STIFTUNG DATENSCHUTZ

Neue Wege bei der Einwilligung im Datenschutz – technische, rechtliche und ökonomische Herausforderungen

Studie

STIFTUNG DATENSCHUTZ

Stiftung Datenschutz
rechtsfähige Stiftung bürgerlichen Rechts
Karl-Rothe-Straße 10–14
04105 Leipzig
Deutschland

Telefon 0341 / 5861 555-0
mail@stiftungdatenschutz.org
www.stiftungdatenschutz.org

gestiftet von der Bundesrepublik Deutschland
vertreten durch den Vorstand Frederick Richter

Gefördert durch das Bundesministerium des Innern

Inhalt

A. Neue Wege bei der Einwilligung im Datenschutz – technische, rechtliche und ökonomische Herausforderungen

Dr. Nikolai Horn, Prof. Dr. Anne Riechert, Christian Müller, LL.M., Stiftung Datenschutz

B. Stellungnahme
Rechtliche Aspekte eines Einwilligungsassistenten

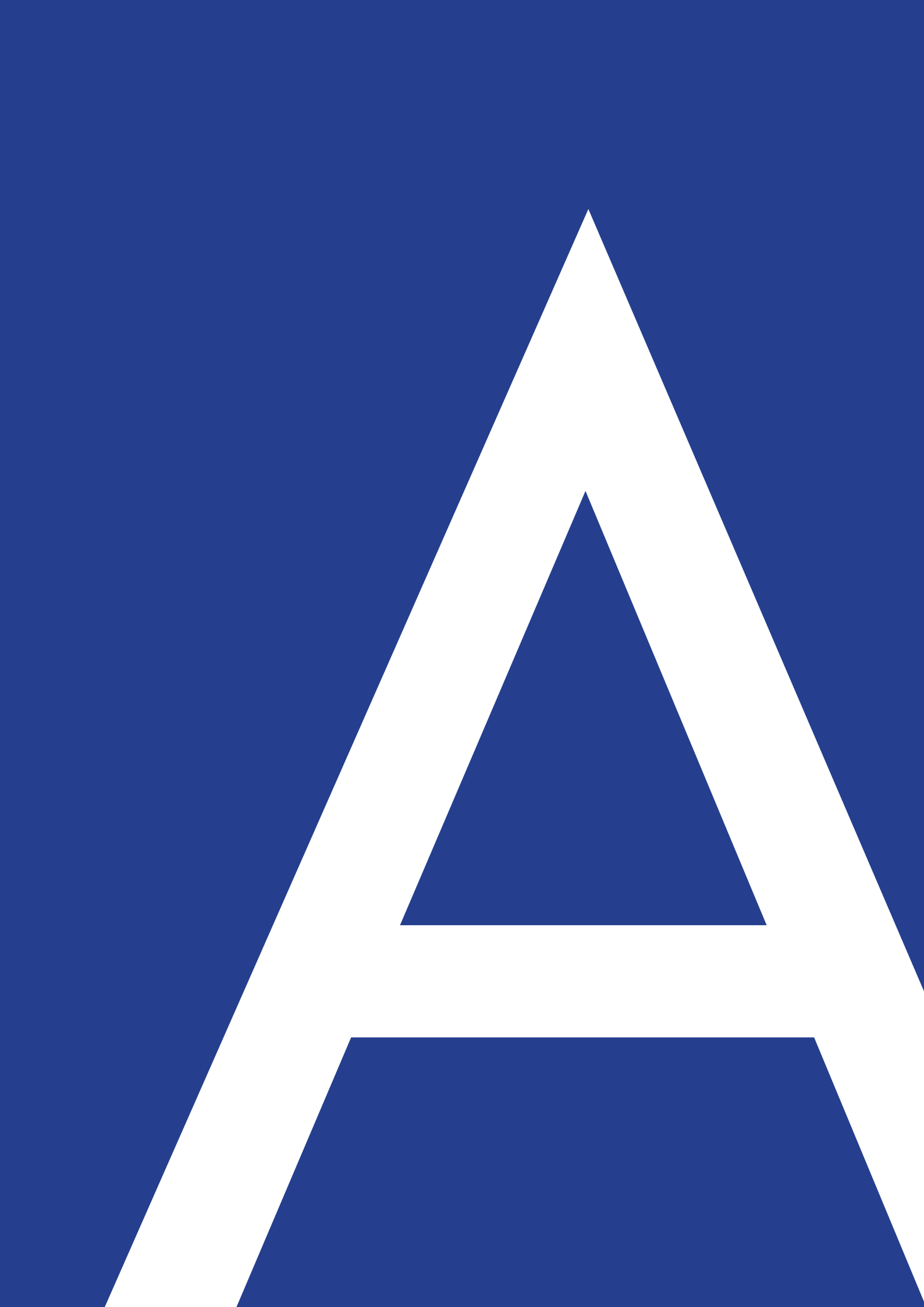
Prof. Dr. Anne Riechert, Stiftung Datenschutz / Frankfurt University of Applied Sciences

C. Gutachten
Die persönliche Datenökonomie: Plattformen, Datentresore und persönliche Clouds

Dr. Nicola Jentzsch, Deutsches Institut für Wirtschaftsforschung Berlin (DIW Berlin)

D. Weiterführende Informationen

Dr. Nikolai Horn, Prof. Dr. Anne Riechert, Christian Müller, LL.M., Stiftung Datenschutz



Inhaltsverzeichnis

	Seite
I. Anlass und Gegenstand der Studie	7
II. Technische Lösungsansätze	9
1. Einführung	9
2. Darstellung der im Projekt betrachteten Ansätze	10
3. Bewertung der verschiedenen Ansätze	23
a) Bewertungskriterien	23
b) Reichweite und Diversität	25
c) Wirtschaftlicher Hintergrund und Vertrauensbildung der Projekte	27
d) Technische Erwägungen – Datenstandort und Datenschutzniveau am Standort	29
e) Nutzerkontrolle und Transparenz	32
4 Schlussbetrachtung	35
5. Allgemeine Herausforderungen	37
III. Rechtliche Aspekte von Einwilligungsassistenten	38
1. Anforderungen an den Einwilligungsassistenten	38
2. Anforderungen an ein gleichwertiges Datenschutzniveau	41
3. Klärungsbedarf	45
IV. Ökonomische und verbraucherpolitische Herausforderungen	47
1. Ökonomische Rahmenbedingungen innovativer Lösungen zu Datenschutz-Einwilligungen	47
2. Verhaltensökonomische Herausforderungen am Beispiel der Einwilligung	49
3. Klärungsbedürftige Punkte	50
V. Handlungsempfehlungen	51
1. Politik und Praxis	51
2. Ökonomische Rahmenbedingungen	53
3. Institutionelle Förderung	54
4. Forschungsmaßnahmen	54
5. Sektorübergreifende Maßnahmen	55
VI. Fazit	57

Abrufdatum der Internetlinks in Teil A: 24. Februar 2017

I. Anlass und Gegenstand der Studie

Ob beim Einkaufen oder sich mit Freunden verabreden, ob beim Spazierengehen oder Fahren, ob beim Unterhaltungsprodukte konsumieren oder Fitness betreiben – die Preisgabe von persönlichen Daten gehört längst zum Alltag der Menschen in unserer vernetzten Welt. Die Bürger werden sehr häufig um Zustimmung zur Nutzung der sie betreffenden Daten gebeten. Ohne Einwilligung zur Datenverarbeitung kommen sie regelmäßig nicht in den Genuss der digitalen Dienstleistungen. Die zugehörigen Datenschutzerklärungen sind jedoch meist lang und werden wegen juristischer Anforderungen, technischer Komplexität und Zeitmangel fast nicht gelesen, sodass dem Inhalt dieser „Daten-AGB" für gewöhnlich mehr oder minder blind zugestimmt wird. „Schließlich erfahren die Nutzer oft erst aus Datenskandalen oder von *Whistleblowern*, wie persönliche Informationen verwendet werden, also zu einem Zeitpunkt, zu dem es bisweilen zu spät ist, um Erfahrungen zu machen und aus diesen zu lernen."[1]

Immer mehr Anfragen nach datenschutzrechtlichen Einwilligungen führen beim Dateninhaber außerdem zu Entscheidungsüberforderung, Abstumpfung im Sinne einer „rationalen Ignoranz" und schließlich zu einer Entwertung der Einwilligung. Die datenschutzrechtliche Idealvorstellung einer „informierten Einwilligung" findet sich im realen Leben der Menschen faktisch kaum wieder. Angesichts der weiter steigenden Zahl tatsächlich nicht-informierter Einwilligungen wächst auf Verbraucherseite die Unsicherheit über den Umgang mit persönlichen Daten. Es entstehen außerdem Asymmetrien zwischen dem, was die Nutzer über sich wissen, und dem, was die datenverarbeitenden Dienste wissen. In gleichem Maße sinkt das Vertrauen, das der datenverwendenden Wirtschaft entgegengebracht wird. Angesichts der Unsicherheit auf Seiten der Verbraucher sowie ausgeweiteten Verpflichtungen im Zuge der EU-Datenschutz-Grundverordnung haben zugleich auch die Unternehmen verstärktes Interesse daran, mit nachvollziehbar dokumentierten und möglichst informiert erteilten Einwilligungserklärungen mehr Rechtssicherheit zu erlangen und Kundenvertrauen zu erhöhen.

Die EU-Datenschutz-Grundverordnung wird voraussichtlich an diesem Zustand wenig ändern können. Zwar werden die Nutzer demnächst rechtlich in die Lage versetzt, einzelnen Datenverwendungen ihre Zustimmung zu verweigern. Damit dies aber eine bewusste Handlung wird, werden sie sich zuvor mit dem Inhalt der einzelnen Verarbeitungszwecke auseinandersetzen müssen – und gerade dieser Aufwand ist schon heute vielen zu groß. Die Zahl der vom Anwender erbetenen Einwilligungen wird auch zukünftig weiter steigen. Zudem werden Informationspflichten ausgeweitet; damit wächst die „Informationsflut" für Kundschaft und Interessenten, was die Menschen weiter in die Resignation und zum routinierten, unreflektierten Kästchenankreuzen treiben wird. Denn die Menschen wollen innovative Dienste nutzen und in den Genuss technologischer Errungenschaften kommen. Sie wollen aber nicht ihre Privatsphäre am Eingang zur digitalen Welt abgeben. Die informierte Einwilligung bleibt dabei ein ganz entscheidendes Werkzeug der Informationsautonomie und letzten Endes eine Voraussetzung für die Ausübung des Grundrechts auf informationelle Selbstbestimmung. Allerdings scheinen die aktuellen technischen Anforderungen und die veränderten Gegebenheiten der automatisierten Datenverarbeitung nur schwer „mit den geltenden nationalen und europäischen Vorschriften in einer Art und Weise (zu) vereinbaren, welche die Interessen aller Beteiligten in einen angemessen Ausgleich bringt".[2]

1 *Hermstrüwer, Y., Informationelle Selbstgefährdung, Tübingen, 2016, S. 367.*

2 *Pollmann, M. /Kipker, D.-K., Eingeschränkte Selbstbestimmung im Onlineverkehr; Stärkung der Einwilligungserklärung durch Einführung vorformulierter Datenschutzbestimmungen, IGMR, 01.04.2016, S. 9. https://www.jura.uni-bremen.de/uploads/IGMR/Pollmann_Kipker_Working-Paper_Eingeschrankte_Selbstbestimmung_im_Onlineverkehr_2016.pdf*

Wie kann dieser Entwicklung Rechnung getragen werden? Kann man den betroffenen Personen womöglich durch den Einsatz „intelligenter Technik“ die Verfügungsmacht über ihre Daten zurückgeben und eine verbesserte Einwilligungsmöglichkeit erzeugen? Um diese Fragen zu klären, hat die gemeinnützige Stiftung Datenschutz im Rahmen eines vom Bundesministerium des Innern geförderten Projekts eine Reihe von unterschiedlichen Einwilligungsprojekten verglichen sowie die rechtlichen[3] und ökonomischen[4] Rahmenbedingungen für die Implementierung von Einwilligungsplattformen untersucht. In der vorliegenden Studie werden mögliche Wege zur technikbasierten Erleichterung rechtssicherer Einwilligungen hin zu mehr Selbstbestimmung und Nutzerkontrolle aufgezeigt. Es werden anschließend Vorschläge entwickelt, auf welche Weise der Vorgang der Einwilligung im Datenschutzrecht und in der Datenschutzpraxis praktikabler ausgestaltet und technisch unterstützt werden kann. Dabei wird geprüft, welche Möglichkeiten sich innerhalb des neuen europäischen Rechtsrahmens und nach dem Stand der Technik bieten, um den Wert der Einwilligung wieder zu erhöhen. Ein besonderes Augenmerk wird dabei auf die technischen Lösungswege gelegt.

Eine große Chance bestünde aus Stiftungssicht dann, wenn es zukünftig gelingen würde, inflationär häufige und teils rechtsunsichere Einverständniserklärungen durch einen anwenderfreundlichen und automatisierten Lösungsansatz handhabbarer zu machen.

Um dies zu ermöglichen, wird auf der technischen Seite gefragt: Welche aktuellen Probleme der Einwilligung könnten die sogenannten „Personal Information Management Services“ (PIMS) bzw. „Privacy Enhancing Technology“ (PET) lösen? Inwiefern kann es gelingen, durch technische Einwilligungsassistenten und Einwilligungsplattformen die Stärkung der Auskunftsrechte, eine Automatisierung des Einwilligungsverfahrens, die Eindeutigkeit und Verständlichkeit der Einwilligung sowie die Transparenz von Datenverarbeitungszwecken zu gewährleisten? Welche Lösungsansätze – sowohl international als auch in Deutschland – existieren bereits und wo besteht weiterhin der Forschungsbedarf?

Auf der rechtspolitischen Ebene wird die Frage nach der rechtlichen Anschlussfähigkeit von automatisierten Einwilligungsverfahren erörtert. Es wird untersucht, welche gesetzlichen Rahmenbedingungen erfüllt werden müssen, um die Weiterentwicklung von automatisierten Einwilligungsverfahren zu fördern, und wo aktuell noch Regulierungsbedarf besteht? Inwiefern entspricht eine automatisierte Einwilligung den Einwilligungsanforderungen aus der EU-Datenschutz-Grundverordnung? Wie könnten die rechtlichen Anforderungen an automatisierte Einwilligungsverfahren europaweit vereinheitlicht werden?

Aus der ökonomischen und verbraucherpolitischen Perspektive wird nach den praktischen Implementierungschancen von automatisierten Einwilligungsverfahren gefragt. Wie sehen Marktdynamiken und förderliche ökonomische Rahmenbedingungen für das innovative Einwilligungsmanagement aus? Wo könnte der wirtschaftliche Mehrwert des Einsatzes von PIMS-Technologien liegen, damit sich diese am Markt durchsetzen? Wie bringt man außerdem die Nutzer in der Praxis dazu, sich über die Datenverarbeitung zu informieren und die Einwilligung von diesen Informationen abhängig zu machen?

3 *Dazu: „Stellungnahme zu rechtlichen Aspekten eines Einwilligungsassistenten“, Prof. Dr. Anne Riechert, Stiftung Datenschutz, Anhang 1. https://stiftungdatenschutz.org/themen/projekt-einwilligung-und-transparenz/*

4 *Dazu: Gutachten „Die persönliche Datenökonomie: Plattformen, Datentresore und persönliche Clouds“, Dr. Nicola Jentzsch, Deutsches Institut für Wirtschaftsforschung (DIW Berlin), Anhang 2. https://stiftungdatenschutz.org/themen/projekt-einwilligung-und-transparenz/*

II. Technische Lösungsansätze

1. Einführung

Eine informierte Einwilligung ist eine ganz entscheidende Voraussetzung für eine bewusste Ausübung des Rechts auf informationelle Selbstbestimmung. Immer mehr personenbezogene Daten werden von Unternehmen gesammelt und für die Erstellung von Kundenprofilen verwendet. Die Datenschutzerklärungen zu digitalen Produkten sind dabei meist lang und werden wegen juristischer Anforderungen, technischer Komplexität und Zeitmangel von den Verbrauchern fast nicht gelesen, sodass dem Inhalt dieser „Daten-AGB" für gewöhnlich mehr oder minder blind zugestimmt wird. Die bewusste Ausübung des Rechts auf informationelle Selbstbestimmung wird daher immer schwieriger.

Kann man womöglich den Nutzern durch den Einsatz „intelligenter Technik" die Verfügungsmacht über ihre Daten und ihre Online-Identität zurückgeben und eine verbesserte Einwilligungsmöglichkeit erzeugen? Inwiefern kann es gelingen, durch technische Einwilligungsassistenten und Einwilligungsplattformen die Stärkung der Auskunftsrechte, die Automatisierung des Einwilligungsverfahrens, die Eindeutigkeit und Verständlichkeit der Einwilligung sowie die Transparenz von Datenverarbeitungszwecken zu gewährleisten? Können die aktuellen Probleme der Einwilligung mittels sogenannter „Personal Information Management Services" (PIMS) oder „Privacy Enhancing Technology" (PET) gelöst werden? Welche Lösungsansätze – sowohl international als auch in Deutschland – existieren bereits und wo besteht weiterhin Forschungsbedarf?

Die Auseinandersetzung mit automatisierten Einwilligungsverfahren und Einwilligungsassistenten befindet sich in Deutschland noch in den Anfängen, während diese Themen auf der europäischen Ebene bereits intensiv behandelt werden. So wurden im September 2016 in einer Stellungnahme[5] des EDPS (European Data Protection Supervisor) die Chancen und Herausforderungen von PIMS bewertet und die besondere Unterstützungswürdigkeit der Entwicklung solch innovativer Ansätze gegenüber der Kommission hervorgehoben. Dazu gehört neben der Implementierung und Co-Finanzierung durch den öffentlichen Sektor auch die Zusammenarbeit mit anderen strategischen Projekten wie der Digital Single Market Strategy oder Projekten zu Cloud Computing und zum „Internet der Dinge". Auch der im November 2016 veröffentlichte PIMS-Report der Europäischen Kommission setzt sich eingehend mit besonderen Herausforderungen bei der Implementierung von PIMS-Plattformen auseinander.[6]

Das Ziel der nachfolgenden Untersuchung ist eine Evaluation verschiedener technischer Möglichkeiten, welche Voraussetzungen für die legale Verarbeitung personenbezogener Daten schaffen und Auskunftsrechte oder Rechte zur Beschränkung der Verarbeitung bzw. zur Löschung erleichtern. Indem dabei nicht stets erneut eine direkte Nutzerinteraktion erforderlich ist, soll das Einwilligungsverfahren erheblich erleichtert werden. Die Idee hinter den PIMS-Ansätzen ist, dass es dem Nutzer möglich sein soll zu entscheiden, wann, an wen, zu welchen Zwecken, in welchem Umfang und für wie lange er seine Daten übermittelt, sowie die Nutzung dieser Daten nachzuverfolgen und ggf. zu widerrufen. Dementsprechend werden die Ansätze auch daraufhin untersucht, inwiefern sie mehr Transparenz schaffen, z. B. durch die automatisierte Erstellung einer Übersicht über Zugriffsrechte verschiedener Applikationen, und inwiefern sie Nutzer selbstbestimmt im Vorfeld entscheiden lassen, wer welche Daten zu welchem Zweck erhalten soll.

5 *https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consultation/Opinions/2016/16-10-20_PIMS_opinion_EN.pdf*

6 *https://ec.europa.eu/digital-single-market/en/news/emerging-offer-personal-information-management-services-current-state-service-offers-and*

Es wird verglichen, auf welche Weise Selbstkontrolle und individuelle Nutzungsübersicht ermöglicht werden und inwieweit der Selbstdatenschutz der Nutzer motiviert wird, beispielsweise bei der Wahrnehmung von Auskunftsrechten.

Im Folgenden werden dementsprechend zunächst bestehende internationale und nationale Ansätze dargestellt (2.). Anschließend (3.) werden sie auf der strukturellen Ebene im Hinblick auf ihre Reichweite und Diversität sowie auf jeweilige Finanzierungsmodelle und Potenziale zur Vertrauensbildung (b. und c.) und auf der technischen Ebene im Hinblick auf Datenstandorte und Datenschutzniveau sowie auf Nutzerkontrolle und Transparenz der Ansätze (d. und e.) bewertet. Die Bewertung von technischen Lösungsansätzen wird mit einer zusammenfassenden Betrachtung (4.) abgeschlossen. Der Abschnitt „Allgemeine Herausforderungen“ (5.) bietet eine stichwortartige Auflistung von technischen Herausforderungen, die mit der Entwicklung, Umsetzung und einer breiten Implementierung von automatisierten Einwilligungsverfahren stehen.

2. Darstellung der im Projekt betrachteten Ansätze

Im Folgenden werden diejenigen Lösungsansätze im Bereich der „Personal Information Management Services“ (PIMS) dargestellt, die von der Stiftung Datenschutz während der Projektlaufzeit betrachtet und bewertet wurden. Die Auswahl der Unternehmen und Projekte ist rein exemplarisch und spiegelt den Kenntnisstand der Verfasser zum Zeitpunkt der Erhebung wider. Ein Anspruch auf Vollständigkeit ist damit nicht verbunden, ebenso keine generelle Wertung. Der hochdynamische Markt kann sich bereits während der Projektlaufzeit verändert haben. Zudem wurden weitere Initiativen erst nach Abschluss der Arbeiten an der Studie bekannt und konnten daher nicht berücksichtigt werden. Teilweise bestand zu Protagonisten der hier betrachteten Ansätze Kontakt, teilweise konnte nur auf Erkenntnisse aus allgemein zugänglichen Quellen und aus anderweitigen eigenen Recherchen zurückgegriffen werden.

P3P

Das World Wide Web Consortium (W3C) hat am 16.04.2002 die „Platform for Privacy Preferences“ (P3P) als Empfehlung verabschiedet.[7] Außerdem hat das Unabhängige Landeszentrum für Datenschutz aus Schleswig-Holstein den P3P-Standard in einem Projekt unterstützt, das vom Ministerium für Wirtschaft, Arbeit und Verkehr des Landes Schleswig-Holstein gefördert wurde.[8]

P3P ist ein kostenloses Protokoll und ermöglicht die maschinenlesbare Beschreibung von Datenschutzerklärungen. Dazu ist erforderlich, dass sowohl Nutzer als auch Webseiten-Betreiber dieses Protokoll implementieren.
Der Nutzer muss einen sogenannten P3P-Agenten oder P3P-fähigen Browser installieren und im Vorfeld eine standardisierte Liste von Multiple-Choice-Fragen zum gewünschten Umgang mit seinen personenbezogenen Daten beantworten. Diese Antworten werden in ein maschinenlesbares Format (XML) umgewandelt, sodass ein automatisierter Vergleich dahingehend erfolgen kann, ob die Datenschutzerklärung einer Webseite mit den Voreinstellungen des Nutzers zum Datenschutz übereinstimmt. So erscheint bei Abweichungen ein Warnhinweis (z. B. bei der Akzeptanz von Cookies).

7 http://www.w3.org/2002/04/p3p-pressrelease
8 https://www.datenschutzzentrum.de/projekte/p3p/p3p_anbieter.htm

Insgesamt hängt diese Funktionsweise allerdings ebenso davon ab, dass der Webseiten-Betreiber die von ihm erstellte Datenschutzerklärung in der Struktur des P3P-Standards erstellt und auf seinem Webserver ablegt („welche personenbezogenen Daten der Nutzer werden zu welchen Zwecken und zu welchem Zeitpunkt erhoben und verarbeitet und/oder gegebenenfalls an Dritte übermittelt"). Dazu muss er zum einen Software-Tools einsetzen und zum anderen die Datenschutzerklärung auf ihre technische Übereinstimmung mit dem P3P-Standard überprüfen. Zu Letzterem hat das W3C ein Werkzeug entwickelt (P3P-Validator, https://www.w3.org/P3P/validator.html). Das Unabhängige Landeszentrum für Datenschutz Schleswig-Holstein hat den Webseiten-Betreibern außerdem empfohlen, eine Referenzdatei im Verzeichnis „/w3c" mit dem Namen „p3p.xml" zu erstellen, um dem P3P-Agenten des Nutzers das Auffinden der P3P-Datenschutzerklärung zu ermöglichen.[9] Die Erstellung der Referenzdatei könnten dabei ebenfalls Software-Tools oder spezialisierte Firmen übernehmen.

