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

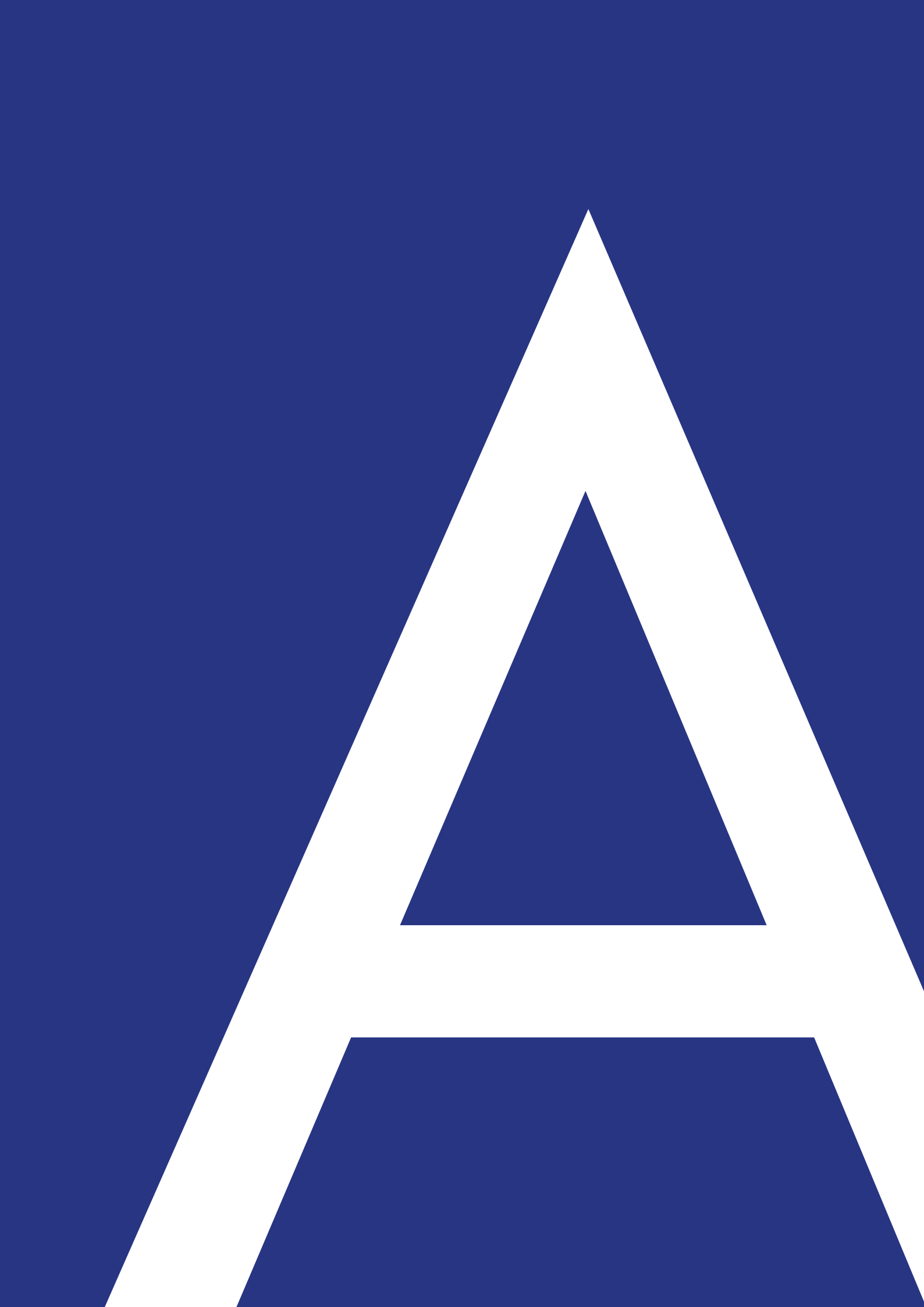
Prof. Dr. Anne Riechert, Stiftung Datenschutz / Frankfurt University of Applied Sciences

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 Datenverarbeitungsvorgänge 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

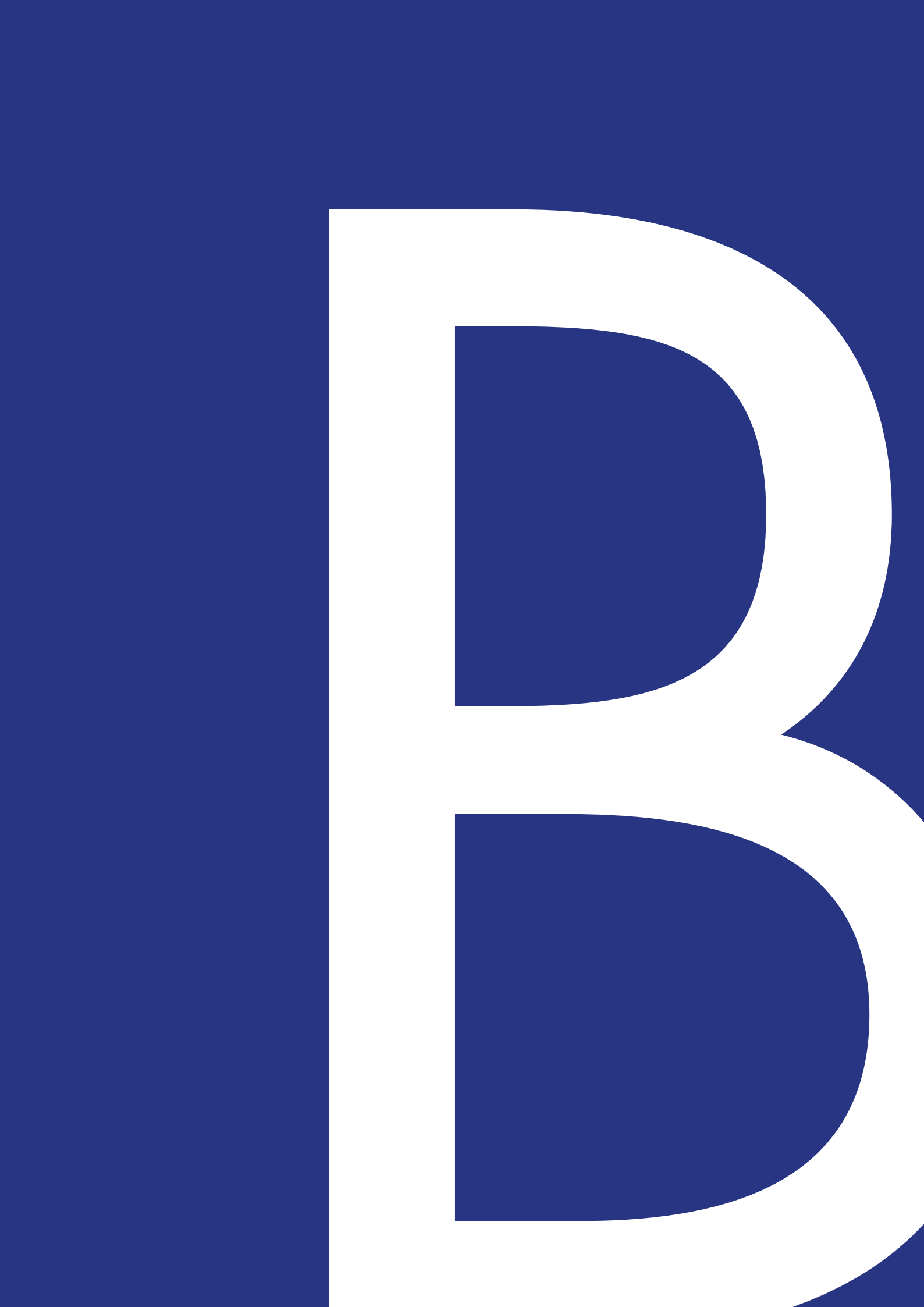
Zusammenfassend lässt sich feststellen, dass durch die PIMS-Ansätze viele aktuelle Probleme im Bereich der Einwilligung gelöst werden können und dass der Einsatz der „intelligenten Technik“ die Verfügungsmacht über personenbezogene Daten stärken kann. Der Datenschutz durch Technikgestaltung kann dabei 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.



Stellungnahme zu rechtlichen Aspekten eines Einwilligungsassistenten

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

Stand: Dezember 2016

Inhaltsverzeichnis

Anhang 1 – Seite

A. Einführung 4
I. Allgemein 4
II. Technische Konzepte 5

B. Ziel und Vorgehensweise 6

C. Voraussetzungen der Einwilligung 8
I. Die Einwilligung im Gemeinschaftsrecht 8
1. Richtlinie 95/46/EG und Datenschutz-Grundverordnung 8
2. Richtlinie 2002/58/EG 10
(1) Verkehrsdaten und Standortdaten 10
(2) Informationen, die bereits im Endgerät des Nutzers gespeichert sind 10
II. Die Einwilligung unter Berücksichtigung der Datenschutz-Grundverordnung 11
1. Elektronische Kommunikationsdienste 11
(1) Richtlinie 2002/58/EG 11
Fazit Nr. 1 15
(2) Richtlinie 2002/58/EG in der Fassung 2009/136/EG 15
Fazit Nr. 2 20
2. Dienste der Informationsgesellschaft 21
Fazit Nr. 3 24

D. Einwilligungsassistent 24
I. Willensbekundung und Einverständnis 26
1. Definition 26
Fazit Nr. 4 30
2. Relevanz für den Einwilligungsassistenten 30
(1) Aktives Tun 30
(2) Standortdaten 31
(3) IP-Adresse 32
(4) Cookies 33
Fazit Nr. 5 34

Inhaltsverzeichnis

Anhang 1 – Seite

D. Einwilligungsassistent
II. „Für den bestimmten Fall in informierter Weise“ 35
1. Allgemeine Voraussetzungen 35
(1) Bestimmter Fall 35
(2) Bestimmter Zweck 38
(3) Kenntnis der Sachlage 41
(4) Informiertheit und Transparenz 43
Fazit Nr. 6 45
2. Relevanz für den Einwilligungsassistenten 46
(1) Granularität 46
(2) Exkurs: UWG 49
Fazit Nr. 7 52
III. Freiwilligkeit und Kopplungsverbot 54
1. Voraussetzungen 54
2. Relevanz für den Einwilligungsassistenten 56
Fazit Nr. 8 58
IV. Dauer der Einwilligung 59
1. Definition 59
2. Relevanz für den Einwilligungsassistenten 60
Fazit Nr. 9 60

E. Verantwortlichkeit 60
I. Allgemein 61
II. Relevanz für den Einwilligungsassistenten 64
Fazit Nr. 10 66

F. Zukünftige Fragestellungen 67
I. Automatisierte Entscheidungsfindung 67
II. Datenschutzrecht und Zivilrecht 68

G. Zusammenfassung der Anforderungen an den Einwilligungsassistenten 70

H. Fazit und Zusammenfassung der Handlungsempfehlungen 73

I. Zusatz zur rechtlichen Stellungnahme 77

Abrufdatum der Internetlinks in Teil B: 24. Februar 2017

A. Einführung

I. Allgemein

Im Fokus dieser rechtlichen Stellungnahme stehen technische Konzepte, die zum Ziel haben, Nutzer (als im datenschutzrechtlichen Sinne „betroffene Personen“) bei Ausübung ihrer Einwilligung automatisiert zu unterstützen. Hierbei soll die Zustimmung für unterschiedliche Datenverarbeitungsprozesse und Empfänger im Voraus erteilt werden. Im Folgenden werden die zugrunde liegenden Prozesse auch als „Einwilligungsassistenten“ bezeichnet.

Die Prüfung orientiert sich hierbei an den technischen Möglichkeiten, die das Projekt „LETsmart“ und die Plattform „CoMaFeDS“ bieten.[1]

In die Betrachtung fließen ebenso grundsätzliche rechtliche Erwägungen zur Anwendbarkeit und Auslegung der Datenschutz-Grundverordnung mit ein, um hieraus insgesamt und nicht nur für den Einwilligungsassistenten Handlungsempfehlungen für die Voraussetzungen der Einwilligung entwickeln zu können. Zudem erfolgen Darstellungen zur angewandten Praxis der so genannten Cookie-Richtlinie, da dies zum einen für die Auslegung der Einwilligungsvoraussetzungen relevant ist aber zum anderen für die Entwickler ein Prüfungsansatz darstellen soll, ob ihre Konzepte auf diese Einwilligungsprozesse ausgedehnt werden können. 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.[2]

Da sich die Konzepte „LETsmart“ und „CoMaFeDS“ hinsichtlich möglicher Einsatzzwecke und Anwendungsgebiete in der Entwicklung befinden und Details teilweise der Geheimhaltung unterliegen, kann diese Stellungnahme darüber hinaus keine abschließende Begutachtung darstellen.

Insgesamt werden ausschließlich rechtliche und keine technischen Bewertungen vorgenommen.

1 *Siehe Studie der Stiftung Datenschutz, Kapitel II. 2.*

2 *Bei der Artikel-29-Datenschutzgruppe handelt es sich um ein unabhängiges Beratungsgremium der Europäischen Kommission und setzt sich aus Vertretern der nationalen Datenschutzbehörden, dem Europäischen Datenschutzbeauftragten sowie der Europäischen Kommission zusammen. Zu der gerade zitierten Aufforderung: Artikel-29-Datenschutzgruppe, WP 171 Stellungnahme 2/2010 zur Werbung auf Basis von Behavioural Targeting, angenommen am 22. Juni 2010, S. 27.*

II. Technische Konzepte

Zunächst werden nun in abstrakter Weise die Ziele und Funktionen der geplanten „Einwilligungsassistenten“ nochmals zusammengefasst (nähere Beschreibungen und Details sind in der Bestandsaufnahme der Studie enthalten):

Der Nutzer[3] soll im Vorhinein Vorgaben erteilen,
- welche Daten
- an welche Empfänger
- zu welchem Zweck

weitergegeben werden.

Ein System speichert die Daten der betroffenen Person entweder dezentral (bei der betroffenen Person) oder zentral (Cloud). „LETsmart“ bezeichnet die dezentrale Speicherung als „Datentresor“, über den der Nutzer die Kontrolle ausübt.

Das System ist darüber hinaus in der Lage, Datenschutzhinweise der Empfänger in eine maschinenlesbare Form zu übersetzen und die darin enthaltenen Angaben in Form einer Liste zusammenzufassen, so dass die betroffene Person die Möglichkeit hat, in die Verarbeitung der dort aufgezählten Daten, Zwecke und Empfänger detailliert einzuwilligen. Bei der Plattform „CoMaFeDS“ wird dies wie folgt beschrieben: „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, so dass Definitionen von zahlreichen Unterkategorien möglich sind. Dies würde etwa Zustimmungen erlauben wie „Meine Daten dürfen von unterschiedlichen Forschungsinstitutionen für den Zwecke von demografischen Untersuchungen verarbeitet werden, aber nicht durch Regierungsbehörden für Steuerschätzungen“[4].

„LETsmart“ ist zunächst darauf ausgelegt, im Rahmen eines einzigen laufenden Vertragsverhältnisses zwischen betroffener Person und dem Vertragspartner die Einwilligungserklärungen automatisiert zu unterstützen, wobei nach Wegfall des Verwendungszwecks die Daten automatisiert gelöscht werden. Eine Erweiterung ist jedoch dahingehend geplant, dass auch die Datenschutzhinweise mehrerer Vertragspartner automatisiert in entsprechende Einwilligungserklärungen „übersetzt“ werden könnten.
Die Plattform „CoMaFeDS“ verfolgt aktuell, das Wissen über vorhandene Einwilligungserklärungen von betroffenen Personen auf einer zentralen Plattform bereitzustellen. Empfänger erhalten zunächst nur die Information, dass eine kompatible Einwilligungserklärung vorliegt, jedoch noch keine Information über die betroffene Person. Die Übereinstimmung soll automatisiert geprüft werden und die betroffene Person eine entsprechende Rückmeldung erhalten.

3 Im Verlauf dieser rechtlichen Stellungnahme wird die im datenschutzrechtlichen Sinne betroffene Person entweder als „Nutzer“ oder als „betroffene Person“ bezeichnet.

4 Siehe Studie der Stiftung Datenschutz, Kapitel II. 2.

Entsprechende Vorhaben gab es bereits in der Vergangenheit, wie beispielsweise P3P oder Sticky Policies, an denen sich diese Projekte teilweise orientieren: Bei den so genannten „Sticky Policies“ werden persönliche Daten, die die betroffene Person zuvor im Hinblick auf Zwecke und Konditionen spezifiziert hat, vom System des Datenhalters erfasst, verschlüsselt und diese Vorgaben in eine standardisierte Datenschutzerklärung umgewandelt. P3P verfolgt den Sticky Policy-Ansatz.[5] Die betroffenen Personen nehmen Voreinstellungen bezüglich der von ihnen präferierten Datennutzung vor.[6]

Weiterhin ist „CoMaFeDS“ von dem Wissen abhängig, wo spezifische Datensätze zu finden sind. Um dieses Problem zu lösen, soll eine detaillierte Beschreibung der Datensätze erfolgen. Für jede mögliche Datenquelle soll ein maschinenlesbares Dokument vorliegen, das spezifiziert, wo ein jeweiliges Datum liegt. Außerdem sollen für jeden Datensatz detaillierte Präferenzen verfügbar sein, und zwar bezogen auf die vielfältigen Verarbeitungsprozesse sowie Empfänger. Basierend auf diesen Dokumentationen führt „CoMaFeDS“ interne Konvertierungen durch und die Datenbank- und Datensatzbezogenen Informationen und Spezifikationen werden genutzt, um einen ontologisch-basierten „Wissensgraph“ 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“).

Eine dynamische Einholung der Einwilligungserklärung ist geplant.
Offen, aber besonders interessant ist, ob diese technischen Möglichkeiten mit bereits angebotenen Diensten wie DigiMe (siehe Bestandsaufnahme) oder Konzepten wie MyData (siehe Bestandsaufnahme) zukünftig kombiniert werden können, so dass in Bezug auf mehrere Empfänger ein automatisierter Datenaustausch erfolgen könnte.

B. Ziel und Vorgehensweise

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.

Zu untersuchen ist daher, ob die unter dem vorangegangen Punkt A. dargestellten Konzepte den rechtlichen Vorgaben der ab Mai 2018 geltenden Datenschutz-Grundverordnung entsprechen, welche Anforderungen bei der Technikgestaltung zu beachten sind und ob insgesamt im Hinblick auf die Einwilligungsvoraussetzungen der einheitliche Rechtsrahmen gewahrt wird. Gemäß Erwägungsgründen 10 und 13 Datenschutz-Grundverordnung sollte das Schutzniveau für die Rechte und Freiheiten von natürlichen Personen bei der Verarbeitung personenbezogener Daten in allen Mitgliedstaaten gleichwertig und es sollten gleichmäßige Kontrollen und gleichwertige Sanktionen gewährleistet sein.

5 Siehe unter https://www.datenschutzzentrum.de/projekte/p3p/P3P_AK-IT.pdf

6 P3P wird jedoch vom Windows-Browser seit der Version Windows 10 nicht mehr unterstützt (siehe in der Bestandsaufnahme der Studie). Bei „CoMaFeDS“ soll allerdings 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.

Unter dem nachfolgenden Punkt C. erfolgt zunächst die Darstellung der rechtlichen Voraussetzungen und der Anforderungen an eine rechtmäßige Datenverarbeitung. Vergleichend wird hierbei auf die aktuell geltende EU-Datenschutzrichtlinie (95/46/EG) Bezug genommen.[7] Außerdem wird die praktische Umsetzung der so genannten Cookie-Richtlinie anhand von Beispielen erläutert, um damit gleichermaßen die Einwilligungsvoraussetzungen und zugrundeliegenden Rechtsauffassungen näher beleuchten und Empfehlungen aussprechen zu können.

Zudem werden unter Punkt C. die Einwilligungsvoraussetzungen für elektronische Kommunikationsdienste und Dienste der Informationsgesellschaft sowie die Regelungen des Telekommunikations- und des Telemediengesetzes dahingehend diskutiert, ob deren Intentionen weiterhin Geltung beanspruchen können oder durch die Datenschutz-Grundverordnung vollständig abgelöst werden. Dies geschieht zum einen im Hinblick auf Anbieter von elektronischen Telekommunikationsdiensten oder von Diensten der Informationsgesellschaft, bei denen im Zusammenhang mit ihren Dienstleistungen ebenso die Verwendung eines Einwilligungsassistenten denkbar wäre. Zum anderen ist zum jetzigen Zeitpunkt des technischen Entwicklungsstands noch nicht absehbar, ob die in dieser Stellungnahme geprüften Konzepte darüber hinaus als eigenständige Dienste eingestuft werden könnten (im Sinne eines elektronischen Kommunikationsdienstes oder Dienstes der Informationsgesellschaft).

Unter D. wird sodann die Relevanz der unter C. festgestellten Ergebnisse für die so genannten Einwilligungsassistenten geprüft, wobei Empfehlungen in Bezug auf die Auslegung der Regelungen der Datenschutz-Grundverordnung eingebunden sind.

Unter E. werden Fragen der „Verantwortung und Haftung“ behandelt und unter Punkt F. erfolgen Überlegungen zu zukünftigen Problemstellungen von automatisierten Entscheidungen.
Zusammenfassungen zur rechtlichen Bewertung des Einwilligungsassistenten sowie Handlungsempfehlungen werden abschließend in den Punkten G. und H. dargestellt.

7 *Um die Vollharmonisierung ab Inkrafttreten der Datenschutz-Grundverordnung sicherzustellen, sollte frühzeitig mit der Prüfung begonnen werden, ob und in welchem Umfang eine unterschiedliche Interpretation der Datenschutz-Grundverordnung durch die Mitgliedstaaten und Vorgehensweise in der Praxis in Betracht kommen und dem in den Grundsätzen der Datenschutz-Grundverordnung geforderten gleichwertigen Datenschutzniveau entgegenstehen könnte. Die Richtlinie 95/46/EG enthält teilweise identische Begriffe und könnte daher für die Einschätzung hilfreich sein, ob abweichende Definitionen in den einzelnen Mitgliedstaaten auch zukünftig im Hinblick auf die Datenschutz-Grundverordnung zu erwarten sein könnte. Siehe auch 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“). Ferner ist der Vergleich aufgrund der Regelung in Erwägungsgrund 171 Datenschutz-Grundverordnung relevant. Danach ist nicht erforderlich, dass die betroffene Person erneut ihre Einwilligung erteilt, wenn die Art der bereits erteilten Einwilligung den Bedingungen der Datenschutz-Grundverordnung entspricht, so dass der Verantwortliche die Verarbeitung nach dem Zeitpunkt der Anwendung der Datenschutz-Grundverordnung fortsetzen kann. Siehe hierzu außerdem Düsseldorfer Kreis, Beschluss vom 13./14.09.2016 zur Fortgeltung bisher erteilter Einwilligungen unter der Datenschutz-Grundverordnung, https://www.ldi.nrw.de/mainmenu_Service/submenu_Entschliessungsarchiv/Inhalt/Beschluesse_Duesseldorfer_Kreis/Inhalt/2016/Fortgeltung_bisher_erteilter_Einwilligungen_unter_der_Datenschutz-_Grundverordnung/Fortgeltung_bisher_erteilter_Einwilligungen_unter_der_Datenschutz-_Grundverordnung1.pdf*

C. Voraussetzungen der Einwilligung

Für die Verarbeitung personenbezogener Daten normiert Artikel 6 Datenschutz-Grundverordnung[8] als allgemeinen Grundsatz das sogenannte Verbotsprinzip mit Erlaubnisvorbehalt. Demnach ist die Verarbeitung von personenbezogenen Daten nur zulässig, wenn eine Einwilligung vorliegt oder eine andere in dieser Vorschrift geregelte Ausnahme vorliegt. Dies entspricht weiterhin den Vorgaben der EU-Datenschutzrichtlinie 95/46/EG.[9] Dort knüpfen Artikel 7 sowie Art. 8 Abs. 1 EG-Datenschutzrichtlinie die Verarbeitung personenbezogener Daten an bestimmte Voraussetzungen. Darüber hinaus sind in Artikel 6 der Datenschutzrichtlinie für elektronische Kommunikation Anforderungen bezüglich der Einwilligung enthalten.[10]

Für das Projekt und vorliegende Gutachten ist insgesamt die Einwilligung als Zulässigkeitsvoraussetzung für eine rechtmäßige Datenverarbeitung von Relevanz. Daher werden im Folgenden die hierfür relevanten Regelungen näher dargestellt.

I. Die Einwilligung im Gemeinschaftsrecht

1. Richtlinie 95/46/EG und Datenschutz-Grundverordnung

Artikel 7a) der EU-Datenschutzrichtlinie 95/46/EG, die gemäß Artikel 94 Datenschutz-Grundverordnung mit Wirkung vom 25. Mai 2018 aufgehoben wird, erlaubt die Verarbeitung personenbezogener Daten unter anderem dann, wenn die betroffene Person „ohne jeden Zweifel ihre Einwilligung gegeben“ hat. Hier sollen die denkbar höchsten Anforderungen an die Zweifelsfreiheit gelten, da diese Formulierung keine relativierenden oder einschränkenden Adjektive enthalte.[11]

Diese Anforderung „ohne jeden Zweifel“ ist in der Datenschutz-Grundverordnung nicht mehr enthalten. Gemäß Artikel 6 Absatz 1a) der Datenschutz-Grundverordnung ist die Datenverarbeitung nunmehr rechtmäßig, „wenn die betroffene Person ihre Einwilligung zu der Verarbeitung der sie betreffenden personenbezogenen Daten für einen oder mehrere bestimmte Zwecke gegeben hat.“

8 Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung); http://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=CELEX:32016R0679&from=DE

9 Richtlinie 95/46/EG des Europäischen Parlaments und des Rates vom 24. Oktober 1995 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr, Amtsblatt Nr. L 281 vom 23.11.1995, S. 31 – 50.

10 Richtlinie 2002/58/EG des Europäischen Parlaments und des Rates vom 12. Juli 2002 über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre in der elektronischen Kommunikation (Datenschutzrichtlinie für elektronische Kommunikation); Amtsblatt Nr. L 201 vom 31.07.2002, S. 37 - 47.

11 Philip Radlanski, Das Konzept der Einwilligung in der datenschutzrechtlichen Realität, S. 43. Siehe außerdem Brühann: in Grabitz/Hilf, Das Recht der Europäischen Union, 40. Auflage 2009, Loseblattsammlung, Stand: Mai 1999 Ergänzungslieferung 13, Artikel 2 Begriffsbestimmungen „Einwilligung der betroffenen Person“ mit dem Hinweis, dass der Bezug auf den ausdrücklichen Charakter der Einwilligung gestrichen wurde, um zu verhindern, dass dies als Erfordernis einer schriftlichen Erklärung ausgelegt werde.

