Alexander Novotny and Sarah Spiekermann

Personenbezogene Daten privatwirtschaftlich nachhaltig nutzen. Regulatorische und technische Zukunftskonzepte

Article (Accepted for Publication)
(Refereed)

Alexander Novotny, Sarah Spiekermann

Personenbezogene Daten privatwirtschaftlich nachhaltig nutzen

Regulatorische und technische Zukunftskonzepte

Zunehmende wirtschaftliche Vernetzung und Lobbyismus fordern die Sicherstellung von informierter Zustimmung, Transparenz und Verantwortlichkeit in der privatwirtschaftlichen Verwendung personenbezogener Daten heraus. Unser neues Modell verbindet durch das Zusammenspiel regulatorischer und technischer Datenschutzkonzepte mehr Sicherheit und Selbstbestimmung mit verstärkten Innovationsmöglichkeiten.

1 Einleitung

Personenbezogene Daten sind zunehmend ein Wirtschaftsgut dessen Nutzung die Schaffung zahlreicher neuer, nie dagewesener Wertpositionen verspricht. Neue Geschäftsmodelle zur Personalisierung und kundenspezifischen Ausgestaltung von Produkten und Inhalten entstehen. Die Aggregation personenbezogener Daten ermöglicht einen Einblick in menschliches Verhalten mit bemerkenswerter Genauigkeit. Beispielsweise können personenbezogene Mobilfunkverbindungsdaten zur Optimierung öffentlicher Verkehrsnetze und zur Analyse sozioökonomischer Chancen in ländlichen Gemeinden verwendet werden [1]. Die gefahrenlose und datenschutzfreundliche Extraktion dieser Wertpotentiale ist unabdingbar um Innovation und Wettbewerb bei digitalen Diensten in Europa zu sichern.

Gleichzeitig versucht eine kurzsichtige Politik destruktiver Interessensvertretung europäische Datenschutzprinzipien systematisch auszuhebeln. Eine Studie der Bürgerrechtsorganisation Lobbyplag zeigte im März 2015, dass der Brüsseler Ministerrat 87% der von der Kommission eingebrachten Datenschutzreformen schwächen will. Jeder vierte Änderungswunsch im Rat senkte das Datenschutzniveau sogar unter das Niveau der aktuell gültigen Datenschutzrichtlinie 95/46/EG [2].

Ein Kernbereich der Versuche Datenschutzstandards für die privatwirtschaftliche Nutzung personenbezogener Daten zu schwächen ist die informierte Zustimmung. Während die Zustimmung von Datensubjekten zur Verwendung ihrer Daten aktiv, nicht stillschweigend, eindeutig, nicht standardmäßig, im Einzelfall, vorherig, nachweisbar und freiwillig eingeholt werden sollte [3], werden diese Kriterien in der Praxis meistens nicht erfüllt. Datenschutzerklärungen sind so generisch formuliert, dass spezifisch bestimmte Verwendungszwecke für Daten kaum auslegbar und eine informierte Zustimmung im Einzelfall kaum möglich ist. Zustimmungshäkchen werden standardmäßig angekreuzt und quasi-monopolartige Anbieter lassen Datensubjekte keine Wahlmöglichkeit als vordefinierten Bedingungen zuzustimmen. Andernfalls wird die Dienstleistung wie beispielsweise die Nutzung der Suchmaschine oder des Kartendiensts verweigert. Als „Lösung“ des Zustimmungsproblems schlagen einige Interessensvertreter vor, die informierte Zustimmung abzuschaffen und damit das Kernelement informationeller Selbstbestimmung einfach aus dem Weg zu räumen.