Für den Webseiten-Betreiber beinhaltet die Verwendung von P3P insgesamt keine Vereinfachung seiner Geschäftsprozesse, zumal P3P auch keine automatisierte Überprüfung der Datenschutzerklärungen hinsichtlich ihrer Vereinbarung mit den geltenden Datenschutzvorschriften zur Verfügung stellt. Bei der Beauftragung externer Dienstleister zur Implementierung von P3P kommen zudem zusätzliche Kosten auf ihn zu. Im Sinne des Nutzers ist das Ziel einer transparenten Datenverarbeitung und verbesserten informationellen Selbstbestimmung nur dann erfüllt, wenn die Datenschutzerklärung vollständige und wahrheitsgemäße Angaben enthält. Hier muss er sich also auf den Webseiten-Betreiber vollständig verlassen. Für den Nutzer wird die Anwendbarkeit zudem dadurch erschwert, dass in der Vergangenheit die Browser-Software, die in der Lage ist, P3P-Datenschutzerklärungen zu lesen und zu verarbeiten, nur vom Microsoft Internet Explorer (ab Version 6.0) und wenigen anderen Browsern, wie etwa Netscape, unterstützt wurde. Der Bayerische Landesbeauftragte für den Datenschutz hat in seinem 20. Tätigkeitsbericht dazu näher ausgeführt, dass der Nutzer bei Verwendung des Microsoft Internet Explorer 6 unter dem Menü „Anzeigen Datenschutzbericht" nach dem Anzeigen von „allen Websites", der Selektion einer Seite und durch Klicken auf „Zusammenfassung" schließlich zu einer lesbaren Darstellung der P3P-Datenschutzerklärung gelangt – interpretiert durch den Microsoft Internet Explorer. Nutzer könnten ein solches Verfahren daher ebenso als umständlich betrachten. Hinzu kommt, dass Microsoft mittlerweile die Unterstützung für P3P in Windows 10 entfernt hat und empfohlen hat, das Bereitstellen von P3P-Datenschutzrichtlinien auf den Webseiten zu vermeiden (https://msdn.microsoft.com/de-de/library/mt146424(v=vs.85).aspx).

Aus rechtlicher Sicht hat P3P gemäß einer Stellungnahme des Unabhängigen Landeszentrums für Datenschutz Schleswig-Holstein den Nachteil.[10]
Eine Einwilligung durch die Aktivierung und Nutzung von P3P, z. B. in die Akzeptanz von Cookies, sei deshalb bereits nicht möglich, weil im Zeitpunkt der Erklärungshandlung (Aktivierung von P3P) noch nicht konkretisiert ist, worin überhaupt eingewilligt wird.

Somit kann der Anforderung an die Transparenz nicht ausreichend Rechnung getragen werden. Außerdem kommt das Unabhängige Landeszentrum für Datenschutz Schleswig-Holstein zu dem Ergebnis, dass es nicht möglich ist, die Einwilligungserklärung einem bestimmten Nutzer zuzuweisen. In der Praxis könne daher der Web-Anbieter eine bestimmte Einwilligung eines bestimmten Betroffenen mithilfe von P3P nicht nachweisen.

9 https://www.datenschutzzentrum.de/projekte/p3p/p3p_anbieter.htm

10 Stellungnahme zu juristischen Aspekten des P3P-Einsatzes in mobilen Endgeräten, https://www.datenschutzzentrum.de/projekte/p3p/Gutachten_Mobilgeraete.pdf

digi.me

Das 2009 gegründete Unternehmen hat sich zum Ziel gesetzt, den Nutzern die Möglichkeit zu geben, ihre Daten von verschiedenen Anbietern zusammenzufügen und lokal zu verwalten. So gegenwärtig etwa die Zentralisierung der Daten aus Plattformen wie Instagram, Facebook, Twitter, Flickr, LinkedIn, Google+, Pinterest und Viadeo.[11] digi.me stellt dabei zwei verschiedene Modelle zur Nutzung bereit: einen kostenlosen Service für maximal vier verschiedene soziale Netzwerke oder aber die kostenpflichtige Version mit bis zu 20 sozialen Netzwerken plus weitere Vorteile, wie etwa statistische Zusammenfassungen. Je nach Anzahl der gewünschten Accounts zur Einbindung, kostet die erweiterte Version 6-24 EUR pro Jahr.[12]

Die Datensammlung und Archivierung finden über ein auf dem Nutzerrechner zu installierendes Programm statt. digi.me unterstützt Betriebssysteme ab Windows 7 und Macs ab OS 10.7 und für mobile Geräte Android und iOS. Das Programm legt die Daten in einer verschlüsselten Datenbank auf dem Nutzerrechner/-gerät ab. Zum gegenwärtigen Zeitpunkt lässt sich diese Datenbank noch nicht verschieben, daher sind etwaig gesicherte Daten noch nicht sehr flexibel auf andere Geräte übertragbar. Zugriff auf die Daten des Nutzers in den jeweiligen sozialen Plattformen erhält das Programm über die Eingabe von Account-Informationen. Das Programm lädt dann über die jeweiligen API's der Plattformen die relevanten Daten auf den Nutzerrechner bzw. das Nutzergerät herunter. Veränderungen bei den Einstellungen der sozialen Netzwerke (etwa den Datenschutz betreffend) oder aber bei den gespeicherten Daten auf den Plattformen finden nicht statt. Es handelt sich um einen reinen Download der Daten. Eine Übertragung der Daten an digi.me existiert laut Unternehmen nicht und ist auch nicht geplant.

LETsmart (Legalisation, Exchange, Transparency)

An der Universität Leipzig arbeiten Wirtschaftsinformatiker unter der Leitung von Prof. Dr. Rainer Alt an IT-Werkzeugen, welche die Um- und Durchsetzung von Datenschutzvorschriften automatisieren. Dort entstand in interdisziplinärer Zusammenarbeit mit dem Rechtswissenschaftler Gunnar Hempel die Idee für LETsmart – einen Ansatz für automatische rechtskonforme Einwilligungen und Datennutzungskontrolle. Die Entwicklung befindet sich gegenwärtig in der Testphase. Das Produkt soll erforderliche Transparenz für die legale Verarbeitung betroffener Daten und schnelle und rechtssichere Autorisierungen schaffen. Ziel ist die maschinelle Erkennung von Anfragen zum Zugriff auf personenbezogene Daten und eine automatisierte rechtswirksame Autorisierung im Sinne des Nutzers.

Der Ansatz sieht eine maschinelle Erkennung von Anfragen zum Zugriff auf personenbezogene Daten vor, eine automatisierte rechtswirksame Einwilligung und Mechanismen zum Einwilligungsmanagement. LETsmart filtert heraus, welche Daten vom Datennehmer angefordert werden, wie beispielsweise eine Anforderung von Standort- und Nutzerdaten für einen App-Dienst. Für den Nutzer wird sichtbar, von welchem Umfang und welcher Art die beabsichtigte Datenerhebung sein soll. Er kann erkennen, welcher Datenfluss zu welchem Verwendungszweck beabsichtigt ist (z. B. welche Daten will der App-Dienst übermittelt haben, wer soll die Daten verarbeiten und wie werden sie insgesamt verwendet). Der Nutzer erhält alle notwendigen Informationen, die für eine rechtswirksame Autorisierung des Datenumgangs erforderlich sind, um eine gesetzlich vorgeschriebene Einwilligung zu erteilen. LETsmart integriert dazu die betroffenen Daten in einen Container. Ein eingebettetes Datenmanagementsystem (DMS) sichert die autorisierte Verwendung der Daten auch nach der Übermittlung ab. LETsmart kann damit ausdrücklich auch zur Datenpflege eingesetzt werden.

11 https://digi.me/supported-networks

12 https://digi.me/pricing

Es sichert ab, dass übermittelte Daten nach der Verwendung gemäß der Autorisierung beispielsweise zu anonymisieren oder zu löschen sind oder dass der Nutzer seine Autorisierung gemäß den Vorschriften der DSGVO organisieren und aktualisieren kann. Durch Mechanismen zum Datenmanagement und zur Datenpflege im Anschluss an die Übertragung sollen Datennehmer weitgehend von der rechtlichen und haftungstechnischen Verantwortung für Datenpannen und sonstige nicht autorisierte Vorgänge befreit werden.

Consent Management for Federated Data Sources (CoMaFeDS)

An der Technischen Universität Berlin wurde ein Konzept für eine sogenannte „Consent Management Plattform“ (kurz: CoMaFeDS) entwickelt. Hiermit soll die Gewinnung von Datensätzen ermöglicht werden, die aus unterschiedlichen, autonomen und verteilten Quellen stammen. Allerdings sollen die betroffenen Personen gleichermaßen die informationelle Selbstbestimmung über ihre Datensätze ausüben können, indem sie die Zustimmung bezüglich unterschiedlicher Datenverarbeitungsprozesse und Empfänger im Voraus erteilen. Dies entspricht dem bereits bestehenden Konzept der sogenannten „Sticky Policies“: Persönliche Daten, die die betroffene Person zuvor im Hinblick auf Zwecke und Konditionen spezifiziert hat, werden von dem System des Datenhalters erfasst und verschlüsselt und diese Vorgaben werden in eine standardisierte Datenschutzerklärung umgewandelt.

Die Plattform CoMaFeDS soll jedoch insgesamt die identifizierten Nachteile der bisherigen Herangehensweisen angehen. So ist – anders als bei Sticky Policies – keine vertrauenswürdige Instanz erforderlich, die den Schlüssel für die Entschlüsselung der Datensätze verwahrt und an die interessierte Institutionen ihre Anfrage zur Datennutzung stellen. Für CoMaFeDS wird zurzeit ein Prototyp unter Berücksichtigung der im Folgenden aufgeführten Voraussetzungen realisiert:
Potenzielle Empfänger der Daten sowie mögliche Verarbeitungszwecke sollen kategorisiert werden, indem Datenschutzerklärungen in definierten Formaten, die eine kurz gefasste Spezifikation von Kategorien und Empfängern beinhalten, dargestellt werden. Das gewählte Format muss außerdem willkürliche Detailstufen in den betrachteten Datenschutzerklärungen erlauben, sodass Definitionen von zahlreichen Unterkategorien möglich sind. Dies würde etwa Zustimmungen erlauben wie „Meine Daten dürfen von unterschiedlichen Forschungsinstitutionen für den Zweck demografischer Untersuchungen verarbeitet werden, aber nicht von Regierungsbehörden für Steuerschätzungen“.

Weiterhin ist CoMaFeDS von dem Wissen abhängig, wo spezifische Datensätze zu finden sind. Um dieses Problem zu lösen, soll ein Datenerheber oder Datenhalter, der an der Partizipation von Datamining interessiert ist, eine Beschreibung seiner Datenbank erstellen, die Details über die bereitgehaltenen Datensätze und die interne Struktur der Datenbank präzisiert.
Voraussetzung ist dementsprechend, dass ein Datenhalter überhaupt bereit ist, seine Datensätze für den Zweck von Big Data-Analysen durch Dritte (externe Organisationen) zu öffnen. In diesem Falle kann er sich zu der CoMaFeDS-Plattform verbinden. Während des Verbindungsprozesses können sowohl die Beschreibung der Datensätze und der Spezifikationen der internen Strukturen seiner Datenbank als auch die Datenschutzerklärungen zu der Plattform übertragen werden.

In der Systemarchitektur wird CoMaFeDS als eine Verbindung zwischen den Datamining -Applikationen und den Datenquellen installiert, die letztendlich analysiert werden sollen. Zu diesem Zwecke hat CoMaFeDS standardisierte Schnittstellen in beiden Richtungen entwickelt.

Da das System flexibel sein soll, kann es sowohl in einer Cloud gehostet als auch als „stand-alone“ Softwarekomponente eingesetzt werden, die ein bereits existierendes Datamining-Werkzeug erweitert.

Für jede mögliche Datenquelle soll ein maschinenlesbares Dokument vorliegen, das auf die gespeicherten Daten verweist. Außerdem sollen für jeden Datensatz detaillierte Präferenzen verfügbar sein, und zwar bezogen auf die vielfältigen Verarbeitungsprozesse sowie Empfänger. Basierend auf diesen Dokumentationen führt CoMaFeDS einige interne Konvertierungen durch und die datenbank- und datensatzbezogenen Informationen und Spezifikationen werden genutzt, um einen ontologisch-basierten „Wissensgraphen“ zu entwickeln. Dieser Graph verschlüsselt das Wissen über den Speicherort und die Zugriffsmöglichkeiten zu den spezifischen Datensätzen („wo diese zu finden sind, um welche Art von Daten es sich handelt und wie diese zu erlangen sind“).

Umgekehrt werden die Datenschutzerklärungen genutzt, um ein internes, sogenanntes hippokratisches Integrationsmodell zu entwickeln. Wie oben bereits dargestellt, möchte CoMaFeDS bisherige Herangehensweisen in sein Konzept integrieren, aber die Nachteile verhindern. Gemäß der Untersuchung der Entwickler von CoMaFeDS waren rein hippokratische Datenbanken bislang nur innerhalb von akademischen Darstellungen zu finden, wurden jedoch nicht praxisbezogen eingesetzt. Innerhalb von CoMaFeDS wird dieses Modell nun realisiert, und zwar basierend auf speziell dafür vorgesehenen Tabellen oder anderen Arten von Speicherstrukturen, die in der Lage sind, diese Informationen zu erfassen (welche Attribute der spezifischen Datensätze für welchen Empfänger und für welchen Verarbeitungszweck zugänglich sind).

Entsprechend den „Hippokratischen Standalone Datenbanken“ führt dieses Design zu einem System, das jedwede Datenzugriffe verhindert, die nicht mit der richtigen Kombination von Empfänger und Zweck zusammenpassen.

Als eine Verbesserung und Erweiterung von CoMaFeDS ist zudem ein Mechanismus denkbar, der den betroffenen Personen eine dynamische Zustimmung erlaubt. Sofern ein möglicher Datenempfänger einen passenden Datensatz innerhalb des generierten Graphen findet, aber keine Zustimmung für die beabsichtigten Verarbeitungsprozesse existiert, soll die Plattform ermöglichen, eine solche neue Erlaubnis zu erfragen. In diesem Fall kann die betroffene Person ihre Zustimmung ändern.

Ansätze der Deutschen Telekom AG

Die Deutsche Telekom verfolgt ein ganzheitliches Datenschutzkonzept. Durch eine Reihe von Teilprojekten (die sich gegenwärtig noch in der Entwicklungsphase befinden) soll dem Nutzer auf lange Sicht eine bessere Information zu seinen datenschutzrechtlichen Möglichkeiten gegeben und durch Projekte wie die Privacy-Data-Bots ein datenschutzfreundlicher Umgang mit persönlichen Daten ermöglicht werden.

Die Projekte befinden sich noch in einem relativ frühen Entwicklungsstadium. Grundsätzlich lassen sich die Projekte in einer Stufenform beschreiben, bei der jede Stufe eine Verbesserung von der reinen Information über Datenschutzbestimmungen (Projekt zu Datenschutzhinweisen und Icons) und über eigene Datenschutz-Apps (Privacy App bzw. Integration in die Magenta App) hin zur umfangreichen Datenschutzunterstützung der Nutzer im Alltag (Data Dashboards + Data Cockpits) gewährleisten soll.

Darüber hinaus soll mit dem Projekt zu Privacy-Data-Bots[13] am Ende der Entwicklung ein vollumfänglicher Dienst entstehen, welcher die Nutzer bei den Einwilligungen bzw. Datenschutzeinstellungen unterstützen soll.

Bei Data Cockpits bzw. Data Dashboards soll über verschiedene Widgets dem Nutzer gezielt die Möglichkeit gegeben werden, in die Datenweitergabe bei einzelnen (Telekom-) Angeboten und Projekten einzuwilligen. Dies könnte etwa die Weitergabe von GPS-Daten oder aber auch die Nutzung von Funkzellendaten und deren Auswertung betreffen. Daran anschließend plant die Telekom, für den Nutzer beispielsweise eine übersichtliche Nutzungsverlaufskarte zu erstellen oder aber auch gezielt auf Kundeninteressen und Anforderungen frühzeitig einzugehen. Das erklärte Ziel dabei ist, die Nutzer optimal zu beraten und maßgeschneiderte Lösungen anbieten zu können.

MesInfos[14]

„MesInfos“ ist ein Projekt des französischen think tanks Fondation Internet Nouvelle Génération (Fing). Fing erforscht und entwickelt neue und praxisnahe Ideen auf dem Gebiet der digitalen Technologien. Das selbst erklärte Ziel der Stiftung lautet, den digitalen Fortschritt und dessen Folgen an der Schnittstelle zwischen wirtschaftlichen Interessen und der menschlichen Innovationsfähigkeit zu unterstützen. Das Ziel des Projekts MesInfos ist, dass die teilnehmenden Unternehmen die gesammelten Kundendaten mit den Kunden teilen, sodass die Kunden die Kontrolle über ihre Daten behalten. Im Jahr 2016 startete Fing zusammen mit mehreren größeren Unternehmen (wie etwa Banken, Versicherungs-, Telekommunikations- und Energieunternehmen) ein Projekt unter dem Namen „MesInfosPilot“, im Rahmen dessen die von Unternehmen erhobenen personenbezogenen Daten einer bestimmten Anzahl von Kunden an diese wiedergegeben werden sollen. Zunächst startete das Pilotprojekt mit der Plattform „Cozy Cloud“ eines französischen Start-up-Unternehmens.

Cozy Cloud bietet eine Cloud-Plattform sowie einen personalisierten Server mit einer Datenbank an. (Zukünftig sollen zu diesem Zweck weitere Plattformen mit unterschiedlichen Diensten entwickelt werden.) Im Rahmen des Pilotprojekts erhalten die Testpersonen zunächst ihren eigenen gesicherten Bereich, in dem sie die von ihnen erhobenen Daten einsehen und verarbeiten können. Das Hosting kann von einem Provider oder vom Nutzer selbst durchgeführt werden. Der persönliche Bereich ist über einen persönlichen Domainnamen oder eine SubDomain (Nachname-Vorname. Cozycloud.cc) erreichbar. Die Nutzer können dort persönliche Daten speichern und Applikationen einbinden. So wird es möglich, Daten aus Rechnungen oder allgemeinen Dokumenten (wie Schriftverkehr mit Anbietern) zu integrieren. Weiterhin soll es die Möglichkeit geben, Fotos, Musik, Kontakte, Kalenderdaten und Daten aus Drittapplikationen einzubinden und so einen umfassenden Überblick über die Daten zu gewährleisten.

MyData

MyData ist ein Gemeinschaftsprojekt der Aalto University, der Open Knowledge Finnland (OKFI) und der Fing. MyData sieht sich als Verbundgemeinschaft verschiedener Initiativen und Unternehmen mit dem Ziel, Big Data und datenschutzrechtliche Regelungen bzw. Grundrechte in Einklang zu bringen. Teil dieser Initiative sind regelmäßige Treffen mit Vorträgen. Das weitere Ziel ist das Zusammenbringen internationaler Unternehmen und Entscheidungsträger, um das Data-Management datenschutzgerecht zu gestalten.

13 *Am 27.01.2017 startete Telekom einen Wettbewerb zu Konzepten der technischen Umsetzung von Privacy-Bots: https://www.telekom.com/de/medien/medieninformationen/detail/faktenseite-und-teilnahmebedingungen-481808*

14 *http://mesinfos.fing.org/english*

Beworben wird das von MyData in einem Whitepaper[15] beschriebene Modell einer einheitlichen Datenspeicherung und -weitergabe. Die Kernpunkte sind dabei:

1. der Fokus auf die Kontrolle des Nutzers über seine Daten.

2. die Standardisierung der Daten- und Zwischenverbindungen (API's) der jeweiligen teilnehmenden Unternehmen. Dies soll die Nutzbarkeit der Daten für verschiedene Unternehmen ermöglichen und erweitern.

3. die Offenheit der Daten. Die Daten sollen (sofern der Nutzer dem zustimmt) für Unternehmen einfacher erreichbar sein als bisher. Dies soll den Nutzern auch die Möglichkeit geben, zwischen Anbietern zu wechseln, da die Daten einfach „mitgenommen“ werden können.

Beschrieben wird dabei eine dezentralisierte Schnittstelle zwischen den teilnehmenden Unternehmen, auf welche der Nutzer einen direkten Einfluss hat. Somit soll es zum einen für Unternehmen einfacher werden, auf bereits vorhandene Daten zuzugreifen etwa wenn diese bei einem anderen Unternehmen verortet sind. Zum anderen soll dem Nutzer ermöglicht werden, auf alle bei den teilnehmenden Unternehmen gespeicherten Daten zuzugreifen und diese ggf. zu ändern oder zu löschen. So wird dem Nutzer ein höheres Maß an Kontrolle gegeben. Den Unternehmen wird zugleich ein vereinfachter Weg zugeteilt, auf Daten zuzugreifen und diese zu nutzen. Der zentrale Punkt liegt dabei bei dem MyData-Account des Nutzers, über den dieser den Zugriff auf alle Daten bei den teilnehmenden Unternehmen hat (bzw. haben soll). Im Account-Bereich sollen dann die Einstellungen für die gespeicherten Daten transparent vorgenommen werden können. Weiterhin soll dort auch die Möglichkeit bestehen, den Einblick in die gespeicherten Daten zu bekommen. Somit wird Transparenz geschaffen; die Einwilligung zur Datennutzung wird zentral verwaltet. Die zentralisierte Verwaltung der Daten ermöglicht es dem Nutzer, leichter zu regeln, welche Daten er weitergeben möchte. Auch soll es weit einfacher werden, Kenntnis über die von ihm abgerufenen Daten zu erlangen (etwa wenn im Rahmen einer rechtlich geregelten staatlichen Abfrage keine Einwilligung notwendig ist).

MyPermissions

MyPermissions startete als ein auf den englischsprachigen Raum ausgerichtetes Unternehmen, hat sich aber im Verlauf der Zeit besonders auch dem deutschsprachigen Raum etwa durch eine durchweg deutschsprachige Webseite zugewendet. Bei dem Projekt handelt es sich um eine Linksammlung auf „mypermissions.org“, bei der ein direkter Link zu den Privatsphäre-Einstellungen verschiedener Internetdienste angeboten wird. Ziel dieser Methode ist, die unübersichtlichen Einstellungen von Anbietern wie Facebook für den Nutzer auf einfache Weise zusammenzuführen und einen schnellen Zugriff darauf zu ermöglichen.[16] Einige Artikel beschreiben die Vorteile dieser für den Nutzer einfachen und zeitsparenden Methode und bewerben die Webseite[17]. In der letzten Zeit wird das Hauptaugenmerk verstärkt auf mypermissions.com und mypermissions.de gelegt. Es wird besonders betont, dass bei dieser Methode keine Nutzerdaten gesammelt werden.

Ist das Plugin einmal installiert, gibt es die Möglichkeit, die bereits installierten Apps bzw. Dienste zu überprüfen und gegebenenfalls zu deinstallieren bzw. sie zu einer Vertrauensliste hinzuzufügen. Weiterhin besteht die Möglichkeit, einen Link zu öffnen, welcher auf die Webseite des jeweiligen Dienstanbieters mit den Privatsphäre-Einstellungen führt. Grundsätzlich handelt es sich bei der Browser-Version

15 http://www.lvm.fi/-/mydata-a-nordic-model-for-human-centered-personal-data-management-and-processing-860616

16 https://webapps.stackexchange.com/questions/31595/how-safe-is-my-permissions

17 https://nakedsecurity.sophos.com/2012/01/05/mypermissions-clean-up-social-media-permissions/

allerdings nicht wirklich um ein „Plugin“ (also einen Programmbestandteil des Browsers), es wird vielmehr die Webseite von MyPermissions aufgerufen.

Durch das Plugin wird einzig ein Zugriff auf Cookies möglich, wodurch MyPermissions in die Lage versetzt wird, alle verbundenen Dienste aufzurufen und zu „scannen“. Besonderer Wert wird außerdem darauf gelegt, dass MyPermissions selbst keinen Zugriff auf die Daten bekommt, der Nutzer sich also selbst auf den entsprechenden Webseiten anmeldet. Aber gerade aus der Funktionsweise des Plugins und der App muss jedoch geschlossen werden, dass die Zugangsdaten zumindest bei der Bewertung des Dienstes direkt oder zumindest indirekt MyPermissions (mit einem hohen Aufwand) zugänglich sein könnten.

Im Zusammenhang mit dem Browser-Plugin ist weiterhin zu erwähnen, dass die auf der Homepage des Projektes angebotene Version sich nicht in Mozilla Firefox installieren lässt. Das Problem dabei ist die Einschränkung durch Mozilla, nur von Mozilla signierte Plugins installierbar zu machen. Dies kann zwar umgangen werden, ist für den Normalnutzer jedoch nicht zu bewerkstelligen, bzw. der Prozess der Freigabe erfordert ein hohes Maß an Vertrauen in die App. Auf der Seite von Mozilla wird eine vorläufig signierte Version zwar angeboten, was aber auch hier zu einer Hemmschwelle bei einem sensiblen Nutzer führen könnte.