Insgesamt haben sich im Verlauf der Verhandlungen zur Datenschutz-Grundverordnung bei der Definition der Einwilligung weder die ursprünglich geforderte „explizite“[12] oder „ausdrückliche“[13] Willensbekundung noch die Formulierung „ohne jeden Zweifel“[14] durchsetzen können. Die Artikel-29-Datenschutzgruppe hat schon im Verlaufe der Verhandlungen zur Datenschutz-Grundverordnung angemerkt, dass die Beibehaltung von “explicit” im Rahmen der Einwilligung eine wichtige Klarstellung bedeutet, die notwendig ist, um den betroffenen Personen die Ausübung ihrer Rechte zu ermöglichen.[15] Dennoch wurde in der englischen Originalfassung der Datenschutz-Grundverordnung der Begriff „explicit“ in der Endfassung durch „unambiguous“ ersetzt.[16] Lediglich gemäß Erwägungsgrund 32 der Datenschutz-Grundverordnung „sollte“ eine Einwilligung „unmissverständlich“ („unambiguous“) durch eine bestätigende Handlung bekundet sein. Im Verordnungstext selbst (siehe Artikel 6 Absatz 1a) der Datenschutz-Grundverordnung) ist diese Verpflichtung jedoch nicht enthalten. Ergänzend anzumerken ist, dass in der deutschen Fassung des Berichts des LIBE-Ausschusses vom 22.11. der Begriff „explicit“ nicht mehr wie zuvor mit „explizit“, sondern nunmehr mit „ausdrücklich“ übersetzt und als Änderung markiert wurde, obwohl in der Originalfassung weiterhin „explicit“ verwendet und keine begriffliche Abwandlung vorgenommen wurde. Dieser Begriff wurde bereits in der Vergangenheit unterschiedlich übersetzt.[17]

Eine ausdrückliche Einwilligung ist gemäß Artikel 9 Absatz 2a) Datenschutz-Grundverordnung nur bei besonderen Kategorien von personenbezogenen Daten für die Verarbeitung erforderlich.[18]

12 *Siehe Artikel 4 Nr. 8 in Datenschutz-Grundverordnung der EU-Kommission vom 25.1.2012, KOM(2012) 11 endgültig 2012/0011 (COD) - Vorschlag für Verordnung des Europäischen Parlaments und des Rates zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr (Datenschutz-Grundverordnung): http://ec.europa.eu/justice/data-protection/document/review2012/com_2012_11_en.pdf*

13 *Siehe Artikel 4 Nr. 8 gemäß LIBE-Ausschuss - Bericht über den Vorschlag für eine Verordnung des Europäischen Parlaments und des Rates zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr (allgemeine Datenschutzverordnung)(COM(2012)0011 – C7-0025/2012 – 2012/0011(COD), - dieser Vorschlag erfolgte in Kenntnis des Berichts des Ausschusses für bürgerliche Freiheiten, Justiz und Inneres sowie der Stellungnahmen des Ausschusses für Beschäftigung und soziale Angelegenheiten, des Ausschusses für Industrie, Forschung und Energie, des Ausschusses für Binnenmarkt und Verbraucherschutz und des Rechtsausschusses -; http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//NONSGML+REPORT+A7-2013-0402+0+DOC+PDF+V0//DE*

14 *Interinstitutionelles Dossier mit dem Hinweis, dass „explizit“ unrealistisch sei – Siehe Rat der Europäischen Union 31.Mai 2013 10227/13 Interinstitutionelles Dossier 2012/0011 (COD) ; Betr.: Vorschlag für eine Verordnung des Europäischen Parlaments und des Rates zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr (Datenschutz-Grundverordnung) – Kernfragen zu den Kapiteln I-IV; http://register.consilium.europa.eu/doc/srv?l=DE&f=ST%2010227%202013%20INIT*

15 *Artikel-29-Datenschutzgruppe, WP 199 “Opinion 08/2012 providing further input on the data protection reform discussions”, adopted on 5 October 2012, S. 7: The Working Party understands that doubts have been raised as to the feasibility of the word “explicit” in the context of consent in Article 4 (8). The Working Party is of the opinion that the inclusion of the word “explicit” is an important clarification in the text, which is necessary to truly enable data subjects to exercise their rights, especially on the Internet where there is now too much improper use of consent. It would be highly undesirable should this important clarification be deleted from the text.*

16 *Siehe http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//NONSGML+REPORT+A7-2013-0402+0+DOC+PDF+V0//EN und http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//NONSGML+REPORT+A7-2013-0402+0+DOC+PDF+V0//DE*

17 *Auf die unterschiedliche Auslegung von „explicit“ wird im Folgenden näher Bezug genommen werden, siehe S. 37 ff.*

18 *Gemäß Artikel 9 Absatz 1 Datenschutz-Grundverordnung (Verarbeitung besonderer Kategorien personenbezogener Daten) ist die Verarbeitung personenbezogener Daten, aus denen die rassische und ethnische Herkunft, politische Meinungen, religiöse oder weltanschauliche Überzeugungen oder die Gewerkschaftszugehörigkeit hervorgehen, sowie die Verarbeitung von genetischen Daten, biometrischen Daten zur eindeutigen Identifizierung einer natürlichen Person, Gesundheitsdaten oder Daten zum Sexualleben oder der sexuellen Orientierung einer natürlichen Person untersagt. Die Definitionen von genetischen Daten, biometrischen Daten sowie Gesundheitsdaten sind in Artikel 4 Nr. 13, 14 und 15 Datenschutz-Grundverordnung geregelt. Zur näheren Auslegung dieser Daten sind ebenso die Erwägungsgründe 34, 35 und 51 heranzuziehen.*

2. Richtlinie 2002/58/EG

(1) Verkehrsdaten und Standortdaten

Weitere Voraussetzungen einer Einwilligung sind in Artikel 6 Abs. 3 der Richtlinie 2002/58/EG für elektronische Kommunikation hinsichtlich Verkehrsdaten enthalten.[19]

Danach ist die Verarbeitung von Verkehrsdaten[20] zum Zwecke der Bereitstellung von Diensten mit Zusatznutzen oder zum Zwecke der Vermarktung elektronischer Kommunikationsdienste lediglich mit der Einwilligung des betroffenen Nutzers oder Teilnehmers möglich. Die Legaldefinition des öffentlich zugänglichen elektronischen Kommunikationsdiensts regelt Artikel 2 c) Rahmenrichtlinie 2002/21/EG[21].

Dabei handelt es sich um gewöhnlich gegen Entgelt erbrachte Dienste, die ganz oder überwiegend in der Übertragung von Signalen über elektronische Kommunikationsnetze bestehen, einschließlich Telekommunikations- und Übertragungsdienste in Rundfunknetzen, ausgenommen jedoch Dienste, die Inhalte über elektronische Kommunikationsnetze und –dienste anbieten oder eine redaktionelle Kontrolle über sie ausüben. Es gehören keine Dienste der Informationsgesellschaft im Sinne von Artikel 1 der Richtlinie 98/43/EG dazu, die nicht ganz oder überwiegend in der Übertragung von Signalen über elektronische Kommunikationsnetze bestehen. Insgesamt betreffen die Verkehrsdaten daher den Vorgang der Übertragung, nicht den Inhalt der Nachricht, da die Richtlinie 2002/58/EG die telekommunikationsrechtliche Materie regelt.[22]

Der Dienst mit Zusatznutzen, auf den sich Artikel 6 Absatz 3 der Richtlinie 2002/58/EG ebenso bezieht, wird gemäß Artikel 2 g) dieser Richtlinie definiert als „jeder Dienst, der die Bearbeitung von Verkehrsdaten oder anderen Standortdaten als Verkehrsdaten in einem Maße erfordert, das über das für die Übermittlung einer Nachricht oder die Fakturierung dieses Vorgangs erforderliche Maß hinausgeht." Beispielhaft werden hierzu in Erwägungsgrund 18 die Beratung hinsichtlich der billigsten Tarifpakete, Navigationshilfen, Verkehrsinformationen, Wettervorhersage oder touristische Informationen genannt. Die damit verbundenen Standortdaten[23], die keine Verkehrsdaten sind, dürfen gemäß Artikel 9 Absatz 1 der Richtlinie 2002/58/EG nur anonymisiert oder mit der Einwilligung des Nutzers zur Bereitstellung von Diensten mit Zusatznutzen verarbeitet werden.

(2) Informationen, die bereits im Endgerät des Nutzers gespeichert sind

Zudem sieht die Richtlinie 2002/58/EG (in der Fassung 2009/136/EG)[24] für Informationen, die bereits im Endgerät des Nutzers gespeichert sind („Cookies"), folgende Regelung vor (Artikel 5 Absatz 3):

19 *Richtlinie 2002/58/ÆG des Europäischen Parlaments und des Rates vom 12. Juli 2002 über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre in der elektronischen Kommunikation (Datenschutzrichtlinie für elektronische Kommunikation); Amtsblatt Nr. L 201 vom 31.07.2002, S. 37 - 47.*

20 *Siehe Artikel 2b) der Richtlinie 2002/58/ÆG.*

21 *Richtlinie 2002/21/ÆG des Europäischen Parlaments und des Rates vom 7. März 2002 über einen gemeinsamen Rechtsrahmen für elektronische Kommunikationsnetze und -dienste (Rahmenrichtlinie) , Amtsblatt Nr. L 108 vom 24.04.2002 S. 33 – S. 50.*

22 *Siehe hierzu auch die Ausführungen zur Inhaltsneutralität einer Nachricht bei Peukert in: Teplitzky/Pfeifer/Leistner, UWG, Großkommentar zum Gesetz gegen den unlauteren Wettbewerb mit Nebengesetzen, Band 1: Einleitung; 2. Auflage 2013, §§ 1- 3, Rn. 510 (S. 882).*

23 *Siehe Artikel 2c) der Richtlinie 2022/58/ÆG.*

24 *Richtlinie 2009/136/ÆG des Europäischen Parlaments und des Rates vom 25. November 2009 zur Änderung der Richtlinie 2002/22/ÆG über den Universaldienst und Nutzerrechte bei elektronischen Kommunikationsnetzen und -diensten, der Richtlinie 2002/58/ÆG über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre in der elektronischen Kommunikation und der Verordnung (EG) Nr. 2006/2004 über die Zusammenarbeit im Verbraucherschutz, Amtsblatt Nr. L 337 vom 18.12.2009, S. 11 - 36.*

„Die Mitgliedstaaten stellen sicher, dass die Speiche¬rung von Informationen oder der Zugriff auf Informationen, die bereits im Endgerät eines Teilnehmers oder Nutzers gespeichert sind, nur gestattet ist, wenn der betreffende Teil¬nehmer oder Nutzer auf der Grundlage von klaren und umfassenden Informationen, die er gemäß der Richtlinie 95/46/EG u. a. über die Zwecke der Verarbeitung erhält, seine Einwilligung gegeben hat."

Gemäß Artikel 2f) der Richtlinie 2002/58/EG stellt eine „Einwilligung" eines Nutzers oder Teilnehmers die Einwilligung der betroffenen Person im Sinne von Richtlinie 95/46/EG dar. Die entsprechende Definition der Einwilligung der betroffenen Person regelt die Datenschutzrichtlinie 95/46/EG in Artikel 2h): „Im Sinne dieser Richtlinie bezeichnet der Ausdruck „Einwilligung der betroffenen Person" jede Willensbekundung, die ohne Zwang für den konkreten Fall und in Kenntnis der Sachlage erfolgt und mit der die betroffene Person akzeptiert, dass personenbezogene Daten, die sie betreffen, verarbeitet werden."

II. Die Einwilligung unter Berücksichtigung der Datenschutz-Grundverordnung

1. Elektronische Kommunikationsdienste[25]

(1) Richtlinie 2002/58/EG

Gemäß Erwägungsgrund 173[26] soll die Richtlinie 2002/58/EG entsprechend geändert werden, um das Verhältnis zur Datenschutz-Grundverordnung klarzustellen. Diese Überarbeitung der so genannten e-Privacy-Richtlinie findet zurzeit statt (Stand: Dezember 2016).

Artikel 95 Datenschutz-Grundverordnung regelt dies wie folgt:
„Diese Verordnung erlegt natürlichen oder juristischen Personen in Bezug auf die Verarbeitung in Verbindung mit der Bereitstellung öffentlich zugänglicher elektronischer Kommunikationsdienste in öffentlichen Kommunikationsnetzen in der Union keine zusätzlichen Pflichten auf, soweit sie besonderen in der Richtlinie 2002/58/EG festgelegten Pflichten unterliegen, die dasselbe Ziel verfolgen."

Die Datenschutz-Grundverordnung enthält zur Verarbeitung personenbezogener Daten in Verbindung mit der Bereitstellung elektronischer Kommunikationsdienste keine gesonderten Regelungen. Sie erlaubt den Mitgliedstaaten lediglich hinsichtlich der Voraussetzungen für eine rechtmäßige Datenverarbeitung gemäß Artikel 6 Absatz 2 die Einführung konkreter Bestimmungen in Bezug auf die Verarbeitung zur Erfüllung von Absatz 1c und e.[27]

25 *Aufgrund des jetzigen Entwicklungsstandes ist noch offen, ob der Einwilligungsassistent als (Teil) eines elektronischen Kommunikationsdienstes oder Dienst mit Zusatznutzen qualifiziert werden könnte (bei dem in diesem Falle selbst Verkehrsdaten anfallen könnten), siehe auch Einleitung sowie S. 21 und S. 55.*

26 *Erwägungsgrund 173: Diese Verordnung sollte auf alle Fragen des Schutzes der Grundrechte und Grundfreiheiten bei der Verarbeitung personenbezogener Daten Anwendung finden, die nicht den in der Richtlinie 2002/58/EG des Europäischen Parlaments und des Rates (18) bestimmte Pflichten, die dasselbe Ziel verfolgen, unterliegen, einschließlich der Pflichten des Verantwortlichen und der Rechte natürlicher Personen. Um das Verhältnis zwischen der vorliegenden Verordnung und der Richtlinie 2002/58/EG klarzustellen, sollte die Richtlinie entsprechend geändert werden. Sobald diese Verordnung angenommen ist, sollte die Richtlinie 2002/58/EG einer Überprüfung unterzogen werden, um insbesondere die Kohärenz mit dieser Verordnung zu gewährleisten.*

27 *Artikel 6 Absatz 1c Datenschutz-Grundverordnung betrifft die Rechtmäßigkeit der Verarbeitung, zur Erfüllung einer rechtlichen Verpflichtung erforderlich ist, der der Verantwortliche unterliegt. Artikel 6 Absatz 1e Datenschutz-Grundverordnung betrifft die Rechtmäßigkeit der Verarbeitung, die für die Wahrnehmung einer Aufgabe erforderlich ist, die im öffentlichen Interesse liegt oder in Ausübung öffentlicher Gewalt erfolgt, die dem Verantwortlichen übertragen wurde.*

Die Rechtmäßigkeit der Verarbeitung durch Einwilligung gemäß Artikel 6 Absatz 1a Datenschutz-Grundverordnung ist von dieser Ausnahme nicht betroffen, so dass die Voraussetzungen der Datenschutz-Grundverordnung im Hinblick auf die Einwilligung eine abschließende Regelung enthalten. Dies entspricht gleichermaßen der Rechtsauffassung des Europäischen Gerichtshofs, die er zu Artikel 7f Richtlinie 95/46/EG in Bezug auf die angestrebte Vollharmonisierung vertreten hat. Gemäß der Intention des Europäischen Gerichthofs dürfen die Mitgliedstaaten weder neue Grundsätze in Bezug auf die Zulässigkeit der Verarbeitung personenbezogener Daten neben Art. 7 der Richtlinie 95/46/EG einführen, noch zusätzliche Bedingungen stellen, die die Tragweite eines der sechs in diesem Artikel vorgesehenen Grundsätze verändern würden.[28] Überträgt man diesen Gedanken auf die geplante Vollharmonisierung des Datenschutzrechts durch die Datenschutz-Grundverordnung -die keine konkreten Regelungen zur Datenverarbeitung in Verbindung mit elektronischen Kommunikationsdiensten enthält- ist daher fraglich, ob das aktuell geltende Telekommunikationsgesetz[29] zusätzliche Pflichten auferlegt bzw. auferlegen darf, die die Tragweite der Anforderungen an eine Einwilligung ändern.

In Bezug auf die inhaltliche Ausgestaltung der Einwilligung müsste hier die Überprüfung der Anforderungen im Rahmen einer elektronischen Einwilligung gemäß § 94 Telekommunikationsgesetz erfolgen und somit der Maßstab der Datenschutz-Grundverordnung sowie der Richtlinie 2002/58/EG zugrunde gelegt werden.[30] Bei dieser Auslegung können ebenso die Regelungen der Richtlinie 95/46/EG unterstützen. Denn Einwilligung bedeutet gemäß Artikel 2 f der Richtlinie 2002/58/EG eine Einwilligung im Sinne der Richtlinie 95/46/EG. Auch wenn letztere gemäß Artikel 94 Datenschutz-Grundverordnung aufgehoben wird, kann sie einen Hinweis dafür geben, was ursprünglich intendiert war oder nun als zusätzliche Verpflichtung bei Aufrechterhaltung der Voraussetzungen des Telekommunikationsgesetzes verstanden werden könnte.

Gemäß Artikel 94 Telekommunikationsgesetz ist eine elektronische Einwilligung möglich, wenn der Diensteanbieter sicherstellt, dass

1. der Teilnehmer oder Nutzer seine Einwilligung bewusst und eindeutig erteilt hat,
2. die Einwilligung protokolliert wird,
3. der Teilnehmer oder Nutzer den Inhalt der Einwilligung jederzeit abrufen kann und
4. der Teilnehmer oder Nutzer die Einwilligung jederzeit mit Wirkung für die Zukunft widerrufen kann.

28 Urteil des Europäischen Gerichtshofs (Dritte Kammer) vom 24.11.2011 bezüglich „Verarbeitung personenbezogener Daten – Richtlinie 95/46/ÆG – Art. 7 Buchst. f – Unmittelbare Wirkung“, in den verbundenen Rechtssachen C 468/10 und C 469/10 betreffend Vorabentscheidungsersuchen nach Art. 267 AEUV, eingereicht vom Tribunal Supremo (Spanien) mit Entscheidungen vom 15. Juli 2010: Die Vorabentscheidungsersuchen betrafen die Auslegung von Artikel 7f EU-Richtlinie 95/46/ÆG. Vom Europäischen Gerichtshof wurde hinsichtlich der Harmonisierung entschieden, dass die nationalen Rechtsvorschriften nicht auf eine Mindestharmonisierung beschränkt sind, sondern zu einer grundsätzlich umfassenden Harmonisierung führen. Art. 7 der Richtlinie 95/46 sehe eine erschöpfende und abschließende Liste der Fälle vor, in denen eine Verarbeitung personenbezogener Daten als rechtmäßig angesehen werden kann. Diese Auslegung werde durch die Formulierung „lediglich erfolgen darf, wenn eine der folgenden Voraussetzungen erfüllt ist“ in Art. 7 der Richtlinie 95/46 bestätigt, die den erschöpfenden und abschließenden Charakter der in diesem Artikel enthaltenen Liste unterstreicht. Der Europäische Gerichtshof hat insgesamt für Recht erkannt, dass dieser Artikel unmittelbare Wirkung hat und dahin auszulegen ist, „dass er einer nationalen Regelung entgegensteht, die für die Verarbeitung personenbezogener Daten, die zur Verwirklichung des berechtigten Interesses, das von dem für diese Verarbeitung Verantwortlichen oder von dem bzw. den Dritten wahrgenommen wird, denen diese Daten übermittelt werden, erforderlich ist, ohne Einwilligung der betroffenen Person nicht nur verlangt, dass deren Grundrechte und Grundfreiheiten nicht verletzt werden, sondern auch, dass diese Daten in öffentlich zugänglichen Quellen enthalten sind, und damit kategorisch und verallgemeinernd jede Verarbeitung von Daten ausschließt, die nicht in solchen Quellen enthalten sind.“

29 Telekommunikationsgesetz vom 22. Juni 2004 (BGBl. I S. 1190), das durch Artikel 9 des Gesetzes vom 26. 07.2016 (BGBl. I S. 1818) geändert worden ist.

30 Zur Verarbeitung von Verkehrsdaten siehe § 96 Telekommunikationsgesetz und die entsprechende Regelung in Artikel 6 der Richtlinie 2002/58/ÆG.

Erwägungsgrund 17 der Richtlinie 2002/58/EG legt fest, dass „für die Zwecke dieser Richtlinie die Einwilligung des Nutzers oder Teilnehmers unabhängig davon, ob es sich um eine natürliche oder eine juristische Person handelt, dieselbe Bedeutung haben sollte wie der in der Richtlinie 95/46/EG definierte und dort weiter präzisierte Begriff „Einwilligung der betroffenen Person. Die Einwilligung kann in jeder geeigneten Weise gegeben werden, wodurch der Wunsch des Nutzers in einer spezifischen Angabe zum Ausdruck kommt, die sachkundig und in freier Entscheidung erfolgt; hierzu zählt auch das Markieren eines Feldes auf einer Internet-Website."

Damit steht die elektronische Form im Einklang mit der Richtlinie 95/46/EG und der Datenschutz-Grundverordnung, da auch in letzterer keine gegenteiligen Anforderungen oder zusätzliche Pflichten enthalten sind.

Die jederzeitige Widerrufbarkeit gemäß § 94 Nr. 3 Telekommunikationsgesetz entspricht zudem Artikel 6 Absatz 3 der Richtlinie 2002/58/EG und legt dem Diensteanbieter damit keine zusätzlichen Pflichten auf.

Allerdings finden sich in der Richtlinie 2002/58/EG keine Anforderungen an die jederzeitige Abrufbarkeit oder die Protokollierung. Lediglich Artikel 5 Absatz 3 der Richtlinie 2002/58/EG regelt die Zulässigkeit der Verarbeitung von Verkehrsdaten im Zusammenhang mit Nachrichten, wenn es zum Nachweis einer kommerziellen Transaktion oder sonstigen geschäftlichen Nachricht geschieht. Eine Protokollierung von Text und Zeitpunkt der Einwilligung kann zwar den erforderlichen Nachweis gemäß Artikel 5 Absatz 2 und Artikel 7 Absatz 1 Datenschutz-Grundverordnung liefern, aber es könnten im Sinne einer europaweiten Vereinheitlichung gegebenenfalls weitere Methoden einer „Rechenschaftsverpflichtung" in Betracht kommen – was gesondert zu prüfen wäre. Daher kann sich an dieser Stelle ebenso die Ausarbeitung von Verhaltensregeln gemäß Artikel 40 Datenschutz-Grundverordnung empfehlen.[31] Wenn die Verarbeitungstätigkeit in mehreren Mitgliedstaaten betroffen ist, hat die Kommission die Möglichkeit, deren allgemeine Gültigkeit in der Union zu beschließen (Artikel 40 Absatz 7 bis Absatz 10 Datenschutz-Grundverordnung).

Fraglich ist daher, ob die Protokollierung und jederzeitige Abrufbarkeit im Telekommunikationsgesetz als zusätzliche Pflichten aufzufassen sind oder ob diese gerade eine erforderliche Transparenz sicherstellen und von den einzelnen Mitgliedstaaten gesetzlich geregelt werden können. Die Anforderungen an die Transparenz lassen sich nicht immer klar von der Einwilligung trennen.

Die ursprüngliche Intention ergibt sich aus Richtlinie 95/46/EG, auf deren Anforderungen die Richtlinie 2002/58/EG derzeit Bezug nimmt. Diese regelt hierzu zum einen, dass die Einwilligung gemäß Artikel 7a Richtlinie 95/46/EG „ohne jeden Zweifel" erteilt sein muss, was dafür sprechen kann, die Protokollierung regeln zu dürfen. Zum anderen sind in Erwägungsgrund 38 Vorgaben zur Transparenz enthalten. Danach setzt eine Datenverarbeitung nach Treu und Glauben voraus, dass die betroffenen Personen in der Lage sind, das Vorhandensein einer Verarbeitung zu erfahren und außerdem ordnungsgemäß und umfassend über die Bedingungen der Erhebung informiert werden, wenn Daten bei ihnen erhoben werden.

31 Verhaltensregeln, die die Anforderungen an die Rechtmäßigkeit der Datenverarbeitung der Datenverarbeitung präzisieren, können durch Verbände und andere Vereinigungen, die Kategorien von Verantwortlichen und Auftragsverarbeitern vertreten, ausgearbeitet werden (Artikel 40 Absatz 2 Datenschutz-Grundverordnung). Entwürfe der beabsichtigten Verhaltensregeln können der zuständigen Aufsichtsbehörde zur Genehmigung vorgelegt werden, die sie in ein Verzeichnis aufnimmt und veröffentlicht.

Im Vergleich dazu muss gemäß Artikel 4 Nr. 11 und Erwägungsgrund 32 der Datenschutz-Grundverordnung die Einwilligung informiert und unmissverständlich sein und nach Artikel 7 Absatz 1 obliegt dem Verantwortlichen der entsprechende Nachweis, ohne jedoch die konkrete Ausführung zu regeln. Gemäß dem aktuellen Verständnis sind Informationen „jederzeit abrufbar“, wenn sie für den Nutzer ohne großen Suchaufwand ständig zur Nutzung bereitgehalten werden.[32]

Die Abrufbarkeit der Information enthält zudem das Recht auf Auskunft, welches in der Datenschutz-Grundverordnung in Artikel 15 geregelt ist. In dieser Regelung findet sich jedoch ebenso wenig eine Verpflichtung der „jederzeitigen“ Abrufbarkeit. Erwägungsgrund 63 regelt vielmehr, dass eine betroffene Person ein Auskunftsrecht hinsichtlich der sie betreffenden personenbezogenen Daten, die erhoben worden sind, besitzen und dieses Recht problemlos und in angemessenen Abständen wahrnehmen können sollte, um sich der Verarbeitung bewusst zu sein und deren Rechtmäßigkeit überprüfen zu können.

Die Frage ist folglich, ob die oben genannten Regelungen des Telekommunikationsgesetzes tatsächlich über die ursprüngliche Intention der Richtlinie 2002/58/EG in Verbindung mit der Richtlinie 95/46/EG hinausgehen und zusätzliche Pflichten auferlegen, die gemäß Artikel 95 Datenschutz-Grundverordnung nicht beabsichtigt sind - unter der Maßgabe, dass diese hinsichtlich der Einwilligungsvoraussetzungen abschließende Regelungen enthält.

Ähnliche Fragestellungen ergeben sich für die Verarbeitung von Standortdaten. § 98 Telekommunikationsgesetz regelt folgendes:
Werden die Standortdaten für einen Dienst mit Zusatznutzen verarbeitet, der die Übermittlung von Standortdaten eines Mobilfunkendgerätes an einen anderen Teilnehmer oder Dritte, die nicht Anbieter des Dienstes mit Zusatznutzen sind, zum Gegenstand hat, muss der Teilnehmer abweichend von § 94 Telekommunikationsgesetz seine Einwilligung ausdrücklich, gesondert und schriftlich gegenüber dem Anbieter des Dienstes mit Zusatznutzen erteilen.

In der Richtlinie 2002/58/EG sind Regelungen über Standortdaten in Artikel 9 enthalten. Ein Dienst mit Zusatznutzen ist in Artikel 2g sowie Erwägungsgrund 18 definiert und umfasst beispielsweise die Beratung hinsichtlich der billigsten Tarifpakete, Navigationshilfen, Verkehrsinformationen, Wettervorhersage oder touristische Informationen.

Dies bedeutet etwa bei einem Dienst, der Standortdaten zum Zwecke einer Wettervorhersage oder touristischen Informationen an Dritte übermittelt, dass vor der ersten Ortung eine ausdrückliche, gesonderte und schriftliche Einwilligung gegenüber dem Ortungsdiensteanbieter erfolgen muss.[33]

Hier ist fraglich, ob diese Regelung nicht eher dem Teilnehmer als betroffener Person eine „zusätzliche Pflicht“ auferlegt und ob dies ebenso von dem Gedanken des Artikel 95 Datenschutz-Grundverordnung umfasst ist. Außerdem könnten die Erteilung der Einwilligung „ohne jeden Zweifel“ gemäß der Richtlinie 95/46/EG sowie „unmissverständlich“ gemäß dem Erwägungsgrund 32 der Datenschutz-Grundverordnung ebenso dafür sprechen, die ausdrückliche und schriftliche Einwilligung beizubehalten und nicht als zusätzliche Pflicht zu sehen.