Neben den Herausforderungen um die informierte Zustimmung, mangelt es ebenso an Transparenz und Verantwortlichkeit. Kunden sind häufig der irrigen Annahme, dass sie ihre Daten nur ihrem unmittelbaren Geschäftspartner preisgegeben. Jedoch sind beim Besuch einer Webseite durchschnittlich 56 Datensammler beteiligt [4]. Selbst den direkten Geschäftspartnern der Kunden (wie etwa Nachrichtenportalen) ist es oftmals nicht möglich Übersicht zu wahren, welche Entitäten welche Daten für welche Zwecke im Rahmen ihrer Kundenbeziehungen nutzen. Unternehmen verlieren innerhalb ihrer eigenen Kundenbeziehungen die Kontrolle über ein für sie essentielles Wirtschaftsgut: die Daten ihrer Kunden.

Die fehlende Transparenz führt zu großer Unsicherheit wer für die gesammelten Daten die Verantwortung trägt. Im Falle eines Datenmissbrauchs besteht die Gefahr, dass Unternehmen für Dienstleister, derer sie sich im Rahmen der Erfüllung ihrer Kundenbeziehungen bedienen, ohne effektive Kontrollmöglichkeit haften. Kunden haben ein zunehmend misstrauisches Unbehagen gegenüber Geschäftsbeziehungen in denen die Verantwortlichkeiten unsicher sind und keine effektive Rechtsdurchsetzung existiert. Verantwortlichkeit stärkende Lösungen sind nicht in Sicht. Im Zuge der kommenden Datenschutzgrundverordnung wird sogar diskutiert, dass Unternehmen im Falle des Bekanntwerdens eines Datenmissbrauch selbst definieren können, wann ein hohes Risiko für die Grundrechte betroffener Datensubjekte besteht und selbst entscheiden, ob sie diese informieren möchten.

Doch sollten bestehende Datenschutzkonzepte, anstatt sie abzuschaffen, nicht verbessert und an deren effektiven Durchsetzung gearbeitet werden? Kann ein zukunftsfähiges Konzept für eine nachhaltige und sichere privatwirt-

schaftliche Nutzung personenbezogener Daten geschaffen werden?

2 Ein neues Modell für die privatwirtschaftliche Datenverwendung

Um den Herausforderungen von informationeller Selbstbestimmung, Transparenz und Verantwortung bei gleichzeitig zunehmender Ökonomisierung personenbezogener Daten zu begegnen, haben wir in zwei Schritten ein neues Modell entwickelt, das auf technischen und regulatorischen Maßnahmen aufsetzt. Das Modell ist ausführlich in der „Computer Law & Security Review" beschrieben [5]. Ein erster Modellentwurf wurde mit Hilfe von 13 Interviews mit international führenden Experten von Technologie- und Handelsunternehmen, Datenhändlern, Datenschutzbehörden, Standardisierungsorganisationen, Branchenverbänden, Rechtsberatungskanzleien, und NGOs validiert und angepasst. Das Modell organisiert die an der privatwirtschaftlichen Verwendung personenbezogener Daten beteiligten Akteure in vier Bereiche mit klar definierten Rechten und Pflichten:

1. Direkter Kundenbeziehungsbereich
2. Unternehmensseitiger Datenverarbeitungsbereich
3. *Neu:* Kundenseitiger Datenverarbeitungsbereich
4. *Neu:* Offener Volksdatenmarkt

Im Folgenden werden diese vier Bereiche vorgestellt, um in Abschnitt 3 ausgewählte regulatorische und technische Konzepte zu skizzieren, die in diesen Bereichen gelten sollen.