Auffällig ist außerdem, dass am Ende der Webseite, welche das Plugin aufruft, eine Art Facebook Like-Button versteckt zu sein scheint (siehe Screenshot unten). Dieser baut üblicherweise (auch ohne Benutzerzugriff) eine Verbindung zu Facebook auf, was gerade bei der Zielsetzung des Produkts, keine Nutzerdaten zu erheben, kontraproduktiv zu sein scheint. Außerdem wird von der Webseite Google Analytics eingesetzt, was auch hier durchaus als problematisch für die anvisierte Zielgruppe zu betrachten ist.

Auch die Datenschutzbestimmung der Webseite ist durchaus als nicht unproblematisch zu betrachten. So wird unter anderem die Möglichkeit offengehalten, die Daten für Facebook-Aktionen (Werbung etc.) zu nutzen; aber auch eine freie Weiternutzung der Daten durch potenzielle Käufer des Unternehmens ist nicht ausgeschlossen. Durchaus problematisch ist ebenso, dass das Löschen eines Accounts nur über das Kontaktformular möglich ist, womit auch hier eine gewisse Hemmschwelle aufgebaut wird. Sollte es also wirklich zutreffend sein, dass My-Permissions keine sensiblen Daten speichert, so ist dieses Vorgehen nicht nachvollziehbar; ein einfacher Klick (mit einer Sicherheitsnachfrage) hätte an dieser Stelle auch ausreichen können.

Zu einer Bewertung des Projekts durch Dritte siehe:
https://nakedsecurity.sophos.com/2012/01/05/mypermissions-clean-up-social-media-permissions/

Access my Info

Das kanadische Unternehmen Citizen Lab, Toronto, hat das Online-Tool „Access My Info“ entwickelt und im Jahre 2014 auf den Markt gebracht. Vor Kurzem wurde es aktualisiert. Dieses Tool soll kanadischen Bürgern transparent aufzeigen, welche Informationen über sie zugänglich sind, ob sie geteilt werden und wenn ja, mit wem.

Ermöglicht wird dies durch die automatische Erstellung einer detaillierten Fragenliste (im pdf-Format), die vom Betroffenen an seinen Service-Provider mit der Aufforderung zur Beantwortung übersendet werden soll. Diese Fragenliste wird anhand von Angaben des Betroffenen erzeugt, die er auf einem Online-Portal unter Angabe des auskunftspflichtigen Unternehmens mitteilen soll.

Das kanadische Recht verpflichtet die Unternehmen unter Androhung von Bußgeldern zur Beantwortung dieser Fragen. Die neue Version von „Access My Info" ermöglicht nicht nur die Anfrage bei Telekommunikationsunternehmen (wie noch im Jahre 2014), sondern ebenso bei Fitness-Trackers, Dating-Apps und sogar bei der Kanadischen Regierung. Die Erweiterung auf Transport-Apps wie Uber oder Zipcar ist geplant.

Die Ausdehnung auf unterschiedliche Branchen stellt eine wesentliche Anforderung dar, um zu verhindern, dass Nutzer ohne ihr Wissen kategorisiert und sensible Daten über sie gesammelt werden, die letztendlich Einfluss auf die Ausübung ihres Berufs, Ablehnung von Versicherungen oder sogar auf die Einreise in andere Länder haben könnten.

Intention von „Access My Info": Das Tool „Access My Info" kann betroffene Nutzer im Sinne des Selbstdatenschutzes motivieren, ihre Daten zu kontrollieren. Es geht um die automatisierte Vereinfachung eines komplexen Prozesses, damit Nutzer allgemeinverständlicher erfahren können, wer welche persönlichen Daten über sie speichert. Dies ist insbesondere in der heutigen Zeit wichtig, in welcher auf Smartphones Apps, etwa Fitness-Apps, installiert werden und hierfür schwer lesbare Nutzungsbedingungen akzeptiert werden müssen. Es ist für die Nutzer leichter, den Nutzungsbedingungen insgesamt zuzustimmen, als diese auf dem Smartphone durchzulesen und sich des Weiteren darüber Gedanken zu machen, ob z. B. Informationen über den Aufenthaltsort oder die Nutzung von sozialen Netzwerken erhoben werden und mit wem die Informationen unter welchen Bedingungen geteilt werden.

Citizenme

Citizenme konzentriert sich vorwiegend auf die Sammlung und Verwertung von direkten und indirekten Nutzerdaten. Personenbezogene Daten sollen durch den Nutzer selbst geldwert verwertet werden. Das Unternehmen behält sich einen Teil dieses Verkaufserlöses als Vermittlerprovision bzw. als Plattformanbieter zurück. Die vom Nutzer in die von Citizenme angebotene App eingegebenen Daten sollen durch Verarbeitung und Aufwertung (unter anderem durch Nutzung künstlicher Intelligenz) den Unternehmen anonym zur Verfügung gestellt werden. Der Nutzer (und anteilig Citizenme) erhält je nach Umfang und Qualität dieser Daten eine finanzielle Gegenleistung, welche er ggf. auch über Citizenme an gemeinnützige Projekte spenden kann. Es wird dabei betont, dass der Nutzer die Verwertungsrechte an seinen Daten zurückerhält. Dies wird als Transparenzzugewinn für den Nutzer dargestellt.

Es existieren Apps für iOS und Android. In die App können verschiedene Soziale Medien-Accounts, wie etwa die von Twitter oder Facebook, eingebunden werden. Dies dient unter anderem der Bestimmung der „Echtheit" der Person und dem Verhindern von unrechtmäßigen Accounts. So wird sichergestellt, dass es sich um keine Fake-Accounts handelt. Dies ist entscheidend, um den Unternehmen die „echten" Daten zur Verfügung zu stellen. Außerdem können die Accounts auch zum Scannen durch Citizenme freigegeben werden und dann in das Charakterprofil einfließen. Laut

Webseite werden hierbei keine Daten ohne Zustimmung des Nutzers ausgelesen. Die Daten werden laut Citizenme auf dem Smartphone gespeichert und nicht an deren Server weitergeleitet. Die Daten werden außerdem nur dann übermittelt, wenn eine finanzielle Verwertung der Daten vom Nutzer eingeleitet wird. Die Daten werden neben dem direkten Abruf/Download von Social Media-Seiten hauptsächlich über ein umfrageähnliches System erhoben. Dem Nutzer werden Fragen gestellt, auf die er per Multiple-Choice-Verfahren oder per direkter Texteingabe antworten kann. Es existiert ein Farbsystem, das signalisiert, welche Daten wirtschaftlich verwertet werden und welche zur Verbesserung der Nutzeranalyse durch den Hersteller dienen. Die finanzielle Gegenleistung wird an den Nutzer über PayPal überwiesen. Personenbezüge würden wegen der Anonymisierung wegfallen und es würde sich beim Verkaufsgut um rein statistische Daten handeln. Diese können durchaus umfangreichen Wert für Unternehmen haben. Das Geschäftsmodell ist somit nachvollziehbar. Jedoch muss betont werden, dass anonyme Daten weit weniger wert sind als an Personen angeknüpfte Daten. Citizenme generiert den Mehrwert über die Auswertung der Daten durch künstliche Intelligenz. Grundsätzlich lässt sich dabei ein detailliertes Personenbild erstellen, welches umfangreicher ist als bei reinen Statistikdaten.

Bewertung des Projekts durch Dritte:
https://www.thesun.co.uk/living/1256885/this-app-reveals-your-social-media-personality-and-the-results-might-shock-you/;

Datacoup

Das 2012 gegründete Unternehmen Datacoup bietet die Möglichkeit, eigene anonymisierte Daten an Unternehmen zu verkaufen. Weiterhin wird auch die Möglichkeit gegeben, die eigenen Daten zusammengefasst auszuwerten und anzuzeigen, wobei dies eher als Nebenfunktionalität zu verstehen ist. Eine Verknüpfung ist möglich mit Kreditkartenanbietern, Facebook, Twitter, LinkedIn, Foursquare, Google+, YouTube, Tumblr, Meetup und Instagram.

Im Moment werden die Daten noch von Datacoup selbst gekauft, um ein Portfolio für spätere „echte“ Datenkäufer aufzubauen. Auszahlungen werden über den Zahlungsdienstleister Stripe abgewickelt und erfolgen per Kreditkarten-Gutschrift (Visa oder Mastercard). Eine Auszahlung ist gegenwärtig auf die Vereinigten Staaten beschränkt.

Datacoup positioniert sich zwar als Bulkverkäufer für statistische Daten, jedoch ist die praktische Datensatzgröße wegen Nutzermangel nicht sehr umfangreich. Für die Unternehmen ist es jedoch nicht rentabel, Kleinstdatensätze abzunehmen, somit fällt es Datacoup schwer, die Anfangsphase ohne eine Vielzahl neuer Nutzer zu verlassen. Neue Nutzer werden aber gerade bei den von Datacoup gezahlten geringen Preisen nur langsam zu finden sein. Aus dieser unvorteilhaften Verbindung folgt ein sehr träger Startprozess und dies erklärt, warum auch nach vier Jahren keine echte Bewegung für das Unternehmen zu verzeichnen ist.

Datacoup betreibt eine Webplattform, auf der ein Account erstellt werden muss. In diesen Account können alle Social Media-Accounts bzw. der Kreditkarten-Account der Nutzer eingebunden werden. Es werden Zugangsdaten gespeichert und bei finanziellen Accounts werden Händlername, Transaktionsdatum und Transaktionsmenge abgerufen. Bei den sozialen Accounts werden grundsätzliche

Informationen, Likes, Check-ins, Aktivitäten, die Freundesliste usw. über die API der Anbieter verschlüsselt abgerufen. Daten werden auf den Servern von Datacoup (in den USA) verschlüsselt abgelegt. Die Daten sollen dann je nach Bedarf von Datenkäufern gekauft werden können. Ab einer Summe von 5 USD kann das Guthaben von den Nutzern abgerufen werden.

Bewertung durch Dritte:
https://www.technologyreview.com/s/524621/sell-your-personal-data-for-8-a-month/

personiq (Unternehmen Emvolution)

Gegründet Anfang 2015 ist das selbst erklärte Ziel von Emvolution (dem Unternehmen hinter personiq), dem Nutzer Kontrolle und Transparenz über seine Daten zu geben.[18] Leistungsumfang der Plattform personiq ist dabei, dem Nutzer eine Übersicht über sein Surfverhalten zu präsentieren und ihm somit zu ermöglichen, die Kontrolle über seine Daten selbst zu übernehmen. Erreicht wird dies über eine grafische Darstellung von Statistiken. So gehört dazu, welche Webseiten aufgerufen werden/wurden, wie lang auf diesen verweilt wird (bzw. die Nutzungsdauer des Dienstes) und inwieweit durch diese Plattformen ein Profil über den Nutzer erstellt werden kann. Dabei werden die Daten ausschließlich von Geräten des Nutzers gesammelt, ein Zugriff auf Daten von Google (etwa über Account-Informationen) findet nicht statt. Grundsätzlich obliegt es dabei dem Nutzer selbst, sein Verhalten anzupassen und seine Privatsphäre zu schützen. Die Plattform ermöglicht dabei keine direkte Kontrolle über etwaige Privatsphäre-Einstellungen der jeweiligen Dienstbetreiber. Die Nutzungsdaten werden, wie das Unternehmen ausdrücklich betont, nicht an Dritte weitergegeben und sind somit nur für den Nutzer zugänglich.

Webseite für Unternehmen: https://b2b.emvolution.me/

Den Zugriff auf das Surfverhalten erhält Emvolution durch Plugins für die Browser Firefox und Google Chrome. Dabei werden jegliche aufgerufenen Seiten, Pop-ups, Werbung etc. abgegriffen und zur Auswertung durch Emvolution herangezogen. Im Moment werden noch alle Daten an Emvolution weitergeleitet. Das erklärte Ziel ist aber, die Daten lokal auf dem Nutzergerät anzuzeigen und Emvolution keinen Zugriff darauf zu ermöglichen.[19] Im Artikel von Internetworld[20] wird zwar von einer „Verschleierung" der Bewegung im Internet gesprochen, auf der Webseite von Emvolution ist aber von einer solchen nicht die Rede. Auch die durch Internetworld angesprochene Möglichkeit, durch den Plugin bestimmen zu können, welche Nutzungsdaten durch Plattformen aufgenommen werden dürfen, ist durch Emvolution nicht erwähnt bzw. beworben und wurde auch bei der Betrachtung der Funktionsweise der Plattform an keiner Stelle aufgefunden. Möglicherweise basieren diese Aussagen auf zukünftigen Vorhaben von Emvolution (sodass diese Features demnächst eingeführt werden). Nach dem Rebranding der Plattform zu personiq wurden personalisierte Funktionen (wie die ausgehend vom Surfverhalten des Nutzers relevanten Nachrichten) ergänzt.

Bewertung durch Dritte:
http://www.best-practice-business.de/blog/geschaeftsidee/2016/05/24/emvolution-will-den-digitalen-fussabdruck-sichtbar-machen-und-die-datenhoheit-zurueckgeben/

http://www.internetworld.de/onlinemarketing/start-up/emvolution-eigene-daten-kontrollieren-1114688.html

Meeco

18 https://www.personiq.de/aboutus

19 https://www.personiq.de/help

20 http://www.internetworld.de/onlinemarketing/start-up/emvolution-eigene-daten-kontrollieren-1114688.html

Meeco kann als eigenes soziales Netzwerk betrachtet werden. Dem Nutzer soll die Möglichkeit gegeben werden, für verschiedene Themenschwerpunkte „Tiles“ mit Informationen zu erstellen, welche dann mit anderen Nutzern geteilt werden können. Ein besonderer Wert wird dabei laut Anbieter auf Sicherheit gelegt. Die Daten werden verschlüsselt abgelegt. Die Funktionalitäten von Meeco beinhalten dabei einen Cloud-Speicher, eine Plattform für private Nachrichten (zwischen Meeco Nutzern), einen integrierten Web-Browser und weitere kleine Funktionalitäten, ähnlich wie bei anderen sozialen Netzwerken. Die Wertschöpfung erfolgt bei Meeco durch die Anbindung von Waren- und Dienstleistungsanbietern. So kann der Nutzer den Anbietern seine Daten preisgeben oder – z.T. anonym – Interesse an bestimmten Waren erhalten. Der Anbieter soll dadurch einen direkten Kontakt zu dem Kunden bekommen. Meeco bietet dabei eine Plattform an, auf der sich beide begegnen können. Eine Anbindung an andere Dienste, wie etwa die von Google, findet dabei nicht statt.

Momentan existieren eine App für iOS sowie Plugins für die Desktop-Browser Google Chrome und Firefox. Sowohl auf dem Smartphone als auch auf dem Desktop-Computer wird dabei ein Zugriff auf die Meeco-Plattform ermöglicht. Der Nutzer erstellt einen Account, mit dem er den Zugriff auf die Dienste von Meeco erhält. Meeco ist dabei als eigenständiges Ökosystem zu betrachten, in dem sich der Nutzer bewegt, sei es zum Surfen, zum Kommunizieren oder auch nur, um Notizen aufzuschreiben. Hauptaugenmerk wird offensichtlich darauf gelegt, dem Nutzer alle Möglichkeiten der modernen Kommunikationswelt innerhalb einer Plattform zur Verfügung zu stellen. Umschrieben wird die Plattform daher auch als „life management“-Applikation.

Bewertung durch Dritte:
http://www.launchgroup.com.au/2016/03/31/trust-economy-startup-meeco-launches-meeco-labs-and-european-office-off-back-of-a3-2m-seed-round/

PGuard

PGuard soll sowohl als App als auch als Web-Plattform dem Verbraucher/Nutzer ermöglichen, basierend auf eigenen Präferenzen eine datenschutzrechtliche Auswertung von genutzten bzw. zur Nutzung vorgesehenen Apps zu erhalten und damit das Risiko zu bewerten. Das Projekt läuft seit Anfang 2016 bis Mitte 2018. Das Projektvolumen beläuft sich auf 1,94 Mio. EUR (davon 72 % Förderanteil durch das BMBF).[21]

Technisch ist das Projekt in zwei Teilbereiche gegliedert:
Teilbereich 1 des Projekts hat zum Ziel, dass eine Textanalyse der Datenschutzbestimmungen bzw. der AGB durch die Plattform oder die PGuard-App eigenständig durchgeführt werden soll. Basierend auf dieser Analyse und in Verbindung mit den Präferenzen des Nutzers wird alsdann eine Risikobewertung bzw. zumindest eine Zusammenfassung der datenschutzrechtlichen Position der zu prüfenden App erstellt und dem Nutzer zugänglich gemacht. Gerade für „Mainstream Apps“ kann der Ansatz von PGuard ausgesprochen hilfreich sein und einen Beitrag zur Entscheidungsfindung beim interessierten Nutzer leisten.
Im Teilbereich 2 des Projekts soll der Datenaustausch mit den App-Betreibern untersucht werden. So wird beispielsweise analysiert, auf welche Daten die Apps zugreifen und welche Daten auf welche Weise (verschlüsselt/unverschlüsselt) an den Betreiber der App weitergegeben werden. So kann auch eine technische Bewertung der einzelnen Apps durchgeführt werden und ggf. vor technisch unausgereiften Apps (etwa ohne Verschlüsselung der Transitdaten) gewarnt werden.

Der im Projekt PGuard verfolgte Lösungsansatz kombiniert eine Analyse des Kommunikationsverhaltens der Apps mit einer Prüfung der rechtlichen Bestimmungen der App-Anbieter und kann damit den

21 *Dazu: http://www.forschung-it-sicherheit-kommunikationssysteme.de/projekte/pguard; http://infai.org/de/Presse/Pressemitteilungen/pguard; https://sriw.de/index.php/pguard*

Nutzern eine besonders umfassende Risikoanalyse bieten. Eine abschließende rechtliche Einordnung wird jedoch nicht vorgenommen.

Bewertung durch Dritte:
http://www.openpr.de/news/896409/PGUARD-neue-Moeglichkeiten-beim-Selbstdatenschutz-fuer-App-Anwendungen.html

Humada

Der in 2016 gegründete Anbieter Humada zielt auf die Entwicklung einer Datenverarbeitungslösung ab, die auf den Nutzer ausgerichtet ist. Es werden dabei vier Produkte angeboten/beworben: Humada Care, Humada Trust, Humada Match und Humada Rep. Humada Care wurde Ende 2016 als Produkt veröffentlicht. Es stellt zur Zeit das Core Business des Unternehmens dar.

Humada Trust[22] soll eine Plattform für Hardware-Unternehmen anbieten, auf der die Kundendaten gesetzeskonform und flexibel gespeichert bzw. verwaltet werden können.

Humada Match[23] soll eine Art App Store darstellen, auf der die datenverarbeitenden Unternehmen mehr über ihre Kunden erfahren können und die Erstellung von maßgeschneiderten Anwendungen ermöglicht wird. Die Verknüpfung von „App Store“ und Entwicklerplattform ist jedoch gegenwärtig nicht hinreichend beschrieben. Es lässt sich daher noch nicht exakt darlegen, wie die Plattform ausgestaltet werden soll, bzw. inwiefern der Datenschutz bei diesem Produkt eine maßgebende Rolle spielt.

Nur für das Produkt Humada Care[24] ist gegenwärtig eine Broschüre erhältlich, die die aktuellen Entwicklungen des europäischen Datenschutzes zusammenfasst und kurz auf das Produkt selbst eingeht.

Kernbereich der Software sind demnach folgende Funktionen:

- Analyse der vorhandenen (Kunden-)Daten
- Auditieren der Daten
- Vorbereitung zur Zertifizierung
- integriertes Datenschutzmanagementsystem – ob es sich hierbei um ein „rechtliches“ oder ein „technisches“ (etwa zum Schutz vor dem Datenzufriff Unbefugter) handelt, ist gegenwärtig noch nicht ersichtlich
- Informationssicherheitsmanagement nach ISO 27001[25]
- Projektberatung und Auswertung

Consberry

Consberry bietet die Softwarelösung „Customer Consent Control Suite“ für Unternehmen sowie Beratungsleistungen an. Die Software „CCC Suite“ stellt Unternehmen der datenverwendenden Wirtschaft Werkzeuge zum Einwilligungsmanagement zur Verfügung, z. B. für die individuelle Verwaltung von Kundenzustimmungen. Dabei wird die Einverständniserklärung in ihre Bestandteile aufgegliedert und den verschiedenen Teilen eine definierte Funktion zugewiesen. Falls beispielsweise ein Kunde seine Einwilligung widerruft, hilft die „CCC Suite“ ab diesem Zeitpunkt dabei, die Daten des Betroffenen in allen Systemen zu löschen, zu deaktivieren oder zu anonymisieren.

22 http://humada.com/humada-trust/
23 http://humada.com/humada-match/
24 http://humada.com/humada-care/
25 https://www.iso.org/obp/ui/#iso:std:iso-iec:27001:ed-2:v1:en

Es handelt sich um ein Datenbanksystem, welches Kundendaten speichert und je nach Umfang der Freigabe die Daten verschiedenen Abteilungen des Nutzerunternehmens zugänglich machen soll. Der Mehrwert im Vergleich zu konventionellen Kundendatenbanksystemen muss sich in der Praxis erst zeigen. Vielversprechend dürfte die eingegangene Partnerschaft des Unternehmens mit dem führenden deutschen Versandhändler sein.

3. Bewertung der verschiedenen Ansätze

a) Bewertungskriterien

Zwischen den für die vorliegende Studie betrachteten Ansätzen bestehen erhebliche Unterschiede, sowohl im Hinblick auf die technische Herangehensweise als auch auf die wirtschaftliche Umsetzung und die Reichweite der Anwendungen. Im Rahmen der Analyse werden die unterschiedlichen Projekte und Unternehmen daher in den Fällen, wo es möglich ist, unter folgenden Gesichtspunkten eingeordnet und bewertet:

Strukturelle Erwägungen

- Reichweite

Für die erfolgreiche Implementierung eines Lösungsansatzes ist die Akzeptanz des Produktes bei den Nutzern entscheidend. Nur mit einer hohen Zahl von Nutzern wird es den meisten Projekten möglich sein, weiter zu bestehen und die notwendige Finanzierung zu sichern. Wesentliche Faktoren sind dabei:

- Mehrsprachigkeit bzw. Ausrichtung auf einen bestimmten Sprachraum

- Intensität des Outreachs; so etwa, ob Werbung geschaltet wird und wie intensiv auf Nutzerempfehlungen gesetzt wird

- Für die Marktdurchsetzung sind außerdem die technische Nutzbarkeit und die Kompatibilität des Produkts mit verschiedenen Betriebssystemen von großer Wichtigkeit.

- Diversität

Weiterhin ist zu berücksichtigen, wie breit die Projekte aufgestellt sind. So kann ein Lösungsansatz nur einen Schwerpunkt oder nur ein technisches „Produkt“ beinhalten oder aber auch breit aufgestellt sein und mehrere unterschiedliche Angebote in sich zu vereinen suchen. Beide Möglichkeiten haben ihre Vor- und Nachteile. Einerseits bedeutet die breite Aufstellung, dass ein Unternehmen auf neue Trends und Marktsituationsveränderungen flexibler reagieren und ggf. die Schwerpunkte seines Angebots verschieben kann. Andererseits würde die Fokussierung auf ein Einzelthema (z. B. Datenportabilität) zur höheren Ressourcenbindung führen und hätte dadurch eine bessere technische Spezialisierung und damit häufig einen Qualitätsvorteil des Produkts zur Folge. Aber auch die Spezialisierung auf ein Einzelthema führt ihrerseits zu einer Konkurrenzverschärfung mit anderen Anbietern.

- Wirtschaftlicher Hintergrund

Der wirtschaftliche und z.T. ideelle Hintergrund eines Projektes ist für die Bewertung seiner Finanzierbarkeit nicht unerheblich. Die Notwendigkeit der Balance zwischen der Wirtschaftlichkeit eines Produkts und dem eigenen Anspruch der Entwickler auf Schutz der Privatsphär hat mitunter auch einen Einfluss auf unterschiedliche Finanzierungsmodelle (etwa bei der Weitergabe von Daten an Dritte). Auch für die Konkurrenzfähigkeit und die Bewertung von Zukunftsaussichten eines Lösungsansatzes ist sein

Finanzierungsmodell entscheidend, da bei fehlender Wirtschaftlichkeit bzw. bei fehlender staatlicher Subventionierung die Aussicht auf ein nachhaltiges Bestehen auf dem Markt schwindet.