32 Siehe Spindler/Nink in: Spindler/Schuster, Recht der elektronischen Medien, 3. Auflage 2015, § 13 TMG Rn. 8, jedoch als Auslegung für die sprachlich identische Regelung im Telemediengesetz.

33 Siehe auch „Die Bundesbeauftragte für den Datenschutz und die Informationsfreiheit“, Datenschutz und Telekommunikation, 7. Auflage 2015, S. 25; https://www.bfdi.bund.de/SharedDocs/Publikationen/Infobroschueren/INFO5.pdf?__blob=publicationFile&v=6

In Erwägungsgrund 32 ist zudem die Möglichkeit der schriftlichen Einwilligung benannt, die gleichermaßen die Nachweispflicht des Artikel 7 Absatz 1 Datenschutz-Grundverordnung unterstützt. Auf der anderen Seite ist in der Richtlinie 2002/58/EG geregelt (Erwägungsgrund 17), dass die Einwilligung „in jeder geeigneten Weise“ erfolgen kann.

! Fazit Nr. 1

Es empfiehlt sich eine Klarstellung,

- was unter „zusätzlichen Pflichten“ (im Verhältnis zur Richtlinie 2002/58/EG) zu verstehen ist und welche eigenständigen gesetzlichen Regelungen der Mitgliedstaaten einer Vollharmonisierung (dennoch) entsprechen (z. B. jederzeitige Abrufbarkeit und Protokollierung oder in Bezug auf Standortdaten: „ausdrücklich, gesondert und schriftlich“). 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.

- ob sich der Begriff „zusätzlichen Pflichten“ sowohl auf die betroffene Person als auch auf den Verantwortlichen bezieht.

(2) Richtlinie 2002/58/EG in der Fassung 2009/136/EG

Die Richtlinie 2002/58/EG (in der Fassung 2009/136/EG) enthält in Artikel 5 folgende Regelung:
„(3) Die Mitgliedstaaten stellen sicher, dass die Speicherung von Informationen oder der Zugriff auf Informationen, die bereits im Endgerät eines Teilnehmers oder Nutzers gespeichert sind, nur gestattet ist, wenn der betreffende Teilnehmer oder Nutzer auf der Grundlage von klaren und umfassenden Informationen, die er gemäß der Richtlinie 95/46/EG u. a. über die Zwecke der Verarbeitung erhält, seine Einwilligung gegeben hat. Dies steht einer technischen Speicherung oder dem Zugang nicht entgegen, wenn der alleinige Zweck die Durchführung der Übertragung einer Nachricht über ein elektronisches Kommunikationsnetz ist oder wenn dies unbedingt erforderlich ist, damit der Anbieter eines Dienstes der Informationsgesellschaft, der vom Teilnehmer oder Nutzer ausdrücklich gewünscht wurde, diesen Dienst zur Verfügung stellen kann.“

Erwägungsgrund 17 der Richtlinie 2002/58/EG regelt hierzu näher, dass die Einwilligung dieselbe Bedeutung haben sollte wie der in der Richtlinie 95/46/EG definierte und dort weiter präzisierte Begriff „Einwilligung der betroffenen Person“. Gemäß Artikel 94 Absatz 2 Datenschutz-Grundverordnung gelten Verweise auf die aufgehobene Richtlinie als Verweise auf die Datenschutz-Grundverordnung. Daher ist fraglich, ob Unterschiede in Bezug auf die Einwilligungsvoraussetzungen der Datenschutz-Grundverordnung vorliegen könnten. Hierbei ist gleichermaßen relevant, wie die Richtlinie derzeit umgesetzt wird.

Gemäß der Richtlinien 2002/58/EG und 95/46/EG könne die Einwilligung in jeder geeigneten Weise abgegeben werden, wodurch der Wunsch des Nutzers in einer spezifischen Angabe zum Ausdruck komme, die sachkundig und in freier Entscheidung erfolgt; hierzu zähle auch das Markieren eines Feldes auf einer Internet-Website.

In Bezug auf Cookies enthalten jedoch Erwägungsgründe 24 und 25 der Richtlinie 2002/58/EG gesonderte Regelungen. Es wird zwar einerseits auf das Risiko von Cookies Bezug genommen, welches eine ernsthafte Verletzung der Privatsphäre beinhalten könnte.[34] Gleichzeitig wird aber ebenso die Nützlichkeit als legitimes Hilfsmittel hervorgehoben, um die Wirksamkeit von Website-Gestaltung und Werbung zu untersuchen und die Identität der an Online-Transaktionen beteiligten Nutzer zu überprüfen.[35] In diesem Sinne könnten solche Instrumente, z. B. „Cookies", einem rechtmäßigen Zweck dienen, z. B. der Erleichterung der Bereitstellung von Diensten der Informationsgesellschaft. Daher sollte deren Einsatz auch unter der Bedingung zugelassen werden, dass die Nutzer gemäß der Richtlinie 95/46/EG klare und genaue Informationen über den Zweck von Cookies oder ähnlichen Instrumenten erhalten, d. h., der Nutzer müsse wissen, dass bestimmte Informationen auf dem von ihm benutzten Endgerät platziert werden.

Erwägungsgrund 66 der Richtlinie 2009/136/EG betont gleichermaßen die legitimen Zwecke bei Verwendung von Cookies. Daher sei es wichtig, den Nutzern klare und verständliche Informationen bereit zu stellen. Es sollten ebenso benutzerfreundliche Methoden zur Ablehnung von Cookies gestaltet werden. Ausnahmen von der Informationspflicht und der Einräumung des Rechts auf Ablehnung sollten zudem auf jene Situationen beschränkt sein, in denen die technische Speicherung oder der Zugriff unverzichtbar sind, um die Nutzung eines vom Teilnehmer oder Nutzer ausdrücklich angeforderten Diens¬tes zu ermöglichen. Wenn es technisch möglich sei, könne der Nutzer außerdem seine Einwilligung im Einklang mit den entsprechenden Bestimmungen der Richtlinie 95/46/EG über die Handhabung der entsprechenden Einstellungen eines Browsers oder einer anderen Anwendung ausdrücken. Letzteres sieht die Artikel-29-Datenschutzgruppe allerdings als kritisch an.[36]

In einzelnen Mitgliedsstaaten der Europäischen Union ist die Richtlinie 2002/58/EG (2009/136/EG) jedoch unterschiedlich angewendet worden. Die Ausführungen in den oben genannten Erwägungsgründen zur Rechtmäßigkeit von Cookies zur Webseitengestaltung sind im Jahre 2015 von der niederländischen Regierung im Sinne eines weiten Verständnisses ausgelegt worden, obwohl die Niederlande bislang die engste Interpretation der Richtlinien 95/46/EG sowie 2002/58/EG (2009/136/EG) hatten.

34 *Erwägungsgrund 24 der Richtlinie 2002/58/ÆG: Die Endgeräte von Nutzern elektronischer Kommunikationsnetze und in diesen Geräten gespeicherte Informationen sind Teil der Privatsphäre der Nutzer, die dem Schutz aufgrund der Europäischen Konvention zum Schutze der Menschenrechte und Grundfreiheiten unterliegt. Sogenannte „Spyware", „Web-Bugs", „Hidden Identifiers" und ähnliche Instrumente können ohne das Wissen des Nutzers in dessen Endgerät eindringen, um Zugang zu Informationen zu erlangen, oder die Nutzeraktivität zurückzuverfolgen und können eine ernsthafte Verletzung der Privatsphäre dieser Nutzer darstellen. Die Verwendung solcher Instrumente sollte nur für rechtmäßige Zwecke mit dem Wissen der betreffenden Nutzer gestattet sein.*

35 *Erwägungsgrund 25 der Richtlinie 2002/58/ÆG: Solche Instrumente, z. B. so genannte „Cookies", können ein legitimes und nützliches Hilfsmittel sein, um die Wirksamkeit von Website-Gestaltung und Werbung zu untersuchen und die Identität der an Online-Transaktionen beteiligten Nutzer zu überprüfen. Dienen solche Instrumente, z. B. „Cookies", einem rechtmäßigen Zweck, z. B. der Erleichterung der Bereitstellung von Diensten der Informationsgesellschaft, so sollte deren Einsatz unter der Bedingung zugelassen werden, dass die Nutzer gemäß der Richtlinie 95/46/ÆG klare und genaue Informationen über den Zweck von Cookies oder ähnlichen Instrumenten erhalten, d. h., der Nutzer muss wissen, dass bestimmte Informationen auf dem von ihm benutzten Endgerät platziert werden. Die Nutzer sollten die Gelegenheit haben, die Speicherung eines Cookies oder eines ähnlichen Instruments in ihrem Endgerät abzulehnen. Dies ist besonders bedeutsam, wenn auch andere Nutzer Zugang zu dem betreffenden Endgerät haben und damit auch zu dort gespeicherten Daten, die sensible Informationen privater Natur beinhalten. Die Auskunft und das Ablehnungsrecht können einmalig für die Nutzung verschiedener in dem Endgerät des Nutzers während derselben Verbindung zu installierender Instrumente angeboten werden und auch die künftige Verwendung derartiger Instrumente umfassen, die während nachfolgender Verbindungen vorgenommen werden können. Die Modalitäten für die Erteilung der Informationen oder für den Hinweis auf das Verweigerungsrecht und die Einholung der Zustimmung sollten so benutzerfreundlich wie möglich sein. Der Zugriff auf spezifische Website-Inhalte kann nach wie vor davon abhängig gemacht werden, dass ein Cookie oder ein ähnliches Instrument von einer in Kenntnis der Sachlage gegebenen Einwilligung abhängig gemacht wird, wenn der Einsatz zu einem rechtmäßigen Zweck erfolgt.*

36 *Artikel-29-Datenschutzgruppe, WP 171 Stellungnahme 2/2010 zur Werbung auf Basis von Behavioural Targeting, angenommen am 22. Juni 2010, S. 16 ff.*

Nun ist per Gesetz der Einsatz von Cookies auch ohne vorheriges ausdrückliches Einverständnis für Analysezwecke des Webseitenbetreibers erlaubt, die die Privatsphäre des Nutzers nicht wesentlich beeinträchtigen.[37]

In Deutschland gelten für Cookies §§ 12 und 15 Telemediengesetz. Die deutsche Bundesregierung erläutert in ihren Antworten an die Europäische Kommission zur Umsetzung von Artikel 5 Absatz 3 Richtlinie 2002/58/EG, dass „§ 12 Telemediengesetz klarstellt, dass personenbezogene Daten im Zusammenhang mit der Bereitstellung von Telemedien ohne Einwilligung nur verarbeitet werden dürfen, wenn der Gesetzgeber dies ausdrücklich erlaubt. Eine solche gesetzliche Erlaubnis enthalte § 15 Telemediengesetz. Danach dürfen Nutzerdaten bei Inanspruchnahme von Telemedien ohne Einwilligung nur verarbeitet werden, wenn das für diesen Zweck erforderlich ist. Für die Speicherung und den Abruf von Informationen wie z. B. Cookies bedeutet dies, dass solche Verfahren in Deutschland ohne Einwilligung des Nutzers nur zulässig sind, wenn dies aus technischen Gründen für die Inanspruchnahme erforderlich ist. Im Übrigen dürfen solche Verfahren ohne Einwilligung des Nutzers nicht verwendet werden."[38]

Die unabhängige Datenschutzaufsichtsbehörde (ICO) von Großbritannien hat eine Empfehlung für die Verwendung von Cookies veröffentlicht und unterteilt zwischen den erforderlichen Zwecken (etwa für elektronischen Einkauf) ohne Einwilligung und „nützlichen" Zwecken, für die eine Einwilligung erforderlich sein soll. Eine konkludente, bewusste Einwilligung sei möglich:[39]

! You must tell people if you set cookies, and clearly explain what the cookies do and why. You must also get the user's consent. Consent can be implied, but must be knowingly given.

! There is an exception for cookies that are essential to provide an online service at someone's request (e.g. to remember what's in their online basket, or to ensure security in online banking).

The same rules also apply if you use any other type of technology to store or gain access to information on someone's device.[40]

37 *https://www.acm.nl/en/publications/publication/11917/Frequently-asked-questions-about-the-Dutch-cookie-act/; https://zoek.officielebekendmakingen.nl/stb-2015-100.html; http://www.vbk.nl/en/sharing-knowledge/legal-update/new-dutch-cookie-law-is-now-in-force/ Siehe außerdem Artikel-29-Datenschutzgruppe, WP 194, Stellungnahme 04/2012 zur Ausnahme von Cookies von der Einwilligungspflicht, angenommen am 07. Juni 2012, insbesondere S. 11/12 zu den so genannten First-Party-Analysecookies.*

38 *Siehe unter: https://circabc.europa.eu/sd/d/9762ba56-a9b0-48e2-9858-1e25f2ea05cc/COCOM11-20%2520Questionnaire%25 5200n%2520Art.%25205(3)%2520e-Privacy%2520Dir..pdf+&cd=6&hl=de&ct=clnk&gl=de*

39 *https://ico.org.uk/; https://ico.org.uk/media/for-organisations/documents/1545/cookies_guidance.pdf*

40 *https://ico.org.uk/for-organisations/guide-to-pecr/cookies-and-similar-technologies/*

Die Datenschutzaufsichtsbehörde (ICO) vertritt außerdem die Auffassung, dass die Einwilligung nicht ausdrücklich zu erteilen ist[41]:

! Consent does not necessarily have to be explicit 'opt-in' consent. Implied consent can also be valid. If you are relying on implied consent, you need to be confident that your users fully understand that their actions will result in cookies being set. However, in some circumstances (for example, collecting sensitive personal data such as health details) it is likely that explicit opt-in consent is more appropriate.

Des weiteren lässt auch die eigene Webseite der Datenschutzaufsichtsbehörde (ICO) zur „Verbesserung ihrer Webseite" Cookies sowie ein Opt-Out zu. Fraglich ist zudem, was unter „anonymer Form einer Cookie-Sammlung" im Rahmen der Informationen auf der Webseite verstanden wird:

! We have placed cookies on your device to help make this website better.

You can use this tool to change your cookie settings. Otherwise, we´ll assume you are OK to continue.

I'm fine with this

Information and SettingsAbout this tool:
You can use this tool to change your cookie settings. Otherwise, we'll assume you're OK to continue.
Some of the cookies we use are essential for the site to work.

We also use some non-essential cookies to collect information for making reports and to help us improve the site. The cookies collect information in an anonymous form.

To control third party cookies, you can also adjust your browser settings.

Turn cookies off

I'm fine with this

Die Artikel-29-Datenschutzgruppe hat in ihrer Stellungnahme zu Cookies eine solche Unterscheidung nicht vorgenommen und die Richtlinie 2002/58/EG als Spezialgesetz gegenüber der Richtlinie 95/46/EG eingestuft.[42] In diesem Sinne soll die Richtlinie 95/46/EG vollumfänglich anwendbar bleiben mit der Ausnahme der Bestimmungen, die in der Datenschutzrichtlinie für elektronische Kommunikation direkt behandelt werden.

41 https://ico.org.uk/for-organisations/guide-to-pecr/cookies-and-similar-technologies/

42 Artikel-29-Datenschutzgruppe, WP 171 Stellungnahme 2/2010 zur Werbung auf Basis von Behavioural Targeting, angenommen am 22. Juni 2010, S. 11/12.

Dies gelte in erster Linie für die Regelung des Artikels 7 der Richtlinie 95/46/EG zu den Rechtsgrundlagen für die Datenverarbeitung, wobei aber die verbleibenden Bestimmungen der Richtlinie 95/46/EG einschließlich der Grundsätze bezüglich der Datenqualität, der Rechte der betroffenen Personen (wie das Auskunftsrecht, das Recht auf Löschung und das Widerspruchsrecht), der Vertraulichkeit, der Sicherheit der Verarbeitung und der internationalen Datenübermittlungen vollumfänglich anzuwenden seien.[43]

Soweit die Neufassung von Richtlinie 2002/58/EG (2009/136/EG) keine anderweitige Klarstellung schafft, muss dies gleichermaßen im Hinblick auf die Datenschutz-Grundverordnung gelten – mit Ausnahme der Regelungen die den Diensteanbietern zusätzliche Pflichten auferlegen.

Die Artikel- 29-Datenschutzgruppe führt insgesamt aus:
Soweit die Neufassung von Richtlinie 2002/58/EG (2009/136/EG) keine anderweitige Klarstellung schafft, muss dies gleichermaßen im Hinblick auf die Datenschutz-Grundverordnung gelten – mit Ausnahme der Regelungen die den Diensteanbietern zusätzliche Pflichten auferlegen.

! Die Artikel- 29-Datenschutzgruppe führt insgesamt aus:
Aus dem Wortlaut von Artikel 5 Absatz 3 ergibt sich, dass: i) die Einwilligung eingeholt werden muss, bevor der Cookie platziert wird und/oder auf dem Endgerät des Nutzers gespeicherte Informationen gesammelt werden, was üblicherweise als vorherige Einwilligung bezeichnet wird und ii) eine Einwilligung in Kenntnis der Sachlage nur dann eingeholt werden kann, wenn dem Nutzer vorher Informationen über das Versenden und die Zwecke des Cookies erteilt wurden. In diesem Zusammenhang muss berücksichtigt werden, dass eine Einwilligung ungeachtet der jeweiligen Umstände, nur dann gültig ist, wenn sie ohne Zwang, für den konkreten Fall und in Kenntnis der Sachlage erfolgt ist. Die Einwilligung muss vor Erhebung der personenbezogenen Daten eingeholt werden, damit die betroffenen Personen voll und ganz erkennen, dass sie einwilligen und in was sie einwilligen. Darüber hinaus muss eine Einwilligung zurückziehbar sein.

Einwilligungen über Browserseinstellungen sieht die Artikel-29-Datenschutzgruppe als kritisch an,[44] auch wenn Erwägungsgrund 66 der geänderten Datenschutzrichtlinie für elektronische Kommunikation darauf hinweist, dass die Einwilligung ebenso über Handhabung der entsprechenden Einstellungen eines Browsers oder einer anderen Anwendung, wenn es technisch durchführbar und wirksam ist, im Einklang mit den Bestimmungen der Richtlinie 95/46/EG ausgedrückt werden kann.

Zusammenfassend ist festzuhalten:
In Artikel 5 Absatz 3 der Richtlinie 2002/58/EG (2009/136/EG) wird die Einwilligungspflicht für Cookies normiert. Fraglich ist jedoch, aus welchem Grunde in den Mitgliedstaaten eine unterschiedliche Auslegung erfolgt und ob dies durch die Erwägungsgründe hervorgerufen wird, oder ob tatsächlich ein Vertragsverletzungsverfahren eingeleitet werden müsste.

Für eine unterschiedliche Auslegungsmöglichkeit könnten die nicht eindeutig formulierten Erwägungsgründe sowie die Möglichkeit einer konkludenten Einwilligung sprechen: Erwägungsgrund 66 normiert eine Ausnahme von der Informationspflicht und dem Recht auf Ablehnung für unverzichtbare Cookies.

43 *Artikel-29-Datenschutzgruppe, WP 171 Stellungnahme 2/2010 zur Werbung auf Basis von Behavioural Targeting, angenommen am 22. Juni 2010, S.12.*

44 *Siehe bereits oben, Fn. 34.*

In Erwägungsgrund 25 werden Cookies als legitime und nützliche Hilfsmittel zur Webseiten-Gestaltung und zur Untersuchung von Werbung erläutert. Im Anschlusssatz erfolgt dann die Klarstellung, dass bei Verwendung von Cookies zu einem rechtmäßigen Zweck dem Nutzer klare und genaue Informationen bereitgestellt werden müssen und die Nutzer die Gelegenheit haben, diesen abzulehnen.[45]

Im Übrigen lässt sich bei einem Cookie der Nachweis der Einwilligung (immanent) gemäß Artikel 7 Absatz 1 Datenschutz-Grundverordnung bzw. aufgrund der Darstellung der Webseite leicht erbringen.

! Fazit Nr. 2

Es empfehlen sich europaweite, einheitlich geltende Verhaltensregeln zur Auslegung der Einwilligungsvoraussetzungen, soweit diese aufgrund einer Verarbeitungstätigkeit in mehreren Mitgliedstaaten ausgearbeitet werden können. Aktuell ist in Bezug auf Cookies unklar, ob die Einleitung von Vertragsverletzungsverfahren durch die Kommission versäumt wurde.

Ohne europaweite Verhaltensregelungen läuft außerdem die Nachweispflicht der Einwilligung gemäß Artikel 7 Absatz 1 Datenschutz-Grundverordnung ins Leere bzw. wird den Aufsichtsbehörden in den Mitgliedstaaten überlassen. Schutzniveau und Sanktionen sollten im Sinne einer Harmonisierung gleichwertig sein.

Darüber hinaus empfiehlt sich der Vergleich zwischen der Richtlinie 95/46/EG, der Umsetzung durch die Mitgliedstaaten sowie der Datenschutz-Grundverordnung im Hinblick auf die Anforderungen der Einwilligung. So kann ebenso geprüft werden, ob eine Tendenz für den Inhalt der auszuarbeitenden Verhaltensregeln hergeleitet werden könnte, vor allem dahingehend, was als zusätzliche Pflicht gemäß Artikel 95 Datenschutz-Grundverordnung und was als sinnvolle Ergänzung zu verstehen ist.

Konkret könnte eine Klarstellung dahingehend erfolgen,

- ob die Datenschutz-Grundverordnung grundlegend andere Voraussetzungen an die Einwilligung oder Anonymisierung stellt als die Richtlinie 95/46/EG und ob bislang die Einleitung von Vertragsverletzungsverfahren versäumt wurde,

- welche Grenzen eine konkludente Einwilligung hat, etwa dass eine Weiternutzung des Dienstes gleichzusetzen ist mit „voreingestellte Kästchen“ und dass ein Mehr an Transparenz in diesem Falle nicht die Einwilligung ersetzen kann.

- was unter einer sonstigen eindeutigen bestätigenden Verhaltensweise gemäß Artikel 4 Nr. 11 Datenschutz-Grundverordnung zu verstehen ist.[46]

45 *Siehe Spindler/Nink in: Spindler/Schuster, Recht der elektronischen Medien, 3. Auflage 2015, § 13 TMG Rn. 6 mit dem Hinweis auf nicht hinreichende Bestimmtheit der Richtlinie: „Dem ist entgegen zu halten, dass Bestimmungen aus Richtlinien nach erfolglosem Ablauf der Umsetzungsfrist nur dann unmittelbar in den EU-Mitgliedstaaten gelten, wenn sie derart hinreichend bestimmt sind, dass sie ohne weiteres angewandt werden können. Dies wird jedoch bei der Cookie-Regelung der ePrivacy-Richtlinie gerade kontrovers diskutiert. Denn nach wie vor ist unklar, wie die Umsetzung der Einwilligung in Cookies erfolgen kann. Die Mitgliedstaaten, welche die ePrivacy-Richtlinie bislang ungesetzt haben, implementierten teilweise völlig unterschiedliche Anforderungen an die Einwilligung in den nationalen Gesetzen. Es bestehen daher erhebliche Zweifel, ob die Cookie-Regelung der ePrivacy-Richtlinie tatsächlich hinreichend bestimmt ist.“*

46 *Hier ist die Auffassung der Artikel-29-Datenschutzgruppe zu berücksichtigen, die feststellt, dass ein Opt-Out bei Cookies im Allgemeinen keinen angemessenen Mechanismus in Kenntnis der Sachlage darstellt.*

! Die bisherigen Empfehlungen der Artikel-29-Datenschutzgruppe könnten bei der Ausarbeitung von Verhaltensregeln zugrunde gelegt werden. Hierzu gehört ebenso die Stellungnahme WP 194 zur Ausnahme von Cookies von der Einwilligungspflicht[47], die unter anderem Leitlinien zu „erforderlichen" Cookies und Cookies für eigene Analysezwecke des Dienstanbieters enthält, die nach Ansicht der Artikel-29-Datenschutzgruppe kaum ein Datenschutzrisiko darstellen, wenn sie ausschließlich für die aggregierten Statistiken des Erstanbieters genutzt werden. In diesem Zusammenhang sollten darüber hinaus jedoch klare Kriterien entwickelt werden, unter welchen Voraussetzungen „keine erhebliche Persönlichkeitsrechtsverletzung" der Nutzer oder „kaum ein Datenschutzrisiko" vorliegt, was aufgrund der (zukünftig) noch unbekannten Verknüpfungsmöglichkeiten von persönlichen Daten mit Schwierigkeiten verbunden sein könnte. Entsprechendes gilt für Cookies zur Webseitengestaltung und Werbung. Insoweit sind die Erwägungsgründe der Richtlinie 2002/58/EG nicht eindeutig, die Cookies zur Webseitengestaltung und Werbung als legitimes Mittel betrachten.

2. Dienste der Informationsgesellschaft

Die Datenschutz-Grundverordnung lässt gemäß Artikel 2 Absatz 4 die Anwendbarkeit der Richtlinie 2000/31/EG unberührt.[48] Gegenstand dieser Richtlinie sind Dienste der Informationsgesellschaft. Gemäß Artikel 1 Nr. 2 der Richtlinie 98/34/EG in der Fassung von der Richtlinie 98/48/EG bedeutet Dienst der Informationsgesellschaft jede in der Regel gegen Entgelt elektronisch im Fernabsatz und auf individuellen Abruf eines Empfängers erbrachte Dienstleistung.[49] Allerdings enthält diese Verordnung keine speziellen Regelungen zur Einwilligung und Transparenz. Artikel 5 der Richtlinie 2000/31/EG enthält zwar Regelungen zu Impressumsangaben, Artikel 6 Maßnahmen im Hinblick auf kommerzielle Kommunikation und Artikel 10 verbraucherschutzrechtliche Bestimmungen bezüglich der Abgabe einer Bestellung unter Inanspruchnahme eines Dienstes der Informationsgesellschaft. Es werden jedoch weder allgemeine Pflichten im Hinblick auf die Informiertheit bei Erteilung der Einwilligung noch konkrete Anforderungen an die Einwilligung festgelegt.

47 *Artikel-29-Datenschutzgruppe, WP 194, Stellungnahme 04/2012 zur Ausnahme von Cookies von der Einwilligungspflicht, angenommen am 07. Juni 2012, insbesondere S. 11/12 zu den so genannten First-Party-Analysecookies.*

48 *Richtlinie 2000/31/EG des Europäischen Parlaments und des Rates vom 8. Juni 2000 über bestimmte rechtliche Aspekte der Dienste der Informationsgesellschaft, insbesondere des elektronischen Geschäftsverkehrs, im Binnenmarkt („Richtlinie über den elektronischen Geschäftsverkehr") (Amtsblatt Nr. L 178 vom 17.7.2000, S. 1 – S. 16). Das Telemediengesetz dient der Umsetzung der Richtlinie 2000/31/EG.*

49 *Richtlinie 98/48/EG des Europäischen Parlaments und des Rates vom 20. Juli 1998 zur Änderung der Richtlinie 98/34/EG über ein Informationsverfahren auf dem Gebiet der Normen und technischen Vorschriften*
Amtsblatt Nr. L 217 vom 05.08.1998 S. 18 – S. 26.
Im Sinne dieser Definition bezeichnet der Ausdruck
- ´im Fernabsatz erbrachte Dienstleistung' eine Dienstleistung, die ohne gleichzeitige physische Anwesenheit der Vertragsparteien erbracht wird;
- ´elektronisch erbrachte Dienstleistung' eine Dienstleistung, die mittels Geräten für die elektronische Verarbeitung (einschließlich digitaler Kompression) und Speicherung von Daten am Ausgangspunkt gesendet und am Endpunkt empfangen wird und die vollständig über Draht, über Funk, auf optischem oder anderem elektromagnetischem Wege gesendet, weitergeleitet und empfangen wird;
- ´auf individuellen Abruf eines Empfängers erbrachte Dienstleistung' eine Dienstleistung, die durch die Übertragung von Daten auf individuelle Anforderung erbracht wird.
Zur Auslegung eines Dienstes mit Zusatznutzen im deutschen Recht anhand der Frage, ob es sich um einen Telemediendienst mit Anwendbarkeit des Telemediengesetzes handelt oder ob die Regelungen des Telekommunikationsgesetzes abschließend anwendbar sind: Schnabel, Datenschutz bei profilbasierten Location-based Services, Die datenschutzadäquate Gestaltung von Service-Plattformen zur Mobilkommunikation, S. 275, 276 ff. Außerdem Janner/Holst/Kopp, Social Media im Kulturmanagement, S. 109 mit dem Hinweis, dass sich die Verwendung von Standortdaten für Telekommunikationsdiensteanbieter nicht nach dem Telemediengesetz, sondern nach §§ 96 und 98 Telekommunikationsgesetz richtet.

