kein Missbrauchspotenzial. Da die Datenbriefe nicht etwa elektronisch mittels E-Post zugestellt und somit zentralisiert gesammelt werden, schafft der dezentrale Abruf des elektronischen Datenbriefes über einen standardisierten Elektronischen-Datenbrief-Dienst zudem keine weiteren potenziellen Angriffsziele. Zudem ist der Aufwand für die Internet-Dienst-Anbieter überschaubar, da durch die Integration des Elektronischen-Datenbrief-Dienstes in den bestehenden Internet-Dienst lediglich einmalige Kosten anfallen. Da der Elektronische-Datenbrief-Dienst standardisiert sein soll, bietet er eine sehr hohe Vertrauenswürdigkeit und Sicherheit.

Aktuelle Situation bei einigen Internet-Dienst-Anbietern

Aktuell bieten bereits einige Internet-Dienste Teilaspekte der Idee des elektronischen Datenbriefs an. Diese Schnittstellen wurden beispielhaft an den drei Internet-Diensten Facebook, SCHUFA und Amazon evaluiert.

Facebook

Das soziale Netzwerk Facebook speichert laut Max Schrems, dem Gründer der Initiative „Europe versus Facebook“, über 100 verschiedene Datensätze über jeden Nutzer. Da Facebook einen Sitz im irischen Dublin besitzt, haben alle Europäer nach Art. 12 der EU-Datenschutz-

Abb. 1: Ansicht der herunterladbaren Profilinformationen auf Facebook

richtlinie (95/46/EG) ein Anrecht auf die Zusendung der über sie gespeicherten Daten. Max Schrems forderte im Juni 2011 die über ihn gespeicherten Daten bei Facebook Irland an. Er erhielt ein 1222 Seiten langes Dokument, in dem insgesamt 57 der mindestens 100 verschiedenen Datensätze zu finden sind. Die restlichen Datensätze, die zum Beispiel Daten der automatischen Gesichtserkennung, Handysynchronisation und Friend Finders enthalten, fehlten. Die enthaltenen Datensätze unterteilen sich in die Profilinformationen, die 22 Datensätze, und die im Hintergrund generierten Daten, die zusätzlich 35 Datensätze umfassen. Aufgrund des hohen Zuwachses an Anfragen, die Facebook Irland durch die von Max Schrems gegründete Initiative „Europe versus Facebook“ erhält, bietet Facebook seit November 2011 jedem Benutzer in den Kontoeinstellungen die Möglichkeit an, die über ihn gespeicherten Informationen in einem Archiv herunterzuladen. Dieser Download enthält jedoch lediglich die Profilinformationen; die im Hintergrund generierten Daten fehlen komplett. Nach Rückfrage bei Facebook handele es sich bei den Nutzerdaten um ein Geschäftsgeheimnis und geistiges Eigentum des Unternehmens. Außerdem gestalte sich der Transfer der angeforderten Daten „überproportional schwierig“.

Abbildung 1 zeigt eine anonymisierte Ansicht der herunterladbaren Profilinformationen auf Facebook. Bereits hier ist zu erkennen, dass nicht alle über den Betroffenen gespeicherten Daten sowie deren Ursprung enthalten sind. Es ist somit festzustellen, dass die Möglichkeit des Datendownloads lediglich der Irritation des Benutzers dient, da keine volle Dateneinsicht erfolgt. Des Weiteren haben Nicht-Mitglieder gar keine Möglichkeit, die über sie gespeicherten Daten einzusehen.

SCHUFA

Die deutsche Wirtschaftsauskunftei SCHUFA bietet über den Internet-Dienst meineSCHUFA.de die Möglichkeit, nach einer kostenpflichtigen Registrierung jederzeit auf gespeicherte persönliche Daten zuzugreifen. Die bei der Registrierung notwendige Identifikation erfolgt mittels Personalausweis. Für den anschließend jederzeit möglichen Zugriff auf die gespeicherten Daten ist neben den Zugangsdaten eine erneute Identifikation erforderlich. Diese kann wahlweise mittels der Online-Funktion des neuen Personalausweises oder einer Login-TAN erfolgen. Der anschließende Überblick über die von der SCHUFA gespeicherten Daten ist in Abbildung 2 anonymisiert dargestellt. Die Detailansichten der verschiedenen Kategorien lassen sich mittels der Pfeile ausklappen. Über den R-Button können Rückfragen bezüglich der Einträge gesendet werden. Dies umfasst eine Korrektur- sowie Widerspruchsmöglichkeit.