• Vertrauensbildung

Datenschutzfreundlichkeit der Ansätze trägt erheblich zur Vertrauensbildung bei den Nutzern bei. Es ist davon auszugehen, dass der Grad der Datenschutzfreundlichkeit und die Transparenz der Datenverwendung wesentliche Faktoren bezüglich der Präferenz eines Ansatzes seitens der Verbraucher und damit einen Wettbewerbsvorteil darstellen. Vertrauensbildend sind hier etwa die Vollständigkeit und Verständlichkeit der AGB oder aber auch das positive Auftreten der Verantwortlichen im Umgang mit Presse oder Kunden etwa wenn Fehler eingestanden werden und Verantwortung übernommen wird.

Technische Erwägungen

• Standort der Daten

Für die Bewertung der datenschutzrechtlichen Unbedenklichkeit, aber auch hinsichtlich anderer Faktoren wie des Vertrauens in eine Plattform und der Sicherheit der Daten, ist es entscheidend, wo und wie die personenbezogenen Daten gespeichert werden. Dabei kann bei den Ansätzen zwischen zwei Extremen unterschieden werden: Auf der einen Seite stehen cloud-basierte Lösungen, bei denen die Daten auf externen Servern gespeichert werden und der Zugriff den Nutzern über Client-Applikationen gewährt wird. Auf der anderen Seite stehen rein lokale Applikationen, bei denen Daten dezentral beim Nutzer gespeichert werden. Beide Methoden haben Vor- und Nachteile: So kann lokale Datenhaltung die Kompatibilität mit anderen Systemen beeinträchtigen und einer hohen Marktverbreitung entgegenwirken. Hingegen können Cloud-Lösungen Probleme bei der Datensicherheit aufwerfen. So sind z. B. Angriffe auf zentrale Speicherorte leichter möglich und wegen der erbeutbaren Datenmenge attraktiver („honeypot“) als ein Abschöpfen beim Nutzer (etwa durch Trojaner).

• Datenschutzniveau am Standort der Daten

Dies ist nicht zuletzt auch aus rechtlicher Perspektive wichtig, da von dem Datenschutzniveau eine Reihe anderer Faktoren beeinflusst wird. So kann ein höheres Datenschutzniveau zu einer höheren Vertrauensbildung führen. Langfristig ist es auch notwendig zu berücksichtigen, wie stabil das Datenschutzniveau über einen längeren Zeitraum in der betreffenden Jurisdiktion bleibt. Ist ein stabil hohes Datenschutzniveau vorhanden, so kann dies dem Anbieter auf lange Sicht helfen, Kunden zu binden und Vertrauen aufzubauen. Auf der anderen Seite kann die ständige Anpassung des Datenschutzniveaus für die Unternehmen einen erheblichen Aufwand bedeuten, datenschutzkonform zu agieren. Gerade für kleinere Unternehmen könnte ein zu strikt wirkendes Datenschutzrecht zu einer erheblichen Ressourcenbindung führen und die Konkurrenzfähigkeit beeinträchtigen.

• Nutzerkontrolle

Für die technischen Umsetzungen ist es außerdem wichtig zu berücksichtigen, wie viel Einfluss der Nutzer auf die Weitergabe seiner Daten hat und ob ihm dynamische Anpassungsmöglichkeiten und somit eine umfassende Nutzerkontrolle auf technischem Wege ermöglicht werden. Auch der Daten-Standort – wie etwa beim Nutzer-Rechner – spielt in diesem Zusammenhang eine wichtige Rolle. Allerdings können auch bei einer cloud-basierten Lösung dem Nutzer dynamische Anpassungsmöglichkeiten und somit eine umfassende Nutzerkontrolle auf technischem Wege ermöglicht werden.

• Transparenz

Gerade für den weder technisch noch juristisch vorgebildeten Nutzer ist es darüber hinaus wichtig, ein Mindestmaß an Verständnis über die technischen Vorgänge zu bekommen. Die Transparenz der Lösungsansätze ist dafür entscheidend und die Anbieter sind gehalten, die Struktur bzw. das Konzept ihres Projektes dem Nutzer verständlich zu machen. Dazu gehört z. B. eine übersichtliche Datenschutzerklärung oder aber auch einfache und stimmige Erläuterungen zum Projekthintergrund und dessen Funktionsweise.

b) Reichweite und Diversität

Anmerkung: Bei der Darstellung wird ggf. ein Rang bei dem Online-Dienst Alexa Internet Inc. angeführt, der Daten über Seitenabrufe von Webseiten sammelt und darstellt. Ein niedriger Rang bedeutet dort höhere Besucherzahlen und größere Reichweite. Dies kann einen Hinweis auf die potenzielle globale Reichweite geben, jedoch sollte diese Zahl nicht überbewertet werden.

P3P

Bei P3P handelt es sich um ein Einzelfokusprojekt (zum Kern des Projekts gehören das Protokoll und dessen Implementierung), bei dem das P3P-Protokoll vom World Wide Web Consortium entwickelt und als kostenloses Protokoll zur Verfügung gestellt wurde. Um nutzbar zu sein, muss P3P in die Internet-Browser implementiert werden. Das wurde aber nur für den Internet Explorer (später Edge) umgesetzt und mit Windows 10 wieder entfernt. Dadurch ist die Reichweite des Protokolls und damit auch des Projektes sehr gering.

digi.me

Bei digi.me handelt es sich um eine Einzelapplikation zur Sicherung von Daten in sozialen Netzwerken. Der Fokus liegt auf dem englischsprachigen Raum. Das beschriebene Supportforum (https://socialsafe.uservoice.com/) war zum Bewertungszeitpunkt noch nicht funktionsfähig. Die Software ist für iOS, Android, macOS 10.7+ und Windows 7+ verfügbar. Dies deckt den Markt umfangreich ab, lässt jedoch Lücken für Linux-Nutzer. digi.me hält einen globalen Alexa-Rang von um die 500.000.[26]

LETsmart

LETsmart ist noch in der Entwicklungs- bzw. Testphase an der Universität Leipzig, daher ist noch keine Bewertung zur Reichweite des Projektes möglich. Es handelt sich im Prinzip um eine Einzelapplikation, d.h. um einen Personaldatenmanager mit Fokus auf Rechtskonformität der Autorisierung bzw. der Einwilligung zu Datenverarbeitung von personenbezogenen Daten.

Consent Management for Federated Data Sources

In der Entwicklung an der TU Berlin, daher ist noch keine Reichweitenbemessung möglich. Es handelt sich um ein Einzelprojekt im Bereich einer technischen Implementierung eines Personaldatenmanagers mit Fokus auf die datenschutzfreundliche Konsolidierung von personenbezogenen Daten.

26 http://www.alexa.com/siteinfo/digi.me

MesInfos

MesInfos ist ein Unterprojekt der Fing-Stiftung und beschäftigt sich mit der Verwaltung von Kundendaten bzw. der Erweiterung der Nutzerkontrolle über diese. Ein Unterprojekt von MesInfos stellt dabei das Pilotprojekt „Cozy Cloud“ dar. Die Reichweite ist etwa in der Größenordnung des Mutterprojektes von Fing einzuordnen (Fing.org hat einen Alexa-Rang von ca. 330.000).[27]

MyPermissions

MyPermissions startete als ein auf den englischsprachigen Raum ausgerichtetes Unternehmen, hat sich aber im Verlauf der Zeit besonders auch dem deutschsprachigen Raum – etwa durch eine durchweg deutschsprachige Webseite – zugewendet. MyPermissions hat seine Reichweite durch die Entwicklung von Browser-Add-ons und weitergehenden Analysefunktionen vergrößert, ohne seinen Privacy-Bezug aufzugeben. Auch bei den Besucherzahlen liegt MyPermissions bei einem vergleichsweise guten Rang von ca. 395.000.[28]

Access my Info

Das von Citizen Lab entwickelte System (bzw. die Plattform) ist – da der Ansatz vorwiegend auf kanadischem Recht aufbaut – allein auf Kanada beschränkt. Mitte 2016 wurde jedoch auch ein Test der Plattform in Hongkong durchgeführt, welcher aber eher ernüchternde Rückmeldequoten der Anfragen bei den Unternehmen zur Folge hatte. Dies zeigt allerdings, dass das Modell grundsätzlich ausgeweitet werden könnte, sofern eine rechtliche Grundlage für derlei Anfragen in anderen Staaten vorhanden ist. Eine Besucherreichweitenanalyse ist für das Projekt wegen einer fehlenden Projektwebseite nur unvollständig möglich. Citizen Lab selbst hat einen Rang von 240.000.[29]

Citizenme

Citizenme konzentriert sich vorwiegend auf die Sammlung und Verwertung von direkten und indirekten Nutzerdaten. Dies wird hauptsächlich über das App-Angebot (iOS und Android) betrieben. Die Apps haben eine Nutzungszahl (10.000-50.000 Installs für Android[30]), der Alexa-Rang schwankt im 7-stelligen Bereich um etwa 2.000.000, was eine relativ geringe Reichweite ausdrückt.

Datacoup

Der primäre Fokus von Datacoup bestand ursprünglich in der Auswertung von Kreditkartentransaktionen und wurde auf die Analyse und den Verkauf von Nutzungsdaten verschiedener Unternehmen wie Facebook oder Google ausgeweitet. Die Auswertung von Kreditkartendaten ist auf US-Bürger beschränkt, und der Hauptfokus des Unternehmens liegt somit in den USA. Beim Alexa-Rang bewegt sich Datacoup um den Rang 1.000.000.[31]

personiq (Unternehmen Emvolution)

Emvolutions Kernprojekt sind Browser-Add-ons, mit denen Daten gesammelt, ausgewertet und grafisch dargestellt werden sollen. Begonnen hat das Projekt mit dem Fokus auf den deutschsprachigen Raum; es wird jedoch über die Add-ons auch versucht, den englischsprachigen Raum zu erreichen.

27 http://www.alexa.com/siteinfo/fing.org
28 http://www.alexa.com/siteinfo/mypermissions.com
29 http://www.alexa.com/siteinfo/citizenlab.org
30 https://play.google.com/store/apps/details?id=com.citizenme&hl=en_GB
31 http://www.alexa.com/siteinfo/datacoup.com

Meeco

Meeco fokussiert sich auf die Schaffung einer breiten Plattform mit sehr unterschiedlichen Diensten. Es soll ein eigenes Ökosystem geschaffen werden, in welchem die Nutzer von anderen Diensten abgebunden werden, sodass alle Informationen in Meeco verwaltet werden. Angeboten werden eine iOS App und Browser-Erweiterungen für Firefox und Chrome. Meeco ist eher auf den englischsprachigen Raum ausgerichtet, die Applikationen sind jedoch auch in weiteren Sprachen verfügbar (darunter auch Deutsch). Meeco bewegt sich beim Alexa-Nutzerranking um den Rang 2.000.000.[32]

PGuard

Es ist geplant, dass PGuard den Nutzern eine Auswertung und Darstellung der datenschutzrechtlichen Einordnungen von Apps ermöglicht. Aufgeteilt ist das Projekt in 2 Teilbereiche: Zum einen in die Auswertung von AGB bzw. von Datenschutzbestimmungen und zum anderen in eine Datenanalyse von Apps bezüglich der Auswertung von Verbindungsdaten. Dadurch soll eine umfassende Bewertung über die Datenschutzfreundlichkeit ermöglicht werden. Ausgerichtet ist das Projekt auf den deutschsprachigen Raum. Eine Nutzer-/Besucherstatistik ist wegen fehlender Projektwebseite nicht möglich.

c) Wirtschaftlicher Hintergrund und Vertrauensbildung der Projekte

P3P

P3P hatte keinen direkten ökonomischen Hintergrund, bzw. das Projekt war nicht auf die Generierung von Umsatz ausgelegt. Verabschiedet vom World Wide Web Consortium (W3C) als Standardisierungsorganisation ohne Gewinnmaximierungsabsicht, war das Ziel, eine Standardisierung für den Umgang mit personenbezogenen Daten im Internet zu schaffen. Vertrauen in das System war anfänglich zwar vorhanden, jedoch wurde schnell die zu hohe Komplexität des Systems als Hauptproblem für die Nutzbarkeit festgestellt. Dadurch wurde der Standard nie wirklich für einen breiten Nutzerkreis verfügbar und es konnte auch kein Vertrauen in den Standard aufgebaut werden.

digi.me

Das Geschäftsmodell von digi.mMe baut auf dem Verkauf von Lizenzen für seine Softwarelösung auf. digi.me ist darauf bedacht, seine Software zu verkaufen und diese für den Nutzer so ansprechend wie möglich zu gestalten. Der durch das Tool verbesserte Datenschutz wird dabei als zusätzlicher Vorteil des Produkts dargestellt. Vertrauensbildend ist dabei, dass das Geschäftsmodell gerade den Verkauf von personenbezogenen Daten ausschließt. Somit besteht für das Unternehmen ein direkter Ansporn, datenschutzkonform zu agieren und so wenig Nutzerdaten wie möglich zu verarbeiten. Außerdem ist digi.me ausgesprochen aktiv in der Fachöffentlichkeit. Dies schafft Vertrauen in die Anwendung und das Unternehmen selbst.

LETsmart

LETsmart ist noch in der Entwicklungsphase, daher lässt sich noch wenig über die finale Ausrichtung sagen. Offen bleibt die Frage, wie die Finanzierung des Tools erfolgen soll. Da von einer Nutzerbereitschaft, für das Angebot zu bezahlen, nicht auszugehen ist, wären die Kosten voraussichtlich von den Datennehmern zu tragen. Hieran schließt sich die Frage, ob dies mit einem Basismodell (d.h. Pauschalpreis für die Verwendung von LETsmart) erfolgen soll oder eine (noch näher zu bestimmende) Gebühr pro Transaktion erhoben wird. Da die Universität Leipzig als Schirmherr agiert und in Projekte mit akademischem Hintergrund meist mehr Vertrauen gesetzt werden, ist ein höheres Vertrauenspotenzial anzunehmen.

32 http://www.alexa.com/siteinfo/meeco.me

Consent Management for Federated Data Sources

Das von der TU Berlin entwickelte System hat zumindest im Moment keine wirtschaftliche Ausrichtung und lässt sich als akademisch dominiert definieren. Auf welche Weise Umsetzung und praktischer Einsatz finanziert werden, scheint noch offen zu sein. Möglicherweise sollen die verwendenden Unternehmen selbst die Kosten tragen. Auch hier ist – basierend auf dem universitären Hintergrund – eine erhöhte Vertrauensgrundlage anzunehmen.

MesInfos

Fing als Träger von MesInfos finanziert sich hauptsächlich durch Spenden seitens der Unternehmen des Netzwerkes. Vertrauensbildend führt Fing eine Reihe von kleineren und größeren Projekten und Veranstaltungen durch. Auch der Gründer und Geschäftsführer von Fing, Daniel Kaplan, ist äußerst aktiv in der Öffentlichkeitsarbeit. Inwieweit die Finanzierung von Fing durch die Unternehmen des Netzwerkes Einfluss auf dessen Neutralität hat, lässt sich nur schwer bewerten; es sind in diesem Zusammenhang jedenfalls keine offensichtlichen Probleme erkennbar.

MyPermissions

MyPermissions positioniert sich als Anlaufpunkt für Nutzer, welche einen vereinfachten Zugriff auf ihre Datenschutzeinstellungen bei den einzelnen Anbietern (wie etwa Google) suchen. Die Finanzierung von MyPermissions ist jedoch undurchsichtig. Die Software ist frei verfügbar und es besteht kein ersichtliches Geschäftsmodell.

Eine Finanzierung über Werbung und Werbeangebote ist ebenfalls nicht ersichtlich. MyPermissions scheint sich seit 2013 aus Venturecapital zu finanzieren. Dank seiner Webseite macht MyPermissions durchaus einen professionellen Eindruck. Jedoch führen Dinge wie die Integration in Facebook-Kampagnen über die AGB und Einbindungen eines Facebook-Like-Buttons zu negativen Wirkungen hinsichtlich der Vertrauenswürdigkeit der durchaus sehr datenschutzfreundlichen Rhetorik des Unternehmens.

Access my Info

Das Projekt Citizen Lab hinter Access my Info ist ein Teil der Munk School of Global Affairs an der Universität Toronto. Dieser akademische Hintergrund macht das Projekt durchaus vertrauenswürdig, da im Kern keine monetären Interessen verfolgt werden. Anzumerken ist aber auch, dass das Projekt von Datenanalyseunternehmen wie Palantir Technologies und Oculus Info Inc. umfangreich finanziell unterstützt wurde. Eine Einflussnahme ist zwar nicht ersichtlich, potenzielle Interessenkonflikte können aber zukünftig auch nicht völlig ausgeschlossen werden.

Citizenme

Citizenme betreibt ein äußerst transparentes Geschäftsmodell. Personenbezogene Daten sollen durch den Nutzer selbst verwertet werden. Das Unternehmen behält einen Teil dieses Verkaufserlöses als Vermittlerprovision bzw. als Plattformanbieter ein. Es handelt sich um ein transparentes System, bei dem – sofern man seine personenbezogenen Daten denn nun aktiv verkaufen möchte – ein eindeutiges Geschäftsmodell erkennbar ist. Fraglich ist dennoch, ob dies ausreicht, um Nutzer davon zu überzeugen, ihre Daten für einen relativ geringen Erlös weiterzugeben, gerade weil auch der Wert solcher Daten nur sehr schwer (wenn überhaupt) bezifferbar ist. Offen bleibt auch, wie wertvoll diese Daten für den Käufer wirklich sind, da die Daten über Umfragen erhoben werden, wobei von einer zutreffenden Beantwortung einer Umfrage nicht immer zwangsläufig ausgegangen werden kann.

Datacoup

Das Geschäftsmodell ist transparent: Personen verknüpfen ihre Kreditkartendaten bzw. ausgewählte Netzwerke wie Facebook oder Google mit der Plattform, woraufhin diese Daten anonymisiert an interessierte Unternehmen zwecks Auswertung verkauft werden. Trotz dieses einfachen und nachvollziehbaren Finanzierungsmodells bleibt offen, wieviel diese Daten wirklich wert sind und inwieweit die Anonymisierung der Daten aufrechterhalten werden kann. Auch im Zusammenhang mit Kreditkartendaten, welche vom Unternehmen ausgewertet werden können, ist fraglich, ob ein so hohes Vertrauensniveau geschaffen werden kann, dass die Nutzer freizügig jegliche Transaktionsinformationen dem Unternehmen zur Verfügung stellen würden.

personiq (Unternehmen Emvolution)

Emvolution hat ein großes Ziel, jedoch ist bei diesem Start-up noch nicht erkennbar, wie die Finanzierung dieses Zieles erfolgen soll. Momentan zehrt das Unternehmen noch von Venturecapital, es muss jedoch früher oder später ein funktionierendes Finanzierungsmodell aufbauen. Eine Nutzerfinanzierung ist gerade bei dem geringen Mehr im Vergleich zu anderer freier Software nicht anzunehmen.

Meeco

Meeco spekuliert auf eine Finanzierung durch partizipierende Unternehmen. Diesen soll nach der Zahlung einer Gebühr ein Zugang in das Meeco-Ökosystem gewährt werden. Gegenwärtig ist noch nicht absehbar, inwieweit dies auf die Privatsphäre der Nutzer Einfluss haben wird. Meeco macht zwar deutlich, dass ihm die Privatsphäre der Nutzer wichtig ist, es muss jedoch noch abgewartet werden, wie die Umsetzung tatsächlich aussehen wird. Meeco ist nichtsdestotrotz auf einem guten Weg, Vertrauen in seine Plattform zu schaffen und Nutzer zu binden. Es wird öffentlichkeitswirksam an Datenschutz-Events teilgenommen und aktiv an datenschutzfreundlichen Lösungen gearbeitet.

PGuard

PGuard befindet sich gegenwärtig in der Entwicklung, eine wirtschaftliche Ausrichtung des Projekts scheint jedoch nicht geplant zu sein. Die Finanzierung erfolgt durch staatliche Zuschüsse.

Beim Nutzer sollen keine Daten gesammelt werden, es soll lediglich die Datenschutzfreundlichkeit von den jeweiligen Apps bewertet werden. Das fehlende wirtschaftliche Interesse und das Fehlen einer Datensammlung beim Nutzer sollten zu einem hohen Vertrauensgewinn des Projekts führen, welches sich als „Tester“ oder gar Zertifizierer von Apps positionieren könnte.

d) Technische Erwägungen – Datenstandort und Datenschutzniveau am Standort

P3P

Es erfolgt ein Austausch zwischen Nutzern und Plattformanbietern. Daten werden beim Aushandlungsprozess nicht direkt beim Anbieter gespeichert, es erfolgt lediglich ein Abgleich von Daten und eine Aushandlung der Reichweite der Nutzung bzw. – sofern ein Mindestlevel an „Einwilligung“ (rechtlich ist dies ggf. unwirksam; siehe dazu Beschreibungen zur Rechtssicherheit der Einwilligung im Kapitel III) nicht vorhanden ist – die Ablehnung der Plattformnutzung. Die Daten werden nach der Aushandlung zwischen

Nutzer und Webseite ausgetauscht. Je nachdem, wie umfangreich der Nutzer seine Freigaben eingestellt hat, können personenbezogene Daten (wie etwa das allgemeine Surfverhalten) ausgetauscht werden. Allerdings stellt die Komplexität des Systems für den Normalnutzer eine große Hürde dar und kann zu einer sehr weitreichenden (unerwünschten) Datenpreisgabe führen, wenn Einstellungen nicht korrekt vorgenommen werden.

Das Datenschutzniveau am Standort der temporären Daten (zum Datenabgleich) ist vom Serverstandort des Betreibers abhängig und kann somit nicht allgemein bewertet werden. Grundsätzlich würde dies jedoch eine Standardisierung des Datenschutzniveaus mit Kontrolle beim Nutzer ermöglichen. Der Nutzer legt das Datenschutzniveau bzw. die Reichweite der Auswertung selbst fest. Sind Daten erst einmal ausgetauscht, so verliert der Nutzer aber die Kontrolle über seine Daten.

digi.me

Daten werden durch das Tool direkt beim Nutzer, also lokal, und verschlüsselt gespeichert. Die Kontrolle des Nutzers und das Datenschutzniveau sind somit sehr hoch. Allein der Nutzer hat die Möglichkeit, seine Daten zu verändern oder zu löschen. Die Weitergabe und Nutzung von Daten ist von digi.me angedacht, es ist jedoch noch keine aktive Nutzung dieser Daten über eine Plattform o.Ä. vorhanden. Eine Bewertung dieser Möglichkeiten ist daher noch nicht möglich.

LETsmart

Daten sollen hier lokal in einem „Container“ beim Nutzer abgelegt werden. Der Zugriff darauf soll über ein Datenmanagementsystem erfolgen. Dabei sollen nur diejenigen Daten aus dem Container übermittelt werden, für die der Nutzer seine Einwilligung erteilt hat. Des Weiteren soll über das System eine Datenaktualisierung bzw. Löschung möglich sein. Daten werden daher zwar auch auf dem Server eines Dienstleisters gespeichert, LETsmart soll jedoch die Kontrolle über diese Daten und deren Weitergabe auf der Nutzerseite verorten. Dennoch werden auch hier Daten auf externen Servern zur Verarbeitung abgelegt und gespeichert. Besonders hervorzuheben ist aber, dass der Nutzer Verwaltungshoheit über seine Daten auf den „fremden“ Servern hat und sie dort ggf. löschen kann. Das Datenschutzniveau hängt auch hier vom jeweiligen Anbieter und dem Standort der Datenverarbeitungsanlage ab.

Consent Management for Federated Data Sources

Die Daten sollen in verschlüsselten Datensätzen in Verbindung mit Sticky Policies bei den verschiedenen Datenhaltern (etwa Regierungsorganisationen) abgelegt werden. Von diesen können weitere Unternehmen oder Organisationen die Datensätze abfragen.

Sofern sich an die Regeln des Systems gehalten wird (eine Kontrolle der zertifizierten Datenhalter ist notwendig), gibt der Datenhalter die Datensätze verschlüsselt an den Interessenten weiter. Die Datensätze werden somit bei den an den Datensätzen interessierten Einrichtungen abgelegt.