Im Hinblick auf die Transparenz (Informations- und Auskunftspflichten) sowie die Einwilligung sind daher die Datenschutz-Grundverordnung sowie die Richtlinie 2002/58/EG (2009/136/EG) zugrunde zu legen, soweit letztere den Umgang mit „Informationen, die im Endgerät des Kunden gespeichert sind“ oder „Dienste mit Zusatznutzen“ regelt.[50]

Daher müssen im Hinblick auf die Vorgaben für Transparenz und Einwilligung die Regelungen der Datenschutz-Grundverordnung herangezogen werden, anhand derer auch die datenschutzrechtlichen Regelungen des Telemediengesetzes für elektronische Informations- und Kommunikationsdienste zu prüfen sind:

Die Datenschutz-Grundverordnung regelt in Artikel 12 ff. die Modalitäten der Transparenz, in Artikel 13 dazu näher die Informationspflichten, sofern personenbezogene Daten bei der betroffenen Person erhoben werden. Diesbezüglich enthält die Datenschutz-Grundverordnung außerdem keine generelle Öffnungsklausel für Regelungen durch die Mitgliedstaaten. Beschränkungen dieser Rechte und Pflichten dürfen allenfalls unter den Voraussetzungen des Artikel 23 Datenschutz-Grundverordnung erfolgen. Daher müssen auch die datenschutzrechtlichen Regelungen des Telemediengesetzes mit diesen Anforderungen vereinbar sein: Im Hinblick auf die Informiertheit ist § 13 Telemediengesetz einschlägig, bezüglich der elektronischen Einwilligung enthält § 13 Absatz 2 Telemediengesetz eine zu § 94 Telekommunikationsgesetz inhaltsgleiche Regelung. Für letztere gelten die obigen Ausführungen entsprechend,[51] so dass im Hinblick auf die elektronische Einwilligung gemäß § 13 Absatz 2 Telemediengesetz fraglich ist, ob die Regelungen zur inhaltlichen Ausgestaltung der Einwilligung, nämlich „jederzeit abrufbar und protokolliert“, aufrechterhalten werden können.

Die Datenschutz-Grundverordnung verlangt bezüglich der vorformulierten Einwilligung gemäß Erwägungsgrund 42 lediglich die leicht zugängliche Form. § 13 Absatz 2 Nr. 3 Telemediengesetz enthält allerdings bereits jetzt eine insoweit konforme Regelung, als auch in Artikel 7 Absatz 3 Datenschutz-Grundverordnung vorgegeben ist, dass die betroffene Person vor Abgabe der Einwilligung von der Widerrufsmöglichkeit in Kenntnis zu setzen ist.

50 Zur Auslegung eines Dienstes mit Zusatznutzen im deutschen Recht anhand der Frage, ob es sich um einen Telemediendienst mit Anwendbarkeit des Telemediengesetzes handelt oder ob die Regelungen des Telekommunikationsgesetzes abschließend anwendbar sind: Schnabel, Datenschutz bei profilbasierten Location-based Services, Die datenschutzadäquate Gestaltung von Service-Plattformen zur Mobilkommunikation, S. 275, 276 ff. Außerdem Janner/Holst/Kopp, Social Media im Kulturmanagement, S. 109 mit dem Hinweis, dass sich die Verwendung von Standortdaten für Telekommunikationsdiensteanbieter nicht nach dem Telemediengesetz, sondern nach §§ 96 und 98 Telekommunikationsgesetz richtet.

51 Siehe S. 9 ff.

Hinsichtlich der grundsätzlichen Transparenz der Datenverarbeitung und Informiertheit besteht gemäß § 13 Absatz 1 Satz 3 Telemediengesetz außerdem die Verpflichtung des Diensteanbieters, dass der Inhalt der Unterrichtung für den Nutzer jederzeit abrufbar sein muss. In der Datenschutz-Grundverordnung ist zwar nun der Grundsatz der Transparenz ausdrücklich benannt (siehe Artikel 5 Absatz 1a, Artikel 12). Eine Verpflichtung, dass Informationen für den Nutzer jederzeit abrufbar sein müssen, ist jedoch nicht enthalten. Im Gegensatz zu den in Artikel 5 der Richtlinie 2000/31/EG geregelten Impressumsangaben, nach denen die Mitgliedstaaten sicherstellen müssen, dass der Diensteanbieter den Nutzern des Dienstes die dort aufgeführten Informationen leicht, unmittelbar und ständig verfügbar machen muss, ist im Hinblick auf die datenschutzrechtlichen Informationspflichten eine solche ständige Verfügbarkeit nicht verlangt.[52] Aus der Datenschutz-Grundverordnung (Artikel 15 und Erwägungsgrund 63) kann eine solche Verpflichtung ebenso wenig unmittelbar hergeleitet werden.[53]

Für die Dienste der Informationsgesellschaft ergibt sich im Vergleich zwischen Telemediengesetz und Datenschutz-Grundverordnung ein weiterer Unterschied dahingehend, dass gemäß § 13 Absatz 1 Telemediengesetz die Unterrichtung eines Nutzers über Art, Umfang und Zwecke der Erhebung und Verwendung personenbezogener Daten zu Beginn des Nutzungsvorgangs erfolgen muss.[54] Hiervon abweichend regelt Artikel 13 Absatz 1 Datenschutz-Grundverordnung, dass die Informationspflichten seitens des Verantwortlichen gegenüber den betroffenen Personen zum Zeitpunkt der Erhebung der personenbezogenen Daten zu erfüllen sind.[55]

Der Zeitpunkt „zu Beginn des Nutzungsvorgangs“ gemäß § 13 Telemediengesetz kann „vom Zeitpunkt der Erhebung“ der Daten gemäß Artikel 13 Datenschutz-Grundverordnung grundsätzlich abweichen. Für die Einwilligung gilt jedoch (immer), dass diese auf (vorher) informierter Basis stattfinden muss. Im Übrigen ist in Bezug auf die grundsätzliche Informiertheit der Datenverarbeitung zu erwähnen, dass „zum Zeitpunkt der Erhebung“ den Schluss auf eine Zeitgleichheit nahe legt. Die Fassung des Teledienstedatenschutzgesetzes (TDDSG) von 1997 nahm auf den „Zeitpunkt vor Erhebung der Daten“ Bezug, seit dem Teledienstegesetz (TDDSG 2001) stellt der deutsche Gesetzgeber auf den Beginn des Nutzungsvorgangs ab. Hintergrund dafür sei, dass bereits beim ersten Webseitenbesuch personenbezogene Daten erhoben werden können.[56]

52 *Gemäß Erwägungsgründen 39 sowie 58 der Datenschutz-Grundverordnung setzt der Grundsatz der Transparenz lediglich voraus, dass eine für die Öffentlichkeit oder die betroffene Person bestimmte Information präzise, leicht zugänglich und verständlich sowie in klarer und einfacher Sprache abgefasst ist und gegebenenfalls zusätzlich visuelle Elemente verwendet werden. Erwägungsgrund 42 regelt speziell für die Einwilligung mit Bezug zum Verbraucherschutz, dass gemäß der Richtlinie 93/13/EWG des Rates eine vom Verantwortlichen vorformulierte Einwilligungserklärung in verständlicher und leicht zugänglicher Form in einer klaren und einfachen Sprache zur Verfügung gestellt werden und keine missbräuchlichen Klauseln beinhalten sollte.*

53 *Siehe bereits die Ausführungen zum Telekommunikationsgesetz, S. 7 ff.*

54 *Das Telemediengesetz dient der Umsetzung der Richtlinie 2000/31/EG.*

55 *Gemäß Artikel 13 Absatz 1 Datenschutz-Grundverordnung bestehen die Informationspflichten aus folgendem: den Namen und die Kontaktdaten des Verantwortlichen sowie gegebenenfalls seines Vertreters; gegebenenfalls die Kontaktdaten des Datenschutzbeauftragten; die Zwecke, für die die personenbezogenen Daten verarbeitet werden sollen, sowie die Rechtsgrundlage für die Verarbeitung; wenn die Verarbeitung auf Artikel 6 Absatz 1 Buchstabe f beruht, die berechtigten Interessen, die von dem Verantwortlichen oder einem Dritten verfolgt werden; gegebenenfalls die Empfänger oder Kategorien von Empfängern und gegebenenfalls die Absicht des Verantwortlichen, die personenbezogenen Daten an ein Drittland oder eine internationale Organisation zu übermitteln.*

56 *Spindler/Nink in: Spindler/Schuster, Recht der elektronischen Medien, 3. Auflage 2015, § 13 TMG Rn. 3. Dieselben: „Diese Unterrichtungspflicht diene letztlich der Ermöglichung der aktiven Mitwirkung des Betroffenen an der Preisgabe seiner Daten, wobei sich die Unterrichtungspflicht von der in § 4a Abs. 1 Satz 2 BDSG verankerten Hinweispflicht insofern unterscheide, dass der Hinweis in § 4a Abs. 1 Satz 2 BDSG immer vor der Einwilligung erfolgen muss, während die Unterrichtungspflicht von der Einwilligung völlig unabhängig ist, wobei beide aber zeitlich zusammenfallen könnten.“ Zu berücksichtigen könnte jedoch ebenso sein, ob sich der Dienst an Nutzer in mehreren Mitgliedstaaten richtet.*

! Fazit Nr. 3:

Eine „jederzeitige Abrufbarkeit“ der Information ist nach der Datenschutz-Grundverordnung nicht gefordert, auch die „Protokollierung“ der Einwilligung wird nicht ausdrücklich benannt und die Anforderungen an einen Nachweis inhaltlich nicht definiert. 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.

Daher empfiehlt sich bei Diensten der Informationsgesellschaft die Ausarbeitung einer europaweiten Verhaltensregel, welche Maßnahmen zukünftig gefordert, gewünscht und weiterhin in praktischer Hinsicht für die Unternehmen umsetzbar sind, ebenso im Hinblick auf den geforderten Nachweis der Einwilligung (vgl. auch Artikel 24 Absatz 3, Artikel 40 Datenschutz-Grundverordnung). Es könnte erläutert werden, ob „leicht zugänglich“ mit „jederzeit abrufbar“ gleichzusetzen ist und einem jederzeitigen Auskunftsanspruch gleichsteht. Dies steht unter der Voraussetzung, dass diese aufgrund einer Verarbeitungstätigkeit in mehreren Mitgliedstaaten ausgearbeitet werden können, wobei hier die grundsätzliche „weltweite“ Abrufbarkeit zu berücksichtigen ist.[57]

Anders als bezüglich der Impressumsangaben ist in der Richtlinie 2002/31/EG keine „ständige Verfügbarkeit“ gefordert.

Fraglich ist stets, ob eine europaweit geltende Verhaltensregel mit Schwierigkeiten oder einer langen Zeitdauer behaftet sein könnte, da sich gemäß Artikel 40 Datenschutz-Grundverordnung die Verhaltensregel auf Verarbeitungstätigkeiten in mehreren Mitgliedstaaten beziehen muss und von der zuständigen Aufsichtsbehörde dem Europäischen Datenschutzausschuss vorzulegen ist, bevor die Kommission ihre allgemeine Gültigkeit in der Union erklären kann.

Daher empfiehlt sich bereits zum jetzigen Zeitpunkt die Benennung und Prüfung von offenen Punkten, für die Verhaltensregeln ausgearbeitet werden sollten und deren Klärung für eine auch in praktischer Hinsicht notwendige Harmonisierung des Datenschutzrechts erforderlich ist. Die deutschen Aufsichtsbehörden könnten bereits zum jetzigen Zeitpunkt mit der Förderung der Ausarbeitung von Verhaltensregeln beginnen und klärungsbedürftige Fragen erstellen, die sich auf Verarbeitungstätigkeiten in mehreren Mitgliedstaaten beziehen, verbunden mit der Aufforderung an Verbände, diese zu prüfen und Vorschläge zu unterbreiten.

D. Einwilligungsassistent

In der Einführung A. dieser Stellungnahme (S. 4 ff. | Anhang 1) wurde bereits darauf hingewiesen, dass sich die Konzepte und Verwendungszwecke derzeit in der Entwicklung befinden. Sofern Anbieter von elektronischen Kommunikationsdiensten oder Diensten der Informationsgesellschaft zukünftig den Einwilligungsassistenten im Zusammenhang mit ihren Diensten verwenden, müssten die oben dargestellten Überlegungen zum Telekommunikationsgesetz und zum Telemediengesetz mit berücksichtigt werden.

57 Zu berücksichtigen könnte jedoch ebenso sein, ob sich der Dienst an Nutzer in mehreren Mitgliedstaaten richtet.

Die nachfolgende Prüfung muss allerdings unter der Maßgabe erfolgen, dass noch nicht absehbar ist, ob der Einwilligungsassistent „selbst“ als eigenständiger Dienst oder als Bestandteil eines Dienstes (z. B. Dienst der Informationsgesellschaft) rechtlich einzuordnen ist. Möglich ist ebenso die Einstufung als Software-Tool im Einsatzbereich des Nutzers. In diesem Falle stellt sich die Frage, wer Verantwortlicher dieses Systems ist (siehe S. 56 ff.).

Insgesamt ist nach der Datenschutz-Grundverordnung zu berücksichtigen, dass Verantwortlicher gemäß Artikel 4 Nr. 7 Datenschutz-Grundverordnung die natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle ist, die allein oder gemeinsam mit anderen über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheidet.

Es muss daher zukünftig entschieden werden, ob ein Einwilligungsassistent „nur“ als Software, oder darüber hinaus als Dienst der Informationsgesellschaft im Sinne eines „Inhaltsdienstes“ gemäß der Richtlinie 2000/31/EG[58] oder „inhaltsneutral“ als (Bestandteil eines) elektronischen Kommunikationsdienstes gemäß den Richtlinien 2002/21/EG, 2002/58/EG(2009/136/EG)[59] lediglich den Vorgang der Übertragung betrifft oder als Dienst mit Zusatznutzen[60] verstanden werden kann. Die Frage ist, ob die Installation einer Hilfesoftware tatsächlich als eigener Online-Dienst betrachtet werden kann, so dass der Empfänger der Daten auch zum Dienstanbieter wird und damit ebenso zum Verantwortlichen. Dies hängt ebenso davon ab, wer den Einwilligungsassistenten einsetzt und in welcher Weise „betreibt.“ Möglich wäre sogar ein zwischengeschalteter „weiterer Anbieter“, etwa ein Anbieter von Telekommunikationsdiensten, der einen solchen Dienst zur Verfügung stellt.

Insgesamt muss bei dieser Beurteilung beachtet werden, ob der Einwilligungsassistent vorwiegend nur die Übertragung sicherstellt oder „mehr“ kann, so dass bereitgestellte Inhalte im Vordergrund stehen. Sofern die betroffene Person den Assistenten lediglich als Tool dezentral in ihrem Bereich einsetzt, um den Selbstdatenschutz zu stärken, so kann lediglich eine unterstützende Software in Betracht kommen, für die der Nutzer allein verantwortlich ist. Außerdem wäre denkbar, dass der Einsatz beim Empfänger der Daten nicht als eigenständiger Dienst, sondern als die Datenverarbeitung unterstützende Softwarelösung verstanden wird. In diesem Sinne wäre er zwar Verantwortlicher, aber nicht im Sinne eines (Online)Dienstanbieters.

Diese Frage kann abschließend erst zu dem Zeitpunkt beantwortet werden, wenn nähere Details über die Technik und geplanten Einsatzzweck vorliegen.

Unabhängig davon sind für das Vorliegen einer wirksamen Einwilligung jedoch stets die folgenden Überlegungen und Voraussetzungen zu berücksichtigen:

58 Gemäß Artikel 1 Nr. 2 der Richtlinie 98/34/ÆG in der Fassung von der Richtlinie 98/48/ÆG bedeutet Dienst der Informationsgesellschaft jede in der Regel gegen Entgelt elektronisch im Fernabsatz und auf individuellen Abruf eines Empfängers erbrachte Dienstleistung.

*59 Richtlinie 2002/21/ÆG des Europäischen Parlaments und des Rates vom 7. März 2002 über einen gemeinsamen Rechtsrahmen für elektronische Kommunikationsnetze und -dienste (Rahmenrichtlinie)
Artikel 2c) „elektronische Kommunikationsdienste“: gewöhnlich gegen Entgelt erbrachte Dienste, die ganz oder überwiegend in der Übertragung von Signalen über elektronische Kommunikationsnetze bestehen, einschließlich Telekommunikations- und Übertragungsdienste in Rundfunknetzen, jedoch ausgenommen Dienste, die Inhalte über elektronische Kommunikationsnetze und -dienste anbieten oder eine redaktionelle Kontrolle über sie ausüben; nicht dazu gehören die Dienste der Informationsgesellschaft im Sinne von Artikel 1 der Richtlinie 98/34/ÆG, die nicht ganz oder überwiegend in der Übertragung von Signalen über elektronische Kommunikationsnetze bestehen.*

60 Dienst mit Zusatznutzen wird gemäß Artikel 2 g) der Richtlinie 2002/58/ÆG definiert als „jeder Dienst, der die Bearbeitung von Verkehrsdaten oder anderen Standortdaten als Verkehrsdaten in einem Maße erfordert, das über das für die Übermittlung einer Nachricht oder die Fakturierung dieses Vorgangs erforderliche Maß hinausgeht.“ Beispielhaft werden hierzu in Erwägungsgrund 18 die Beratung hinsichtlich der billigsten Tarifpakete, Navigationshilfen, Verkehrsinformationen, Wettervorhersage oder touristische Informationen genannt.

I. Willensbekundung und Einverständnis

1. Definition

Gemäß Artikel 2h) der Richtlinie 95/46/EG stellt eine Einwilligung eine Willensbekundung des Betroffenen dar.

Eine Willensbekundung ist eine nach außen tretende, vom Adressaten erkennbare Handlung, die bei objektiver Würdigung als Ausdruck der Zustimmung zu verstehen ist.[61] Der Betroffene muss positiv eine bestimmte Meinung zum Ausdruck gebracht haben.[62] Allerdings ist umstritten, ob eine konkludente Einwilligung ausreicht.[63] Gemäß § 4a Absatz 1 Satz 3 Bundesdatenschutzgesetz bedarf die Einwilligung der Schriftform, soweit nicht wegen besonderer Umstände eine andere Form angemessen ist. Damit ist gemäß der Intention des Bundesdatenschutzgesetzes eine konkludente Einwilligung grundsätzlich unzulässig. Die Artikel-29-Datenschutzgruppe führt aus, dass eine „Willensbekundung" darauf hindeute, dass eine Handlung nötig ist (im Gegensatz zu einer Situation, in der eine Einwilligung aus dem Ausbleiben einer Handlung gefolgert werden kann).[64]

Gemäß Artikel 4 Nr. 11 Datenschutz-Grundverordnung ist eine Einwilligung ebenfalls eine Willensbekundung, und zwar in Form einer Erklärung oder einer sonstigen eindeutigen bestätigenden Handlung, mit der die betroffene Person zu verstehen gibt, dass sie mit der Verarbeitung der sie betreffenden personenbezogenen Daten einverstanden ist („jede freiwillig für den bestimmten Fall, in informierter Weise und unmissverständlich abgegebene Willensbekundung in Form einer Erklärung oder einer sonstigen eindeutigen bestätigenden Handlung, mit der die betroffene Person zu verstehen gibt, dass sie mit der Verarbeitung der sie betreffenden personenbezogenen Daten einverstanden ist").

Erwägungsgrund 32 regelt dazu näher, dass die Einwilligung durch eine eindeutige bestätigende Handlung erfolgen sollte („Die Einwilligung sollte durch eine eindeutige bestätigende Handlung erfolgen, mit der freiwillig, für den konkreten Fall, in informierter Weise und unmissverständlich bekundet wird, dass die betroffene Person mit der Verarbeitung der sie betreffenden personenbezogenen Daten einverstanden ist, etwa in Form einer schriftlichen Erklärung, die auch elektronisch erfolgen kann, oder einer mündlichen Erklärung"). Dies kann gleichermaßen durch Anklicken eines Kästchens beim Besuch einer Internetseite, durch die Auswahl technischer Einstellungen für Dienste der Informationsgesellschaft oder durch eine andere Erklärung oder Verhaltensweise geschehen. Ausdrücklich als Willensbekundung ausgeschlossen ist dagegen (Still-)Schweigen („Silence"), bereits angekreuzte Kästchen oder Untätigkeit der betroffenen Person.

61 *Dammann/Simitis, EG-Datenschutzrichtlinie – Kommentar, Baden-Baden 1997, Artikel 2 Nr. 22.*

62 *Brühann: in Grabitz/Hilf, Das Recht der Europäischen Union, 40. Auflage 2009, Loseblattsammlung, Stand: Mai 1999 Ergänzungslieferung 13, A30, Artikel 2 Rn. 27.*

63 *Zur Richtlinie 95/46/EG bejahend: Dammann/Simitis, EG-Datenschutzrichtlinie, Baden Baden 1997, Artikel 2 Nr. 22; dagegen: Brühann: in Grabitz/Hilf, Das Recht der Europäischen Union, 40. Auflage 2009, Loseblattsammlung, Stand: Mai 1999 Ergänzungslieferung, A30, Artikel 2 Rn. 27. Siehe außerdem 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") und dort zur Umsetzung der Einwilligungsvoraussetzungen, S. 4/5: "Neither the French nor the UK and Irish laws define the concept of 'consent' at all. It appears that under UK and also Finnish law in some cases implied consent may be valid but not if the data is sensitive data, so the character of the data gathered is significant in this regard."*

64 *Artikel-29-Datenschutzgruppe, WP 187, Stellungnahme 15/2011 zur Definition von Einwilligung, angenommen am 13. Juli 2011, S. 13.*

Die Frage ist daher, ob eine konkludente Willensbekundung nach der Datenschutz-Grundverordnung möglich ist.[65] Zu berücksichtigen ist, dass gemäß Wortlaut eine „Erklärung“ oder „sonstige bestätigende Handlung“ denkbar ist. Insgesamt kann Erwägungsgrund 32 als Auslegungshilfe herangezogen werden: Eine Person muss eindeutig ihr Einverständnis mit der beabsichtigten Verarbeitung ihrer personenbezogenen Daten signalisieren und ihr Einverständnis unmissverständlich bekunden. Eine konkludente Willenserklärung erfüllt grundsätzlich diese Voraussetzungen und ist nicht mit „Schweigen“ gleichzusetzen. Hier kann sich aus den Gesamtumständen eine Einwilligung ergeben, wobei es nach deutschem Recht nicht auf das tatsächlich Erklärte, sondern auf den objektiven Empfängerhorizont ankommt. Maßstab sind §§ 133, 157 BGB, wonach eine Willenserklärung nach Treu und Glauben auszulegen ist.

Bloßes Schweigen kann kein Einverständnis darstellen. Allerdings gibt es die so genannte „stillschweigende“ Willenserklärung, die in einem schlüssigen bzw. konkludenten Verhalten bestehen kann und nicht in einem reinen Schweigen. Insoweit ist der Begriff „stillschweigend“ missverständlich. Willenserklärungen können grundsätzlich konkludent abgegeben werden, es sei denn, es bestehen besondere Formvorschriften. Ausdrückliche und konkludente Willenserklärungen sind im Zivilrecht als gleichwertig zu betrachten. Bei letzterer findet das Gewollte nicht unmittelbar in einer Erklärung Ausdruck, sondern der Erklärende nimmt Handlungen vor, die mittelbar einen Schluss auf einen bestimmten Rechtsfolgewillen zulassen.[66] Sofern die Person kein entsprechendes Erklärungsbewusstsein hat („Trierer Weinversteigerungsfall“), gelten nach deutschem Recht die Regelungen der Auslegung gemäß §§ 133, 157 BGB und der Anfechtung gemäß §§ 119 ff. BGB.[67] Es wird außerdem zum Bundesdatenschutzgesetz vertreten, dass „konkludent“ derselbe Wert zukomme wie „ausdrücklich“.[68]

Da sich aus der Historie der Datenschutz-Grundverordnung ergibt, dass das im ersten Entwurf vorgesehene Merkmal „explizit“ oder „ausdrücklich“ gestrichen wurde bzw. sich nicht durchsetzen konnte,[69] ist fraglich, ob die Möglichkeit einer konkludenten Einwilligung angenommen werden kann. – unabhängig davon, dass der Diensteanbieter für deren Vorliegen gemäß Artikel 7 Absatz 1 Datenschutz-Grundverordnung nachweispflichtig ist. Für die grundsätzliche Zulässigkeit einer konkludenten Einwilligung könnte sprechen, dass die Datenschutz-Grundverordnung in Artikel 4 Nr. 11 formuliert, dass die betroffene Person zu verstehen gibt, dass sie mit der Verarbeitung der sie betreffenden personenbezogenen Daten einverstanden ist. Die Artikel-29-Datenschutzgruppe vertritt in Bezug auf die Richtlinie 95/46/EG die Auffassung, dass das Verfahren zur Einholung und Erteilung der Einwilligung keinen Zweifel an der Einwilligungsabsicht der betroffenen Person lassen darf.[70] Die für die Datenverarbeitung Verantwortlichen seien damit zur Schaffung stabiler Verfahren gezwungen und könnten entweder eine klare, ausdrückliche Einwilligung anstreben oder sich auf Verfahren verlassen, die die eindeutige, konkludente

65 Für die Möglichkeit einer konkludenten Einwilligung (allerdings noch im Hinblick auf den ersten Entwurf der Datenschutz-Grundverordnung) siehe Rogosch, Die Einwilligung im Datenschutzrecht, S. 62 (und die dortigen Verweise). Gemäß Wortlaut des ersten Entwurfs der Datenschutz-Grundverordnung (2012) bedeutete Einwilligung “ any freely given specific, informed and explicit indication of his or her wishes…“). Hier ist wichtig, in welchem Sinne „explicit“ zu verstehen ist. In anderem Kontext wurde dieser Begriff von den Mitgliedstaaten unterschiedlich ausgelegt (siehe hierzu S. 34 ff.). „Explicit“ kann jedoch gleichermaßen eine konkludente Einwilligung sein, sofern dies wie im Rahmen der Zweckbestimmung („explicit purposes“, Artikel 5 Absatz 1b) Datenschutz-Grundverordnung) mit „eindeutig“ und nicht mit „ausdrücklich“ übersetzt wird und ein objektiver Maßstab zugrunde gelegt wird. Die aktuelle Fassung der Datenschutz-Grundverordnung enthält die Formulierung „unambigous indication“, was mit „unmissverständlich“ übersetzt wird und daher auch in einem konkludenten Sinne verstanden werden kann.