- Der **direkte Kundenbeziehungsbereich** umfasst Kunden und Unternehmen, welche unmittelbar Dienstleistungen, Waren und Daten austauschen. Beispielsweise kauft ein Kunde bei einem Online-Händler ein, welcher personenbezogene Daten über diesen (z.B. Interessen, Profile in sozialen Netzwerken, Versandadresse, Bonität, etc.) verwendet.
- Der **unternehmensseitige Datenverarbeitungsbereich** umfasst das heute weit verteilte Dienstleisternetzwerk, dessen sich ein Geschäftspartner des Kunden bedient, um die Leistung am Kunden zu erbringen. Beispielsweise beauftragen Online-Händler Cloud-Dienstleister mit der Verarbeitung personenbezogener Daten und Online-Werbeagenturen mit der Zusendung personalisierter Marketingmitteilungen. Im Folgenden nutzen wir den Begriff „Geschäftspartner", um nur solche Unternehmen zu bezeichnen, die mit dem Kunden in einer direkten Geschäftsbeziehung stehen und deren „Marke" dem Kunden bekannt ist.
- Der **kundenseitige Datenverarbeitungsbereich** wurde insbesondere von den befragten Experten angeregt. Er umfasst jene neuen Dienste und Dienstleister, welche es dem Kunden ermöglichen sollen, in Zukunft selbst ihre personenbezogenen Daten zu speichern, zu verwalten und über deren Verwendung zu bestimmen. Zum Beispiel vertraut der Kunde seine Interessensdaten einem persönlichen Datentresor-Dienstleister an. Dieser gibt Online-Händlern bei Bedarf und unter Kontrolle des Kunden Zugriff auf diese Interessensdaten und lädt die Händler ein, passende Angebote zu stellen. Einen ersten kritischen Einblick in solche Dienstleistungen gibt das Sonderheft „Personal Data Markets" in der Zeitschrift „Electronic Markets" [6] sowie die Webseiten des „Personal Data Ecosystem Consortiums" (http://pde.cc).
- Der **offene Volksdatenmarkt** ermöglicht jedermann die eigenen anonymisierten Daten unter nicht diskriminierenden Bedingungen mit staatlich organisierten und finanzierten Stellen zu teilen, welche diese Daten wiederum Unternehmen zu Innovationszwecken zur Verfügung stellen. Volksdaten sind Daten, die nach aktuellen Anonymisierungsverfahren de-identifiziert wurden und die unter Strafe nicht re-identifiziert werden dürfen. Sie sollen es erlauben, einen Einblick in das aggregierte soziale Verhalten einer (Teil-)Population zu gewinnen. Beispielsweise könnte der Geschäftspartner Volksdaten von einer Volksdatenmarktplattform beziehen. Die Daten könnten die aggregierten Kaufinteressen weiblicher Kunden abbilden, welche „Gefällt mir" Angaben zum Thema „Fahrrad" machten und täglich zwischen 8 und 10 Uhr morgens zur Arbeit fahren. Andere Unternehmen und Kunden können anonymisierte Daten auf Volksdatenmärkten freiwillig zur Verfügung stellen. Da Volksdaten hinreichend anonymisiert sind, und eine Re-identifikation strafbar wäre, unterliegen sie nicht dem Datenschutzregime.

Nur regulatorische Maßnahmen und Datenschutztechnologien gemeinsam können dem Modell zu einer effektiven Durchsetzung verhelfen. Ein Recht ohne effektive technologische Durchsetzungsmöglichkeit wäre nur theoretisch gültig. Genauso gäbe es ohne eine rechtliche Umsetzungsverpflichtung für Datenschutztechnologien nur einen geringen Anreiz zur Implementierung. Im Folgenden stellen wir ein Gefüge neuartiger regulatorischer und technischer Zukunftskonzepte vor, welche eine datenschutzfreundliche privatwirtschaftliche Verwendung personenbezogener Daten nach unserem Modell ermöglichen.

3 Regulatorische und technische Zukunftskonzepte

Zustimmungsagenten, das Prinzip der ungeteilten Datenverantwortlichkeit, technisch nachverfolgbare Datennutzungsvereinbarungen, persönliche Datentresore und Anonymisierungsstandards für offene Volksdaten können helfen das Modell zu realisieren.

3.1 Zustimmungsagenten zur Vereinfachung der Kundenbeziehung

Persönliche Zustimmungsagenten sind Software-Bots, welche den Zustimmungsvorgang für eine Datenverarbeitung automatisieren [7]. Kunden können Zustimmungsagenten ihren Privatsphäre-Präferenzen entsprechend konfigurieren. Beispielsweise könnte der Kunde der Verwendung seiner Daten für die Zusendung von Marketingmitteilungen zustimmen, der Weitergabe seiner Daten an Adresshändler jedoch nicht zustimmen und eine maximale Speicherfrist von einem Jahr verlangen. Die Konditionen der Datennutzung werden in Datennutzungsvereinbarun-

gen verankert und den Daten angehängt (siehe unten 3.3 sowie [8]).