Bei dem in Abbildung 3 beispielhaft dargestellten Basisscore handelt es sich um einen Orientierungswert, der alle drei Monate neu berechnet wird. Die Vertragspartner der SCHUFA erhalten in der Regel spezielle branchenspezifische oder individuelle Scores. Diese können durchaus von dem Basisscore abweichen.

Über den kostenpflichtigen SCHUFA-Update-Service besteht zudem die Möglichkeit, über Änderungen an den gespeicherten Daten sofort informiert zu werden. Der aktuelle Internet-Dienst meineSCHUFA.de kommt dem elektronischen Datenbrief näher, jedoch werden auch hier nicht alle über den Betroffenen gespeicherten Daten angezeigt. So fehlen zum Beispiel die Branchenscores. Auch wird der Ursprung der Daten nicht angegeben.

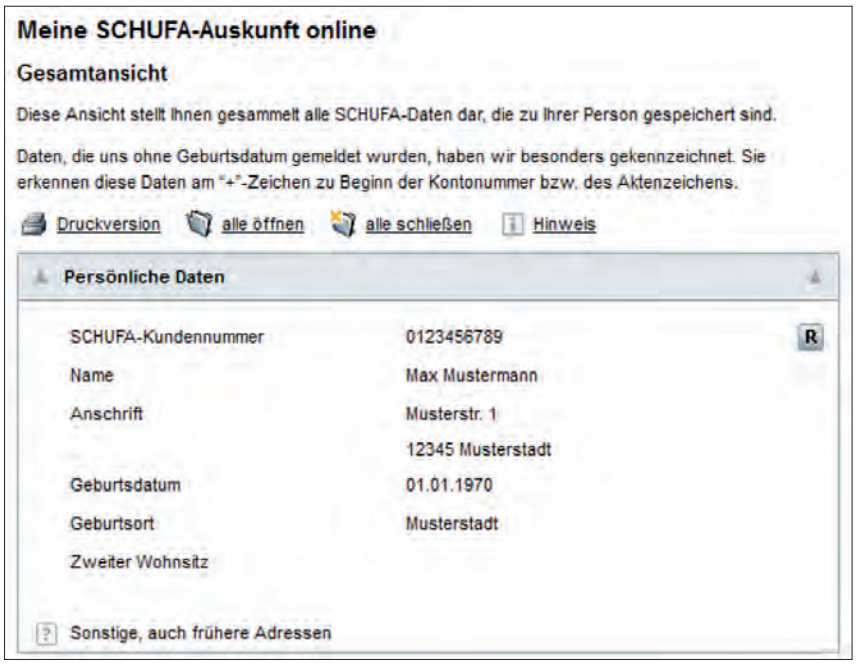

Abb. 2: Gesamtansicht der SCHUFA-Auskunft online

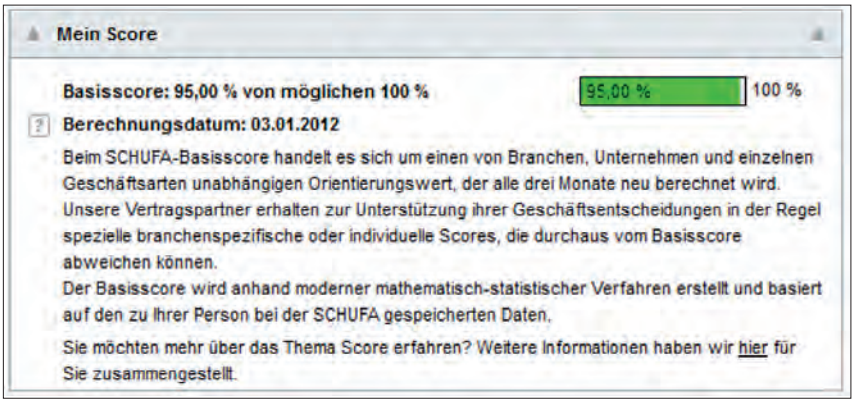

Abb. 3: Detailansicht des SCHUFA-Basisscores

Abb. 4: Verwaltung des Verlaufs besuchter Seiten

Abb. 5: Empfehlungen durch gekaufte Artikel verwalten

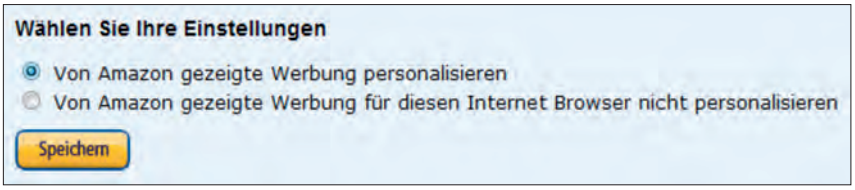

Abb. 6: Deaktivieren der personalisierten Werbung

Amazon

Das Onlineversandhaus Amazon bietet den Nutzern keine Möglichkeit, alle über sie gespeicherten Daten einzusehen. Jedoch bietet Amazon an, die Generierung der personalisierten Werbung in dem Menüpunkt Mein Konto zu steuern. Abbildung 4 zeigt die Verwaltung des Verlaufs besuchter Seiten. Dort können nicht nur einzelne kürzlich angesehene Artikel entfernt, sondern auch der komplette Verlauf besuchter Seiten gelöscht werden. Zudem besteht die Möglichkeit, den Verlauf besuchter Seiten komplett zu deaktivieren.

Daraufhin wird die personalisiere Werbung ausschließlich mittels der bereits gekauften Artikel generiert. Welche gekauften Artikel dafür verwendet werden, lässt sich ebenfalls in dem Menüpunkt Mein Konto einstellen. In Abbildung 5 ist ersichtlich, dass für jeden Artikel die Option „Nicht für Empfehlungen berücksichtigen“ aktiviert werden kann.