66 Siehe Ellenberger in: Palandt, Bürgerliches Gesetzbuch, 76. Auflage 2017, Einführung vor § 116 BGB Rn. 6/7.

67 Siehe Ellenberger in: Palandt, Bürgerliches Gesetzbuch, 76. Auflage 2017, Einführung vor § 116 BGB Rn. 6.

68 Zum BDSG: Steidle, Multimedia-Assistenten im Betrieb, S. 205 mit Verweis auf die gegenteiligen Ansichten. Gegenteilige Ansicht etwa Simitis in: Simitis, Bundesdatenschutzgesetz, 8. Auflage 2014, § 4a Rn. 78, dass konkludente Erklärungen nicht den gesetzlichen Anforderungen entsprechen.

69 Siehe Anhang 3. „Historie Einwilligung und Transparenz unter der EU-Datenschutz-Grundverordnung“ der Studie der Stiftung Datenschutz.

70 Artikel-29-Datenschutzgruppe, WP 187, Stellungnahme 15/2011 zur Definition von Einwilligung, angenommen am 13. Juli 2011, S. 25.

Einwilligung der Person übermitteln.[71] Es kann also grundsätzlich ebenso ein Verhalten sein, aus dem zu Recht die Einwilligung geschlossen werden kann.[72]

Die Artikel-29-Datenschutzgruppe führt weiterhin klarstellend aus, dass sowohl in der Offline- als auch in der Online-Welt dieselben Anforderungen gelten, und zwar einschließlich der Einwilligung „ohne jeden Zweifel", wobei allerdings das Risiko einer missverständlichen Einwilligung in der Online-Welt größer sei.[73] Dennoch sei es möglich, unter manchen Umständen eine Einwilligung „ohne jeden Zweifel" aus bestimmten Handlungen zu schließen. Dazu müssten jedoch die einschlägigen Informationen über die Datenverarbeitung gegeben worden sein, so dass die betroffene Person wirklich eine Entscheidung treffen könne (wer ist der für die Datenverarbeitung Verantwortliche, was sind die Zwecke der Verarbeitung usw.).[74]

Im Hinblick auf die Datenschutz-Grundverordnung wären diese Ausführungen unter der Maßgabe der oben dargestellten Einwilligungsvoraussetzungen anzuwenden, so dass eine solche Einwilligung nicht in der irreführenden Bezeichnung „stillschweigende Willenserklärung" zu verstehen ist, sondern vielmehr im Sinne eines unterstellten „Tuns" in der Erklärung.

Zu berücksichtigen ist ebenso, dass bei einer Beeinträchtigung des grundrechtlich anerkannten Persönlichkeitsschutzes (Recht am eigenen Bild, Recht am gesprochenen Wort) eine Einwilligung konkludent erteilt werden kann. Hier kann es nach dem Bundesverfassungsgericht gleichermaßen darauf ankommen, ob „ein bestimmtes Verhalten in einem solchen Maße üblich und geradezu selbstverständlich ist, dass entsprechend dem Grundgedanken des § 157 BGB nach Treu und Glauben und mit Rücksicht auf die Verkehrssitte vernünftigerweise nur von einer Zustimmung des Betroffenen ausgegangen werden kann, sofern er dem Verhalten nicht widerspricht."[75] [76]

Die Frage ist allerdings, was bei einem interaktiven Dialog zwischen Betroffenem und Diensteanbieter unter einem solchen „Tun" zu verstehen ist, ob - etwa bei entsprechender transparenter Darstellung und Information - die bloße Weiternutzung des Dienstes einer solchen Handlung entspricht und mit Rücksicht auf die „Verkehrssitte" vernünftigerweise von einer Zustimmung des Betroffenen ausgegangen werden kann. Hier kann beispielhaft auf die Vorgehensweise der Datenschutzaufsichtsbehörde von Großbritannien in Bezug auf Cookies verwiesen werden. Es muss jedoch im Einzelfall stets geprüft werden, ob ein Erklärungsakt vorliegt.
Insgesamt ist Vorsicht geboten, ob tatsächlich ein Mehr an Transparenz ein Weniger an Einwilligung aufwiegen kann, da der Erklärungsempfänger (hier der Diensteanbieter) bei digitalen Diensten nicht

71 Artikel-29-Datenschutzgruppe, WP 187, Stellungnahme 15/2011 zur Definition von Einwilligung, angenommen am 13. Juli 2011, S. 25.

72 Artikel-29-Datenschutzgruppe, WP 187, Stellungnahme 15/2011 zur Definition von Einwilligung, angenommen am 13. Juli 2011, S. 13/14.

73 Artikel-29-Datenschutzgruppe, WP 187, Stellungnahme 15/2011 zur Definition von Einwilligung, angenommen am 13. Juli 2011, S. 27.

74 Artikel-29-Datenschutzgruppe, WP 187, Stellungnahme 15/2011 zur Definition von Einwilligung, angenommen am 13. Juli 2011, S. 27.

75 BVerfG, Beschluss des Ersten Senats vom 09. Oktober 2002 - 1 BvR 1611/96 - Rn. (1-63), http://www.bverfg.de/e/rs20021009_1bvr161196.html

76 BVerfG, Beschluss der 1. Kammer des Ersten Senats vom 02. April 2003 - 1 BvR 215/03 - Rn. (1-10), http://www.bverfg.de/e/rk20030402_1bvr021503.html: „Eine stillschweigende Einwilligung lässt sich zwar nicht allein aus der faktischen Verbreitung von Mithöreinrichtungen und dem Fehlen eines Widerspruchs gegen deren Benutzung herleiten. Anders liegt es aber, wenn entsprechend dem Grundgedanken des § 157 BGB nach Treu und Glauben und mit Rücksicht auf die Verkehrssitte vernünftigerweise nur von einer Zustimmung des Betroffenen ausgegangen werden kann, sofern er dem Verhalten nicht widerspricht"; siehe außerdem Gola, Handbuch zum Arbeitnehmerdatenschutz, Rn. 776 und 795, letzteres zu der Frage, ob ein Arbeitnehmer seine Einwilligung zu Kontrollmaßnahmen der privaten Nutzung von Telekommunikationstechniken inzident erklären kann, wenn er Kenntnis von diesen hat.

im Sinne eines tatsächlichen „Gegenüberstehens“ handelt und damit nicht in gleichem Maße schutzwürdig ist. Er gibt schließlich die Bedingungen vor. Fraglich ist, welche (besonders hohen) Anforderungen einer transparenten Information erfüllt sein müssen, um letztendlich eine konkludente, aber unmissverständliche und freiwillige Einwilligung unterstellen zu können. Entsprechend den allgemeinen Grundsätzen muss der Erklärungsempfänger schutzbedürftig sein. Er darf Vertrauen auf einen bestimmten Erklärungsinhalt haben. Ansonsten ist zu prüfen, ob er mit dem Fehlen des Erklärungsbewusstseins rechnen musste.[77]

Bei der Bewertung muss gleichermaßen folgendes berücksichtigt werden: Gemäß der Richtlinie 95/46/EG muss die betroffene Person die Datenverarbeitung akzeptieren.[78] Die Datenschutz-Grundverordnung regelt in Artikel 4 Nr. 11 hingegen, dass die betroffene Person zu verstehen gibt, dass sie mit der Verarbeitung der sie betreffenden personenbezogenen Daten einverstanden ist.

Diese Änderung des Wortlauts könnte dafür sprechen, dass inhaltlich nun weniger auf die innere Haltung, sondern eher auf den objektiven Empfängerhorizont Bezug genommen wird (was wiederum für eine konkludente Einwilligung sprechen könnte). Insgesamt scheint daher eine Verlagerung von Betroffenensicht auf die Empfängersicht einzutreten.

Dies bedeutet aber auch, dass sich hier die Anforderungen an die Einwilligung im Laufe der Zeit auch ändern können, da an den verständigen Durchschnittsverbraucher zukünftig andere Maßstäbe angelegt werden könnten als zur jetzigen Zeit, entsprechend dem Vergleich zu Zeiten der Verabschiedung der Richtlinie 95/46/EG zu dem heutigen Wissen des „Durchschnittsbetroffenen“. Hierzu hat die Artikel-29-Datenschutzgruppe bereits ausgeführt, dass ein regelmäßiger/durchschnittlicher Nutzer dazu in der Lage sein sollte, die Einwilligung zu verstehen.[79] Auch wenn sich dies auf die Qualität von verständlichen Informationen bezieht, ist fraglich, wie zukünftig der durchschnittliche Nutzer im Netz aussieht und welche Verhaltensweise man ihm (entsprechend dem „Trierer Weinversteigerungsfall“) als Willensbekundung unter dem Gesichtspunkt des Vertrauensschutzes unterstellen kann.

77 Ellenberger in: Palandt, Bürgerliches Gesetzbuch, 76. Auflage 2017, Einführung vor § 116 BGB Rn. 17.

78 Gemäß Artikel 2h) der Richtlinie 95/46/EG ist eine Einwilligung der betroffenen Person“ jede Willensbekundung, die ohne Zwang, für den konkreten Fall und in Kenntnis der Sachlage erfolgt und mit der die betroffene Person akzeptiert, dass personenbezogene Daten, die sie betreffen, verarbeitet werden.

79 Artikel-29-Datenschutzgruppe, WP 187, Stellungnahme 15/2011 zur Definition von Einwilligung, angenommen am 13. Juli 2011, S. 23.

! Fazit Nr. 4

Die Datenschutzaufsichtsbehörden in Deutschland sollten bereits zum jetzigen Zeitpunkt gemeinsam klare Anforderungen für die Gestaltung einer Einwilligungserklärung formulieren.[80] Damit könnten vorausschauend Leitlinien festgelegt werden, vor allem im Hinblick auf die zukünftige Ausarbeitung von Verhaltensregeln sowie auf die Formulierung, dass der Ausdruck „Einwilligung" ebenso „eine sonstige eindeutige bestätigende Handlung bezeichnet, mit der die betroffene Person zu verstehen gibt, dass sie mit der Verarbeitung der sie betreffenden personenbezogenen Daten einverstanden ist" (siehe auch die vorangegangenen Fazits). In diesem Zusammenhang kann gleichermaßen dazu Stellung genommen werden, ob auch im Datenschutzrecht eine konkludente Einwilligung möglich ist, womit im besonderen Maße berücksichtigt werden muss, ob ein „Mehr" an Transparenz ein „Weniger" an Einwilligung aufwiegen kann.

Aufgrund der in der Vergangenheit unterschiedlichen Auslegung durch die Mitgliedsstaaten und Aufsichtsbehörden (siehe Cookies), sollte der Europäische Datenschutzausschuss zukünftig eine Leitlinie hinsichtlich der Einwilligungskriterien formulieren, um die einheitliche Anwendung der Datenschutz-Grundverordnung sicherzustellen oder die bereits vorhandenen Empfehlungen der Artikel-29-Datenschutzgruppe als bewährtes Verfahren bekräftigen.

Der Europäische Datenschutzausschuss könnte im besonderen Maße die Ausarbeitung von Verhaltensregeln durch Verbände und andere Vereinigungen bezüglich der Einwilligungskriterien fördern und durch eine Leitlinie klarstellen, unter welchen Voraussetzungen eine Verarbeitungstätigkeit im Zusammenhang mit der Bereitstellung von Webinhalten und einer damit verbundenen elektronischen Einwilligung aufgrund der grundsätzlichen weltweiten Abrufbarkeit regelmäßig „mehrere Mitgliedstaaten" betrifft.

2. Relevanz für den Einwilligungsassistenten

(1) Aktives Tun

Der Einwilligungsassistent könnte diese Unklarheiten für den Betroffenen insoweit beseitigen, wenn dieser im Vorhinein die Datenverarbeitung selbstständig durch seine Voreinstellung bestimmen kann und sich damit die Frage einer konkludenten Einwilligung nicht stellt.

Dazu müsste der Nutzer durch aktives Anklicken von einzelnen Daten, Zwecken und Empfängern seinen Willen im Sinne eines „Tuns" ausdrücklich vornehmen können. Die Artikel-29-Datenschutzgruppe hat bereits im Jahre 2005 die Verwendung von leeren Kästchen empfohlen, die die Betroffenen zur Bekundung der vorherigen Einwilligung auf Websites ankreuzen können. Die Verwendung von bereits angekreuzten Kästchen erfülle die Voraussetzung nicht, dass die Einwilligung eine klare und eindeutige Willensbekundung sein muss.[81]

80 *Siehe hierzu auch Düsseldorfer Kreis, „Orientierungshilfe zur datenschutzrechtlichen Einwilligungserklärung in Formularen", März 2016.*

81 *Artikel-29-Datenschutzgruppe, WP 114, Arbeitspapier der Artikel-29-Datenschutzgruppe über eine Gemeinsame Auslegung des Artikels 26 Absatz 1 der Richtlinie 95/46/EG vom 24. Oktober 1995, Arbeitspapier vom 25. November 2005, S. 12.*

Eine bewusste und eindeutige Einwilligung könne nicht über eine Opt-Out-Lösung erlangt werden, bei dem der Nutzer erst die entsprechende Voreinstellung abwählen muss, indem er z. B. ein bereits aktiviertes Kreuzchen deaktivieren müsse.[82]

Zu berücksichtigen ist allerdings (insbesondere bei einer automatischen und maschinenlesbaren Erstellung einer Einwilligungsliste für unterschiedliche Daten und Zwecke durch Abgleich mit den Datenschutzhinweisen des Empfängers bzw. Vertragspartners/Dienstanbieters), inwieweit tatsächlich eine Einwilligung für unterschiedliche Daten und Zwecke eingeholt werden muss oder diese Verarbeitung nicht bereits durch eine andere Legitimationsgrundlage abgedeckt ist. Die Artikel-29-Datenschutzguppe führt hierzu aus, dass entweder die Verarbeitung für die Erfüllung eines Vertrags notwendig ist oder die Einwilligung (ohne Zwang) eingeholt werden muss, wobei bei einigen Transaktionen gleichzeitig eine Reihe von Rechtsgrundlagen Anwendung finden könnten[83]: Das schließe zwar die gleichzeitige Anwendung mehrerer Rechtsgrundlagen nicht aus, aber diese müssten auch im richtigen Zusammenhang genutzt werden. Angeführt wird das Beispiel eines Autokaufs, bei welchem einige Datenerhebungen und Weiterverarbeitungen möglicherweise gemäß dem Vertrag mit der betroffenen Person erforderlich sind, andere Verarbeitungen könnten als Ergebnis einer rechtlichen Verpflichtung notwendig sein, andererseits könnte die Erhebung zusätzlicher Informationen eine gesonderte Einwilligung erfordern oder sogar unter dem Ausgleich der Interessen zulässig sein.[84]

Dies bedeutet für den Einwilligungsassistenten gleichermaßen, dass hier gegebenenfalls eine automatisierte Erstellung einer Einwilligungsliste durch Abgleich und Übersetzung der Datenschutzhinweise (d.h. der Information über die geplante Datenverarbeitung) mit Schwierigkeiten verbunden sein könnte, da die rechtliche Bewertung immer für den Einzelfall vorgenommen werden muss. Hier kommt es darauf an, inwieweit die rechtlichen Vorgaben überhaupt automatisiert technisch berücksichtigt werden können. Zu berücksichtigen ist jedoch, dass bei Einholung einer Einwilligung immer auch das Widerspruchsrecht gemäß Artikel 7 Absatz 3 Datenschutz-Grundverordnung gilt.

(2) Standortdaten

Der Einwilligungsassistent könnte im Rahmen von Arbeitsverhältnissen eingesetzt werden, wo es nach den Erwägungen der Artikel-29-Datenschutzgruppe erforderlich ist, dass der Arbeitnehmer bei Fahrzeugen, die ihm auch für den privaten Gebrauch zur Verfügung gestellt werden, mit einem System ausgestattet werden, das es dem Arbeitnehmer erlaubt, die Standortbestimmungsfunktion auszuschalten.[85]

In Bezug auf Standortdaten ist insgesamt besonders zu berücksichtigen, dass Artikel 9 der Richtlinie 2002/58/EG entweder die Anonymisierung oder die Einwilligung verlangt. Dies kann der Einwilligungsassistent durch vorheriges Anklicken der Verwendung von Standortdaten für bestimmte Zwecke sicherstellen. Ansonsten ist zu berücksichtigen, dass wie oben dargestellt - anders als im Sinne von § 98 Telekommunikationsgesetz und der Intention von § 4a BDSG - eine konkludente Einwilligung ausreichend sein könnte und nicht mehr wie bisher sogar eine schriftliche Einwilligung erforderlich ist,

82 *Düsseldorfer Kreis, S. 15 -Orientierungshilfe- Datenschutzanforderungen an App-Entwickler und App-Anbieter vom 16.06.2014.*

83 *Artikel-29-Datenschutzgruppe, WP 187, Stellungnahme 15/2011 zur Definition von Einwilligung, angenommen am 13. Juli 2011, S. 9.*

84 *Artikel-29-Datenschutzgruppe, WP 187, Stellungnahme 15/2011 zur Definition von Einwilligung, angenommen am 13. Juli 2011, S. 9.*

85 *Artikel-29-Datenschutzgruppe, WP 115, Stellungnahme 5/2005 der Gruppe 29 zur Nutzung von Standortdaten für die Bereitstellung von Diensten mit Zusatznutzen, angenommen am 25. November 2005, S.11.*

wenn die Standortdaten für einen Dienst mit Zusatznutzen verarbeitet werden, der die Übermittlung von Standortdaten eines Mobilfunkendgerätes an einen anderen Teilnehmer oder an Dritte, die nicht Anbieter des Dienstes mit Zusatznutzen sind, zum Gegenstand hat.

Der Düsseldorfer Kreis verweist außerdem darauf, dass es bei Standortdaten häufig nicht notwendig ist, dass der Standort des Nutzers metergenau erhoben wird.[86] Auch die Speicherdauer ist von besonderer Relevanz und muss sich für jedes personenbezogene Datum am Grundsatz der Erforderlichkeit messen lassen.[87]

(3) IP-Adresse

Bei der Inanspruchnahme von Webangeboten fällt notwendigerweise ebenso die IP-Adresse an.
In Bezug auf die IP-Adresse ist zu berücksichtigen, dass die automatisierte Erstellung einer Einwilligungsliste durch Abgleich mit den Datenschutzhinweisen zu einem Widerspruchsrecht gemäß Artikel 7 Absatz 3 Datenschutz-Grundverordnung führen könnte, wenn dadurch eine Einwilligung für die Verarbeitung der IP-Adresse durch einen Anbieter eines Dienstes der Informationsgesellschaft eingeholt werden würde: In Datenschutzhinweisen wird regelmäßig auch über die Verarbeitung der IP-Adressen informiert, aber in vielen Fällen ist eine Rubrik „Datenschutz“ zu finden, in welcher sämtliche Verarbeitungstätigkeiten beschrieben werden. Der Einwilligungsassistent müsste also in der Lage sein, zwischen „einwilligungsbedürftig“ und „nur informationspflichtig“ innerhalb der Datenschutzerklärung zu unterscheiden, sofern ein automatisierter Abgleich erfolgt. Anderenfalls muss ein Anbieter im Vorhinein auf die entsprechende Unterscheidung achten.

In Bezug auf IP-Adressen ist das Urteil des Europäischen Gerichtshofs vom 19.10.2016 zu berücksichtigen, nach dem eine Verarbeitung personenbezogener Daten (wozu auch eine IP-Adresse gehören kann) gemäß Artikel 7f der Richtlinie 95/46/EG rechtmäßig sein kann, wenn sie zur Verwirklichung des berechtigten Interesses des für die Verarbeitung Verantwortlichen erforderlich ist, sofern nicht das Interesse oder die Grundrechte und Grundfreiheiten der betroffenen Person überwiegen.[88] Damit kann die Funktionsfähigkeit eines Online-Medium grundsätzlich gegen das Interesse oder die Grundrechte oder die Grundfreiheiten der Nutzer abgewogen werden. Diesbezüglich erscheint es schwierig, eine solche Interessenabwägung automatisiert durchzuführen.

Diese Erwägungen müssen gleichermaßen für die Datenschutz-Grundverordnung und Artikel 6f gelten. Zu berücksichtigen ist, dass die Voraussetzungen der Einwilligung nicht mit dem Widerspruchsrecht verwechselt werden dürfen: Eine Einwilligung muss vor Datenverarbeitung eingeholt werden, erst dann dürfen die Daten verarbeitet werden. Nur gemäß Artikel 6f Datenschutz-Grundverordnung dürfen die Daten verarbeitet werden (wenn die entsprechenden Voraussetzungen nach Interessenabwägung vorliegen), wenn die betroffene Person der Datenverarbeitung nicht widersprochen hat.[89]

86 *Düsseldorfer Kreis, S. 17 -Orientierungshilfe- Datenschutzanforderungen an App-Entwickler und App-Anbieter vom 16.06.2014.*

87 *Düsseldorfer Kreis, S. 17 -Orientierungshilfe- Datenschutzanforderungen an App-Entwickler und App-Anbieter vom 16.06.2014.*

88 *Urteil des Europäischen Gerichtshofs vom 19.10.2016 C-582/14; http://curia.europa.eu/juris/document/document.jsf?text=&docid=184668&pageIndex=0&doclang=de&mode=lst&dir=&occ=first&part=1&cid=780392 sowie Urteilsberichtigung vom 06.12.2016 http://curia.europa.eu/juris/document/document.jsf?text=&docid=186141&pageIndex=0&doclang=DE&mode=req&dir=&occ=first&part=1 . Siehe ebenso Pressemitteilung des Europäischen Gerichtshofs http://curia.europa.eu/jcms/upload/docs/application/pdf/2016-10/cp160112de.pdf*

89 *Siehe hierzu bzw. zu den Voraussetzungen von Artikel 7a und 7f der Richtlinie 95/46/EG die Ausführungen der Artikel-29-Datenschutzgruppe, WP 187, Stellungnahme 15/2011 zur Definition von Einwilligung, angenommen am 13. Juli 2011, S. 11.*

(4) Cookies

Aufgrund der Ausführungen zur konkludenten Einwilligung sowie der beispielhaften Darstellung der Vorgehensweise in den Niederlanden sowie der Datenschutzaufsichtsbehörde von Großbritannien stellt sich die Frage, ob in Cookies nicht ausdrücklich eingewilligt werden muss und ob die Voreinstellungen eines verwendeten Einwilligungsassistenten unterstützend zur Wahrung der Selbstbestimmungsrechte der Nutzer eingesetzt werden könnten.

Die Artikel-29-Datenschutzgruppe steht -wie oben bereits ausgeführt- den Einstellungsmöglichkeiten durch Browser kritisch gegenüber. Zu prüfen ist daher, ob es andere technische Verfahren gibt oder solche entwickelt werden können, die die betroffenen Personen besser in ihrer informationellen Selbstbestimmung unterstützen und ob der Einwilligungsassistent ein solches technisches Verfahren bewerkstelligen kann. Dabei sind folgende Erwägungen zu berücksichtigen:

Die Artikel-29-Datenschutzgruppe ist weiterhin der Ansicht, dass Cookie-basierte Opt-Out-Mechanismen im Allgemeinen keinen angemessenen Mechanismus zur Einholung der Einwilligung in Kenntnis der Sachlage darstellen. In den meisten Fällen werde die Einwilligung des Nutzers impliziert, wenn er von der Opt-Out-Möglichkeit nicht Gebrauch mache. Tatsächlich machten aber nicht deshalb nur so wenige Leute von der Opt-out-Möglichkeit Gebrauch, weil sie sich in Kenntnis der Sachlage für eine Einwilligung in die Werbung auf Basis des Behavioural Targeting entschieden haben, sondern weil sie nicht wissen, dass eine Verarbeitung stattfindet und erst recht nicht, wie sie von dem Opt-out Gebrauch machen könnten.[90]

Außerdem wird nochmals die Wichtigkeit von Privacy by Design betont.[91]

In ihrer Stellungnahme zur verhaltensorientierten Online-Werbung stellt die Artikel-29-Datenschutzgruppe klar, dass im Sinne einer gültigen und wirksamen Einwilligung Browser oder andere Einstellungen die betroffenen Personen auffordern müssten, durch eine bejahende Handlung sowohl das Setzen eines Cookies als auch die fortdauernde Übermittlung von in den Cookies enthaltenen Informationen zu akzeptieren.[92]

Ein Einwilligungsassistent könnte dies sinnvoll unterstützen. Dies gilt insbesondere vor dem Hintergrund, dass gemäß der obigen Ausführungen (s. S. 19 ff.) die betroffene Person gemäß Artikel 13 Datenschutz-Grundverordnung bei Erhebung der Daten und nicht entsprechend § 13 Telemediengesetz zu Beginn des Nutzungsvorgangs informiert werden muss. Die Schutzfunktion der Einwilligung wäre also gewahrt, da die betroffene Person vor der übereilten Preisgabe ihrer personenbezogenen Daten bewahrt werden könnte. Lässt man hier Voreinstellungen zu, um diese anschließend mit den Datenschutzhinweisen der Webseite abzugleichen, wäre der Übereilungsschutz unter der Voraussetzung erfüllt, dass der Webseitenbetreiber tatsächlich erst dann Cookies erhebt, wenn die Einstellungen dies zulassen. Dies erfordert aber gleichermaßen eine technische Zusammenarbeit, die etwa bei P3P (siehe Bestandsaufnahme) in der Vergangenheit nicht funktioniert hatte. Im Hinblick auf die Information gilt zudem aktuell gemäß § 13 Absatz Satz2 Telemediengesetz, dass die Unterrichtungspflicht auch

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

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

92 Artikel-29-Datenschutzgruppe, WP 188 Stellungnahme 16/2011 zur Best-Practice-Empfehlung von EASA und IAB zu verhaltensorientierter Online-Werbung, angenommen am 8. Dezember 2011; S. 11/12

dann greift, wenn die Daten zunächst ohne Personenbezug erhoben werden, ein solcher aber jederzeit hergestellt werden kann.[93] Je nachdem, wie der Zeitpunkt der Unterrichtung zukünftig definiert wird, wäre auch dieser Umstand zu beachten.

Zu berücksichtigen sind hierbei außerdem die obigen Ausführungen: Nach der Intention der Richtlinie 2002/58/EG dürfen erforderliche Cookies (etwa für den Warenkorb oder zur technischen Funktionsfähigkeit der Webseite) ohne Einwilligung des Nutzers erhoben werden. Der Einwilligungsassistent sollte daher in Bezug auf solche Cookies keine Einwilligung einholen, sondern es müsste eine transparente Information sichergestellt sein, dass diese Cookies erhoben werden. Anderenfalls würden dem Nutzer bei jeder Einwilligung auch Widerrufsrechte gemäß Artikel 7 Absatz 3 Datenschutz-Grundverordnung zustehen.

! Fazit Nr. 5

Der Einwilligungsassistent sollte die Übersetzung der Datenschutzhinweise in eine maschinenlesbare Form durch die Darstellung von leeren Kästchen vornehmen, die der Nutzer aktiv ankreuzen muss.
Eine konkludente Einwilligung ist damit ausgeschlossen.

In Bezug auf Standortdaten muss im besonderen Maße die Möglichkeit „einer anderen Verhaltensweise“ und konkludenten Einwilligungsmöglichkeit kritisch geprüft werden. Hier gelten die Anforderungen der Richtlinie 2002/58/EG. Das Telekommunikationsgesetz muss entsprechend angepasst werden.