Damit eine aktive, einzelfallbezogene Zustimmung durch automatische Zustimmungsagenten vorstellbar ist, müssen Kunden ihre Privatsphäre-Einstellungen selbsttätig definieren und diese müssen sich hinreichend spezifisch auf einzelne Geschäftspartner beziehen. Eine benutzerfreundliche, laufende Wartung der Präferenzeinstellungen ist möglich, wenn Zustimmungsagenten aus dem historischen Zustimmungsverhalten ihrer „Besitzer" lernen und diesen mögliche Anpassungen vorschlagen.

Durch den Einsatz von Zustimmungsagenten profitieren Kunden von einer deutlichen Vereinfachung und Beschleunigung des Zustimmungsvorgangs. Der Zustimmungsagent vergleicht die Kundenpräferenzen mit den Datenschutzrichtlinien des Geschäftspartners. Nur wenn ein Konsens vorliegt kommt es zu einer gültigen Zustimmung. In komplexeren Szenarien werden auch automatische Verhandlungen zwischen Zustimmungsagenten und Geschäftspartnern über die Bedingungen der Dienst- und Datennutzung ermöglicht. Automatisierte Verhandlungen wären ein notwendiges (jedoch nicht hinreichendes) Element um Kunden aus der Rolle passiver Zustimmer in die Rolle aktiver, ebenbürtiger Verhandlungspartner zu heben; selbst wenn die Einzelverhandlungen delegiert werden. Eine vorhandene Software-Lösung ist der Zustimmungsagent „Privacy Bird", welcher im Rahmen des „Platform for Privacy Preferences (P3P)" Projekts des World Wide Web Consortiums (W3C) entwickelt wurde [7]. In diesem Zusammenhang wäre als rechtliche Rahmenbedingung wichtig Unternehmen zu verpflichten, ihren Kunden auch dann Zugang zu Dienstleistungen zu gewähren, wenn diese zweckfremden Datenverarbeitungen nicht zustimmen (striktes Koppelungsverbot).

3.2 Ungeteilte Datenverantwortlichkeit zur Rückgewinnung von Vertrauen in der Kundenbeziehung

Um nachhaltige Wertpositionen für Kunden zu stiften, hat sich das Beziehungsmarketing (One-to-one relationship marketing) als vorherrschendes Paradigma etabliert. Geschäftspartner möchten Vertrauen zu ihren Kunden aufbauen und langfristige Beziehungen pflegen. In solchen Beziehungen gehen Kunden davon aus, dass sie ihre Daten nur dem einen, für sie sichtbaren Geschäftspartner anvertrauen. Kauft der Kunde beispielsweise bei einem Online-Versandhaus ein, so ist nur dieses für den Kunden sichtbar. Das Vertrauen droht schwer belastet zu werden, wenn für den Kunden weitere, kaum sicht- und wahrnehmbare Datenverarbeiter, wie Werbenetzwerke, Betreiber sozialer Netzwerke, Kreditauskunfteien und Adresshändler beteiligt sind. Kunden können dann kaum vorhersehen für welche Zwecke ihre Daten tatsächlich verwendet werden und keine informierte Entscheidung treffen.

Um das Vertrauen in Kundenbeziehungen zu stärken und wiederherzustellen, schlagen wir vor, dass den *sichtbaren* Geschäftspartner eine ungeteilte Datenverantwortlichkeit treffen sollte. Dieser haftet für alle Schäden aus der missbräuchlichen Verwendung jener personenbezogenen Daten, die ursprünglich aus der Kundenbeziehung stammen. Die Haftung erstreckt sich auf von anderen Datenverarbeitern verursachte Schäden, welche Daten im Rahmen der Kundenbeziehung erhielten und geht über eine reine Erfüllungsgehilfenhaftung hinaus. Im Schadensfall können sich Geschäftspartner an anderen in der Kundenbeziehung involvierten Datenverarbeitern regressieren. Geschäftspartner fungieren als einziger Kontaktpunkt für Kunden und gewinnen so die Kontrolle über die Datenverwendung zurück, die sich aus ihren eigenen Kundenbeziehungen ergibt.