Der Zugriff auf spezifische Informationen ist aber nur unter Beachtung der Sticky Policies möglich. Somit kann jeder Interessent zwar alle Daten haben, kann aber nur auf diejenigen zugreifen, welche vom Nutzer für den Zugriff freigegeben wurden. Sicherheitsmechanismen sollen einen Zugriff auf nicht freigegebene Daten verhindern. Das System basiert auf einem „Regelungssystem im Regelungssystem“. Die Idee dahinter ist, dass so wenige Informationen wie möglich (je nach Einwilligung des Nutzers) dem Unternehmen vorliegen, jedoch mit der Möglichkeit eines potenziellen Zugriffs auf alle Daten im verschlüsselten Datensatz. Es handelt sich also um eine Vielzahl an (im Idealfall) identischen Datensätzen,

auf welche der Nutzer über die primären Datenhalter eine Aktualisierungs- und Veränderungsmöglichkeit hat. Änderungen werden dann durch Zwischenaktualisierung der Datensätze an weitere Datensatzhalter weitergegeben. Das Datenschutzniveau ist jeweils davon abhängig, wie granular die Einwilligung und die Freigabe der Daten durch den Nutzer gestaltet werden. Potenziell könnte somit eine für verschiedene Rechtsformen angepasste Einwilligung stattfinden. So kann ein einheitliches Datenschutzniveau aufgebaut werden. Inwieweit dieser recht komplexe Aufbau jedoch nicht umgangen werden kann – wenn etwa Daten aus dem Container (auch ohne Zustimmung) extrahiert werden – ist nicht absehbar. Zwar werden Sicherheitsmechanismen angeführt, einem unberechtigten Kopieren von Daten, etwa auf dem Papier, und der Weitergabe auf diesem Wege kann jedoch nur schwer entgegengewirkt werden.

MesInfos

Datensätze sollen zentral vom Nutzer eingesehen werden können und ggf. zur Bearbeitung freigegeben werden. Dem Nutzer soll dadurch die Kontrolle über seine Daten ermöglicht werden. Standort der Daten bleibt aber der Server der MesInfos-Initiative bzw. der teilnehmenden Unternehmen. Der MesInfos-Account dient als eine zentrale Anlaufstelle, über welche Daten aktualisiert werden können. Es ist allerdings noch nicht ersichtlich, ob Nutzer ihre Daten komplett löschen können und eine lückenlose Kontrolle über die Datenverwendung haben werden. Es handelt sich um ein Pilotprojekt, daher sind noch keine ausführlichen Informationen zum (finalen) Umfang der Möglichkeiten vorhanden. Grundsätzlich wird hier die gleiche Idee verfolgt, die auch hinter der MyData-Initiative steht, und darauf aufbaut. Das Projekt ist auf Frankreich beschränkt, kann aber grundsätzlich auch auf andere Staaten ausgeweitet werden. Das Datenschutzniveau ist hierbei vom Standort der Daten auf Unternehmensservern und auf dem MesInfos-Server abhängig.

MyData

MyData strebt mit seinem technischen Ansatz eine Zentralisierung der Daten auf einen eigenen Account an. Die Grundidee ist, verschiedene Anbieter in einem zentralen System zusammenzuführen und dem Nutzer dadurch an einer Stelle („One-Stop-Shop“) die Möglichkeit zu geben, seine Daten bei unbeschränkt vielen (teilnehmenden) Unternehmen zu ändern und ggf. zu löschen. Dies würde dem Nutzer weit mehr Kontrolle geben und zeitraubende Einzelmodifikationen ersparen. Daten wären zwar weiterhin bei den einzelnen Unternehmen gespeichert, jedoch würde jedes der Unternehmen in die Lage versetzt, einen Datenabgleich mit anderen Unternehmen durchführen zu können und Daten aktuell zu halten. Es handelt sich also um eine Art „interconnected Cloud“ mit dem Account des Nutzers als zentralem Steuerungspunkt. Das Datenschutzniveau ist auch hier vom Standort der Daten bei den einzelnen Anbietern abhängig, da die Daten weiterhin auf deren Server gespeichert bleiben (zumindest temporär).

MyPermissions

MyPermissions führt an, keine Nutzerdaten selbst zu speichern. Jedoch ist aus der Funktionsweise und dem Zugriff auf die Webseite des Unternehmens durch das Plugin nicht auszuschließen, dass zumindest anonyme Nutzerdaten gespeichert werden könnten. Eine völlige Trennung von den Systemen des Unternehmens liegt nicht vor und die Personendaten („Welche Apps sind installiert?“) werden zumindest temporär zur Auswertung verarbeitet bzw. abgelegt. Speicherort wäre hier mit hoher Wahrscheinlichkeit Israel bzw. der US-Amazon-Server.[33] Das Datenschutzniveau wäre dadurch eher als gering zu betrachten.

33 *https://whois.domaintools.com/mypermissions.de*

Citizenme

Die Daten aus den Umfragen werden auf den Servern des Unternehmens abgelegt. Diese sind mit hoher Wahrscheinlichkeit im Vereinigten Königreich bzw. in Irland (Dublin).[34] Europäisches Datenschutzrecht wäre also anwendbar. Sollten Daten verkauft werden, so werden diese natürlich auf den Servern des Käufers gespeichert, daher kann auch hier eine umfangreiche Verteilung auf Server in verschiedenen Staaten stattfinden.

Datacoup

Daten werden auf den Servern des Unternehmens gespeichert. Es kommt das Datenschutzrecht der USA bzw. NY (Sitz) oder Virginia[35] (Server) zur Anwendung.

personiq (Unternehmen Emvolution)

Daten aus den Browser-Plugins werden im aktuellen Projektstatus auf den Servern des Unternehmens gespeichert. Es kommt deutsches bzw. europäisches Datenschutzrecht zur Anwendung. Laut Unternehmen wird geplant, alle Daten auf den Geräten der Nutzer zu speichern. Es muss jedoch noch abgewartet werden, ob dies tatsächlich so umgesetzt wird.

Meeco

Alle Daten werden auf den Servern des Unternehmens gespeichert. Sitz des Unternehmens ist Australien. Je nach Serverstandort kann jedoch auch dort lokales Recht anwendbar sein.

PGuard

Vom Endverbraucher sollen keine Daten gespeichert werden. Er soll lediglich Zugriff auf die Auswertung der betreffenden Apps erhalten sowie eine Information zu deren Vertrauenswürdigkeit und dem Einklang mit den Datenschutzbestimmungen. Das Projekt befindet sich z.Z. in der Entwicklungsphase.

e) Nutzerkontrolle und Transparenz

P3P

Nutzerkontrolle sollte durch Auswahl bestimmter Kriterien und Freigabekategorien stattfinden. Der Abgleich mit den Datenschutzbestimmungen der Webseite sollte dann im Hintergrund durchgeführt werden und danach ein Austausch der freigegebenen Daten stattfinden. P3P sah dabei einen (für den Normalnutzer) sehr komplexen Einstellungskatalog vor, welcher – wenn Einstellungen nicht korrekt vorgenommen wurden – zu einer sehr umfangreichen Preisgabe von personenbezogenen Daten führen konnte. Diese fehlende Transparenz wurde frühzeitig bemängelt und war ein Teil der Probleme, warum P3P nicht breit eingesetzt wurde.

digi.me

digi.me ermöglicht dem Nutzer eine weitreichende Kontrolle über seine Daten. Da das Programm darauf ausgelegt ist, die Daten beim Nutzer zu sichern, ist der Nutzer allein für die Datenzusammenstellung verantwortlich. In welchem Umfang die Daten von digi.me tatsächlich verwertet werden, ist noch nicht nachvollziehbar. Daher lassen sich noch keine Aussagen über die Kontrollmöglichkeiten des Nutzers über diese Datentransfers treffen. Das Projekt ist hinsichtlich der eigentlichen Applikation sehr transparent. Die praktische Ausgestaltung hinsichtlich der späteren Verwertung der Daten muss abgewartet werden.

34 https://whois.domaintools.com/citizenme.com/
35 https://whois.domaintools.com/datacoup.com

LETsmart

Nutzerkontrolle ist eines der Hauptziele des Projekts. Der Nutzer soll die Möglichkeit haben, sehr genau zu bestimmen, welche seiner Daten den einzelnen Unternehmen zugänglich gemacht werden sollen. Auch eine dynamische Aktualisierung der Daten ist angestrebt. Für eine endgültige Bewertung muss das fertige Produkt betrachtet werden. Das Projekt hat ein großes Potenzial, wenn es für den Nutzer einfach einsetzbar und dennoch datenschutzkonform arbeitet.

Consent Management for Federated Data Sources

Bei CoMaFeDS gibt es eine Reihe von Parallelen zu LETsmart. Es verfolgt ähnliche und z.T. darüber hinausgehende Ziele. Auch hier soll der Nutzer eine umfangreiche Kontrolle über die Verwendung seiner Daten bekommen. So können im Voraus durch den Nutzer umfangreiche Einstellungen vorgenommen werden, wer seine Daten nutzen darf und zu welchen Zwecken diese verarbeitet werden dürfen. Auch nach der Datenweitergabe sollen Aktualisierungen möglich sein. Darüber hinaus sollen spezielle Applikationen eine weitere Sicherheitsebene schaffen, bei der etwa das Ausdrucken von Daten oder die Umgehung von Sicherheitsmechanismen ausgeschlossen werden sollen. Die Komplexität der Anwendung könnte allerdings schnell zu abnehmender Transparenz für den Nutzer führen. Gerade im Zusammenhang mit den angestrebten Zielen des Projektes bleiben noch viele Fragen offen, und es könnte der Eindruck entstehen, dass es sich hierbei um ein sehr schwer zu bedienendes System handelt. Insbesondere für den Normalnutzer stellt dies eine sehr hohe Barriere dar. Auch hier muss letzten Endes auf die finale Bewertung der Applikation und auf ihre praktische Umsetzung abgewartet werden. Ein denkbares Entwicklungsszenario wäre, dass das System etwa nur zwischen unterschiedlichen Einrichtungen eingesetzt wird und, dass der „Normalnutzer“ nicht in das System integriert wird. Allerdings würde ein solches Entwicklungsszenario die ursprüngliche Ausrichtung des Projektes ändern.

MesInfos

Kontrolle des Nutzers soll hier eines der Hauptprinzipien sein. Der Nutzer soll so über eine Plattform den Zugriff auf alle, bei den teilnehmenden Unternehmen verteilten Daten erhalten. Allerdings wird der Nutzer letzten Endes nicht wirklich die Daten löschen können. MesInfos ist mehr als Aktualisierungs- und Informationsplattform angedacht. Die praktische Ausgestaltung kann an dieser Stelle noch nicht bewertet werden; das Projekt befindet sich in der Testphase mit einem eingeschränkten Nutzerkreis. Es sind einige Parallelen zu MyData festzustellen.

MyData

Das MyData-Konzept beinhaltet ein zentralisiertes Verwaltungstool für verteilte Datensammlungen bei verschiedenen Anbietern. Das Ziel des Projektes ist unter anderem, eine einheitliche zentralisierte Datenkontrolle des Nutzers für verschiedene Anbieter zu ermöglichen. Eine zentralisierte Datenkontrolle soll dem Nutzer mehr Hoheit über die Verarbeitung seiner Daten verschaffen, als es bei einer Einstellung über die Datenverwendung bei jedem Anbieter einzeln der Fall wäre. Gerade wenn viele verschiedene Dienste genutzt werden, führt schon allein der große Aufwand bei der Datenkontrolle beim Normalnutzer zur Resignation – ein Problem, auf das MyData eingeht. Die Transparenz wird hier anhand der Standardisierung von Einstellungen geschaffen. Praktische Umsetzungen müssen zwar im Detail noch genauer bewertet werden, aber es lässt sich feststellen, dass Projekte wie das auf MyData aufbauende MesInfos vielversprechend sind.

MyPermissions

MyPermissions verspricht vollständige Kontrolle über die Daten und sieht sich als reinen Informationsgeber zur Bewertung der Datenpreisgabe. Fraglich bleibt jedoch, ob MyPermissions Nutzerdaten dennoch anonymisiert speichern kann und inwieweit das Projekt Vertrauenswürdigkeit aufweisen wird. Die Darstellung der Daten durch Browser-Plugins ist transparent und einfach gelöst. Es ist z.T. weit einfacher und schneller, die Verbindung zu den Nutzerdaten über das Plugin herzustellen, als den direkten Weg der Einstellung bei den jeweiligen Anbietern zu beschreiten.

Access My Info

Access My Info bietet (kanadischen Bürgern) die Möglichkeit, durch einfache Anfragen bei kanadischen Unternehmen Informationen zu den gespeicherten personenbezogenen Daten zu erhalten. Das Projekt vereinfacht somit die Durchsetzung von digitalen Rechten und schafft Transparenz.

Citizenme

Citizenme bietet dem Nutzer die Möglichkeit, über die Preisgabe seiner personenbezogenen Daten selbst zu entscheiden. Die Daten werden über Umfragen, die mit einer Ausgleichszahlung für die Datenpreisgabe verbunden sind, erhoben. Im Vergleich zum unkontrollierbaren (und für den Nutzer meist nicht wahrnehmbaren) Datenhandel durch Unternehmen stellt dies sicherlich einen Kontrollzugewinn dar. Es muss jedoch auch hier bedacht werden, dass der Wert von personenbezogenen Daten nur schwer (wenn überhaupt) zu beziffern ist und die Gefahr einer inflationären Datenpreisgabe womöglich weiterbestehen könnte.

Datacoup

Das Geschäftsmodell des Weiterverkaufs von personenbezogenen Daten an Dritte ist transparent dargelegt. Der Nutzer erhält eine Kontrolle darüber, welche seiner sozialen Netzwerke und Kreditkarten in die Plattform eingebunden werden. Ist dies jedoch erst einmal geschehen, so ist davon auszugehen, dass die Daten von Datacoup kopiert und auf deren Server gespiegelt werden. Da beim Verkauf der Daten die Nutzungsrechte an Datacoup abgetreten werden, ist eine Rückabwicklung im Nachhinein nur schwer möglich. Somit ist der Zeitpunkt des Verkaufs entscheidend, und es muss hinterfragt werden, ob die Nutzer von der Plattform ausreichend informiert werden und sich tatsächlich der Tragweite ihrer Handlung bewusst sind. Auch wenn Daten laut Unternehmen anonymisiert weitergegeben werden, so ist dennoch der Umfang dieser Daten so enorm, dass fraglich bleibt, ob die Daten tatsächlich anonym bleiben oder vielmehr lediglich pseudo-anonym sind.

personiq (Unternehmen Emvolution)

Emvolution betrachtet die Verbesserung der Transparenz als Hauptziel seines Produkts. Die dahinterstehende Idee ist, dass mehr Kenntnis über die Datenpreisgabe eine bessere (Selbst-)Kontrolle ermöglicht. Statistiken und Diagramme sollen dem Nutzer aufzeigen, wann, wo und wieviel Daten preisgegeben werden. Grundsätzlich stellt dies eine Verbesserung der Nutzersituation dar, da ein besser informierter Nutzer weit mehr auf seine Daten achtet als ein weniger informierter.

Meeco

Meeco gibt dem Nutzer die Möglichkeit, seine Daten innerhalb des Meeco-Systems zu kontrollieren und unerwünschte Datenlecks zu vermeiden. Das System ist weitgehend transparent und bietet eine Reihe von Einstellungsoptionen. Durch die Geschlossenheit des Systems wird außerdem verhindert, dass die Nutzerdaten von Dritten unberechtigt abgeschöpft werden.

PGuard

Die Idee hinter PGuard ist die Erhöhung der Transparenz für den Nutzer und das Angebot einer Plattform zur Selbstinformation. Es ist zu hoffen, dass die Plattform eine übersichtliche Darstellung und Bewertung von einzelnen Apps ermöglichen wird. Dies ist allerdings wegen der frühen Phase des Projekts noch nicht ausreichend bewertbar.

4. Schlussbetrachtung

Die Stiftung Datenschutz hat eine Reihe von sehr unterschiedlichen Projekten und gewerblichen Angeboten verglichen. Bei einigen Initiativen wie PGuard oder auch MyPermissions steht die Nutzeraufklärung als Ziel im Vordergrund. Es wird jeweils davon ausgegangen, dass die Nutzer, wenn sie einen Einblick in die von ihnen gespeicherten personenbezogenen Daten bekommen, sie dadurch angehalten werden, ihr Surfverhalten datensparsamer zu gestalten. Eine Voraussetzung für die Nutzung solcher Ansätze besteht jedoch darin, dass die Nutzer bereits über ein Mindestmaß an Sensibilität oder auch über ein gewisses Vertrauensdefizit gegenüber der datenverarbeitenden Industrie verfügen und interessiert sind, einen Einblick in die Datenverwendung durch Dritte zu bekommen.

Andere Projekte versuchen mehr Kontrolle bei dem Umgang mit personenbezogenen Daten zu ermöglichen bzw. die Datenkontrolle zu vereinfachen. Projekte wie Citizenme und Datacoup zielen darauf ab, dass der Nutzer für diejenigen Daten, die ohnehin abgeschöpft werden, zumindest eine monetäre Kompensation erhält. Dies könnte einerseits als eine Art Resignation vor dem zunehmenden Kontrollverlust gegenüber einer massenhaften Abschöpfung von personenbezogenen Daten betrachtet werden. Andererseits könnte sich die Monetarisierung der Datenweitergabe – bei sehr pessimistischer Betrachtungsweise – zukünftig als dem Nutzer einzig noch verbleibender pragmatischer Weg erweisen, dem unkontrollierten Datenhandel zu begegnen.

Projekte wie LETsmart erscheinen zur Herstellung echter Datensouveränität sehr vielversprechend. Diese Ansätze gehen dabei den Weg, dem Nutzer eine informierte Einwilligung technisch zu ermöglichen und der „Einwilligungsüberforderung“ entgegenzuwirken. Erreicht wird dies, indem der Nutzer an einer zentralen Stelle („One-Stop-Shop“) seine Daten verwalten kann. Das beinhaltet die Möglichkeit, die Weitergabepräferenzen zu ändern oder bereits weitergegebene Daten ggf. zu löschen. Idealerweise sollte dies für mehrere Anbieter gleichzeitig möglich sein.

Zusammenfassend lässt sich feststellen, dass durch die PIMS-Ansätze viele aktuelle Probleme im Bereich der Einwilligung durchaus gelöst werden können und dass der Einsatz der „intelligenten Technik“ die Verfügungsmacht über personenbezogene Daten stärken kann. Je nachdem, auf welchen Teilaspekt oder auf welche Reihe von Schwerpunkten sich die einzelnen Projekte konzentrieren, können durch den Einsatz von automatisierten Einwilligungsverfahren auch viele Anforderungen aus der Datenschutz-Grundverordnung umgesetzt werden – so etwa „data protection by design“ (Art.25), eine informierte Einwilligung (Art.4 Abs. 11), die Zweckbindung und Datensparsamkeit (Art. 5 Abs. 1), Recht auf Datenübertragbarkeit in maschinenlesbarem Format (Art. 20 Abs. 1.) sowie die Sicherheit der Datenverarbeitung.

Viele der hier dargestellten Ansätze befinden sich noch in einer Entwicklungs-, Test- oder Implementierungsphase. Es bleibt daher abzuwarten, inwiefern sich die technischen Lösungsansätze sowohl bei den Datennehmern als auch bei den Nutzern durchsetzen werden und inwieweit die technischen Verfahren an die Anforderungen aus der EU-Datenschutz-Grundverordnung angepasst werden können. Aus der Sicht der Stiftung Datenschutz muss ein „Personal Information Management Service" jedenfalls idealerweise folgende Kriterien erfüllen:

- Eine einheitliche, zentralisierte Datenkontrolle an einer Stelle („One-Stop-Shop") soll dem Nutzer ermöglichen, seine Daten zu verwalten, bei mehreren Dienstanbietern die Weitergabepräferenzen gleichzeitig zu ändern und die geteilten Daten ggf. zu löschen.

- Das Produkt soll idealerweise folgende drei Funktionen beinhalten:
  - 1) Transparenz aufzeigen (die vom Datennehmer begehrten Datenverarbeitungs vorgänge in einer standardisierten maschinenlesbaren Einwilligungserklärung automatisch zusammenfassen);
  - 2) Transparenz vermitteln (mit Einsatz von verständlichen standardisierten Symbolen und Piktogrammen die Datenschutzerklärungen komplexitätsreduzierend vermitteln);
  - 3) eine informierte Entscheidung herbeiführen (anstatt von Opt-In- und Opt-Out-Optionen soll eine Entscheidungsnotwendigkeit gegeben sein, die Datenschutzpräferenzen zu definieren).

- Eine technische Nachverfolgbarkeit der Datenverwendung (Sticky Policies) sowie ein automatisierter Auskunftsanspruch sollen gewährleistet sein.

- Es soll die Möglichkeit beinhalten, die Preisgabe von personenbezogenen Daten je nach Kundenpräferenz granular zu gestalten, verbunden mit der Möglichkeit, die Daten selbst und den sie betreffenden Umfang der Einwilligung dynamisch zu aktualisieren.

- Das System muss einfach, aber bei Bedarf detailliert, gestaltet sein. Der Nutzer darf nicht überfordert werden. Jedoch sollten fortgeschrittene Nutzer die Möglichkeit haben, ihre Interessen über „erweiterte Einstellungen" detailliert einzustellen. Die Balance zwischen unterschiedlichen Nutzerinteressen muss gewahrt sein.

5. Allgemeine Herausforderungen

- Es muss geklärt werden, ob es Einwilligungsassistenten nur für bestimmte Segmente (soziale Netzwerke, Gesundheitsdaten, Finanzwesen etc.) geben kann oder ob universelle Assistenten für alle Bereiche des Datenumganges möglich sind. Welche Voraussetzungen müssen dafür erfüllt sein?

- Um eine möglichst große Anzahl von Nutzern zu erreichen, müssen Produkte mit einer nutzerfreundlichen Bedienung ausgestattet sein, die durch Piktogramme und Symbole ein Mindestmaß an Eindeutigkeit und Verständlichkeit der Einwilligung ermöglicht. Hierbei wird der Bedarf nach einer europaweit einheitlichen Standardisierung von Datenschutzhinweisen und Icons deutlich.
- Für Faktoren wie Vertrauen in die Plattform und Sicherheit der Daten ist der Speicherort der Daten (Cloud oder lokal) entscheidend. Einerseits könnte eine lokale Speicherung die Kompatibilität mit anderen Systemen beeinträchtigen. Andererseits kann die Cloud-Lösung Probleme bei der Datensicherheit oder beim Nutzervertrauen mit sich bringen.

- Für die technische Umsetzung muss berücksichtigt werden, wie viel Einfluss der Nutzer auf die Weitergabe seiner Daten hat und ob dynamische Anpassungsmöglichkeiten und Widerrufbarkeit gegeben sind. Aus technischer Sicht muss dabei erforscht werden, wie die Abstufung von Kundenpräferenzen ermöglicht sein muss.

- Es müssen Möglichkeiten erforscht werden, die Einwilligung an andere Personen oder Maschinen zu delegieren, wenn der Datengeber in bestimmten Situationen nicht im Stande ist, eine rechtswirksame Einwilligung zu erteilen (bedeutend insbesondere für Patienten im Gesundheits-/ E-Health-Bereich).

- Auch das Erfordernis einer eindeutigen Feststellung der Identität der datenverwendenden Stelle bedarf einer technischen Lösung. Außerdem: Was passiert bei Firmenübernahmen? Gehen Pflichten an den Käufer des Unternehmens über? Werden Daten gesperrt, wenn sich etwa das übernehmende Unternehmen nicht an den ausgehandelten Rahmen hält?

- Für adaptive Einwilligungsassistenten muss weiterhin geklärt werden, wie eine Nutzeränderung behandelt wird. Wird der alte Status (etwa eine Vorgabe „keine Daten an Werbetreibende“) in einer Historie gespeichert und wo ist diese Historie abgelegt (bei allen Datenhaltern oder in einem Archiv?), werden Änderungen sofort ausgeführt und ist dies technisch überhaupt möglich? Echtzeitaktualisierungen, gerade bei der Menge der Datensätze, könnten die Systeme überfordern. Wo werden bei verzögerter Aktualisierung Datensätze zur Aktualisierung zwischengespeichert?

- Können und sollten Datensätze und Einwilligungen von Dritten bearbeitet werden (etwa zur Korrektur von Fehlern in der Datenbank)? Oder sollte der Nutzer allein die Korrekturmöglichkeit behalten mit der Gefahr, dass seine Daten nicht fehlerfrei sind. Wer informiert ggf. dann den Nutzer über mögliche Fehler und prüft auf Datensatzvalidität?

- Kernproblem bleibt, wie Vertrauen der Nutzer in die jeweilige Plattform mit technischer Unterstützung aufgebaut werden kann. Der Einsatz solider Kryptografie kann ein Weg sein (ggf. muss hier auch schon Quantenkryptografie-Forschung miteinbezogen werden).