Bei einer automatisierten Erstellung einer Einwilligungserklärung anhand der Übersetzung der Datenschutzhinweise[94] des Dienstanbieters muss beachtet werden, dass die zur Vertragserfüllung erforderlichen Daten nicht der Einwilligung unterliegen. Wird eine Einwilligung dennoch eingeholt, steht der betroffenen Person auch ein entsprechendes Widerspruchsrecht gemäß Artikel 7 Absatz 3 Datenschutz-Grundverordnung zu. Zu prüfen wäre, ob es in diesem Falle sogar unbillig wäre, wenn sich der Dienstanbieter im Nachhinein auf andere Gründe der rechtmäßigen Datenverarbeitung berufen würde (Erforderlichkeit oder berechtigtes Interesse), so dass die Datenverarbeitung vollständig unterbleiben müsste.
Die transparente Information über die Datenverarbeitung aufgrund anderer Rechtsgrundlagen muss somit klar von der Einwilligung abgegrenzt werden. Es muss berücksichtigt werden, inwieweit eine Darstellung und Prüfung insgesamt automatisiert erfolgen kann. Anderenfalls müssten die Datenschutzhinweise entsprechend angepasst werden. Dies bezieht sich auch auf die Verarbeitung der IP-Adresse, sofern über ihre Verarbeitung in den Datenschutzhinweisen informiert wird (an ihrer Verarbeitung könnte der Diensteanbieter ein berechtigtes Interesse haben, was im Einzelfall zu prüfen ist).

Zu berücksichtigen ist, dass die Voraussetzungen der Einwilligung nicht mit dem Widerspruchsrecht verwechselt werden dürfen: Eine Einwilligung muss vor Datenverarbeitung eingeholt werden, erst dann dürfen die Daten verarbeitet werden. Nur gemäß Artikel 6f Datenschutz-Grundverordnung dürfen die Daten verarbeitet werden (wenn die entsprechenden Voraussetzungen nach Interessenabwägung vorliegen), wenn die betroffene Person der Datenverarbeitung nicht widersprochen hat.
Auch vor dem Hintergrund, dass nach der Datenschutz-Grundverordnung eine Information des Nutzers

93 Spindler/Nink in: Spindler/Schuster, Recht der elektronischen Medien, 3. Auflage 2015, § 13 TMG Rn. 3: Dies werde durch § 13 Abs. 1 Satz 2 deutlich, der auch die Erhebung in einem automatisierten Verfahren erfasse, welches die Verwendung personenbezogener Daten vorbereitet, wobei automatisierte Verfahren solche sind, die programmgesteuert, ohne auf einer individuellen Entscheidung des Verantwortlichen zu beruhen, initiiert werden.

94 Siehe hierzu die Beschreibung unter „Technische Konzepte“, S. 3 ff.

! nicht zu Beginn des Nutzungsvorgangs sondern erst bei Erhebung der Daten erfolgen muss, sollten die Entwickler prüfen, ob der von Ihnen geplante Einwilligungsassistent in sinnvoller und für die Nutzer überschaubarer Weise für Cookies in Betracht kommen kann. Hier ist erforderlich, dass insgesamt die technischen Voraussetzungen geschaffen werden und die Systeme kompatibel sind. Daher hat die Artikel-29-Datenschutzgruppe ebenso vorgeschlagen, dass Entwickler und Webseitenbetreiber zur Zusammenarbeit bei Privacy by Design ermutigt werden sollten.[95] Beachtet werden muss dabei stets, dass für „erforderliche Cookies" keine Einwilligung eingeholt werden muss.

Im Sinne einer Vollharmonisierung des Datenschutzrechts sollte frühestmöglich ein einheitliches Verständnis über die Einwilligungsvoraussetzungen (auch bezüglich Cookies) erfolgen, selbst wenn die Tendenz in Deutschland eher in der Umsetzung eines aktiven Verhaltens bei der Einwilligung besteht. Hier ist die Formulierung in der Datenschutz-Grundverordnung entscheidend, nach der eine Einwilligung auch eine andere Verhaltensweise darstellen kann, mit der die betroffene Person in dem jeweiligen Kontext eindeutig ihr Einverständnis mit der beabsichtigten Verarbeitung ihrer personenbezogenen Daten signalisiert. Die Formulierung einheitlicher Verhaltensregeln kann von Nutzen sein, so dass Sanktionen für den mangelnden Nachweis der Einwilligung besser greifen können. Dies sollte europaweit erfolgen, soweit Verhaltensregeln aufgrund einer Verarbeitungstätigkeit in mehreren Mitgliedstaaten ausgearbeitet werden können.

II. „Für den bestimmten Fall in informierter Weise"

1. Allgemeine Voraussetzungen

(1) Bestimmter Fall

Artikel 2h der Richtlinie 95/46/EG regelt, dass die betroffene Person im Zeitpunkt der Willensbekundung die Sachlage und den konkreten Fall kennen muss. Dabei müssen alle Voraussetzungen der gesetzlichen Informationspflichten erfüllt sein.

Nach Artikel 4 Nr. 11 der Datenschutz-Grundverordnung ist eine für den bestimmten Fall, in informierter Weise und unmissverständlich abgegebene Willensbekundung gefordert.

Es ist nun nicht mehr ein „konkreter", sondern ein „bestimmter" Fall genannt. Erwägungsgrund 32 der Datenschutz-Grundverordnung nimmt allerdings wiederum auf den „konkreten" Fall Bezug, so dass diese Begriffe synonym zu verwenden sind. In Erwägungsgrund 42 wird zudem die „Kenntnis der Sachlage" wieder aufgegriffen, auch wenn diese nicht unmittelbar im Verordnungstext steht. In diesem Sinne sollte die betroffene Person mindestens wissen, wer der Verantwortliche ist und für welche Zwecke ihre personenbezogenen Daten verarbeitet werden sollen.

Ein Unterschied zwischen der Richtlinie 95/46/EG und der Datenschutz-Grundverordnung ergibt sich jedoch hinsichtlich der Voraussetzungen der Datenverarbeitung. Nach Erwägungsgrund 28 der Richtlinie 95/46/EG müssen die Zwecke eindeutig sowie rechtmäßig sein und bei der Datenerhebung festgelegt werden. Die Verarbeitung personenbezogener Daten muss gegenüber den betroffenen Personen nach Treu und Glauben erfolgen. Die Zweckbestimmungen der Weiterverarbeitung nach der Erhebung dürfen nicht mit den ursprünglich festgelegten Zwecken unvereinbar sein. In der Datenschutz-Grundver-

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

ordnung wird diese Vorgabe insoweit abgeschwächt, dass gemäß Erwägungsgrund 39 die bestimmten Zwecke, zu denen die personenbezogenen Daten verarbeitet werden, eindeutig und rechtmäßig sein sollten (und nicht „müssen“!) und zum Zeitpunkt der Erhebung der personenbezogenen Daten feststehen sollten. Diese begriffliche Änderung darf jedoch nicht dazu führen, die Zwecke zukünftig flexibler zu gestalten. Hierfür spricht ebenso Erwägungsgrund 43 Datenschutz-Grundverordnung, der klarstellt, dass zu verschiedenen Verarbeitungsvorgängen von personenbezogenen Daten eine gesonderte Einwilligung erteilt werden soll, wenn dies im Einzelfall angebracht ist. Allerdings ist nicht eindeutig definiert, was „ein“ Verarbeitungsvorgang darstellt. Ist dies mit der Festlegung des Zwecks gleichzusetzen?

! Hierzu gilt folgendes:

Verarbeitung bedeutet nach Artikel 4 Nr. 2 Datenschutz-Grundverordnung jeden mit oder ohne Hilfe automatisierter Verfahren ausgeführten Vorgang oder jede solche Vorgangsreihe im Zusammenhang mit personenbezogenen Daten wie das Erheben, das Erfassen, die Organisation, das Ordnen, die Speicherung, die Anpassung oder Veränderung, das Auslesen, das Abfragen, die Verwendung, die Offenlegung durch Übermittlung, Verbreitung oder eine andere Form der Bereitstellung, den Abgleich oder die Verknüpfung, die Einschränkung, das Löschen oder die Vernichtung.

! Die Artikel-29-Datenschutzgruppe nimmt zu Verarbeitungstätigkeiten wie folgt Stellung:[96]

Damit sie für den konkreten Fall ist, muss die Einwilligung verständlich sein: sie sollte sich eindeutig und genau auf den Anwendungsbereich und die Folgen der Datenverarbeitung beziehen. Sie kann nicht für Verarbeitungsaktivitäten gelten, die in keiner Weise eingegrenzt sind. Das heißt mit anderen Worten, dass der Kontext, in dem die Einwilligung gilt, eingeschränkt ist.

Weiter führt die Artikel-29-Datenschutzgruppe aus, dass die Einigung auf den angemessenen Erwartungen der Parteien basieren sollte, wobei die Anforderung der Granularität der Einwilligung in Bezug auf die verschiedenen Elemente, die die Datenverarbeitung ausmachen, zu berücksichtigen sei. Eine Einwilligung könne nicht „alle rechtmäßigen Zwecke“ abdecken, die der für die Datenverarbeitung Verantwortliche verfolgt, so dass sich die Einwilligung auf die Verarbeitung beziehen sollte, die in Bezug auf den Zweck angemessen und erforderlich ist.[97]

Allerdings ist im Sinne der Rechtauffassung der Artikel-29-Datenschutzgruppe zu berücksichtigen, dass es ausreichen soll, wenn der für die Datenverarbeitung Verantwortliche die Einwilligung einmal für verschiedene Verarbeitungstätigkeiten einholt, sofern die betroffene Person diese Tätigkeiten vernünftigerweise erwarten kann.[98] In einem vor dem Europäischen Gerichtshof verhandelten Fall (auf den sich auch die Artikel-29-Datenschutzgruppe in ihren Ausführungen bezogen hat), konnte die Einwilligung des Betroffenen aufgrund der eindeutigen Formulierung des Zwecks gleichzeitig die Weitergabe an unterschiedliche Empfänger abdecken.

96 *Artikel-29-Datenschutzgruppe, WP 187, Stellungnahme 15/2011 zur Definition von Einwilligung, angenommen am 13. Juli 2011, S. 20.*

97 *Artikel-29-Datenschutzgruppe, WP 187, Stellungnahme 15/2011 zur Definition von Einwilligung, angenommen am 13. Juli 2011, S. 20.*

98 *Artikel-29-Datenschutzgruppe, WP 187, Stellungnahme 15/2011 zur Definition von Einwilligung, angenommen am 13. Juli 2011, S. 21.*

Konkret ging es darum, dass das Bundesverwaltungsgericht in einem Vorabentscheidungsersuchen gemäß Artikel 267 AEUV dem Europäischen Gerichtshof die Klärung der Frage vorgelegt hatte, ob im Sinne des Artikel 12 der Richtlinie 2002/58/EG eine erneute Einwilligung des Betroffenen erforderlich ist, wenn dessen Daten durch andere Anbieter öffentlich zugänglicher Telefonauskunftsdienste und Teilnehmerverzeichnisse verwendet werden, obwohl der Betroffene in die Aufnahme seiner Daten in einen Auskunftsdienst bereits eingewilligt hat. Der Europäische Gerichtshof hat dies mit Verweis auf die Verarbeitung für dieselben Zwecke verneint.[99]

Im Sinne der Sicherung der Datenhoheit des Betroffenen sollte diese Entscheidung nicht in dem Sinne verallgemeinert werden, dass nun die Datenempfänger nicht mehr angegeben werden müssten. Ansonsten würde dies zu einer freien Verwendbarkeit von Daten führen.[100] Daher wird es bei der Ausgestaltung eines granularen, aber auch übersichtlichen Einwilligungskonzepts insgesamt davon abhängen, inwieweit der (eingeschränkte) Kontext eine Einwilligung für mehrere Verarbeitungsvorgänge hergibt. Hierfür sollten Verhaltensregeln aufgestellt werden.

Außerdem ist für den Verantwortlichen der Datenverarbeitung stets die Nachweispflicht gemäß Artikel 7 Absatz 1 Datenschutz-Grundverordnung zu berücksichtigen. In einem solchen Falle müsste ein Verantwortlicher daher nachweisen können, dass eine betroffene Person vernünftigerweise mit verschiedenen Verarbeitungstätigkeiten rechnen konnte. In Bezug auf elektronische Patientenakten hat die Artikel-29-Datenschutzgruppe etwa entschieden, dass sich sie Einwilligung „für den konkreten Fall“ auf eine genau umrissene konkrete Situation beziehen müsse, in der die Verarbeitung der medizinischen Daten erfolgen soll. Eine „pauschale Zustimmung“ der betroffenen Person, beispielsweise zur Erfassung ihrer medizinischen Daten in einer elektronischen Patientenakte und zur anschließenden Weitergabe dieser medizinischen Daten an in die Behandlung eingebundenen medizinischen Fachkräfte, wäre keine Einwilligung.[101] In diesem Zusammenhang verweist die Artikel-29-Gruppe auf die entsprechende Auslegung der Einwilligungsvoraussetzungen für Standortdaten. Danach könne die Einwilligung nicht im Zuge der Annahme der allgemeinen Bedingungen für die Nutzung der angebotenen elektronischen Kommunikationsdienste erteilt werden:[102] Abhängig von der Art der angebotenen Dienste könne sich die Einwilligung jedoch auf einen spezifischen Vorgang beziehen oder sie könne die Zustimmung zu einer kontinuierlichen Standortbestimmung darstellen. Die Bereitstellung eines Dienstes, der die automatische Standortbestimmung einer Person erfordert (z. B. die Möglichkeit, eine bestimmte Nummer anzurufen, um eine Wettervorhersage für den jeweiligen Standort zu erhalten), sei zulässig, sofern die Nutzer im Voraus vollständige Informationen über die Verarbeitung ihrer Standortdaten erhalten. In diesem Fall würde das Anrufen der entsprechenden Nummer bedeuten, dass die Einwilligung zur Standortbestimmung erteilt wird.[103]

Ergänzend ist hier außerdem auf die obigen Ausführungen zu verweisen (s. S. 19 ff.), dass zukünftig unklar ist, ob die Protokollierungspflicht (im deutschen Recht) in ihrer derzeitigen Form aufrechterhalten wird oder ob die Art und Weise der Erbringung des Nachweises gemäß Artikel 7 Absatz 1 (aber ebenso Artikel 5 Absatz 2 Datenschutz-Grundverordnung dem Verantwortlichen obliegt.

99 Urteil des Gerichtshofs vom 5. Mai 2011, Deutsche Telekom AG (Rechtssache C-543/09).

100 Siehe hierzu auch Radlaski, Das Konzept der Einwilligung in der datenschutzrechtlichen Realität, S. 49.

101 Artikel-29-Datenschutzgruppe, WP 187, Stellungnahme 15/2011 zur Definition von Einwilligung, angenommen am 13. Juli 2011, S. 21 mit Verweis auf WP 131, Arbeitspapier Verarbeitung von Patientendaten in elektronischen Patientenakten (EPA), 15. Februar 2007.

102 Artikel-29-Datenschutzgruppe, WP 187, Stellungnahme 15/2011 zur Definition von Einwilligung, angenommen am 13. Juli 2011, S. 21 mit Verweis auf WP 115, Stellungnahme 5/2005 der Gruppe 29 zur Nutzung von Standortdaten für die Bereitstellung von Diensten mit Zusatznutzen, angenommen am 25. November 2005, S. 6.

103 Artikel-29-Datenschutzgruppe, WP 115, Stellungnahme 5/2005 der Gruppe 29 zur Nutzung von Standortdaten für die Bereitstellung von Diensten mit Zusatznutzen, angenommen am 25. November 2005, S. 6.

Die Protokollierung kann eine Form des Nachweises sein, aber es könnte gegebenenfalls andere hilfreiche Methoden geben, was näher zu prüfen wäre. Hier empfehlen sich (genehmigte) Verhaltensregeln gemäß Artikel 24 Absatz 3, Artikel 40 Datenschutz-Grundverordnung.

(2) Bestimmter Zweck

Gemäß den obigen Ausführungen sollte sich die Einwilligung also auf die Verarbeitung(stätigkeit) beziehen, die in Bezug auf den Zweck angemessen und erforderlich ist. Auch Erwägungsgrund 32 der Datenschutz-Grundverordnung nimmt „auf einen oder mehrere Zwecke“ Bezug, zu welchen die betroffene Person ihre Einwilligung erteilen sollte, und Erwägungsgrund 39 regelt darüber hinaus, dass die personenbezogenen Daten für die Zwecke, zu denen sie verarbeitet werden, angemessen und erheblich sowie auf das für die Zwecke ihrer Verarbeitung notwendige Maß beschränkt sein sollten. Eine Zweckänderung wäre nur unter den Voraussetzungen des Artikels 6 Absatz 4 Datenschutz-Grundverordnung zulässig.
Durch Artikel 17 Datenschutz-Grundverordnung wird die Zweckbindung außerdem gestärkt, da nun gemäß Absatz 1a dieser Regelung die Daten zu löschen sind, wenn sie für die Zwecke, für die sie erhoben wurden, nicht mehr erforderlich sind.

Hier ist jedoch im europäischen Kontext darauf zu achten, dass die Mitgliedstaaten den Zweckbindungsgrundsatz der Richtlinie 95/46/EG bislang unterschiedlich ausgelegt haben und die Artikel-29-Datenschutzgruppe aus diesem Grunde Kriterien festgelegt hat.[104]

Um zukünftig diese Unterschiede zu vermeiden, ist nun erneut der Vergleich zwischen der Richtlinie 96/46/EG und Datenschutz-Grundverordnung hilfreich, um zu prüfen, ob hier Auslegungsspielräume einer Vollharmonisierung entgegenstehen könnten:
Erwägungsgrund 39 der Datenschutz-Grundverordnung regelt, dass die bestimmten Zwecke, zu denen die personenbezogenen Daten verarbeitet werden, eindeutig und rechtmäßig sein sollten und zum Zeitpunkt der Erhebung der personenbezogenen Daten feststehen sollten.

In der englischen Fassung heißt es: “In particular, the specific purposes for which personal data are processed should be explicit and legitimate and determined at the time of the collection of the personal data.”

Auf diesen Unterschied in der Zweckbestimmung hat bereits die Artikel-29-Datenschutzgruppe verwiesen:[105]
Sie führt im Hinblick auf die Richtlinie 95/46/EG aus, dass das Wort „explicit“ in die unterschiedlichen Sprachen nicht identisch übersetzt wurde. Erwägungsgrund 28 der Richtlinie 95/46/EG regelt: “whereas, in particular, the data must be adequate, relevant and not excessive in relation to the purposes for which they are processed; whereas such purposes must be explicit and legitimate and must be determined at the time of collection of the data”. Gemäß der Stellungnahme der Artikel-29-Datenschutzgruppe liege die Anforderung teilweise darin, den Fokus auf das Endergebnis zu legen, darauf, dass die Zwecke unzweifelhaft sein müssten und von allen Beteiligten in der gleichen Weise verstanden werden müssten (im Zweifel kann also der Zweck durch Auslegung ermittelt werden). In anderen Übersetzungen liege der Fokus dagegen mehr darauf, wie dieses Endergebnis erreicht werden könne, nämlich dass die Zwecke klar ausgedrückt und erklärt werden müssten.

104 Artikel-29-Datenschutzgruppe, „Opinion 03/2013 on purpose limitation“, WP 203 adopted on 2 April 2013, insbesondere S. 5.

105 Artikel-29-Datenschutzgruppe, „Opinion 03/2013 on purpose limitation“, WP 203 adopted on 2 April 2013, S. 17.

Zur näheren Erläuterung verweist die Artikel-29-Datenschutz-Gruppe auf die lateinische Wurzel von „explicit“ und darauf, dass in Deutschland dies mit „eindeutig“ übersetzt werde und dass hier der Fokus auf dem Ergebnis und nicht in der geäußerten und erklärenden Form liege.[106]

Die Artikel-29-Datenschutzgruppe führt im Übrigen aus, dass die Flexibilität der Regelungen zur Zweckbestimmung zu unterschiedlichen Anwendungen in den Mitgliedstaaten geführt habe und dass die Anforderung an „explicit purposes“ von der Bekanntmachung dieses Zwecks an die betroffene Person oder der Benachrichtigung der Datenschutzaufsichtsbehörden (Artikel 18 Richtlinie 95/46/EG) zu unterscheiden sei.[107] Die Mitteilung der Zwecke (gemäß Artikel 6 (1) (b) Richtlinie 96/46/EG) könne auf unterschiedliche Weise durchgeführt werden. So seien in manchen Mitgliedstaaten die „Zwecke“ sehr weit definiert worden und überdies variiere die Herangehensweise im Hinblick auf die Darstellung eines „expliziten“ Zwecks.[108] Teilweise könne dies durch eine Beschreibung der Zwecke in einer Benachrichtigung an die Datenschutzaufsichtsbehörde oder in einer Mitteilung an die betroffene Person umgesetzt werden, bei anderen Mitgliedstaaten genüge eine interne Information an den Datenschutzbeauftragten, wohingegen wieder andere sowohl Mitteilungen als auch Benachrichtigungen als ausreichendes Mittel betrachten, allerdings mit dem Hinweis, dass dies nicht die einzigen Möglichkeiten im Hinblick auf die Anforderungen an eine „explizite Zweckbestimmung“ (im Sinne von „making the purposes of the processing explicit“) sind.[109] Gemäß der Ausführungen der Artikel-29-Datenschutzgruppe kann die schriftliche Spezifizierung sowie die Erstellung einer angemessenen Dokumentation hilfreich sein, wobei im Einzelfall sogar auf die Notwendigkeit der schriftlichen Spezifizierung, etwa bei komplexer Datenverarbeitung, Bezug genommen wird.[110]

In der deutschen Fassung der Datenschutz-Grundverordnung wird „explicit“ in Artikel 9 Datenschutz-Grundverordnung zwar mit „ausdrücklich“ übersetzt, aber im Rahmen der Zweckbestimmung des Artikel 5 Absatz 1b Datenschutz-Grundverordnung mit „eindeutig“, so dass nicht unbedingt die Erklärung des Zwecks verlangt wird. Die von der Artikel-29-Datenschutzgruppe benannte „schriftliche“ Spezifizierung stellt im Übrigen keine Voraussetzung dar.

Die Frage ist, wie die übrigen Mitgliedstaaten im Hinblick auf die Datenschutz-Grundverordnung die Begrifflichkeiten verwenden werden, ob die Zweckbestimmung immer noch in einem weiten Verständnis definiert wird und ob die erklärende Form durch eine andere Übersetzung des Erwägungsgrunds 39 Datenschutz-Grundverordnung hätte erreicht werden können, etwa: „Die näher beschriebenen/einzelnen Zwecke sollten genau/ausdrücklich angegeben und rechtmäßig sein und zum Zeitpunkt der Erhebung festgelegt werden.“

106 Artikel-29-Datenschutzgruppe, „Opinion 03/2013 on purpose limitation“, WP 203 adopted on 2 April 2013, S. 17: “The same Latin root is used in several languages including English, Italian and French as ‚explicit‘, ‚explicite‘ and ‚esplicite‘. The original Latin verb from which these adjectives all originate is ‚explicare‘, with the meaning of ‚unfold, unravel, explain‘, and thus appears to imply a requirement that the purposes must be expressed and explained in some form. Other language versions focus on the requirement of the end-result, that the specification of the purposes must be unambiguous. See, for example, the German ‚eindeutig‘ and the Hungarian, egyértelmü‘, which can be translated as ‚unambiguous‘, and do not necessarily require that the purposes must also be ‚expressed‘ in any way. However, the Dutch ‚uitdrukkelijk omschreven‘ is again similar to ‚explicit‘.

107 Vgl. Artikel-29-Datenschutzgruppe, „Opinion 03/2013 on purpose limitation“, WP 203 adopted on 2 April 2013, S. 10, 18.

108 Vgl. Artikel-29-Datenschutzgruppe, „Opinion 03/2013 on purpose limitation“, WP 203 adopted on 2 April 2013, S. 10. An dieser Stelle wird ebenso darauf verwiesen, dass sich Unterschiede auch für die Zweckänderung ergeben.

109 Vgl. Artikel-29-Datenschutzgruppe, „Opinion 03/2013 on purpose limitation“, WP 203 adopted on 2 April 2013, S. 18.

110 Vgl. Artikel-29-Datenschutzgruppe, „Opinion 03/2013 on purpose limitation“, WP 203 adopted on 2 April 2013, S. 18.

Für die Auslegung von Artikel 5 Datenschutz-Grundverordnung ist dies ebenso relevant:
Artikel 5 Absatz 1b der Fassungen im Vergleich:

⇢ “Personal data shall be:
collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes”

⇢ „Personenbezogene Daten müssen:
für festgelegte, eindeutige und legitime Zwecke erhoben werden und dürfen nicht in einer mit diesen Zwecken nicht zu vereinbarenden Weise weiterverarbeitet werden“
Der Begriff „specified“ wird im Sinne von „determine“ verwendet und „explicit“ mit „eindeutig“ übersetzt.

Auch hier empfiehlt sich daher die Vorabprüfung, ob die übrigen Mitgliedstaaten das gleiche Verständnis haben und ob sich Auslegung und Anforderungen ändern, wenn die deutsche Fassung voraussetzen würde, dass personenbezogene Daten für näher aufgeführte, genau angegebene/ausdrücklich benannte und rechtmäßige Zwecke erhoben werden müssen.

Gleichwohl sollte insgesamt berücksichtigt werden, dass die Artikel-29-Datenschutzgruppe darauf hinweist, dass manchmal sogar der Kontext und die Verkehrssitte ausreichend sein können, wenn die Datenverarbeitung für alle Beteiligten ausreichend klar ist.[111] In einfachen Fällen sei die Bereitstellung detaillierter Informationen nicht unbedingt erforderlich.[112]

Unter Berücksichtigung dieser Auffassung könnte sich in Bezug auf Artikel 5 Absatz 1b Datenschutz-Grundverordnung daher eine Verhaltensregel dahingehend empfehlen, ob die schriftliche Bereitstellung des expliziten Zwecks an die betroffene Person erforderlich ist und in welchen Fallgestaltungen eine ausdrückliche und detaillierte Benennung des Zwecks nicht erforderlich sein könnte.

Diese Überlegungen müssten im Übrigen gleichermaßen im Hinblick auf Cookies und bei der Auslegung der Richtlinien 2002/58/EG und 2009/136/EG berücksichtigt werden. Sofern die Artikel-29-Datenschutzgruppe First-Party-Analysecookies für rechtmäßig erachtet, da sie ein geringes Datenschutzrisiko darstellen,[113] sollte der Anbieter seine Vorgehensweise genau beschreiben, damit die betroffene Person tatsächlich eine freie Entscheidung treffen kann. „Specified“ meint, dass der Verarbeitungsprozess begrenzt sein muss,[114] und dass unklare Formulierungen wie „IT-Sicherheitszwecke“ nicht ausreichen.[115] Entsprechendes muss für die Formulierung „Webanalyse-Cookies“ des Anbieters gelten. Auch hier bedarf es einer näheren Erläuterung des Zwecks und der Durchführung. Dies ist bei Anwendung und Auslegung des Erwägungsgrunds 25 der Richtlinie 2002/58/EG sowie Erwägungsgrunds 66 der Richtlinie 2009/136/EG zu bedenken, wenn es um Cookies als legitime Hilfsmittel geht.

Die gerade dargestellten Erwägungen wirken sich unmittelbar auf die unter den Punkten (3) und (4) aufgeführte Transparenz und „Kenntnis der Sachlage“ aus. Zunächst muss Einigung darüber bestehen, wie die Zweckbestimmung und damit zusammenhängend der Begriff „explicit“ zu verstehen ist.