3.3 Technisch nachverfolgbare Datennutzungsvereinbarungen in der unternehmensseitigen Datenverarbeitung

Um Geschäftspartnern und Kunden im Rahmen der Kundenbeziehung eine effektive Kontrollmöglichkeit über die Verwendung personenbezogener Daten einzuräumen, schlagen wir vor, eine verpflichtende technische Nachverfolgbarkeit der Datenverwendung einzuführen. Erst die Nachverfolgbarkeit der Datenverwendung durch andere Datenverarbeiter im Rahmen der Kundenbeziehung ermöglicht dem Geschäftspartner das Tragen einer ungeteilten Datenverantwortlichkeit.

Technisch gestützte Datenverantwortlichkeit kann mittels elektronischer Datennutzungsvereinbarungen realisiert werden. Das Ergebnis des durch Zustimmungsagenten automationsgestützt abgewickelten Zustimmungsvorgangs wird in elektronischen Datennutzungsvereinbaren festgehalten. Metadaten-basierte Architekturen ermöglichen es die elektronischen Datennutzungsvereinbarungen direkt und untrennbar an die betroffenen personenbezogenen Daten zu binden. Somit „klebt" die geltende Datennutzungsvereinbarung an den personenbezogenen Daten (engl. „sticky policies" [8]). Microsoft schlägt Metadaten-basierte Architekturen vor [9].

Metadaten-basierte Architekturen ermöglichen die Unternehmensgrenzen-überschreitende Rückverfolgung jeglicher Verwendung der Daten (Zugriff, Veränderung, Speicherung, Vervielfältigung, Löschung, etc.). Es wird sichergestellt, dass nur autorisierte Verwender Zugriff auf personenbezogene Daten haben und diese eine Datenverwendung nicht abstreiten können. Somit wird ein hoher Standard an Auditierbarkeit der Datenverwendung erzielt. Die ungeteilte Datenverantwortlichkeit tragenden Geschäftspartner haben damit ein effektives Instrument, um Datenmissbrauch durch an ihren Kundenbeziehungen beteiligten Datenverarbeitern vorzubeugen.

Eine technische Nachverfolgbarkeit der Datenverwendung würde auch Anreize setzen, jene Datenverwender aus Kundenbeziehungen zu verdrängen, welche keinen unmittelbaren Wert für den Kunden stiften. Auf diese Weise würde Datenaggregatoren und Adresshändlern, welche Kundendaten heute meist ohne Bewusstsein der Kunden nutzen, die Geschäftsgrundlage entzogen.

Geschäftspartner könnten die für die technische Nachverfolgbarkeit notwendige Infrastruktur entweder selbst mit Hilfe von Dienstleistern betreiben, oder sich einer von der öffentlich Hand betriebenen Infrastruktur bedienen. Die Kosten für die technische Nachverfolgbarkeit müssten vom Geschäftspartner getragen werden, da dieser in unse-

rem Modell alle Vorteile aus der Verwendung personenbezogener Daten innerhalb seiner Kundenbeziehungen lukriert.

3.4 Persönliche Datentresore im kundenseitigen Datenverarbeitungsbereich

Eine Alternative zur Datenverantwortlichkeit durch Geschäftspartner ist, dass Kunden ihre Daten selbst in persönlichen Datentresoren (engl. „personal data vaults/stores“) speichern. Ein persönlicher Datentresor ist ein sicherer Online-Speicher für personenbezogene Daten, welcher unter vollständiger Kontrolle des Kunden betrieben wird. Kunden können über die Sammlung, den Speicherort, den Zugriff, die Nutzung, Aktualisierung, und Speicherdauer ihrer Daten selbst entscheiden.