III. Rechtliche Aspekte von Einwilligungsassistenten[36]

Die Datenschutz-Grundverordnung schafft einen einheitlichen Rechtsrahmen und stellt Anforderungen an die Umsetzung von transparenten Systemen. In Artikel 25 Datenschutz-Grundverordnung wird der Grundsatz „Datenschutz durch Technikgestaltung“ eingeführt. Dementsprechend sind bereits bei der Entwicklung und Gestaltung von technischen Funktionen datenschutzrechtliche Anforderungen zu berücksichtigen. Im Fokus der rechtlichen Betrachtung (siehe Anhang 1.) standen daher technische Konzepte, die zum Ziel haben, Nutzer bei der Ausübung ihrer Einwilligung automatisiert zu unterstützen. Denn nicht nur der Grundsatz „Datenschutz durch Technikgestaltung“ gemäß Artikel 25 Datenschutz-Grundverordnung fordert zur Entwicklung datenschutzgerechter technischer Lösungen auf, sondern die Artikel-29-Datenschutzgruppe hat ebenso zur Vorlage technischer Mittel zur Einhaltung des Rechtsrahmens bei Cookies aufgerufen[37]. Es musste daher geklärt werden, ob die PIMS-Ansätze grundsätzlich den rechtlichen Vorgaben der ab Mai 2018 geltenden Datenschutz-Grundverordnung entsprechen können, welche Anforderungen bei der Technikgestaltung zu beachten sind und ob insgesamt im Hinblick auf die Einwilligungsvoraussetzungen der einheitliche Rechtsrahmen gewahrt wird. Hierfür mussten die Voraussetzungen an eine Einwilligung nach der Datenschutz-Grundverordnung unter Berücksichtigung der aktuellen Rechtspraxis ausgelegt werden.

1. Anforderungen an den Einwilligungsassistenten

In Bezug auf die von der Stiftung Datenschutz betrachteten technischen Systeme muss berücksichtigt werden, dass die weitere technische Ausgestaltung der Systeme und vor allem der geplante konkrete Einsatzzweck einen erheblichen Einfluss auf die Frage der rechtlichen Einstufung des Einwilligungsassistenten und ebenso der Verantwortlichkeit und Haftung nach sich zieht. Aufgrund der noch nicht näher beschriebenen und veröffentlichten technischen Details und Funktionsweise einzelner Konzepte können daher im Folgenden lediglich grundsätzliche Anforderungen an einen Einwilligungsassistenten benannt, aber keine abschließende rechtliche Beurteilung einzelner Ansätze vorgenommen werden.

Eine eindeutig bestätigende Handlung gemäß Artikel 4 Nr. 11 DSGVO wird durch den Einwilligungsassistenten dann erfüllt, wenn bereits im Voraus präzise, leicht zugänglich und verständlich sowie in klarer und einfacher Sprache ermöglicht wird, dass eine betroffene Person in unterschiedliche Verarbeitungszwecke, Empfänger oder Kategorien von Empfängern und personenbezogene Daten einwilligen kann. Es ist dabei auf die notwendige Granularität zu achten. Bei Standortdaten muss gesondert geprüft werden, wie genau die Standortbestimmung erfolgen muss. Wenn dabei die betroffene Person entsprechend der Vorgaben der Artikel-29-Datenschutzgruppe leere Kästchen mit dem jeweilig gewünschten Verarbeitungszweck ankreuzen kann, würde sogar eine ausdrückliche Einwilligung vorliegen. Dies würde wiederum der Intention der ursprünglich geplanten Datenschutz-Grundverordnung (Entwurf vom 25.01.2012) sowie der Vorgabe „Datenschutz durch Technikgestaltung“ gemäß Artikel 25 Datenschutz-Grundverordnung entsprechen. Die Erkenntnisse von P3P (Platform for Privacy Preferences Project) können bei der Umsetzung berücksichtigt werden.

36 *An dieser Stelle werden Ergebnisse der Stellungnahme zu rechtlichen Aspekten eines Einwilligungsassistenten von Prof. Dr. Anne Riechert (Stiftung Datenschutz) vorgestellt, siehe Anhang 1. Das Gutachten ist ebenfalls einzeln abrufbar unter: https://stiftungdatenschutz.org/themen/projekt-einwilligung-und-transparenz/*

37 *Artikel-29-Datenschutzgruppe, WP 171, Stellungnahme 2/2010 zur Werbung auf Basis von Behavioural Targeting, angenommen am 22. Juni 2010, S. 27.*

Im Sinne einer datenschutzgerechten Auslegung sollte weiterhin der Zweck der Datenverarbeitung ausdrücklich benannt werden, was mittels eines Einwilligungsassistenten gut realisiert werden kann. Der Kontext ist eingeschränkt und eng auszulegen. So wird die zweckgebundene Verarbeitung im Sinne von Artikel 5 Absatz 1b) DSGVO realisiert. Pauschale Einwilligungen sind dagegen unwirksam. Daher muss bei „Interessensbekundungen" eine dynamische Einwilligungsmöglichkeit gegeben sein.[38]

Konzepte wie CoMaFeDS könnten gleichwohl bei Forschungsvorhaben unterstützend eingesetzt werden. Gemäß Erwägungsgrund 33 der Datenschutz-Grundverordnung kann die betroffene Person ihre Einwilligung für bestimmte Bereiche wissenschaftlicher Forschung geben, d.h. ohne vollständige Angabe des Zwecks. Dies könnte ebenso entsprechend für die Empfänger (im Sinne von Datennehmern) gelten.

Die automatisierte Übersetzung von Datenschutzhinweisen in eine Einwilligungserklärung (z. B. in Form einer Liste, deren leere Felder der Nutzer aktivieren muss) muss im Einzelfall aus rechtlicher Sicht überprüfbar sein. Schwierigkeiten können sich beispielsweise dann ergeben, wenn in den Datenschutzhinweisen etwa die Information über vertragsrelevante Zwecke enthalten ist und daraus automatisiert eine Einwilligungserklärung generiert wird. Für vertragliche Zwecke ist jedoch keine Einwilligung erforderlich, wohl aber eine transparente Information. Soll der Einwilligungsassistent zukünftig zur Unterstützung bei Vertragsabschlüssen eingesetzt werden, müssen daher Zivilrecht und Datenschutzrecht getrennt werden. Zivilrechtlich sind übereinstimmende Willenserklärungen für das Zustandekommen eines Vertrages erforderlich, als essentialia negotii eines Kaufvertrages umfasst dies außerdem die Festlegung von Gegenstand und Vertragspartner. Aus datenschutzrechtlicher Sicht dürfen Daten ohne Einwilligung verarbeitet werden, wenn dies für vertragliche Zwecke erforderlich ist. Dennoch muss transparent über die Datenverarbeitung (etwa Verarbeitung für vertragsrelevante Zwecke) informiert werden. Bei der Gestaltung des Einwilligungsassistenten ist daher insgesamt darauf zu achten, dass diese Trennung für den Nutzer deutlich wird.

Außerdem beinhaltet die Einwilligung aus datenschutzrechtlicher Sicht stets ein Widerrufsrecht. Im Hinblick auf die Ausübung des Widerrufsrechts bieten beispielsweise Systeme wie LETsmart dem Nutzer ein Selbstmanagement an, sodass er jederzeit seine Einwilligung ändern, berichtigen und löschen kann. Damit können die Anforderungen an einen jederzeitigen Widerruf gemäß Artikel 7 Absatz 3 DSGVO erfüllt werden. Probleme, die sich im Zusammenhang mit dem Recht auf Datenübertragbarkeit (Artikel 20 DSGVO) ergeben könnten, wären damit ebenso umgangen.[39]

Die Richtigkeit der Daten (Artikel 5 Absatz 1d DSGVO) kann systemseitig erfüllt werden, wenn der Einwilligungsassistent in der Lage ist, alle Datenzugriffe zu verhindern, bei welchen Empfänger, Zweck und die konkreten personenbezogenen Daten nicht übereinstimmen. Die möglichen Empfänger erhalten den Zugriff auf die Datensätze der Nutzer ausschließlich unter der Bedingung, dass die richtige Kombination von legitimierten Empfängern und Verarbeitungszwecken vorliegt. Bei Abweichungen muss der Einwilligungsassistent zudem in der Lage sein, in dynamischer Form die Einwilligungserklärung des Nutzers einzuholen.[40]

38 Die rechtlichen Voraussetzungen einer solchen „dynamischen Einwilligung" müssen gesondert geprüft werden.

39 Davon unberührt bleibt, dass der Empfänger der Daten bei Kopie und Speicherung der Nutzerdaten in seinem eigenen System weiterhin den datenschutzrechtlichen Anforderungen unterliegt.

40 Die rechtlichen Voraussetzungen einer solchen „dynamischen Einwilligung" müssen gesondert geprüft werden.

Im Rahmen der Gestaltung des Einwilligungsassistenten muss im besonderen Maße auf das Kopplungsverbot und die freie Bestimmung durch den Betroffenen geachtet werden. Der Düsseldorfer Kreis hat die Problematik vor allem bei kostenlosen Angeboten betont. Daher müssen die Gesamtumstände berücksichtigt werden, ob die betroffene Person tatsächlich vollständig überblicken kann, für welche Marketing- und/oder Scoringzwecke die persönlichen Daten verwendet werden. Diese Selbstbestimmtheit kann im Einzelfall schwierig zu ermitteln sein. Aber je mehr Zwecke miteinander verknüpft sind oder je mehr Datenempfänger involviert sind, desto wahrscheinlicher ist die Unübersichtlichkeit für die betroffene Person.

Der Einwilligungsassistent sollte automatisiert sicherstellen, dass eine Einwilligung nicht zeitlich unbegrenzt erteilt wird, sondern entweder bei Wegfall des Verwendungszwecks Datenzugriffe automatisiert verhindert werden oder aber nach einer entsprechenden Dauer der Nutzer gefragt wird, ob er die Einwilligung aufrechterhalten möchte. In diesem Falle werden die Gebote der Speicherbegrenzung (Artikel 5 Absatz 1e) DSGVO) sowie der Datenminimierung (Artikel 5 Absatz 1c) DSGVO) erfüllt, da die betroffene Person selbst entscheidet, welche Daten über sie verarbeitet werden, indem die erteilte Einwilligungserklärung mit der Kategorie von Empfängern (im Sinne von Datennehmern) ihrem Zugriff unterliegt.

Der für die Datenverarbeitung Verantwortliche muss die Einwilligung auf informierter Basis bereitstellen. Er muss also vor Erhebung der Daten die Information bereitstellen und er muss die Einwilligung nachweisen können. Zukünftig ist jedoch zu klären, ob bei einer elektronischen Einwilligung die Voraussetzungen des Telekommunikationsgesetzes und Telemediengesetzes in Bezug auf die Protokollierung und jederzeitige Abrufbarkeit weiterhin Geltung beanspruchen. Zu berücksichtigen ist, dass die Protokollierung eine Form des Nachweises darstellen kann, aber im Sinne einer europaweiten Vereinheitlichung gegebenenfalls auch andere Methoden in Frage kommen, was zu prüfen wäre. Für die Nachweispflicht werden zukünftig Verhaltensregeln maßgeblich sein.

Zur Unterstützung einer transparenten Gestaltung der Auswahlmöglichkeiten (Zweck, Empfänger, Daten) und im Sinne einer informierten und unmissverständlichen Willensbekundung könnten bei einem Einwilligungsassistenten zusätzlich visuelle Elemente (Erwägungsgrund 58 DSGVO) verwendet werden. Bei komplexer Datenverarbeitung mit unterschiedlichen Zwecken oder Empfängern könnte jedoch auch bei Verwendung eines Einwilligungsassistenten eine intransparente Darstellung vorliegen. Artikel 5 Absatz 1a) Datenschutz-Grundverordnung fordert aber gerade die Sicherstellung der Transparenz. Hier könnte geprüft werden, inwieweit der sogenannte „One-Pager“ als transparente Zusammenfassung der erteilten Einwilligung unterstützend in Betracht kommt.[41]

In diesem Zusammenhang sind insbesondere verhaltenswissenschaftliche Erkenntnisse zu den tatsächlichen Auswirkungen der Gestaltung und Strukturierung von Datenschutzinformationen auf den Verbraucher von Bedeutung (wie sie beispielsweise durch ConPolicy untersucht werden).[42]

An dieser Stelle muss auch angemerkt werden, dass die rechtlichen Anforderungen an eine informierte Einwilligung und Einwilligungsplattformen ohne zusätzliche verhaltensökonomische Einsichten schwerlich auskommen können.

41 Siehe zum „One-Pager“ die Hinweise des Bundesministeriums der Justiz und für Verbraucherschutz unter http://www.bmjv.de/DE/Themen/FokusThemen/OnePager/OnePager_node.html.

42 http://www.conpolicy.de/referenz/einwilligung-20-entwicklung-und-validierung-von-handlungsoptionen-zur-foerderung-informierter-date/

Denn „was uns Privatheit wert ist, wird stets davon abhängen, welche Rechte auf Privatheit uns die Rechtsordnung zuweist, wie Einwilligungsoptionen dargestellt werden und wie die Anreize gesetzt sind“.[43]

Die Bereitstellung transparenter Informationen ist „allenfalls eine notwendige, aber keine hinreichende Bedingung für die akkurate Einschätzung von Datenschutzrisiken“[44] – die Emotionen und kognitiven Fähigkeiten des Nutzers sind in diesem Zusammenhang ebenso bedeutsam, wenn nicht bedeutsamer. Mit anderen Worten: Die rechtlichen Rahmenbedingungen für eine informierte Einwilligung lassen sich nur angemessen bewerten und gestalten, wenn auch die Gestaltbarkeit von Datenschutzpräferenzen und die tatsächliche Bereitschaft der Nutzer, sich mit dem Schutz der eigenen Privatsphäre aktiv auseinanderzusetzen, in den Blick genommen werden.

2. Anforderungen an ein gleichwertiges Datenschutzniveau

Entsprechend der eingangs dargestellten Zielsetzung wurde das PIMS-Konzept auf grundsätzliche Vereinbarkeit mit rechtlichen Vorgaben überprüft, um entsprechende Anforderungen an seine Umsetzung zu formulieren. Hierfür mussten die Voraussetzungen an eine Einwilligung nach der Datenschutz-Grundverordnung unter Berücksichtigung der aktuellen Rechtspraxis ausgelegt werden. Daher musste gleichermaßen – auch im Hinblick auf entsprechende Empfehlungen – eine grundsätzliche Begutachtung erfolgen. Entscheidend ist stets, wie die Intention der Datenschutz-Grundverordnung, ein gleichmäßiges und hohes Datenschutzniveau für natürliche Personen durch ein gleichwertiges Schutzniveau für die Rechte und Freiheiten von natürlichen Personen bei der Verarbeitung ihrer personenbezogenen Daten in allen Mitgliedsstaaten zu gewährleisten, zukünftig umgesetzt werden kann.

Gemäß den Ausführungen in dieser Stellungnahme ist daher insgesamt folgendes festzuhalten:
Im Sinne einer Vollharmonisierung und der Sicherstellung eines gleichwertigen Datenschutzniveaus in der Europäischen Union sollte insgesamt frühzeitig kontrolliert werden, ob eine unterschiedliche Auslegung des Wortlauts der Datenschutz-Grundverordnung durch die Mitgliedstaaten diesem Ziel entgegenstehen könnte und welche Vorgehensweise in der Praxis vertretbar ist. Einen Indikator für diese Prüfung kann die Umsetzung der Richtlinie 95/46/EG in den einzelnen Mitgliedsstaaten darstellen.

Für eine einheitliche Anwendung des Datenschutzrechts in Europa sollten die Möglichkeiten in der Datenschutz-Grundverordnung wahrgenommen und entsprechende Verhaltensregeln und/oder Leitlinien erarbeitet werden. Festgestellt wurde dies anhand der Prüfung der Einwilligungsvoraussetzungen nach der Datenschutz-Grundverordnung. Dabei sollte die Sicherstellung eines einheitlichen Wettbewerbs mit berücksichtigt werden.

Der Prozess nach Artikel 40 Datenschutz-Grundverordnung bezüglich der Erstellung europaweit geltender Verhaltensregeln könnte in zeitlicher Hinsicht langwierig sein. So müssen sich die Verhaltensregeln auf Verarbeitungstätigkeiten in mehreren Mitgliedsstaaten beziehen, und die zuständige Aufsichtsbehörde muss diese dem Europäischen Datenschutzausschuss vorlegen, bevor die Kommission erklären kann, dass diese in der Union allgemeine Gültigkeit besitzen. Daher empfiehlt sich bereits zum jetzigen Zeitpunkt die Benennung und Prüfung von Fragestellungen, die für eine auch in praktischer Hinsicht notwendige Harmonisierung des Datenschutzrechts erforderlich sind.

43 Hermstrüwer, Y., Informationelle Selbstgefährdung, Tübingen, 2016, S. 249.
44 Ebd., S. 236.

Die deutschen Aufsichtsbehörden könnten bereits zum jetzigen Zeitpunkt

- mit der Förderung der Ausarbeitung von Verhaltensregeln beginnen und außerdem klare Anforderungen im Hinblick auf die Gestaltung einer Einwilligungserklärung formulieren.[45] Hier kann sich darüber hinaus die Formulierung eines Negativkatalogs empfehlen.

Der Europäische Datenschutzausschuss könnte zukünftig

- eine Leitlinie hinsichtlich der Einwilligungskriterien formulieren. Die Formulierung von Artikel 4 Nr. 11 Datenschutz-Grundverordnung in Verbindung mit Erwägungsgrund 32 Datenschutz-Grundverordnung schließt nicht eindeutig aus, dass sich weiterhin europaweit eine unterschiedliche Praxis entwickeln könnte. Unterschiedliche Auslegungsmöglichkeiten der Einwilligung zeigen sich bislang bei Anwendung der Richtlinie 2002/58/EG (in der Fassung von 2009/136/EG) durch die Mitgliedsländer. Hier ist insgesamt unklar, ob tatsächlich eine konkludente (aber nicht im Sinne einer stillschweigenden/schweigenden) Einwilligung durch transparente Information möglich ist oder nur die Einleitung von Vertragsverletzungsverfahren versäumt wurde. Daher ist die Bildung einer einheitlichen Rechtsauffassung wichtig. Denn nur dadurch können gleichwertige Sanktionen bei einer nicht ordnungsgemäßen Datenverarbeitung umgesetzt werden.

- außerdem Leitlinien hinsichtlich der Bedingungen für Direktwerbung unter Beachtung der Überschneidungen zum Wettbewerbsrecht formulieren. Datenschutzrechtlich muss die betroffene Person eine Verarbeitungstätigkeit oder einen Zweck vernünftigerweise erwarten dürfen, aber die Datenschutz-Grundverordnung bezieht sich ebenso auf die Einwilligung „in einem Kontext“. Fraglich ist jedoch, ob dies in einem europaweiten Vergleich stets gleichbedeutend mit „ähnliche Dienstleistung“ zu verstehen ist, was in dieser Stellungnahme nicht näher geprüft werden konnte. Hier kann sich daher ein europaweit einheitliches Verständnis unter Berücksichtigung der Frage empfehlen, inwieweit als Auslegungshilfen das Kartellrecht und/oder Markenrecht heranzuziehen sind. Die Einwilligung „in einem Kontext“, aber auch die Zweckänderung gemäß Artikel 6 Absatz 4 Datenschutz-Grundverordnung bedürfen insgesamt klarer Regelungen. Die bisherigen Ausführungen der Artikel-29-Datenschutzgruppe könnten für deren Ausgestaltung herangezogen werden.

- in Bezug auf den Begriff des „Verantwortlichen“ durch eine Leitlinie klarstellen, inwieweit in Anlehnung an den Entwurf „Regulation on Privacy and Electronic Communications” vom 10.01.2017 (dort für Softwareentwickler) ein Hersteller über Mittel der Datenverarbeitung entscheiden kann.

- die Ausarbeitung von einheitlichen, europaweiten Verhaltensregeln in den genannten Bereichen fördern, soweit dies aufgrund einer Verarbeitungstätigkeit in mehreren Mitgliedsstaaten möglich ist.

Durch Initiative der Europäischen Kommission

- könnte sich ein aktueller Vergleich der Übersetzungen der Datenschutz-Grundverordnung durch die einzelnen Mitgliedsstaaten noch vor deren Inkrafttreten dahingehend empfehlen, inwieweit ein einheitliches europaweites Verständnis der Auslegung der Begriffe „explicit“, „specified“ und

45 *Siehe hierzu auch Düsseldorfer Kreis, „Orientierungshilfe zur datenschutzrechtlichen Einwilligungserklärung in Formularen“, März 2016, https://datenschutz.saarland.de/fileadmin/themen/Orientierungshilfe_zur_datenschutzrechtlichen_Einwilligung_in_Formularen.pdf*

„provide with“ besteht.[46] Dabei sollte berücksichtigt werden, ob unterschiedliche Auslegungen Auswirkung auf die Betroffenenrechte im Sinne eines einheitlichen Schutzniveaus haben könnten. Bereits in der Vergangenheit wurde der Begriff „explicit“ von den Mitgliedsstaaten im Hinblick auf die Zweckbestimmung unterschiedlich übersetzt.

Die deutsche Politik und Gesetzgebung

- sollte in Bezug auf die Einwilligung die Verpflichtung zur Protokollierung und jederzeitigen Abrufbarkeit prüfen. Die Protokollierung kann eine Form des Nachweises sein, aber zu prüfen wäre, ob es weitere Möglichkeiten gibt und welche Anforderungen dazu vorliegen sollten. In diesem Zusammenhang sollte gemäß Artikel 95 Datenschutz-Grundverordnung in Verbindung mit der Richtlinie 2002/58/EG auch klargestellt werden, was unter zusätzlichen Pflichten zu verstehen ist (z. B. „jederzeitige Abrufbarkeit“ und „Protokollierung“ oder in Bezug auf Standortdaten „ausdrücklich, gesondert und schriftlich“). Darüber hinaus sollte darauf hingewirkt werden, auf europäischer Ebene einheitliche Verhaltensregeln auszuarbeiten, soweit dies aufgrund einer Verarbeitungstätigkeit in mehreren Mitgliedsstaaten möglich ist.

- könnte prüfen, inwieweit eine Erweiterung des Produkthaftungsgesetzes in Bezug auf die Sicherstellung des Persönlichkeitsschutzes in Betracht kommen kann. Kann sich auch hier im Laufe der Zeit eine Schmerzensgeldtabelle entsprechend der Verletzung bei Körperschäden herausbilden?

- könnte prüfen, inwieweit eine Bildungsoffensive hinsichtlich der zunehmenden technologischen Entwicklung im Datenschutz gestartet werden sollte.

Die Wirtschaft und Wissenschaft

- sollten bei neuen Technologien generische Datenschutz-Folgenabschätzungen gemeinsam entwickeln. Diese können gleichermaßen eine Grundlage für die konkreten Datenschutz-Folgenabschätzungen der Datenschutz-Grundverordnung darstellen.

Die Entwickler

- müssen bei der Gestaltung des Einwilligungsassistenten, der im Rahmen eines zivilrechtlichen Vertragsabschlusses eingesetzt wird, darauf achten, dass für den Nutzer nicht der Eindruck entsteht, er würde nun ebenso seine datenschutzrechtliche Einwilligung für vertragsrelevante Zwecke erteilen. Aus datenschutzrechtlicher Sicht bedarf es keiner Einwilligung für Zwecke, die für die Vertragserfüllung erforderlich sind. Gleichwohl muss der Nutzer transparent über diese Zwecke informiert werden. Zivilrecht und Datenschutzrecht müssen getrennt werden und diese Trennung muss transparent sein.

46 *Vgl. hierzu auch die Studie zur Umsetzung der Richtlinie 95/46/EG unter http://ec.europa.eu/justice/policies/privacy/docs/lawreport/consultation/technical-annex_en.pdf („Analysis and impact study on the implementation of Directive EC 95/46 in Member States“) sowie Artikel-29-Datenschutzgruppe, „Opinion 03/2013 on purpose limitation“, WP 203, adopted on 2 April 2013.*

- sollten außerdem die Anregungen der Artikel-29-Datenschutzgruppe zur Ausgestaltung technischer Systeme zur „Einwilligung in Cookies“ in ihre Überlegungen einbeziehen und prüfen, ob ihr Konzept entsprechend erweitert werden könnte – immer unter der Maßgabe, dass bei Third-Party-Cookies die vorherige Einwilligung erforderlich ist.