111 Vgl. Artikel-29-Datenschutzgruppe, „Opinion 03/2013 on purpose limitation“, WP 203 adopted on 2 April 2013, S. 18.

112 Vgl. Artikel-29-Datenschutzgruppe, „Opinion 03/2013 on purpose limitation“, WP 203 adopted on 2 April 2013, S. 18.

113 Artikel-29-Datenschutzgruppe, WP 194, Stellungnahme 04/2012 zur Ausnahme von Cookies von der Einwilligungspflicht, angenommen am 07. Juni 2012, S. 12.

114 Artikel-29-Datenschutzgruppe, „Opinion 03/2013 on purpose limitation“; WP 203 adopted on 2 April 2013, S. 12.

115 Artikel-29-Datenschutzgruppe, „Opinion 03/2013 on purpose limitation“; WP 203 adopted on 2 April 2013, S. 15/16.

Ist nicht die erklärende Form umfasst, sondern das Ergebnis entscheidend, könnte letztendlich der Inhalt der Information abweichend sein. Um einen gemeinsamen Nenner zu finden, hat die Artikel-29-Datenschutzgruppe in Bezug auf die Richtlinie 95/46/EG vorgeschlagen, dass so viel wie nötig ausdrücklich erklärt werden muss, um ein einheitliches Verständnis über den Zweck zu erreichen.[116] Wenn der Fokus auf dem Ergebnis liegt, muss für den eindeutigen und unmissverständlichen Zweck, der nach außen hin auch zum Ausdruck gebracht wurde, der Empfängerhorizont entscheidend sein. Sofern der Zweck mangelhaft kommuniziert wurde, können nach Auffassung der Artikel-29-Datenschutzgruppe unterschiedliche Faktoren herangezogen werden, etwa das allgemeine Verständnis und die vernünftigen Erwartungen der betroffenen Person.[117]

(3) Kenntnis der Sachlage

Hinsichtlich der Kenntnis der Sachlage sind die Auslegung und Verknüpfung der Begriffsbestimmungen von „explicit und specified purposes“ sowie „einer Verarbeitungstätigkeit“ (siehe oben unter (1)) relevant, die gemäß der obigen Ausführungen der Artikel-29-Datenschutzgruppe in einem eingeschränkten Kontext verstanden werden sollte. Die Einwilligung müsse sich auf eine genau umrissene konkrete Situation beziehen. In diesem Sinne sollte daher Erwägungsgrund 32 Datenschutz-Grundverordnung zukünftig verstanden werden, der auf „eine andere Erklärung oder Verhaltensweise“ Bezug nimmt, „mit der die betroffene Person in dem jeweiligen Kontext eindeutig ihr Einverständnis mit der beabsichtigten Verarbeitung ihrer personenbezogenen Daten signalisiert.“

Die Datenverarbeitung wird umfangreicher und komplizierter, es gibt immer mehr Auswertungsmethoden. Bei vielen Diensten, z. B. Smart-Grid oder Smart-TV, können außerdem unterschiedliche Akteure einbezogen und Verarbeitungsvorgänge betroffen sein. Ist es hier der betroffenen Person überhaupt möglich, in dem jeweiligen Kontext eindeutig ein Einverständnis zu signalisieren? Der Durchschnittsverbraucher wird die komplexe Datenverarbeitung oftmals nicht mehr nachvollziehen können, so dass die Zwecke und Empfänger in seinem Sinne klar benannt werden müssten. In diesem Sinne wäre eine Auslegung nicht mehr notwendig. Anderenfalls müsste bei einer Auslegung des „Signals eines Einverständnisses der betroffenen Person in dem jeweiligen Kontext“ sehr genau geprüft werden, welche Maßnahmen etwa bei der Erstellung einer persönlichen Senderliste (Smart-TV) oder des Verbrauchs per Zeitintervall (Smart-Grid) ohne weitere gesonderte Einwilligung erfasst sein dürften. Der betroffenen Person müsste außerdem technisch von vorneherein ermöglicht werden, Verarbeitungstätigkeiten im Einzelfall auszuschließen, ohne auf den kompletten Dienst verzichten zu müssen.[118]

Bei der Kontextbestimmung muss jedoch eine weite Auslegung ausgeschlossen sein, so dass nicht - wie bei der Direktwerbung im Wettbewerbsrecht - die Möglichkeit besteht, einen „ähnlichen“ Zweck als rechtmäßig zu unterstellen. Wenn im Rahmen eines laufenden Vertragsverhältnisses die Möglichkeit besteht, nicht nur zur Vertragserfüllung erforderliche, sondern freiwillige, einwilligungsbedürftige Leistungen (unterschiedlich beteiligter Vertragspartner) in Anspruch zu nehmen, sollte aus Transparenzgründen die Datenverarbeitung klar dargestellt sein und eine Interpretation des Kontexts nicht möglich sein.[119] In analoger Anwendung des geschilderten „Telekom-Falls“ ist zudem sehr genau zu prüfen, ob die betroffene Person außerdem vernünftigerweise mit unterschiedlichen Empfängern (die bei Bereitstellung der Dienstleistung beteiligt sind) rechnen konnte.

116 Artikel-29-Datenschutzgruppe, „Opinion 03/2013 on purpose limitation“; WP 203 adopted on 2 April 2013, S. 18.

117 Artikel-29-Datenschutzgruppe, „Opinion 03/2013 on purpose limitation“; WP 203 adopted on 2 April 2013, S. 19, 39.

118 Zum Kopplungsverbot siehe S. 49 ff.

119 Siehe zur Werbung die Ausführungen auf S. 44 ff.

Entscheidend müssen stets gemäß der Empfehlungen der Artikel-29-Datenschutzgruppe die „vernünftigen Erwartungen“ sein, wobei zu bedenken ist, dass sich diese im Laufe der zukünftigen Entwicklung immer offener gestalten könnten. Für die Beibehaltung der Datenhoheit bei der betroffenen Person sollten die Zwecke und Empfänger daher ausdrücklich erklärt werden (müssen).

Der Nachweis der Einwilligung gemäß Artikel 7 Absatz 1 Datenschutz-Grundverordnung ist in diesem Falle im Übrigen nur dann hilfreich, wenn dafür europaweit einheitliche Kriterien festgelegt werden, auch um gleichartige Wettbewerbsbedingungen zu schaffen.

Es sollten daher insgesamt klare Verhaltensregeln oder Leitlinien aufgestellt werden, um eine faire und transparente europaweite Datenverarbeitung sicherzustellen, die ebenso zur Gewährleistung eines einheitlichen Wettbewerbs beitragen könnten.

Zudem sind einheitliche Kriterien wichtig, um eine klare Abgrenzung von einer Zweckänderung gemäß Artikel 6 Absatz 4 Datenschutz-Grundverordnung vorzunehmen. Die Voraussetzungen in Erwägungsgrund 50 und Artikel 6 Absatz 4 Datenschutz-Grundverordnung entsprechen den Ausführungen der Artikel-29-Datenschutzgruppe zur Zweckbestimmung, vor allem der Zusammenhang von ursprünglichen und dem späteren Verwendungszweck, die vernünftigen Erwartungen der betroffenen Personen, die Auswirkung der geänderten Verwendung auf die betroffenen Personen sowie die Schutzmaßnahmen, wie etwa Pseudonymisierung.[120] Aber es wird gleichermaßen im Sinne eines Kompatibilitätstests vertreten, dass diese Faktoren unterschiedlich gewichtet und eine erhöhte oder nachgewiesene Transparenz berücksichtigt werden könnte, wenn dem Betroffenen ein Widerspruchsrecht eingeräumt oder eine funktionale Trennung vorgenommen werde.[121]

Im Ergebnis könnten also geeignete Schutzmaßnahmen durchaus größere oder überraschende Zweckänderungen legitimieren.[122] Verbindet man diesen Gedanken mit der Möglichkeit, dass nun ebenso die datenverarbeitende Stelle durch eine organisatorische Trennung die Pseudonymisierung durchführen kann,[123] bedarf es hier im Besonderen klarer Verhaltensregeln für die Datenverarbeitung. Zu beachten ist stets: Gemäß Artikel 13 Absatz 3 sowie Erwägungsgrund 61 Datenschutz-Grundverordnung muss der Verantwortliche Informationen über den geänderten Zweck vor Weiterverarbeitung zur Verfügung stellen. Dies ist jedoch von der grundsätzlichen Bewertung der Zulässigkeit der Zweckänderung unabhängig, die ohne erneute Einwilligung durchgeführt werden könnte (bei Vorliegen der entsprechenden Voraussetzungen).

Insgesamt muss zukünftig eine weite Auslegung von Zweck und Empfängern vermieden werden. Die Gefahr besteht anhand der oben dargestellten Formulierungen „Signal des Einverständnisses in dem jeweiligen Kontext“ in Verbindung mit der unterschiedlichen europaweiten Auslegung des Begriffs „explicit“ und der darüber hinaus bestehenden Möglichkeit einer Zweckänderung, der bereits zum jetzigen Zeitpunkt teilweise ein weites Verständnis zugrunde liegt.

120 *Vgl. Artikel-29-Datenschutzgruppe, „Opinion 03/2013 on purpose limitation“; WP 203 adopted on 2 April 2013, siehe insbesondere zur Kompatibilität, Vorhersehbarkeit und Nutzerkontrolle S.12-S.14.*

121 *Helbig, K&R 2015, S. 145, 147.*

122 *Helbig, K&R 2015, S. 145, 147.*

123 *Erwägungsgrund 29 Datenschutz-Grundverordnung regelt, dass „um Anreize für die Anwendung der Pseudonymisierung bei der Verarbeitung personenbezogener Daten zu schaffen, sollten Pseudonymisierungsmaßnahmen, die jedoch eine allgemeine Analyse zulassen, bei demselben Verantwortlichen möglich sein, wenn dieser die erforderlichen technischen und organisatorischen Maßnahmen getroffen hat, um — für die jeweilige Verarbeitung — die Umsetzung dieser Verordnung zu gewährleisten, wobei sicherzustellen ist, dass zusätzliche Informationen, mit denen die personenbezogenen Daten einer speziellen betroffenen Person zugeordnet werden können, gesondert aufbewahrt werden.“*

Nur wenn ein einheitliches Verständnis herrscht, kann auch die Information oder Unterrichtung über den zugrundeliegenden Zweck sinnvoll und einheitlich umgesetzt werden (siehe den folgenden Punkt „Informiertheit“).

(4) Informiertheit und Transparenz

Gemäß der Ausführungen der Artikel-29-Datenschutzgruppe bezieht sich eine zweite Dimension der Einwilligung auf die Information als Transparenz gegenüber der betroffenen Person. Dies wurde gerade unter Punkt (3) „Kenntnis der Sachlage“ dargestellt, deckt aber regelmäßig auch alle Informationen ab, die in Artikel 13 Datenschutz-Grundverordnung enthalten sind.[124]

Die Einwilligung muss damit auf informierter Basis erfolgen, was die Artikel-29-Datenschutzgruppe bereits für die Anforderungen nach der Richtlinie 95/46/EG festgestellt hat (Artikel 10 und 11 der Richtlinie 95/46/EG). Obwohl die Informationspflicht eine eigenständige Pflicht darstellt, sei sie mit der Einwilligung verbunden: Vor ihrer Bereitstellung könne keine Einwilligung erteilt werden,[125] wobei in vielen Fällen die Einwilligung zum Zeitpunkt der Erhebung der personenbezogenen Daten erhalten wird, wenn die Verarbeitung beginnt, so dass in diesem Fall die bereitzustellende Information mit den in Artikel 10 der Richtlinie aufgeführten Punkten übereinstimme.[126]

Diese Ausführungen müssen ebenso hinsichtlich der Datenschutz-Grundverordnung gelten.
Insgesamt enthält die Datenschutz-Grundverordnung Regelungen zur Informiertheit und Transparenz in Artikel 12, 13 und 14: Der Nutzer muss stets präzise, leicht zugänglich und verständlich sowie in klarer und einfacher Sprache, insbesondere über Verarbeitungszwecke, Rechtsgrundlage der Verarbeitung, Empfänger der personenbezogenen Daten, informiert sein und ein entsprechendes Auskunftsrecht gemäß Artikel 15 ausüben können.

124 *Siehe auch Artikel-29-Datenschutzgruppe, WP 187, Stellungnahme 15/2011 zur Definition von Einwilligung, angenommen am 13. Juli 2011, S. 11 mit dem folgenden Hinweis: „Um gültig zu sein, muss die Einwilligung in Kenntnis der Sachlage erfolgen. Das bedeutet, dass alle erforderlichen Informationen dann zu erteilen sind, wenn die Einwilligung gefordert wird und dass sie alle wesentlichen Aspekte der Verarbeitung ansprechen, die durch die Einwilligung legitimiert werden sollen. Das würde normalerweise alle Informationen abdecken, die in Artikel 10 der Richtlinie aufgeführt sind. Es hängt aber auch davon ab, wann und unter welchen Umständen die Einwilligung gefordert wird. Unabhängig davon, ob die Einwilligung gegeben wird oder nicht, ist die Transparenz der Datenverarbeitung eine Bedingung der Fairness, die auch nach Bereitstellung der anfänglichen Informationen ihren Wert hat“.*

125 *Artikel-29-Datenschutzgruppe, WP 187, Stellungnahme 15/2011 zur Definition von Einwilligung, angenommen am 13. Juli 2011, S. 22/23.*

126 *Artikel-29-Datenschutzgruppe, WP 187, Stellungnahme 15/2011 zur Definition von Einwilligung, angenommen am 13. Juli 2011, S. 23.*

Diese Informations- und Auskunftsrechte umfassen ebenso

- die Dauer der Verarbeitung,
- die Darlegung der berechtigten Interessen gemäß Artikel 6 Absatz 1f (sofern etwa eine Verarbeitung der personenbezogenen Daten nicht auf der Einwilligung beruht oder zur Vertragserfüllung erforderlich ist),
- Widerspruchsrechte gemäß Artikel 21,
- Beschwerderecht bei der Aufsichtsbehörde,
- Informationen über die öffentlichen zugänglichen Quellen, sofern Daten daraus erhoben wurden
- sowie das Bestehen einer automatisierten Entscheidungsfindung (Artikel 22).

Die Artikel-29-Datenschutzgruppe unterscheidet zwischen Qualität einerseits sowie Zugänglichkeit und Sichtbarkeit der Information andererseits. Qualität (bezogen auf „in Kenntnis der Sachlage“) meint, dass ein regelmäßiger/durchschnittlicher Nutzer in der Lage sein sollte, sie zu verstehen.[127] In der Datenschutz-Grundverordnung wird in Erwägungsgrund 42 zusätzlich die Einhaltung von verbraucherschutzrechtlichen Vorgaben verlangt. Garantien sollten sicherstellen, dass die betroffene Person weiß, dass und in welchem Umfang sie ihre Einwilligung erteilt hat. Eine vom Verantwortlichen vorformulierte Einwilligungserklärung sollte keine missbräuchlichen Klauseln enthalten und in verständlicher und leicht zugänglicher Form sowie in einer klaren und einfachen Sprache zur Verfügung gestellt werden (unter Verweis auf die Richtlinie 93/13/EWG des Rates).

Entsprechendes hat die Artikel-29-Datenschutzgruppe bereits in ihrer Stellungnahme WP 187 empfohlen („Informationen sollten deutlich sichtbar (Art und Größe der Schrift), auffällig und verständlich sein“).[128]

Der Grundsatz der Transparenz setzt gemäß der deutschen Fassung des Erwägungsgrunds 39 Datenschutz-Grundverordnung zwar außerdem voraus, dass alle Informationen und Mitteilungen zur Verarbeitung dieser personenbezogenen Daten leicht zugänglich und verständlich und in klarer und einfacher Sprache verfasst sein müssen. Fraglich ist jedoch (wie oben ausführlich dargestellt) hinsichtlich des Zwecks, „wie“ zu informieren ist bzw. ob entsprechend der Problematik bei Anwendung der Richtlinie 95/46/EG ebenso bei der Datenschutz-Grundverordnung unterschiedliche Sprachverständnisse über „explicit“ und „specified“ bestehen, sich dadurch für die Rechte der betroffenen Personen in den einzelnen Mitgliedstaaten Unterschiede ergeben und einer Vollharmonisierung des Datenschutzrechts entgegenstehen könnten (siehe hierzu die obigen Ausführungen und zur Erinnerung den Wortlaut des Erwägungsgrunds 39 „In particular, the specific purposes for which personal data are processed should be explicit…“).

127 *Artikel-29-Datenschutzgruppe, WP 187, Stellungnahme 15/2011 zur Definition von Einwilligung, angenommen am 13. Juli 2011, S. 23.*

128 *Artikel-29-Datenschutzgruppe, WP 187, Stellungnahme 15/2011 zur Definition von Einwilligung, angenommen am 13. Juli 2011, S. 23. S. 24: Je schwieriger es für den Durchschnittsbürger wird, alle Elemente der Datenverarbeitung zu überblicken und zu verstehen, desto größer sollten die Anstrengungen des für die Datenverarbeitung Verantwortlichen sein, zu zeigen, dass die Einwilligung basierend auf verständlichen Informationen für den konkreten Fall erteilt wurde.*

Die englische Originalfassung regelt zudem in Artikel 13 Datenschutz-Grundverordnung folgendes:
„Where personal data relating to a data subject are collected from the data subject, the controller shall, at the time when personal data are obtained, provide the data subject with all of the following information:
...

(c)
the purposes of the processing for which the personal data are intended as well as the legal basis for the processing;"

Die deutsche Fassung übersetzt "provide with information" mit "mitteilen". Der Zweck muss demnach aufgrund der Regelung des Artikel 13 Datenschutz-Grundverordnung gegenüber der betroffenen Person erklärt werden. Gemäß dem oben Gesagten ist jedoch zum einen offen, „wie" der Zweck (vorher) festgelegt und formuliert sein muss. Zum anderen wäre europaweit zu vergleichen, ob sich gegebenenfalls durch abweichende Übersetzungen von „provide with" Unterschiede ergeben könnten und die Verantwortlichen in den übrigen Mitgliedstaaten die Informationen immer „mitteilen" im Sinne von „erklären" müssen.

Bei einer elektronischen Einwilligung sind zudem die oben dargestellten Ausführungen zu beachten (s. S. 9 ff. und S. 19 ff.). Hier muss zukünftig klargestellt werden, ob die Informationen „jederzeit abrufbar" oder nur „leicht zugänglich" sein müssen oder ob beide Begrifflichkeiten synonym zu verwenden sind.

! Fazit Nr. 6

Zwecke müssen gemäß Artikel 5 Absatz 1b Datenschutz-Grundverordnung festgelegt, eindeutig und legitim sein, aber fraglich ist, ob damit auch europaweit das Verständnis verbunden wird, die Zwecke klar auszudrücken und zu erklären und inwieweit die Zweckbestimmung in einem weiten Verständnis definiert wird (siehe Artikel-29-Datenschutzgruppe WP 203).

Es kann sich daher ein aktueller Vergleich der Übersetzungen noch vor Inkrafttreten der Datenschutz-Grundverordnung im Hinblick darauf empfehlen, inwieweit ein einheitliches, europaweites Verständnis über die Auslegung von „explicit", „specified" und „provide with" besteht. Dabei sollte berücksichtigt werden, ob unterschiedliche Auslegungen Auswirkung auf die Betroffenenrechte im Sinne eines einheitlichen Schutzniveaus haben könnten.

Die bisherigen Ausführungen der Artikel-29-Datenschutzgruppe zur Zweckbestimmung könnten für die Ausgestaltung einer Verhaltensregel herangezogen oder vom zukünftigen Europäischen Datenschutzausschuss bekräftigt werden. Im Sinne des Betroffenenschutzes und im Rahmen der Zweckbestimmung sollten Zwecke klar ausgedrückt und erklärt werden (trotz oder gerade aufgrund komplexer Datenverarbeitungsprozesse). Dies ist insbesondere im Hinblick auf Big Data-Anwendungen und zentrale Datenspeicherungslösungen, bei welchen mehrere Beteiligte eingebunden sind, von Bedeutung.

! Es muss genau geprüft werden, was von einer Verarbeitungstätigkeit sinnvollerweise und vernünftigerweise umfasst sein kann. Hierfür sind das allgemeine Verständnis und die Betroffenensicht entscheidend, die sich jedoch im Laufe der Zeit verändern können. Die rasante technische Entwicklung spielt hierbei eine Rolle. Es muss dementsprechend die Sichtweise und das technische Verständnis eines „Durchschnittsbetroffenen" zum „jeweiligen Zeitpunkt" ermittelt werden.[129]
Die Datenschutzaufsichtsbehörden in Deutschland sollten bereits zum jetzigen Zeitpunkt klare Anforderungen an geeignete Schutzmaßnahmen für eine Zweckänderung formulieren, insbesondere vor dem Hintergrund von Big Data-Anwendungen. Es kann sich ein Negativkatalog empfehlen, etwa inwieweit Transparenz und Pseudonymisierung tatsächlich eine Zweckänderung ermöglichen oder erleichtern kann. Zukünftig bedarf es hierfür im europäischen Kontext klarer Leitlinien für die Datenverarbeitung.

2. Relevanz für den Einwilligungsassistenten

(1) Granularität

Der Verantwortliche muss sicherstellen, dass die betroffene Person die gerade unter 1. (4) aufgelisteten Informationen vor Erteilung der Einwilligung erhält, da die Einwilligung auf informierter Basis erfolgen muss. Dabei ist ebenso zu berücksichtigen, ob der zukünftige Einsatz eines Einwilligungsassistenten einen selbstständigen Dienst der Informationsgesellschaft darstellt, so dass dieser ebenfalls einer Verpflichtung zur Bereitstellung von Informationen unterliegt.[130]

In Bezug auf die Einwilligungsvoraussetzungen hat die Artikel-29-Datenschutzgruppe in ihrer Stellungnahme „Online-Informationsmittel" erwähnt, die besonders in Bezug auf soziale Netzwerkdienste hilfreich sein sollen, um eine ausreichende Granularität und Klarheit der Privatsphären-Einstellungen zu bieten. Auch mehrschichtige Hinweise könnten als ein hilfreiches Mittel dazu beitragen, die richtigen Informationen auf eine einfach zugängliche Weise bereitzustellen.[131] Diese Überlegungen sollten ebenso für die Konzeption des Einwilligungsassistenten herangezogen werden, damit dieser für die betroffene Person ausreichend klare Elemente hinsichtlich Einwilligung und Information anbietet.

Für den Einwilligungsassistenten ist jedoch fraglich, ob er den notwendigen Detaillierungsgrad und die Unterscheidung von Zwecken sowie vernünftigen Erwartungen und Empfängern automatisiert durchführen kann oder vielmehr eine rechtliche Bewertung des Einzelfalls erforderlich bleibt.[132] Der in der Einführung geschilderte automatisierte Abgleich der Datenschutzbestimmungen mit anschließender Übersetzung in ein Formular, welches die Daten, Zwecke und Empfänger für die betroffene Person in einem übersichtlichen Dokument darstellt, müsste ausreichend detailliert sein.

129 Hier kann geprüft werden, ob es hilfreich ist, die Auffassung des Bundesgerichtshofs zur WLan-Haftung heranzuziehen, und -im Sinne des Betroffenenschutzes- bei einem laufenden Dienstleistungsverhältnis den Zeitpunkt der Kenntnis auf den Zeitpunkt des ursprünglichen Abschlusses festzulegen. Bundesgerichtshof, Urteil vom 24.11.2016 - I ZR 220/15: Der Inhaber eines Internetanschlusses mit WLAN-Funktion ist „nur" zur Prüfung verpflichtet, ob der eingesetzte Router über die im Zeitpunkt seines Kaufs für den privaten Bereich marktüblichen Sicherungen, also einen aktuellen Verschlüsselungsstandard sowie ein individuelles, ausreichend langes und sicheres Passwort, verfügt. Eventuell könnte in Anlehnung an diese Rechtsprechung das technische Verständnis der betroffenen Person zum Zeitpunkt des Vertragsabschlusses bei einem laufenden Vertragsverhältnis zugrunde gelegt werden.

130 Siehe hierzu S. 21 und S. 55.

131 Artikel-29-Datenschutzgruppe, WP 187, Stellungnahme 15/2011 zur Definition von Einwilligung, angenommen am 13. Juli 2011, S. 24.

132 Siehe hierzu bereits S. 26 und S. 28.

Zur Bewertung können in diesem Zusammenhang etwa die verbundenen Rechtssachen „C-92/09 und C-93/09“ des Europäischen Gerichtshofs herangezogen werden.[133] Hier wurde verlangt, dass der Betroffene die Möglichkeit hat, nicht nur pauschal in die Veröffentlichung von Daten einzuwilligen, sondern im Einzelfall bezüglich der einzelnen Daten unterschieden werden müsse, die veröffentlicht werden sollen. Dies muss bei der Konzeption des Einwilligungsassistenten sichergestellt sein.

Unter Berücksichtigung der obigen Ausführungen hinsichtlich der Einwilligungsvoraussetzungen „bestimmter Fall und Zweck“ stellt sich dennoch die Frage, wie granular die Voreinstellungen vorgenommen werden müssen oder ob sich nicht durch Verwendung von bestimmten Präferenzen gleichzeitig ergeben könnte, dass der Nutzer ebenso mit Verarbeitung von anderen Daten im gleichen Kontext einverstanden ist. In Bezug auf die Darstellung der Einwilligungs“elemente“ könnte fraglich sein, ob es nicht zulässig wäre, die Zwecke weniger detailliert aufzulisten, stets unter der Maßgabe, dass der Verantwortliche sie als „eine“ Verarbeitungstätigkeit versteht. Aber gerade der Einwilligungsassistent kann aufgrund seiner Möglichkeit der Bereitstellung granularer Komponenten zur Transparenz beitragen, so dass seine technische (Fort-)Entwicklung dahingehend erfolgen sollte, die notwendige Granularität und Transparenz sicherzustellen und nicht diese umzukehren.

Beachtet werden muss gleichwohl, dass die Komplexität der Datenverarbeitung zunimmt und der Kontext der Einwilligung auch aus Betroffenensicht nicht überspannt werden darf, so dass tatsächlich im Einzelfall geprüft werden muss, was unter „einer“ Verarbeitungstätigkeit sinnvollerweise verstanden werden muss. Insbesondere bei intelligenten Stromzählern gibt es unter Umständen eine Menge Akteure, bei denen das Erfordernis einer Einwilligung für die einzelne Datenverarbeitung und unterschiedliche Empfänger genau zu prüfen wäre. Darüber hinaus gilt stets, dass anstatt einer Einwilligung eine transparente Information ausreichen könnte, wenn die Datenverarbeitung bereits durch die Ausgestaltung des Vertragsverhältnisses erforderlich ist,[134] so dass abermals die automatische Prüfung der Datenschutzhinweise unter Erstellung einer Einwilligungserklärung einer kritischen Prüfung zu unterziehen ist.