Persönliche Datentresore können entweder von unabhängigen Drittanbietern oder durch Kunden selbst betrieben werden. Drittanbieter übernehmen die Speicherung der Daten für Kunden und treten für diese als Mittler in Kundenbeziehungen auf. Erste Drittanbieter-Dienste sind beispielsweise das HAT-Projekt (Hub-of-all-things) und der US-amerikanische Dienst Mydex. Selbstbetriebene persönliche Datentresore könnten durch kleine Steckdosen-Computer (z.B. der „Freedom-Box“), welche dauerhaft mit dem Internet verbunden sind, realisiert werden.

3.5 *Anonymisierungsstandards für offene Volksdaten*

Das größte Innovationspotential liegt nicht in der einzelnen Verwendung personenbezogener Daten selbst, sondern in deren Aggregation und offenen Nutzung in Form anonymisierter Volksdaten. Für eine sichere Nutzung von Volksdaten muss für bestimmte Datenverwendungszwecke das geeignete, erforderliche und angemessene Anonymisierungsniveau allgemeingültig festgelegt werden. Denn das Risiko einer Re-Identifizierung offener Volksdaten verändert sich mit dem Stand der Technik stetig. Unter dem Schlagwort „Big Data“ haben verbesserte Möglichkeiten zur Zusammenführung und Analyse größerer Datenvolumina aus unterschiedlichen Quellen das Re-Identifikationsrisiko einst sicher anonymisierter Daten deutlich erhöht [10]. Als Reaktion auf dieses gestiegene Risiko hat die Artikel 29 Datenschutzgruppe in ihrer Meinung 05/2014 zu Anonymisierungstechnologien den Zweckbindungsgrundsatz und das Erfordernis eines Legitimationsgrunds (z.B. informierte Zustimmung) auch auf anonymisierte personenbezogene Daten ausgedehnt. Ohne sichere und anerkannte Referenzstandards für die Anonymisierung offener Volksdaten besteht die Gefahr, dass die privatwirtschaftliche Verwendung dieser in Zukunft erheblich eingeschränkt werden könnte. Im Einklang mit dem Grundsatz der Verhältnismäßigkeit gilt es daher eine angemessene Balance zwischen sozialem Nutzen und den Privatsphäre-Interessen potentiell re-identifizierbarer Personen zu finden.

Vor diesem Hintergrund schlagen wir auf technischer Ebene vor, „Best available techniques for anonymization“ – also einen Referenzstandard – zu entwickeln. Basierend auf aktuellen Anonymisierungskonzepten wie der k-Anonymität, l-Diversität und t-Ähnlichkeit könnten in diesen Referenzstandards beste verfügbare Techniken für die Anonymisierung im Wege supranationaler Co-Regulierung definiert werden. Der Standard könnte von anerkannten Standardisierungsbehörden erarbeitet und regelmäßig erneuert werden. Verwender offener, anonymisierter Volksdaten müssten diesen zwingend implementieren. Darüber hinaus wäre die Re-identifizierung offener Volksdaten unter Strafe gestellt.

Referenzstandards für beste verfügbare Technologien werden bereits in anderen Bereichen erfolgreich genutzt, etwa im Rahmen der Industrieemissionsrichtlinie 2010/75/EU. Die einheitliche Definition technischer Vorgaben für die zweckgebundene Nutzung anonymisierter Daten ist möglich, wie ein Gutachten über die Datenschutzanforderungen an die Verarbeitung und Nutzung anonymisierter Daten in deutschen Apotheken-Rechenzentren zeigt [11]. Anonymisierungsstandards würden das Risiko aus der ökonomischen Volksdatennutzung minimieren und kalkulierbar machen. Volksdatennutzende Unternehmen würden im Gegenzug von hoher Rechtssicherheit und von Innovationspotenzialen aus Big Data profitieren, welche heute vor allem US-amerikanischen Datenmonopolen vorenthalten sind.