Da die Abwahl aller gekauften Artikel sehr mühselig sein kann, besteht in dem Menüpunkt Mein Konto weiterhin die Möglichkeit, die personalisierte Werbung komplett zu deaktivieren. Abbildung 6 veranschaulicht diese Einstellung.

Abschließend ist jedoch zu erwähnen, dass Einstellungen, die die Verbesserung der personalisierten Werbung (Löschen und Ausschließen von Artikeln) betreffen, dauerhaft gespeichert werden und die Deaktivierung des Verlaufs der besuchten Seiten und der kompletten personalisierten Werbung nur als Cookie in dem Internet Browser gespeichert wird. Es ist also festzustellen, dass die Deaktivierung und Behinderung der personalisierten Werbung bewusst flüchtig gestaltet wurde.

Fazit

Der elektronische Datenbrief stellt einen zukunftsweisenden Lösungsvorschlag für die Anbieter von Internet-Diensten dar und zeigt auf, wie eine aktive informationelle Selbstbestimmung im Internet für die Nutzer umgesetzt werden kann. Die Evaluation der aktuellen Situation zeigt, dass die Internet-Dienst-Anbieter den Bedarf eines elektronischen Datenbriefes erkennen, jedoch wird dieser größtenteils so umgesetzt, dass der speichernden Stelle keine Nachteile entstehen und der Betroffene getäuscht wird. Es ist deshalb wichtig, dass der vom Institut für Internet-Sicherheit entwickelte Lösungsvorschlag elektronischer Datenbrief zu einer Richtlinie weiterentwickelt wird, damit in Zukunft für alle Betroffenen jederzeit und bei jedem Internet-Dienst die standardisierte Möglichkeit besteht, die gespeicherten personenbezogenen Daten vollständig, einheitlich, einfach und sicher abrufen, korrigieren und löschen zu können. Nur dies kann der richtige Weg für eine modere Gesellschaft sein, bei der die Wahrung der Grundrechte der Bürger gewährleistet wird.¶