- sollten ihre Konzepte zudem dahingehend analysieren, ob eine Kombination mit bereits bestehenden Diensten und Funktionen, wie sie beispielsweise „MyData“ oder „digi.me“ bieten, möglich und sinnvoll sein könnte.[47]

- sollten sich frühzeitig überlegen, ob ein dezentrales oder zentrales System in Betracht kommt:

- Bei zentraler Datenspeicherung mit Zugriffsmöglichkeiten von unterschiedlichen Empfängern ist vor allem an die Sicherheit des „Wissensgraphen“ (CoMaFeDS) zu denken und die Frage entscheidend, wer Verantwortlicher dieses „Wissensgraphen“ ist und ob sowie in welcher Form diesbezüglich eine zusätzliche Einwilligung des Nutzers vorliegen muss. Für eine solche zentrale Plattform empfiehlt sich eine Zertifizierung, da ein Nutzer die technischen Voraussetzungen, die technische Sicherheit und die Vorgehensweise einer Datenverarbeitung nicht überblicken kann. Gemäß dem aktuellen Entwicklungsstand enthält die Plattform selbst keine Datensätze, sondern nur das (verschlüsselte) Wissen, wo diese zu finden sind. Ein Nutzer muss jedoch die Gewissheit haben, dass die Verschlüsselung ausreichend sowie seine Anonymität gegenüber potenziellen Empfängern gewahrt ist und keine Verknüpfungsmöglichkeiten bestehen, insbesondere da diese Plattform großes Potenzial für Big Data-Anwendungen bietet.

- Bei dezentraler Speicherung und der Verantwortung des Nutzers für das System bzw. die Software stellt sich in gleichem Maße die Frage nach Sicherheit und Zertifizierung sowie nach der Verantwortung der Hersteller/Entwickler. Die Datenschutzaufsichtsbehörden könnten auch hier auf Erklärungen der Industrie hinwirken, dass diese als Hersteller ebenso als datenschutzrechtliche Ansprechpartner agieren (siehe gemeinsame Erklärung mit dem Verband der Automobilindustrie). Dies gilt unter der Maßgabe, dass Hersteller zwar angehalten sind, datenschutzgerechte Technik zu entwickeln, aber ohne konkrete rechtliche Verantwortlichkeit, da ungeklärt ist, inwieweit ein Hersteller als „Verantwortlicher“ im Sinne der Verordnung eingeordnet werden kann, wenn er Mittel der Verarbeitung bereit stellt.

Entscheidend ist stets, wie die Intention der Datenschutz-Grundverordnung, ein gleichmäßiges und hohes Datenschutzniveau für natürliche Personen durch ein gleichwertiges Schutzniveau für die Rechte und Freiheiten von natürlichen Personen bei der Verarbeitung ihrer personenbezogenen Daten in allen Mitgliedsstaaten zu gewährleisten, zukünftig umgesetzt werden kann. In diesem Zusammenhang ist besonders an einheitliche Verhaltensregeln oder Leitlinien zu denken. Bei der praktischen Umsetzung kann jedoch ein Einwilligungsassistent, der granulare und aktive Elemente der Einwilligung bietet, aufgrund einer transparenten Gestaltungsmöglichkeit zum Schutzniveau beitragen. Der Nutzer hat mehr Selbstbestimmungsmöglichkeiten, da Daten direkt bei ihm, mit seiner aktiven Beteiligung und zeitlich befristet erhoben werden können. Allerdings ist die technische Fortentwicklung vor dem Hintergrund einer „automatisierten Entscheidungsfindung“, den Möglichkeiten des Profiling und einer Zweckänderung stets kritisch zu prüfen.

47 *Siehe oben, II. 2. „Darstellung der im Projekt betrachteten Ansätze“.*

3. Klärungsbedarf

- Die Entwickler sollten sich frühzeitig überlegen, ob ein dezentrales oder zentrales System in Betracht kommt. Bei zentraler Datenspeicherung mit Zugriffsmöglichkeiten von unterschiedlichen Empfängern ist vor allem an die IT-Sicherheit zu denken und die Frage entscheidend, wer Verantwortlicher für die Daten ist und ob sowie in welcher Form diesbezüglich eine zusätzliche Einwilligung des Nutzers vorliegen muss. Bei dezentraler Speicherung und der Verantwortung des Nutzers für das System bzw. die Software stellt sich in gleichem Maße die Frage nach Sicherheit und nach der Verantwortung der Hersteller/Entwickler.

- In Bezug auf das Kopplungsverbot muss gefragt werden, wie der Einwilligungsassistent gestaltet sein muss, sodass die betroffene Person frei zwischen unterschiedlichen Daten, Zwecken und Empfängern wählen kann, ohne dass ihr bei Nicht-Einwilligung in einzelne Verarbeitungstatbestände Nachteile entstehen. Die Einwilligung darf in diesem Zusammenhang nicht irreführend sein. Der Einsatz eines solchen Assistenten kann eine Unterstützung für die betroffene Person darstellen, wenn er die Datenverarbeitung übersichtlich auflistet und die betroffene Person sich zwischen den Verarbeitungstatbeständen frei entscheiden kann. Es darf außerdem bei Verwendung eines Einwilligungsassistenten nicht der Eindruck entstehen, dass damit die Datenverarbeitung abschließend abgedeckt wäre, wenn beispielsweise darüber hinaus eine Verarbeitung aufgrund berechtigter Interessen geplant ist.

- In Bezug auf den Nachweis der Einwilligung muss gemäß Artikel 95 Datenschutz-Grundverordnung in Verbindung mit der Richtlinie 2002/58/EG klargestellt werden, was unter „zusätzlichen Pflichten“ zu verstehen ist und welche eigenständigen gesetzlichen Regelungen der Mitgliedsstaaten einer Vollharmonisierung (dennoch) entsprechen (z. B. jederzeitige Abrufbarkeit und Protokollierung oder in Bezug auf Standortdaten: „ausdrücklich, gesondert und schriftlich“). Genauso muss geklärt werden, ob sich der Begriff „zusätzliche Pflichten“ sowohl auf die betroffene Person als auch auf den Verantwortlichen bezieht.

- Es ist zu klären, ob bei einer elektronischen Einwilligung die Voraussetzungen von Telekommunikationsgesetz und Telemediengesetz in Bezug auf die Protokollierung und jederzeitige Abrufbarkeit weiterhin Geltung beanspruchen. Für die Nachweispflicht werden zukünftig Verhaltensregeln maßgeblich sein. Zu berücksichtigen ist auch hier, dass die Protokollierung eine Form des Nachweises darstellen kann, aber im Sinne einer europaweiten Vereinheitlichung gegebenenfalls auch andere Methoden in Frage kommen, was zu prüfen wäre.

- Eine pauschale Einwilligung ist unwirksam. Entwickler könnten zwar die Möglichkeit einer „pauschalen Interessensbekundung“ prüfen. Bei der Umsetzung in Bezug auf einen konkreten Anbieter kann eine Einwilligung jedoch nur dann „für den bestimmten Fall informiert“ erfolgen, wenn keine Daten übermittelt oder bekanntgegeben werden, sondern der Nutzer im Einzelfall eine automatisierte Rückmeldung seitens des Systems erhält, auf deren Grundlage er sich frei entscheiden kann, und er sich (ebenso) mit einer solchen Vorgehensweise zuvor einverstanden erklärt hat.

- In den Informationspflichten muss über die Dauer der Einwilligung transparent informiert werden (Artikel 13 DSGVO). Es muss von Entwicklerseite geprüft werden, inwiefern sichergestellt werden kann, dass die Einwilligung nach einer gewissen Zeit überprüft werden kann oder dass die Einwilligung nur einmalig gilt. Es sollte entwicklerseitig geprüft werden, ob automatisiert nach einer gewissen Zeitspanne oder regelmäßig eine Information der Nutzer über die erteilten Einwilligungen erfolgt, gekoppelt mit der Bereitstellung einer einfachen Widerrufsmöglichkeit.

- Die Hersteller sind zwar angehalten, datenschutzgerechte Technik zu entwickeln, aber ohne konkrete rechtliche Verantwortlichkeit, da ungeklärt ist, inwieweit ein Hersteller als „Verantwortlicher“ im Sinne der Verordnung eingeordnet werden kann, wenn er Mittel der Verarbeitung bereitstellt. Daher stellt sich die Frage nach Sicherheit und der Verantwortung der Hersteller/Entwickler. Die Datenschutzaufsichtsbehörden könnten auch hier auf Erklärungen der Industrie hinwirken, dass diese als Hersteller gleichermaßen als datenschutzrechtliche Ansprechpartner agieren (siehe gemeinsame Erklärung mit dem Verband der Automobilindustrie). Darüber hinaus könnte in Anlehnung an den Entwurf „Regulation on Privacy and Electronic Communications” vom 10.01.2017 (dort für Softwareentwickler) geprüft werden, inwieweit ein Hersteller über Mittel der Datenverarbeitung entscheiden kann.

- Zu klären ist, inwieweit zukünftig die Installation einer Software im Rahmen eines Einwilligungsassistenten oder dessen technische Fortentwicklung als eigener Online-Dienst eingestuft werden kann, sodass der Empfänger der Daten zum Anbieter und damit ebenso zum Verantwortlichen für den Einwilligungsassistenten im Sinne eines Dienstanbieters (etwa Dienst der Informationsgesellschaft oder Dienst mit Zusatznutzen) wird. Die rechtliche Einordnung des Dienstes hängt maßgeblich auch von den geplanten Funktionen und von dem Verwendungszweck ab.

- Zukünftig kann sich außerdem die Frage stellen, ob der Einwilligungsassistent nicht bereits als solcher die Voraussetzungen des Artikels 22 DSGVO erfüllen muss.[48] Für einen Einwilligungsassistenten, der automatisiert Entscheidungen trifft, bedeutet dies: Entweder es muss zuvor ein Vertrag für die „Anwendung des Einwilligungsassistenten an sich“ zwischen Nutzer und Verantwortlichen abgeschlossen werden, der klar regelt, welche Funktionen der Einwilligungsassistent erfüllen soll. Dann wäre die automatisierte Entscheidungsfindung zur Vertragserfüllung erforderlich. Oder es ist für die Nutzung des Einwilligungsassistenten die ausdrückliche Einwilligung des Nutzers einzuholen. Hier ist wiederum entscheidend, ob dies auf informierter Basis und in Kenntnis der Sachlage für eine genau umrissene Situation umsetzbar ist.

- Insgesamt bleibt bei der Anwendbarkeit des Artikel 22 DSGVO vorab die Frage offen, wie die Regelung auszulegen ist, dass eine betroffene Person das Recht hat, nicht einer ausschließlich auf einer automatisierten Verarbeitung beruhenden Entscheidung unterworfen zu werden. Sofern der Nutzer weiterhin selbst die Möglichkeit hat, bei der Nutzung des Einwilligungsassistenten konkrete Vorgaben zu machen, könnte das Merkmal der „Ausschließlichkeit“ hier entfallen.

- Nicht zuletzt bleibt auch die Frage, ob die PIMS den Verbrauchern das notwendige Grundlagenwissen über die Datenverarbeitung vermitteln können, um ansatzweise die Konsequenzen der Datenpreisgabe zu antizipieren.[49] Eine der wesentlichen Aufgaben bestünde dabei darin, die Komplexität der

48 Die rechtliche Stellungnahme der Studie geht davon aus, dass der Einwilligungsassistent im Sinne der granularen Vorgaben einer betroffenen Person die erteilte Einwilligung umsetzt. Das System wird nicht selbstlernend verwendet und trifft darauf basierend keine eigenen Entscheidungen.

49 Hermstrüwer, Y., Informationelle Selbstgefährdung, Tübingen, 2016, S. 237.

Regelungsinhalte von Datenschutzerklärungen so zu verringern, dass die tatsächlich entscheidungsrelevanten Informationen wahrgenommen werden, die bereitgestellten Informationen aufgrund des vereinfachten Darstellungsformates aber nicht als unerheblich abgetan werden.[50]

IV. Ökonomische und verbraucherpolitische Herausforderungen[51]

1. Ökonomische Rahmenbedingungen innovativer Lösungen zu Datenschutz-Einwilligungen

Hauptziel des ökonomischen Gutachtens war es, eine Taxonomie zu entwickeln, die einen Überblick über die Akteure im „Ökosystem" des innovativen Einwilligungsmanagements ermöglicht, sowie Marktdynamiken und förderliche ökonomische Rahmenbedingungen zu erörtern. Hierbei sollten insbesondere solche Projekte einbezogen werden, deren Hauptzweck oder -aktivität das selbstbestimmte Einwilligungsmanagement ist. Die Innovationsleistung durch technisches Einwilligungsmanagement bildet zugleich ihren Mehrwert. Es geht also grundsätzlich um Angebote, die das Erschließen, die Nutzung und Weitergabe von personenbezogenen Daten durch bzw. unter Kontrolle von Verbrauchern (Nutzern) erlauben.

Zum „Ökosystem" gehören hierbei neben Regierungs- und Standardisierungsinitiativen auch Forschungsprojekte sowie gewinnorientiert und sozialorientiert arbeitende Unternehmen. Insgesamt sollten dies international im Zeitraum von 2014-2015 rund 400 Unternehmen sein, schätzt die britische Unternehmensberatung Ctrl-Shift.[52]

Zunächst lassen sich anbieterzentrierte Intermediationsplattformen mit und ohne direkte Kundenbeziehung von nutzerzentrierten Intermediationsplattformen unterscheiden. Hauptunterschied ist, dass bei letzteren der Nutzer eigenverantwortlich das Einwilligungsmanagement übernimmt. In vielen der angestammten Intermediationsformen (z. B. Direktmarketing, Kreditauskünfte) spielt der Nutzer keine sehr aktive Rolle oder unterhält keine direkte Beziehung zum Unternehmen, welches die Daten aggregiert.

Innerhalb der nutzerzentrierten Plattformen gibt es eine Vielfalt von Geschäftsmodellen; bei den meisten handelt es sich allerdings um zwei- oder mehrseitige Plattformen, die Datenanbieter (Nutzer) und Datennachfrager (Unternehmen, App-Entwickler, Forscher) zusammenführen. Viele der PIMS bieten mehrere Dienste an, darunter Einwilligungsassistenz, Übersichtsfunktionen, Suchfunktionen, Marktplatzfunktionalitäten oder Präferenzangaben (sog. intent casting).

Auf der obersten Ebene lassen sich die Unternehmen in Hub-Modelle und verteilte Systeme gliedern. Hub-Modelle speichern Nutzerdaten unter Inanspruchnahme von Cloud-Lösungen (privat/öffentlich),

50 Ebd., S. 312.

51 Dieser Abschnitt stellt die Zusammenfassung des von der Stiftung Datenschutz in Auftrag gegebenen gleichnamigen Gutachtens von Dr. Nicola Jentzsch dar (Deutsches Institut für Wirtschaftsforschung). Siehe unten, Anhang 2. Das Gutachten ist ebenfalls einzeln abrufbar unter: https://stiftungdatenschutz.org/themen/projekt-einwilligung-und-transparenz/

52 Jentzsch, N. (2015). Horizontal and Vertical Analysis of Privacy and Cyber-Security Markets, IPACSO - Innovation Framework for ICT Security Deliverable, No. 4.2 A, https://www.econstor.eu/handle/10419/126224

Datencentern oder hybrider Lösungen. Architektonisch gesehen, können die Datensätze zentral beim Anbieter oder dezentral beim jeweiligen Nutzer abgespeichert werden. Verteilte Systeme hingegen speichern die Daten in Blockchain-Anwendungen oder Abwandlungen derselben.

Die Erlösmodelle unterscheiden sich ebenfalls von Unternehmen zu Unternehmen. Während manche Plattformen transaktionsbasierte Gebühren verlangen, verfolgen andere Abonnement- oder Lizenzierungsansätze.

Plattformen sind durch direkte und insbesondere indirekte Netzwerkeffekte gekennzeichnet. Direkte Netzwerkeffekte entstehen auf derselben Marktseite, insbesondere dann, wenn ein Nutzenzuwachs aus der Nutzung des Dienstes durch andere entsteht. Bei PIMS könnte das, gegenüber der Nutzung anderer Technologien, ein sicherer Datenaustausch mit anderen PIMS-Nutzern sein gegenüber der Nutzung anderer Technologien.[53] Indirekte Netzwerkeffekte entstehen aus seitenübergreifenden Einflüssen, wenn beispielsweise mehr Unternehmen Daten abfragen, weil mehr Nutzer sie anbieten, und sich so die Wahrscheinlichkeit eines „guten Datendeals“ für Nutzer erhöht (sog. Liquidität).

Die Plattformen befinden sich in einem herausfordernden Wettbewerbsumfeld: sie müssen mindestens zwei Kundengruppen (Datenanbieter und -nachfrager) gleichzeitig anziehen. Viele der Plattformen stellen sich als „Ökosysteme“ dar, die mehrere Nutzergruppen zusammenbringen wollen. Bei den Nutzern müssen Vertrauensschwellen überwunden werden, und sie müssen bereit sein, sich aktiv am Einwilligungsmanagement zu beteiligen. Dies kann allerdings nur durch glaubwürdige technische sowie protokollarische Ende-zu-Ende-Sicherheit gelingen.

PIMS müssen sich auf der einen Seite gegen akademische Gratisangebote durchsetzen (z. B. MyDataCan oder OpenPDS). Zum anderen müssten sie sich gegen traditionelle Informationsintermediation behaupten, um mehr Datennachfrage zu generieren. Gerade die großen Konzerne können ebenfalls jederzeit in den Markt des innovativen Einwilligungsmanagements eintreten.[54]

Um sich am Markt durchzusetzen, müssen die PIMS einen deutlichen Mehrwert in der Datenaggregation generieren und bestenfalls Echtzeitdaten abbilden. Datenbasis und Datenqualität werden hier zum Schlüsselfaktor, wenn die Plattformen sich in der Informationsintermediation durchsetzen. Es kann pro Nutzer zwar eine größere Datentiefe erreicht werden, Dynamiken in der Selbstselektion und bei der Informationsoffenlegung auf der Plattform können aber zu Verzerrungen der Informationsbasis führen.

Für Unternehmen, welche PIMS nutzen wollen, ergeben sich zum einen komplexe Umorganisations- und Standardisierungsprozesse durch die neuen Datenmanagement-Architekturen, inklusive potenzieller Initiativen der Datenrückgabe (sog. share back). Gleichzeitig ermöglichen PIMS potenziell eine Zulieferung und Just-in-time-Integration von Echtzeit-Kundeninformationen in die Produktionsprozesse. Eine Automatisierung der Einwilligungsprozesse durch maschinenlesbare Einwilligungserklärungen birgt außerdem große Einsparpotenziale.

Insgesamt lässt sich festhalten, dass eine signifikante Masse von Kunden und Unternehmen sich umorientieren muss, damit diese Plattformen langfristig rentabel sind.

53 Für ein entsprechendes Beispiel sei der Leser auf die Darstellung der persönlichen Clouds verwiesen: Reed, D., Why Personal Clouds Needs a Network, Presentation – Personal Cloud Community Meetup (2013-01-29), http://www.slideshare.net/evanwolf/respect-networkpcloudmeetup20130129

54 Auch wenn viele dieser Offerten nicht die vollständige Datenhoheit den Kunden überantworten, erlauben sie erhöhte Kontrollmöglichkeiten. Beispiele hierfür sind Oracle Data Cloud Registry (BlueKai & Datalogix Cookies), Google Dashboard und Take-out, sowie Facebooks „App Settings“.

2. Verhaltensökonomische Herausforderungen am Beispiel der Einwilligung

Die Einwilligung ist der Ausdruck der Willenserklärung zur Informationspreisgabe eines Verbrauchers im vertraglichen Verhältnis. In vielen der heutzutage abgewickelten Transaktionen setzt sich der Verbraucher allerdings nicht aktiv mit der Einwilligung auseinander. Viele der Entscheidungen der Informationspreisgabe beispielsweise bei Einkäufen online lassen sich als unterbewusste Affektentscheidungen charakterisieren und nicht als bewusste und konkrete Kosten-Nutzen-Kalküle. Außerdem ist der Verbraucher weder mit einem Preis für sein Datenprofil konfrontiert noch mit den Einkünften, welche Dritte mit diesem Datenprofil erwirtschaften.[55]

Es wird eine der wichtigsten Herausforderungen für PIMS sein, Entscheidungsarchitekturen so zu designen, dass konstatierte Präferenzen der Verbraucher für Privatsphäre (sog. stated preferences) mit tatsächlichen Wahlhandlungen (sog. revealed preferences) stärker konvergieren. Es ist daher wichtig zu klären, welche Faktoren die Entscheidung beeinflussen, sich über die Datenverarbeitung zu informieren und die Einwilligung von diesen Informationen abhängig zu machen. Die rechtspolitischen Vorschläge sollten künftig im Hinblick auf ihre praktische Geeignetheit auch im Lichte von empirischen Erkenntnissen aus der Verhaltensforschung geprüft werden.

Verbraucher werden sich nur für PIMS entscheiden, wenn deren Nutzen den Aufwand ihrer Nutzung übersteigt. Ihr Mehrwert wird sich aber nicht allein auf Einwilligungsmanagement begründen. Grund ist, dass es sehr schwierig ist, Nutzer dazu zu bewegen, Zeit, kognitiven Aufwand und Geld in etwas zu investieren, das vorher „umsonst“ war oder „praktisch nebenbei“ ablief.

Künftig sollen die neuen Plattformen es Nutzern erlauben, die Privatsphären- und Vertrauenseinstellungen ihrer Anwendungen optimal ihren Präferenzen anzupassen. Es besteht also das Potenzial die Entscheidungsoptionen in der Datenverarbeitung zu verbessern, vor allem wenn die neuen Anbieter Erkenntnisse aus der Verhaltensökonomie ins Entscheidungsdesign einbeziehen.[56] Hierzu gehören Effekte wie Status quo-Akzeptanz, Entscheidungskomplexität und Verlustaversion, um nur einige zu nennen, die erheblich die Entscheidung des Verbrauchers verzerren können.[57] Die Anwendung solcher und ähnlicher Erkenntnisse aus der ökonomischen Wirtschaftsforschung wird insbesondere dann unabdingbar sein, wenn Marktmechanismen aufgesetzt werden sollen.

55 Es unterscheidet sich von Markt zu Markt, ob Daten in personalisierter Form (mit Klarnamen) gehandelt werden oder ob eine Aggregation von Datensubjekten in Mikrogruppen stattfindet.

56 Siehe dazu: „Die persönliche Datenökonomie: Plattformen, Datentresore und persönliche Clouds“, Dr. Nicola Jentzsch, Deutsches Institut für Wirtschaftsforschung (DIW Berlin), Anhang 2. https://stiftungdatenschutz.org/themen/projekt-einwilligung-und-transparenz/

57 Abweichungen vom optimalen Verhalten (z. B. Maximierung des erwarteten Nutzens) werden als Verzerrungen bezeichnet.

3. Klärungsbedürftige Punkte

- Da die Aggregation persönlicher Daten und Auswertungen derselben Privatsphären-Bedenken hervorrufen können, müssen Plattformen zunächst eine Vertrauensschwelle beim Nutzer überwinden. Hier stellt sich die Frage nach einem optimalen Mix aus Entscheidungsdesign, sowie protokollarischer und technischer Sicherheit.

- Um sich am Markt durchsetzen zu können, muss eine Plattform Nutzer, die ihre Daten einlegen, und Unternehmen, welche die Daten abfragen, möglichst gleichzeitig anbinden. Der Nutzen für die Kundengruppen hängt indirekt voneinander ab, was ein mehrseitiges Start-up-Problem generieren kann.

- Unter Umständen ergeben sich direkt Interessenskonflikte zwischen Nutzern und abfragenden Unternehmen. Dies passiert dann, wenn Kunden die Zweckbindung klar definieren und bestimmte Datenauswertungen unterbinden, an welchen Unternehmen ein großes Interesse haben. So könnte ein Kunde Produktpersonalisierung erlauben, aber die Schätzung von Zahlungswilligkeit durch das Unternehmen aufgrund der Daten untersagen.

- Es stellt sich die Frage, ob PIMS-Märkte von einer hohen Anzahl an Exklusivnutzern geprägt sein werden oder ob Nutzer das sogenannte Multihoming betreiben, also Daten auf mehreren Plattformen einstellen.