4 **Fazit**

Die vorgestellten regulatorischen und technischen Konzepte zielen auf eine sichere, faire und nachhaltige privatwirtschaftliche Nutzbarkeit von Daten bei gleichzeitiger Minimierung auftretender Datenschutzrisiken. Insbesondere die Nutzung anonymisierter, offener Volksdaten birgt großes Potential. Volksdatenanalyse wird zu neuen sozialen Erkenntnissen sowie innovativen, neuen Produkten und Dienstleistungen mit höherer Qualität führen bei gleichzeitigem Aufbrechen gegenwärtiger Datenmonopole. Jedoch müssen neue rechtliche und technische Rahmenbedingungen für eine gefahrlose wirtschaftliche Nutzung personenbezogener Daten und anonymisierter Volksdaten geschaffen werden. Insbesondere brauchen Kunden Technologien, die es ihnen ermöglichen selbstbestimmt an Datenmärkten zu partizipieren oder sich diesen auch zu entziehen und sich zu schützen. Dafür sind Zustimmungsagenten und persönliche Datentresore vielversprechende erste Ansätze. Um der fehlenden Datenverwendungstransparenz in komplexen wirtschaftlichen Prozessen zu entgegnen, werden ebenso technische Datenverantwortlichkeitsmechanismen an Bedeutung gewinnen.

Die Umsetzung neuer regulatorischer und technischer Konzepte wird herausfordernd sein. Doch mittels geeigneter Datenschutztechnologien, supranational harmonisierter, auditierbarer Standards und effektiver Sanktionen ist eine sichere und nachhaltige Zukunft privatwirtschaftlicher Datenverwendung zumindest denkbar.

Literatur

[1] United Nations Global Pulse (2013). *Mobile Phone Network Data for Development*. Oktober 2013.

[2] Wimmer, B. (2015). *Lobbyplag zeigt, welche Länder EU-Datenschutz verhindern*. Futurezone.at, 10.03.2015.

[3] Pachinger, M.M. (2012). *Der neue "Cookie-Paragraph" - Erste Gedanken zur Umsetzung des Art 5 Abs 3 E-Privacy-RL in § 96 Abs 3 TKG 2003 idF BGBl I 2011/102*. jusIT 2012/8, 16-22.

[4] Angwin, J. (2012): *Online Tracking Ramps Up - Popularity of User-Tailored Advertising Fuels Data Gathering on Browsing Habits*. Wall Street Journal, 18.06.2012, B1.

[5] Spiekermann, S., Novotny, A. (2015). *A Vision for Global Privacy Bridges: Technical and Legal Measures for International Data Markets*. Computer Law & Security Review 31(2), 181-200.

[6] Spiekermann, S., Böhme, R., Acquisti, A., Hui, K.-L. (2015). *Personal Data Markets*. Electronic Markets Special Issue, in Erscheinung.

[7] Cranor, L.F., Guduru, P., Arjula, M. (2006). *User Interfaces for Privacy Agents*. ACM Transactions on Computer-Human Interaction, 13(2), 135-178.

[8] Mont, M.C., Pearson, S., Bramhall, P. (2003). *Towards Accountable Management of Identity and Privacy: Sticky Policies and Enforceable Tracing Services*. In Proceedings of the 14th International Workshop on Database and Expert Systems Applications (DEXA), Prag, 01.-05.09.2003, 377-382.

[9] Maguire, S., Friedberg, J., Nguyen, M.-H.C., Haynes, P. (2015). *A Metadata-based Architecture for User-centered Data Accountability*. Electronic Markets, in Erscheinung.

[10] Ohm, P. (2010). *Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization*. UCLA Law Review 57, 1701-1777.

[11] Giesen, T., Schnoor, C. (2013). *Datenschutzrechtliche Anforderungen an die Verarbeitung und Nutzung anonymisierter Daten für andere Zwecke nach § 300 Abs. 2 Satz 2, 2.Halbsatz SGB V durch Apotheken-Rechenzentren*. Datenschutzrechtliches Gutachten, Institut für Informationsordnung e.V.