- Standardisierung ist eine wichtige Grundlage für das Funktionieren dieser neuen Plattformen und es stellt sich hier, wie auch im Bereich der Interoperabilität, die Frage, welche Standards angewandt werden sollten.[58]

- Ein direkter Verkauf im Zuge der Monetarisierung von persönlichen Informationen würde die Frage implizieren, welchen Mechanismus Marktparteien nutzen sollten, um einen Preis für die persönlichen Daten zu setzen. Dies ist insbesondere von großer Bedeutung für Plattformen, die durch eine Verkaufs- bzw. Marktplatzfunktion Nutzer anlocken wollen und/oder über Transaktionsgebühren Einnahmen generieren wollen.

- Unraveling – die Datenpreisgabe aufgrund des Selbstinteresses der Datensubjekte – kann über die entstehenden Privatsphären-Externalitäten alle erfassen.[59] Während Verbraucher mit einem guten track record (Sportlichkeit, Kreditwürdigkeit, etc.) Anreize zur Preisgabe haben, könnten Verbraucher, welche Informationen nicht aktiv preisgeben wollen, negative Erwartungen auf Seiten der Unternehmen wecken. Der Unraveling-Prozess wirft ethische und normative Fragen der Verteilung und der Fairness auf, die nur durch eine breite politische und gesellschaftliche Diskussion beantwortet werden können.

58 *Zu den Protokollen des sicheren Datenaustausches gehören bspw. das XDI-Protokoll (http://xdi.org/).*

59 *Peppet, S.R., Northwestern University Law Review 105, Unraveling Privacy: The Personal Prospectus and the Threat of a Full-Disclosure Future, 2011, S. 1153-1204.*

V. Handlungsempfehlungen

1. Politik und Praxis

Die deutschen Aufsichtsbehörden sollten bereits zum jetzigen Zeitpunkt

- für das Thema „automatisierte Einwilligungsverfahren und Einwilligungsassistenten“ sensibilisiert werden und in einen sektorübergreifenden, internationalen Diskurs eintreten.

- mit der Förderung der Ausarbeitung von Verhaltensregeln beginnen und außerdem klare Anforderungen im Hinblick auf die Gestaltung einer Einwilligungserklärung formulieren.[60] Hier kann sich auch die Formulierung eines Negativkatalogs empfehlen.

Der Europäische Datenschutzausschuss sollte

- aufgrund der in der Vergangenheit erfolgten unterschiedlichen Auslegung durch die Mitgliedsstaaten und Aufsichtsbehörden, zukünftig Leitlinien hinsichtlich der Einwilligungskriterien formulieren, um die einheitliche Anwendung der Datenschutz-Grundverordnung sicherzustellen. Auch wenn für die Einwilligung eine sanktionsbehaftete Nachweispflicht besteht, sollte einheitlich und europaweit sichergestellt sein, dass identische Kriterien gelten.

- Leitlinien aufstellen, inwieweit als Auslegungshilfen das Kartellrecht oder Markenrecht heranzuziehen sind. Bei Direktwerbung können sich im Rahmen der Datenverarbeitung Überschneidungen zum Wettbewerbsrecht ergeben. Datenschutzrechtlich muss die betroffene Person Verarbeitungstätigkeit oder deren Zweck vernünftigerweise erwarten dürfen, aber die Datenschutz-Grundverordnung bezieht sich ebenso auf die Einwilligung „in einem Kontext“. Fraglich ist jedoch, ob dies in einem europaweiten Vergleich stets gleichbedeutend mit „ähnliche Dienstleistung“ zu verstehen ist, was in dieser Studie nicht näher geprüft werden konnte.

- in Bezug auf den Begriff des „Verantwortlichen“ durch eine Leitlinie klarstellen, inwieweit in Anlehnung an den Entwurf „Regulation on Privacy and Electronic Communications” vom 10.01.2017 (dort für Softwareentwickler) ein Hersteller über Mittel der Datenverarbeitung entscheiden kann.

- die Ausarbeitung von einheitlichen, europaweiten Verhaltensregeln in den genannten Bereichen fördern, soweit dies aufgrund einer Verarbeitungstätigkeit in mehreren Mitgliedsstaaten möglich ist.

60 *Siehe hierzu auch: Düsseldorfer Kreis, Orientierungshilfe zur datenschutzrechtlichen Einwilligungserklärung in Formularen, 2016.*

Die Europäische Kommission sollte

- noch vor Inkrafttreten der Datenschutz-Grundverordnung eine Prüfung dahingehend initiieren, inwieweit im Rahmen der sprachlichen Übersetzungen durch die Mitgliedsstaaten ein einheitliches, europaweites Verständnis der Auslegung von „explicit", „specified" und „provide with" besteht und inwiefern dies Auswirkungen auf die Betroffenenrechte haben könnte. Bereits in der Vergangenheit wurde der Begriff „explicit" von den Mitgliedsstaaten im Hinblick auf die Zwecke unterschiedlich übersetzt.[61]

- im Sinne einer Vollharmonisierung und der Sicherstellung eines gleichwertigen Datenschutzniveaus in der Europäischen Union insgesamt frühzeitig kontrollieren, welche Auslegung des Wortlauts der Datenschutz-Grundverordnung durch die Mitgliedsstaaten diesem Ziel entgegenstehen könnte und welche Vorgehensweise in der Praxis vertretbar ist. Einen Indikator für diese Prüfung kann die Umsetzung der Richtlinie 95/46/EG in den einzelnen Mitgliedsstaaten darstellen.

Die deutsche Politik und Gesetzgebung sollte prüfen

- inwieweit eine Erweiterung des Produkthaftungsgesetzes in Bezug auf die Sicherstellung des Persönlichkeitsschutzes in Betracht kommen kann und ob sich auch hier im Laufe der Zeit eine Schmerzensgeldtabelle entsprechend der Verletzung bei Körperschäden herausbilden könnte.

- inwieweit eine Verpflichtung zur Protokollierung und jederzeitige Abrufbarkeit geprüft werden kann. Die Protokollierung kann eine Form des Nachweises sein, aber zu prüfen wäre, ob es weitere Möglichkeiten gibt und welche Anforderungen dazu vorliegen sollten. In diesem Zusammenhang sollte gemäß Artikel 95 DSGVO in Verbindung mit der Richtlinie 2002/58/EG auch klargestellt werden, was unter zusätzlichen Pflichten zu verstehen ist (z. B. „jederzeitige Abrufbarkeit" und „Protokollierung" oder in Bezug auf Standortdaten „ausdrücklich, gesondert und schriftlich"). Darüber hinaus sollte darauf hingewirkt werden, auf europäischer Ebene einheitliche Verhaltensregeln auszuarbeiten, soweit dies aufgrund einer Verarbeitungstätigkeit in mehreren Mitgliedsstaaten möglich ist.

Die Mitgliedsstaaten, die Datenschutzaufsichtsbehörden und der Europäische Datenschutzausschuss sollten

- die Einführung von datenschutzspezifischen Zertifizierungsverfahren und Datenschutzsiegeln fördern. Bei zentraler Datenspeicherung mit Zugriffsmöglichkeiten von unterschiedlichen Empfängern ist die Frage entscheidend, wer Verantwortlicher ist , ob diesbezüglich eine zusätzliche Einwilligung des Nutzers vorliegen muss und wenn ja, in welcher Form. Für eine solche zentrale Plattform empfiehlt sich eine Zertifizierung, da ein Nutzer die technischen Voraussetzungen, technische Sicherheit und die Vorgehensweise einer Datenverarbeitung nicht überblicken kann. Bei dezentraler Speicherung und der Verantwortung des Nutzers für das System bzw. die Software stellt sich in gleichem Maße die Frage nach Sicherheit und Zertifizierung als auch nach der Verantwortung der Hersteller/Entwickler. Die Datenschutzaufsichtsbehörden könnten auch hier auf Erklärungen der Industrie hinwirken, in denen diese sicherstellen, dass sie als Hersteller auch die datenschutzrechtlichen Ansprechpartner sind.

61 *Vgl. hierzu auch die Studie zur Umsetzung der Richtlinie 95/46/EG unter: http://ec.europa.eu/justice/policies/privacy/docs/lawreport/consultation/technical-annex_en.pdf (Analysis and impact study on the implementation of Directive EC 95/46 in Member States) sowie Artikel-29-Datenschutzgruppe, WP 203, Opinion 03/2013 on purpose limitation, adopted on 2 April 2013.*

Die Entwickler

- sollten Vorschläge für die Übersetzung der Datenschutzerklärungen in eine maschinenlesbare Form erarbeiten. Bei jeder Form der Einwilligungsanfrage müssen sie zudem sicherstellen, dass aktives Nutzerhandeln erforderlich wird, z. B. durch Einsatz leerer Kästchen, die der Nutzer aktiv ankreuzen muss. Eine konkludente Einwilligung ist damit ausgeschlossen. Die Erkenntnisse von P3P (Platform for Privacy Preferences Project) sollten bei der Umsetzung berücksichtigt werden.

- müssen bei der Gestaltung eines Einwilligungsassistenten, der im Rahmen eines zivilrechtlichen Vertragsabschlusses eingesetzt wird, darauf achten, dass für den Nutzer nicht der Eindruck entsteht, er würde zugleich seine datenschutzrechtliche Einwilligung für vertragsrelevante Zwecke erteilen. Aus datenschutzrechtlicher Sicht bedarf es keiner Einwilligung für Zwecke, die für die Vertragserfüllung erforderlich sind. Gleichwohl muss der Nutzer transparent über diese Zwecke informiert werden. Zivilrecht und Datenschutzrecht müssen getrennt werden und diese Trennung muss transparent sein.

- sollten die Anregungen der Artikel-29-Datenschutzgruppe zur Ausgestaltung technischer Systeme zur „Einwilligung in Cookies“ in ihre Überlegungen einbeziehen und prüfen, ob ihr Konzept entsprechend erweitert werden könnte – immer unter der Maßgabe, dass bei Third-Party-Cookies die vorherige Einwilligung erforderlich ist.

- sollten ihre Konzepte dahingehend analysieren, ob eine Kombination mit bereits bestehenden Diensten und Funktionen, wie sie beispielsweise MyData oder digi.me bieten, möglich und sinnvoll sein könnte.

- sollten sich aus den oben genannten Gründen frühzeitig überlegen, ob ein dezentrales oder zentrales System in Betracht kommt.

2. Ökonomische Rahmenbedingungen

- Erarbeitung von Richtlinien zur Präzisierung der in Einwilligungserklärungen angewandten Sprache in maschinenlesbarer Art und Weise (u. a. für Datenzweitverwertung).

- Förderung des Austausches über bestehende Interoperabilitäts- sowie Portabilitätsstandards, Unterstützung bei semantischer Klärung von Begriffen.

- Förderung des Austausches über bestehende Standardisierungssysteme (inkl. ISO-Standards), APIs, sowie standardisierte Vereinbarungen, die dem Einwilligungsmanagement zuträglich sind.

- Pilotierung von Projekten, die eine technische Implementation sowie die rechtskonforme Automatisierung von Einwilligungserklärungen zum Gegenstand haben.

3. Institutionelle Förderung

- Bildung einer öffentlich-privaten Partnerschaft (Hub) zum Austausch über wichtige rechtliche, technische sowie standarisierungsbezogene Rahmenbedingungen für die Entwicklung von innovativen Einwilligungssystemen nach dem Vorbild der finnischen MyData-Initiative. Datenschutzbehörden sowie unabhängige Forschungsinstitute sollten hier explizit einbezogen werden.

- Verbindung des oben genannten Hubs mit Ressourcen europäischer Forschungsprojekte in diesem oder artverwandten Bereichen (z. B. IPACSO, FiDiS, Gini SA).

- Erarbeitung eines Plans für einen effizienteren Transfer von Forschungsergebnissen aus der wirtschaftswissenschaftlichen Forschung (insb. empirische Verhaltensforschung) in die Start-up-Szene oder den genannten Hub.

- Organisation oder Förderung einer jährlichen Konferenz oder eines Workshops in Deutschland für Akteure aus Politik, Industrie und Forschung.

- Entwicklung eines Testbeds, das von Start-ups für das Experimentieren mit und das Testen von Beta-Versionen neuer Dienste mit Nutzern (Labor) genutzt werden kann.

4. Forschungsmaßnahmen

- Bei der Förderung der Forschung zum Verbraucherschutz soll verstärkt die Beziehung zwischen Datengebern und Datennehmern berücksichtigt werden. Die Anwendungsszenarien von datenschutzfreundlichen informationstechnischen Lösungsansätzen müssen insbesondere stärker im Hinblick auf Interessen und Notwendigkeiten der datennehmenden Unternehmen evaluiert werden. Die Förderung darf sich nicht allein auf sicherheitstechnische Aspekte konzentrieren, sondern muss zugleich aus der wirtschaftlichen Perspektive die praktischen Anwendungsfälle und die Bereitschaft von Unternehmen, datenschutzfreundliche Ansätze in ihre Geschäftsmodelle zu implementieren, berücksichtigen. Eine stärkere Betrachtung beider Perspektiven ermöglicht Lösungen für einen selbstbestimmten und nutzenstiftenden Umgang mit dem Thema Datenschutz, der auch dessen gesellschaftliche Wahrnehmung erhöht.

- Eine Anschubfinanzierung oder gezielte Förderprogramme zur Validierung von Lösungsansätzen in konkreten Szenarios könnten geeignete Instrumente darstellen, um potenzielle Anwender in den Entwicklungsprozess frühzeitig einzubinden und Lösungen mit einer konkreten Verwertungschance zu entwickeln.

- Die Finanzierung der Grundlagenforschung im Bereich des Ende-zu-Ende-Privatsphären-Managements, insbesondere die Förderung von interdisziplinären Forschungsprojekten im Bereich Verhaltensökonomie, Privatsphäre und Entscheidungsarchitekturen.

- Förderung der interdisziplinären Forschung im Bereich der Auflösungsgleichgewichte (unraveling) sowie der Implementierung von Prinzipien und Mechanismen der Fairness in Datenmärkten.

- Finanzierung von verhaltensökonomischen Arbeiten im Bereich des aktiven Einwilligungsmanagements sowie der Datenmonetarisierung.

- Insbesondere die tatsächliche Nutzer-Bereitschaft, die technischen Einwilligungsassistenten einzusetzen, muss untersucht werden. Die verbraucherpolitischen Vorschläge zur Gestaltung von Entscheidungssituationen bei Einwilligungen müssen, basierend auf verhaltenswissenschaftlichen Erkenntnissen zu den Auswirkungen der Gestaltung und Strukturierung von Wahlentscheidungen im Online-Kontext, untersucht werden. Solche Untersuchungen, wie sie momentan beispielsweise durch ConPolicy im Auftrag des Bundesministeriums der Justiz und für Verbraucherschutz im Hinblick auf „informierte Entscheidungen“ durchgeführt werden[62], sind ausdrücklich zu begrüßen, da sie einen konkreten rechtspolitischen Vorschlag auf seine praktische Geeignetheit durch valide empirische Forschung prüfen.

- Die Datenschutz-Folgenabschätzung muss bereits in die Entwicklungsphase von PIMS-Produkten mit einbezogen werden. Wirtschaft und Wissenschaft sollten generische Datenschutz-Folgenabschätzungen bei neuen Technologien gemeinsam entwickeln. Diese können gleichermaßen eine Grundlage für die konkreten Datenschutz-Folgenabschätzungen der Datenschutz-Grundverordnung darstellen.

- Da die potenzielle Anwender und damit potenzielle Kooperationspartner für den Entwicklungsprozess in unterschiedlichen Bundesländern ungleichmäßig verteilt sind, ist eine Förderung von informationstechnischen Lösungsansätzen auf der Bundes- und Europaebene dringend wünschenswert.

5. Sektorübergreifende Maßnahmen

- Der Datenschutz durch Technikgestaltung (Art. 25 DSGVO) könnte nicht nur den Anforderungen für eine „informierte Einwilligung“ gerecht werden, sondern auch den Übergang von der informierten Einwilligung zu einem „Empowered Consent“ ermöglichen, wodurch es dem Nutzer ermöglicht wird, die Datenschutzpräferenzen selbstbestimmt zu setzen. Damit können die Datenschutzpräferenzen kontextspezifisch, abgestuft und dynamisch gesetzt werden. Als besonders förderungswürdig erweisen sich dabei diejenigen Projekte, welche durch eine einheitliche und zentralisierte Datenkontrolle an einer Stelle („One-Stop-Shop“) dem Nutzer auf eine einfache und verständliche Art und Weise die Möglichkeit geben, seine Daten zu verwalten, bei mehreren Dienstanbietern die Weitergabepräferenzen gleichzeitig zu ändern und die geteilten Daten ggf. zu löschen. Solche Ansätze sind besonders geeignet, um eine „informierte Einwilligung“ technisch zu ermöglichen und der „Einwilligungsüberforderung“ entgegenzuwirken.

- Besondere Förderungswürdigkeit von automatisierten Einwilligungsverfahren ergibt sich nicht zuletzt daraus, dass diese das Potenzial haben, informationelle Selbstbestimmungschancen der Verbraucher zu stärken, zugleich den Interessen der datenverarbeitenden Wirtschaft entgegenzukommen sowie die Innovationsfähigkeit zu stärken. Zum einen könnten die Nutzer in den Stand versetzt werden, die Datenschutzpräferenzen selbstbestimmt zu setzen. Zugleich würde für die Wirtschaftsseite, und insbesondere für den Mittelstand, die Rechtssicherheit bei der Datenverarbeitung gestärkt und die Möglichkeit einer kostensparsamen Umsetzung der Datenschutzvorschriften gegeben. Durch die granulare Preisgabe von personenbezogenen Daten, verbunden mit der Möglichkeit, die Daten dynamisch zu aktualisieren, könnte außerdem die Qualität der Daten gesteigert werden (Smart Data).

62 *http://www.conpolicy.de/referenz/einwilligung-20-entwicklung-und-validierung-von-handlungsoptionen-zur-foerderung-informierter-date/.*

- Die Auseinandersetzung mit dem Thema „automatisierte Einwilligungsverfahren und Einwilligungsassistenten“ befindet sich in Deutschland noch in den Anfängen, während es auf der europäischen Ebene bereits intensiv behandelt wird. Auch die Bekanntheit von solchen Ansätzen ist in Deutschland zum gegenwärtigen Zeitpunkt eher gering. Der Bedarf an politischer und öffentlicher Diskussion zu den PIMS-Ansätzen auf nationaler Ebene ist daher hoch.

- Aufklärungskampagnen und öffentlicher Diskurs über technische Ansätze wie PIMS zur Stärkung der informationellen Selbstbestimmung sind dringend erforderlich, um potenzielle Anwender und Nutzer für das Thema frühzeitig zu sensibilisieren. Ein internationaler Diskurs zwischen Entwicklern, Aufsichtsbehörden, relevanten Stakeholdern, NGOs, politischen Entscheidungsträgern und potenziellen Anwendern bedarf einer verstärkten praktischen Unterstützung seitens der Politik (Koordination und Teilnahme am Diskurs, Bereitstellung der organisatorischen Infrastruktur, Tätigkeit als Multiplikator etc.).

- Es sollte eine internationale Plattform (nach Vorbild von MyData) eingerichtet werden, auf der in regelmäßigen Abständen ein Erfahrungsaustausch zwischen Entwicklern, Aufsichtsbehörden und datenverarbeitenden Unternehmen stattfindet. Unabhängige Einrichtungen wie die Stiftung Datenschutz können dafür eine geeignete Schnittstelle bilden.

- Öffentliche Einrichtungen wie Behörden und Universitäten würden sich als „early adopter“ von PIMS-Ansätzen besonders eignen. Die Implementierung von Einwilligungsassistenten durch die öffentliche Hand könnte sowohl die Akzeptanz und damit die Markteintrittschancen steigern als auch als Best-Praxis-Beispiel für den privaten Sektor dienen.

- Es sind europaweit einheitliche technische Standards dringend erforderlich. Um eine möglichst große Anzahl von Nutzern zu erreichen, müssen Produkte eine nutzerfreundliche Bedienung beinhalten, die durch Piktogramme und Symbole ein Mindestmaß an Eindeutigkeit und Verständlichkeit der Einwilligung ermöglicht. Insbesondere eine europaweite Standardisierung von visuellen Einwilligungshilfen ist dringend wünschenswert.

VI. Fazit

Zusammenfassend lässt sich feststellen, dass durch die PIMS-Ansätze viele aktuelle Probleme im Bereich der Einwilligung gelöst werden können und dass der Einsatz der „intelligenten Technik“ die Verfügungsmacht über personenbezogene Daten stärken kann. Der Datenschutz durch Technikgestaltung kann dabei nicht nur den Anforderungen für eine „informierte Einwilligung“ gerecht werden, sondern auch den Übergang von der informierten Einwilligung zu einem „Empowered Consent“ ermöglichen, bei dem es dem Nutzer ermöglicht wird, Datenschutzpräferenzen selbstbestimmt und kontextbezogen zu setzen. Besonders förderungswürdig erscheinen Ansätze, welche durch eine zentrale Kontrollmöglichkeit dem Nutzer an einer bestimmten Stelle („One-Stop-Shop“) auf einfache und verständliche Art die Möglichkeit geben, seine Daten zu verwalten, bei mehreren Dienstanbietern die Weitergabepräferenzen gleichzeitig zu ändern und die geteilten Daten auch zu löschen. Solche Ansätze sind besonders geeignet, einer „Einwilligungsüberforderung“ entgegenzuwirken.

Initiativen zu erleichterten oder gar automatisierten Einwilligungsverfahren erscheinen förderungswürdig, denn sie haben das Potenzial, die informationelle Selbstbestimmung der Verbraucher zu stärken und zugleich die Interessen der datenverarbeitenden Wirtschaft zu berücksichtigen sowie deren Innovationsfähigkeit zu stärken. Einerseits könnten die Nutzer in den Stand versetzt werden, Datenschutzpräferenzen selbstbestimmt zu setzen. Andererseits würde die Rechtssicherheit bei der Datenverarbeitung auf Wirtschaftsseite gestärkt (Nachweis der Einwilligung, Art. 7 Abd. 1 DSGVO). Gerade für den Mittelstand sind Möglichkeiten zur einfacheren Erreichung von Gesetzeskonformität und damit zur kostensparsamen Umsetzung der Datenschutzvorschriften von großem Vorteil. Durch die bewusstere und granulare Preisgabe von personenbezogenen Daten, verbunden mit der Möglichkeit, die Daten dynamisch zu aktualisieren, könnte außerdem die Qualität der Daten gesteigert werden (Smart Data).

Für die rechtliche Anschlussfähigkeit von automatisierten Einwilligungsverfahren ist stets entscheidend, wie die Intention der Datenschutz-Grundverordnung, ein gleichmäßiges und hohes Datenschutzniveau zu gewährleisten, zukünftig umgesetzt werden kann. Es sind außerdem europaweit einheitliche technische Standards erforderlich. Insbesondere eine europaweite Standardisierung von visuellen Einwilligungshilfen wäre wünschenswert.

Um sich am Markt durchzusetzen, müssen die PIMS einen deutlichen Mehrwert in der Datenaggregation generieren und bestenfalls Echtzeitdaten abbilden. Datenbasis und Datenqualität werden hier zum Schlüsselfaktor, wenn die Plattformen sich in der Informationsintermediation durchsetzen sollen. Für Unternehmen, welche PIMS nutzen wollen, ergeben sich zum einen komplexe Umorganisations- und Standardisierungsprozesse durch die neuen Datenmanagement-Architekturen, inklusive potenzieller Initiativen der Datenrückgabe (sog. share back). Gleichzeitig ermöglichen PIMS potenziell eine Zulieferung und Just-in-time-Integration von Echtzeit-Kundeninformationen in die Produktionsprozesse. Eine Automatisierung der Einwilligungsprozesse durch maschinenlesbare Einwilligungserklärungen birgt außerdem große Einsparpotenziale.

Es wird schließlich eine der wichtigsten Herausforderungen für PIMS sein, Entscheidungsarchitekturen so zu gestalten, dass konstatierte Präferenzen der Verbraucher für die eigene Privatsphäre mit tatsächlichen Wahlhandlungen stärker konvergieren. Künftig sollen es die neuen Plattformen Nutzern erlauben, die Privatsphären- und Vertrauenseinstellungen ihrer Anwendungen optimal ihren Präferenzen anzupassen. Es besteht also das Potenzial, die Entscheidungsoptionen in der Datenverarbeitung zu verbessern, vor allem wenn die neuen Anbieter Erkenntnisse aus der Verhaltensökonomie ins Entscheidungsdesign einbeziehen.

STIFTUNG DATENSCHUTZ

Stiftung Datenschutz
rechtsfähige Stiftung bürgerlichen Rechts
Karl-Rothe-Straße 10–14
04105 Leipzig
Deutschland

Telefon 0341 / 5861 555-0
mail@stiftungdatenschutz.org
www.stiftungdatenschutz.org