Dies entspricht insgesamt der Auffassung der Artikel-29-Datenschutzgruppe, die zum einen die Notwendigkeit der Granularität bei der Einholung der Einwilligung von Fall zu Fall in Abhängigkeit vom Zweck/den Zwecken oder dem Datenempfänger bewertet wissen möchte, und zum anderen die Unterscheidung zwischen Erforderlichkeit der Datenverarbeitung und freiwilliger Einwilligung betont.[135]

Weiterhin ist bei der Konzeption des Einwilligungsassistenten entscheidend, ob die Daten zentral oder dezentral gespeichert werden:

133 *Siehe den Verweis in Artikel-29-Datenschutzgruppe, WP 187, Stellungnahme 15/2011 zur Definition von Einwilligung, angenommen am 13. Juli 2011, S. 26 auf die Schlussanträge der Generalanwältin Sharpston vom 17. Juni 2010, Volker und Markus Schecke GbR, verbundene Rechtssachen C-92/09 und C-93/09.*

134 *Siehe hierzu etwa auch das Beispiel zu den unterschiedlichen beteiligten Akteuren bei Verbrauchsdatenabrechnung per Zeitintervall im Kontext von „Abrechnung bezogener sowie eingespeister Energie im Bilanzierungssystem“. Hier muss die Erforderlichkeit einer Einwilligung genau geprüft werden und von den erforderlichen Zwecken einer Vertragsdurchführung abgegrenzt werden in der Orientierungshilfe datenschutzgerechtes Smart Metering der Konferenz der Datenschutzbeauftragten des Bundes und der Länder von Juni 2012 „Maßnahmen an Hand von Use Cases“, Fallbeispiel S. 28 http://www.bfdi.bund.de/SharedDocs/Publikationen/Entschliessungssammlung/DSBundLaender/Orientierungshilfe_SmartMeter.pdf?__blob=publicationFile*

135 *Artikel-29-Datenschutzgruppe, WP 187, Stellungnahme 15/2011 zur Definition von Einwilligung, angenommen am 13. Juli 2011, S. 21 sowie S. 9, letzteres zur Anwendbarkeit mehrerer Rechtsgrundlagen: Entweder ist die Verarbeitung notwendig für die Erfüllung eines Vertrags oder die Einwilligung (ohne Zwang) muss eingeholt werden.*

- Werden die Daten zentral auf einer Plattform gespeichert -diese Möglichkeit besteht bei CoMaFeDS- muss zwischen dem Verantwortlichen der Plattform und dem jeweiligen (potenziellen) Empfänger der Daten unterschieden werden: Es müsste zum einen sichergestellt sein, dass der Nutzer transparent über die geplante Datenverarbeitung des Empfängers aufgeklärt wird. Zum anderen müsste berücksichtigt werden, wer als Verantwortlicher des „Wissensgraphen" der Plattform einzustufen ist.[136] Wie eingangs dargestellt, sind über die zukünftige geplante Funktionsweise bislang noch keine näheren technischen Details offengelegt. Daher muss sich diese Ausführung auf den allgemeinen Hinweis beschränken, dass hier sowohl die technische Sicherheit zu beachten ist, als auch die Frage beantwortet werden muss, ob der Plattformbetreiber gesondert vom jeweiligen Nutzer eine Einwilligung für die „Datenvermittlung" einholen müsste und wie die „Kenntnis der Sachlage im Einzelfall" sichergestellt ist. Auch hier sollte grundsätzlich die Aktivität stets vom Nutzer ausgehen und es dürfte, gerade unter Berücksichtigung der Zeitdauer, keine pauschale Einwilligung -ohne entsprechende Rückfrage im Einzelfall an den Nutzer- eingeholt werden.

- Im Hinblick auf die dezentrale Speicherung beim Nutzer wird zurzeit nach technischen Lösungen gesucht, die es potenziellen Empfängern erlauben, die erteilte Einwilligung trotz lokaler Speicherung finden zu können. Daher wäre der selbstständige Einsatz beim Nutzer (ohne zentrale Plattform) zukünftig denkbar. Eine solche dezentrale Speicherung ist das Konzept von LETsmart, aber ebenso bei CoMaFeDS in Prüfung und Entwicklung.

Auch wenn Systeme wie LETsmart nach derzeitiger Planung in der Lage sein sollen, nach Wegfall des Verwendungszwecks die Daten automatisiert im dezentral betriebenen System des Nutzers zu löschen, ist nicht ausgeschlossen, dass der Empfänger die Daten, auf die ihm Zugriff gewährt wurde, kopiert und eigenständig verarbeitet. Der jeweilige Empfänger muss also im Sinne der datenschutzrechtlichen Regelungen entweder die Kopie bzw. Speicherung der Daten in seinem System von vorneherein ausschließen oder im Falle einer eigenständigen Speicherung die Löschung der Daten in seinem System sicherstellen. Im Gesamten ist somit wiederum von besonderer Bedeutung, wer Verantwortlicher des Einwilligungsassistenten ist, der sich derzeit weiterhin in der Entwicklung befindet. Entscheidend ist, unter anderem für die Informations- und Löschungspflichten, ob sich der Einwilligungsassistent (ebenso) im „Herrschaftsbereich" des Nutzers befindet oder von einem Anbieter eingesetzt wird.[137]

In diesem Zusammenhang ist auf die übrigen Systeme Bezug zu nehmen, die in der Bestandsaufnahme der Studie dargestellt wurden: Sofern unterschiedliche Daten in einem System zusammengefügt werden (siehe etwa den Dienst DigiMe[138]) und mit einem Einwilligungsassistenten verknüpft würden, ist besonders zu bedenken, inwieweit eine nachträgliche Zweckänderung oder die Formulierung eines Zwecks „in einem Kontext" in Bezug auf andere Empfänger in Betracht kommen kann. Wenn der Nutzer selbst seine persönlichen Daten speichert, Zugriffsberechtigungen vergibt, so dass mehrere Unternehmen darauf Zugriff haben, lässt sich gegebenenfalls einfacher begründen, aus welchem Grunde nun die Formulierung eines Zwecks „in einem Kontext" ausreichen soll, um die Weitergabe an unterschiedliche Empfänger zu begründen oder dies nachträglich zu legitimieren (siehe auch den oben genannten Telekom-Fall).

136 Siehe hierzu auch den Punkt „Verantwortung" auf S. 52 ff.
137 Siehe hierzu auch den Punkt „Verantwortung" auf S. 52 ff.
138 Siehe Kapitel II.2. der Studie der Stiftung Datenschutz.

Dem Nutzer wären die Empfänger in diesem Fall ja sogar bekannt. Hierbei wird zukünftig ganz entscheidend sein, wer im Rahmen der technischen Möglichkeiten als (Mit)Verantwortlicher betrachtet wird und inwieweit sanktionsbehaftete Nachweispflichten gemäß Artikel 7 Absatz 1 Datenschutz-Grundverordnung durchgesetzt werden können.[139]

(2) Exkurs: UWG

In Bezug auf die Einwilligung bei Standortdaten ist bei Verwendung eines Einwilligungsassistenten auf folgendes zu achten: Es ergibt sich zu dem oben dargestellten Telefonanruf im Zusammenhang mit einem Wettervorhersagedienst[140] insofern ein Unterschied, dass die betroffene Person durch Anwählen einer Telefonnummer selbst aktiv tätig wird. Es ist ungewiss, ob tatsächlich an jedem Ort oder bei jeder Hotelankunft eine Restaurantempfehlung oder Wetteransage gewünscht ist. Im Hinblick auf den Einwilligungsassistenten ist daher fraglich, ob im Vorhinein eine informierte Einwilligung für eine automatische Standortbestimmung erfolgen kann: Wird der Nutzer beispielsweise automatisiert bei Ankunft in einem Hotel gefragt, ob er eine Restaurantempfehlung wünscht, wird sein Standort bereits verwendet. Hier spielt außerdem der Zeitablauf einer solchen Einwilligung eine wesentliche Rolle.[141] Dem Nutzer muss bewusst sein, in welchem Falle und zu welchem konkreten Zweck eine automatische Standortbestimmung erfolgt. Weiterhin ist fraglich, ob damit auch „ähnliche“ Zwecke wie die nächstgelegenen Kneipen, Bars oder Tankstellen mit Imbissangebot (Ursprungsdienstleistung: Restaurantempfehlungen) oder Informationen über Schäden, Stromausfälle und Verkehrsbehinderungen (Ursprungsdienstleistung: Wettervorhersage) für einen bestimmten Wintersportort) umfasst sind. In der deutschen Literatur wird beispielsweise vertreten, dass demjenigen , der per E-Mail französischen Rotwein bestellt hat, künftig Werbung für chilenischen Rotwein übersandt werden darf, und wer einen Hotelaufenthalt in Kärnten per E-Mail gebucht hat, dem dürfe eine Werbung für einen Hotelaufenthalt in Sizilien geschickt werden.13[142] Gilt dies ebenso für (entgeltliche) Dienstleistungen wie die gerade genannten und wieweit reicht der datenschutzrechtliche Kontext? Eine solche mutmaßliche Einwilligung wird im Datenschutzrecht abgelehnt,[143] aber bei Direktwerbung innerhalb bestehender Vertragsbeziehungen für eigene ähnliche Produkte gemäß Artikel 13 Absatz 2 und Erwägungsgrund 41 der Richtlinie 2002/58/EG dennoch legitimiert. Dies bezieht sich insgesamt auf die Frage einer zulässigen Zweckänderung nach Artikel 6 Absatz 4 Datenschutz-Grundverordnung oder im Rahmen „derselben“ Einwilligung auf deren „Kontext“ (siehe oben unter (2) und (3)) unter Berücksichtigung des Wettbewerbsrechts. So wird in der deutschen Literatur kritisiert, dass bislang versäumt wurde, eine Homogenisierung der wettbewerbs- und datenschutzrechtlichen Einwilligungen herbeizuführen,[144] und nun muss darüber hinaus eine europaweite Harmonisierung erfolgen.

Gemäß der Rechtslage in Deutschland ist bei Direktwerbung folgendes zu bedenken: Das Bundesdatenschutzgesetz und das Gesetz gegen den unlauteren Wettbewerb (UWG) stehen gleichberechtigt nebeneinander. § 7 Absatz 3 UWG (der Artikel 13 Absatz 2 der Richtlinie 2002/58/EG umsetzt) bietet bei elektronischer Werbung insoweit eine Erleichterung, dass ein Unternehmer, der im Zusammenhang mit dem Verkauf einer Ware oder Dienstleistung von dem Kunden dessen elektronische Postadresse

139 *Siehe S. 47 ff.*

140 *Siehe hierzu S. 31 ff.*

141 *Siehe hierzu S. 50 ff. und aus wettbewerbsrechtlicher Sicht Köhler in: Köhler/Bornkamm, UWG, 34. Auflage 2016, § 7 UWG Rn. 204b zur zeitlichen Begrenzung.*

142 *Köhler in: Köhler/Bornkamm, UWG 34. Auflage 2016, § 7 UWG Rn. 205. Siehe hierzu auch die Ausführungen weiter unten in diesem Abschnitt.*

143 *Rogosch, Die Einwilligung im Datenschutzrecht, S. 68.*

144 *Rogosch, Die Einwilligung im Datenschutzrecht, S. 125.*

erhalten hat, diese zur Direktwerbung für eigene ähnliche Waren oder Dienstleistungen verwenden darf, wenn der Kunde nicht widersprochen hat. Diese Ausnahmeregelung wird von der deutschen Rechtsprechung eng und im Hinblick auf eine bestehende Geschäftsbeziehung ausgelegt.[145] Es wird vertreten, dass sich die Ähnlichkeit auf die bereits gekauften Waren beziehen und dem gleichen typischen Verwendungszweck oder Bedarf des Kunden entsprechen muss.[146] Gegebenenfalls sei es zulässig, Zubehör oder Ergänzungswaren zu bewerben.[147] Die Voraussetzung sei außerdem regelmäßig erfüllt, wenn die Produkte austauschbar sind oder dem gleichen oder zumindest einen ähnlichen Bedarf oder Verwendungszweck dienen.[148]

Umfasst das Geschäftsmodell eines Anbieters etwa das „Angebot von Restaurantempfehlungen aufgrund der Standortbestimmung" an Nutzer, die sich mittels ihrer elektronischen Postadresse[149] registriert haben, könnte unterstellt werden, dass die eigene Zusammenstellung der Empfehlungen auch ein eigenes Produkt des Anbieters darstellt (unter der Voraussetzung, dass der Anbieter die Nutzerdaten nicht an die Restaurantbesitzer weitergibt). Damit könnte er ebenfalls ähnliche Produkte empfehlen. Der Anbieter dieses Geschäftsmodells muss für diesen Dienst selbst Datenschutzhinweise transparent zur Verfügung stellen und hätte die Möglichkeit, gemäß § 7 Absatz 3 UWG ähnliche Dienstleistungen zu empfehlen. Zu beachten ist jedoch, dass der „Verkauf einer Dienstleistung" der Auslegung bedarf.[150] Im Sinne einer Harmonisierung sollte vor allem nicht die Rechtsauffassung zur „Entgeltlichkeit" im europäischen Kontext außer Acht gelassen werden sowie die Frage, wie „eigene Produkte" und „ähnliche Produkte" in anderen Mitgliedstaaten bewertet werden. Datenschutzrechtlich kann sich außerdem stets ein Widerspruch zur Eindeutigkeit der Zweckbestimmung und der klaren Benennung des Zwecks ergeben, sofern „Restaurantempfehlung" auf „ähnliche" Produkte ausgedehnt wird. Die Erforderlichkeit der ausdrücklichen Benennung des Zwecks wird in den Mitgliedstaaten unter Anwendung der Richtlinie 95/46/EG unterschiedlich gehandhabt.[151]

In dieser Stellungnahme kann allerdings keine europaweite Prüfung erfolgen, so dass sich eine zusätzliche Studie dahingehend empfehlen kann, ob sich im Hinblick auf die übrigen Mitgliedstaaten Unterschiede in der Rechtsauffassung ergeben könnten oder eine Harmonisierung des Wettbewerbsrechts bereits vorliegt. Die im Folgenden dargestellten Ausführungen beschränken sich daher weiterhin auf das UWG.

145 *KG, Beschluss vom 18.3.2011, 5 W 59/11.*

146 *OLG Jena, Urteil vom 21. 4. 2010, 2 U 88/10, MMR 2011, 101.*

147 *Köhler in: Köhler/Bornkamm, UWG 34. Auflage 2016, § 7 UWG Rn. 205.*

148 *KG, Beschluss vom 18.3.2011, 5 W 59/11; Köhler in: Köhler/Bornkamm, UWG 34. Auflage 2016, § 7 UWG Rn. 205. Fezer, UWG Lauterkeitsrecht, §§ 5-22, Kommentar, Band 2, München 2005, nimmt auf die Abgrenzungsprobleme und auf das Markenrecht und Kartellrecht als mögliche Auslegungshilfen Bezug (Rn. 136): Aus Sicht des Verbrauchers reichten Äquivalenz und Austauschbarkeit. Wenn also Preissteigerungen bei einem der Produkte zu einer Ausweichbewegung hin zu einem anderen Produkt führe und die Nachfrage bei dem zweiten Produkt steige.*

149 *Siehe Artikel 2h) Richtlinie 2002/58/EG, die ganz allgemein regelt: „elektronische Post" jede über ein öffentliches Kommunikationsnetz verschickte Text-, Sprach-, Ton- oder Bildnachricht, die im Netz oder im Endgerät des Empfängers gespeichert werden kann, bis sie von diesem abgerufen wird.*

150 *Ohly in: Ohly/Sosnitza, Gesetz gegen den unlauteren Wettbewerb, 6. Auflage 2014, § 7 UWG Rn. 73, verweist darauf, dass ein Vertrag tatsächlich zustande gekommen sein muss (Kaufvertrag, Werkvertrag, Reisevertrag, Vertrag über Finanzdienstleistungen) und dass eine konkrete Vertragsanbahnung noch nicht ausreichend ist. Schöler in: Harte-Bavendamm/Henning-Bodewig, UWG, 3. Auflage 2013, § 7 UWG Rn. 351 bezieht sich auf den tatsächlichen „Verkauf" einer Ware oder Dienstleistung, und das bloße Verkaufsgespräche nicht genügen sollen. Fezer, UWG Lauterkeitsrecht. §§ 5-22, Kommentar, Band 2, München 2005 verweist darauf, dass ein vorangegangenes Umsatzgeschäft vorliegen muss (Rn. 122). Unter Rn. 131 nimmt er außerdem auf die unklare Formulierung Bezug, da es den Verkauf von Dienstleistungen nicht gebe und dies in anderen Sprachfassungen leider nicht so deutlich sei. Es sei „mit dem Erbringen einer Dienstleistung" zu lesen.*

151 *Siehe oben S. 34 ff.*

Grundsätzlich wäre gemäß § 7 Absatz 3 UWG denkbar, dass der Vertragspartner ohne Einwilligung Werbung, also Informationen, die nicht für vertragliche Zwecke erforderlich sind, an seinen Kunden versenden dürfte (bei LETsmart ist etwa zunächst ein laufendes Vertragsverhältnis bei Verwendung eines Einwilligungsassistenten angedacht). Im Bundesdatenschutzgesetz gilt bislang für solche Zwecke grundsätzlich ein Einwilligungserfordernis, da das Listendatenprivileg des § 28 Absatz 3 BDSG nicht greift. Erwägungsgrund 47 Datenschutz-Grundverordnung regelt ohne nähere Erläuterung, dass die Verarbeitung personenbezogener Daten zum Zwecke der Direktwerbung als eine einem berechtigten Interesse dienende Verarbeitung betrachtet werden kann. Daher empfehlen sich auch hier entsprechende europaweit einheitliche Verhaltensregeln zur Auslegung dieses Erwägungsgrunds - soweit diese aufgrund einer Verarbeitungstätigkeit in mehreren Mitgliedstaaten ausgearbeitet werden können - oder aber Leitlinien. Datenschutzrechtlich ist außerdem erforderlich, die betroffene Person transparent über die geplante Datenverarbeitung zu informieren und ein Widerspruchsrecht einzuräumen (letzteres verlangt auch das UWG). Der Einwilligungsassistent müsste daher wiederum zwischen Einwilligungserfordernis und („nur“) transparenter Information unterscheiden können.

Hat der Nutzer umgekehrt Interesse an Werbung bzw. fordert diese Informationen ein, könnte eine Wissensplattform wie CoMaFeDS unterstützend eingesetzt werden. Der Plattform ist bekannt, wo welche Datensätze zu finden sind und sie speichert diese Information in verschlüsselter Form. Wie mehrfach erwähnt liegen allerdings noch keine veröffentlichten Details über konkrete Einsatzzwecke und technische Funktionsweise vor. Daher werden im Folgenden anhand eines fiktiven Beispiels mögliche Anforderungen beschrieben:

Plant der Nutzer einen Einkaufsbummel und ist an Angeboten für Kosmetikartikel interessiert, muss beachtet werden, dass gemäß der oben dargestellten Empfehlungen der Artikel-29-Datenschutzgruppe eine pauschale Einwilligung unzulässig ist und die Informiertheit für den bestimmten Fall sichergestellt sein muss. Grundsätzlich müsste in einem Einwilligungsprozess folgendes berücksichtigt werden:

- Der Nutzer gibt an, dass er an Kosmetikangeboten von sämtlichen Geschäften in der Umgebung seines aktuellen Standortes während seines Einkaufbummels interessiert ist. Die Plattform speichert diese Information in verschlüsselter Form. Ein potenzieller Empfänger fragt an, ob für ihn relevante Datensätze vorhanden sind, ohne dass (wie von auch CoMaFeDS geplant) bereits konkrete Daten übermittelt werden. Es erfolgt lediglich eine Beschreibung der Datenstruktur. Datenschutzrechtlich muss sichergestellt sein, dass CoMaFeDS die „Anonymität“ der Nutzer im Hinblick auf die potenziellen Empfänger tatsächlich umsetzen kann. (Nach Offenlegung der technischen Details wäre diese Anforderung zu überprüfen, insbesondere unter Ausschluss von eventuellen Verknüpfungsmöglichkeiten).

- Der Einwilligungsassistent müsste daraufhin in der Lage sein, eine entsprechende granulare Liste mit Auswahlmöglichkeiten von Geschäften (Empfängern) und Kosmetikartikeln automatisiert zum Zwecke der Werbung zu erstellen. Der Nutzer muss die Möglichkeit haben, die einzelnen generierten Felder aktiv anzuklicken. Die Einwilligung und die Verwendung der Standortdaten muss auf die Dauer des Einkaufs begrenzt sein. Es müsste daher ein dynamischer Einwilligungsprozess erfolgen (wie von CoMaFeDS geplant).[152]

152 Die Rechtmäßigkeitsvoraussetzungen sind gesondert zu prüfen.

Der „Kontext“ einer Einwilligung gewinnt somit an Bedeutung, da das Fortschreiten der Technik mehr Möglichkeiten bietet, Daten zu verarbeiten und zu verknüpfen, so dass hier vernünftige Grenzen gefunden werden müssen.

Für Informationen, die als Werbung einzustufen sind wäre im Übrigen in dem oben genannten Beispiel bei Verwendung eines „Wissensgraphen“ (CoMaFeDS) und dynamischer Einwilligung und unter Bezug zum Wettbewerbsrecht zu berücksichtigen, dass bei Erhalt der Daten des Nutzers der Empfänger (Anbieter von Kosmetikartikel) im Sinne von § 7 Absatz 3 UWG noch kein Unternehmer ist, der im Zusammenhang mit dem Verkauf einer Ware oder Dienstleistung von dem Kunden dessen elektronische Postadresse erhalten hat, so dass er diese gerade nicht zur Direktwerbung für eigene ähnliche Waren oder Dienstleistungen verwenden darf. Er muss sich vielmehr an die granularen Vorgaben des Nutzers halten, die dieser aktiv bei Verwendung des Einwilligungsassistenten vorgegeben hat.[153]

! Fazit Nr. 7

Insgesamt kann lediglich eine allgemeinere Betrachtung für den Einwilligungsassistenten erfolgen, da dessen Verwendung, Einsatzzwecke und Betreiben sich bislang in den Anfangsüberlegungen der Entwickler befinden. Diesbezüglich wird ebenso auf die Abschnitte „Zukünftige Fragestellungen“[154] und „Verantwortung“[155] verwiesen.

Festzuhalten ist aber:
Nur wenn Nutzer für den bestimmten Einzelfall eine Vorauswahl der Einwilligungselemente granular aktivieren konnten, kann der Einwilligungsassistent diese Entscheidung überhaupt automatisiert übernehmen. Hier kann es hilfreich sein, wenn sich die Entwickler an der Umsetzung des Projekts „Platform for Privacy Preferences“ (P3P) orientieren, das in der Bestandsaufnahme dargestellt wurde. Damit könnte die Direkterhebung von Daten weiterhin forciert werden, auch wenn diese als Grundsatz in der Datenschutz-Grundverordnung nicht mehr verankert ist.

Bei Unterstützung durch einen Einwilligungsassistenten müssen die unterschiedlichen Rechtsgrundlagen einer Datenverarbeitung (z. B. Erforderlichkeit für vertragliche Zwecke oder berechtigte Interessen) berücksichtigt werden, so dass stets geprüft werden muss, ob eine Einwilligung als Rechtsgrundlage überhaupt in Betracht kommt. Es ist daher zwischen Einwilligungserfordernis und „nur“ transparenter Information über die Datenverarbeitung zu unterscheiden.

Der Einwilligungsassistent kann aufgrund der Möglichkeit der Bereitstellung granularer Komponenten zur Transparenz der Einwilligung beitragen, so dass seine technische Entwicklung dahingehend erfolgen sollte, die Granularität und Transparenz sicherzustellen und nicht diese umzukehren, in dem Verarbeitungsvorgänge oder Zwecke in einem weiten Verständnis ausgelegt werden.

153 *Je nachdem, welche Funktionen geplant sind, könnte zudem die folgenden wettbewerbsrechtlichen Aspekte zu berücksichtigen sein: Das Kammergericht Berlin ist noch von einer möglichen Zulässigkeit der Versendung einer Freundesliste sowie der Versendung von Einladungs-E-Mails ausgegangen mit der Begründung, dass dies dem privaten Nutzer zuzurechnen sei (KG Berlin Urteil vom 24.01.2014, Az.: 5 U 42/12). Der Bundesgerichtshof hat jedoch entschieden, dass die mithilfe der Funktion „Freunde finden“ des Internet-Dienstes „Facebook“ versendeten Einladungs-E-Mails an Personen, die nicht als „Facebook“-Mitglieder registriert sind, eine wettbewerbsrechtlich unzulässige belästigende Werbung darstellen (BGH Urteil vom 14.01.2016, Az.: I ZR 65/14). Überträgt man dies auf den oben genannten Fall, wäre eine Funktion, die Kneipen- oder Restaurantempfehlungen, Einkaufstipps, etc. für „Freunde“ bereitstellt, ebenso kritisch zu beleuchten.*

154 *Siehe S. 56 ff.*

155 *Siehe hierzu auch den Punkt „Verantwortung“ auf S. 52 ff.*

!

In Anlehnung an die Ausführungen der Artikel-29-Datenschutzgruppe muss der Nutzer selbst aktiv werden. Vorstellbar wäre beispielsweise im Hinblick auf Standortdaten ein Tätigwerden unmittelbar vor oder während einer Reise durch aktive Auswahl von Präferenzen, begrenzt auf die Dauer der Reise, für bestimmte Zwecke (z. B. Restaurantempfehlungen oder Wetterinformationen) und für den konkreten Ort. Es ist nicht möglich, eine automatische Standortbestimmung vorzunehmen, wenn der Nutzer zuvor nicht für diesen bestimmten Fall informiert eingewilligt hat. Wichtig wäre bei der Granularität ebenso die Berücksichtigung der Ortungsmöglichkeiten. Eine genaue Standortbestimmung ist nicht immer erforderlich. Unternimmt der Nutzer aber eine Städtereise, möchte er abends bei Ankunft im Hotel gegebenenfalls die Restaurants in unmittelbarer Nähe angezeigt erhalten. Diesen Detaillierungsgrad sollte ein Einwilligungsassistent berücksichtigen.

Konzepte wie CoMaFeDS könnten bei Forschungszwecken unterstützend eingesetzt werden. Gemäß Erwägungsgrund 33 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.

Was unter „einer“ Verarbeitungstätigkeit oder dem „Kontext“ einer Einwilligung innerhalb einer komplexen Datenverarbeitung sinnvollerweise verstanden werden kann, muss bei Verwendung eines Einwilligungsassistenten der Einzelfallbetrachtung obliegen. Hier muss kritisch geprüft werden, inwieweit die Erstellung einer automatisierten Einwilligungserklärung anhand der Datenschutzhinweise systemseitig in Betracht kommen kann. Die Einwilligung „in einem Kontext“ und die Zweckänderung nach Artikel 6 Absatz 4 Datenschutz-Grundverordnung benötigen klare Grenzen.

In Bezug auf Werbung ist dabei folgendes zu berücksichtigen: Das Bundesdatenschutzgesetz und das Gesetz gegen den unlauteren Wettbewerb (UWG) stehen aktuell gleichberechtigt nebeneinander. § 7 Absatz 3 UWG bietet allerdings bei elektronischer Werbung insoweit eine Erleichterung, dass ein Unternehmer, der im Zusammenhang mit dem Verkauf einer Ware oder Dienstleistung von dem Kunden dessen elektronische Postadresse erhalten hat, diese zur Direktwerbung für eigene ähnliche Waren oder Dienstleistungen verwenden darf. Die Frage ist, welche Auswirkung dies auf die datenschutzgerechte Gestaltung eines Einwilligungsassistenten und die Übersendung von ähnlichen Dienstleistungsangeboten haben könnte. Datenschutzrechtlich muss die betroffene Person die geänderte Verarbeitungstätigkeit oder den Zweck vernünftigerweise erwarten dürfen. Fraglich ist jedoch, ob dies in einem europaweiten Vergleich stets gleichbedeutend mit „ähnlicher“ Zweck zu verstehen ist. Hier kommt es ebenso darauf an, ob das Markenrecht oder das Kartellrecht als Auslegungshilfen heranzuziehen sind. Im Übrigen empfiehlt sich hier eine europaweite Gesamtschau und entsprechende Harmonisierung im Falle eines unterschiedlichen Verständnisses in Europa. Rechtsunsicherheiten, die sich durch „berechtigte Interessen“ zur Direktwerbung ergeben, lassen sich ebenso durch einheitliche Verhaltensregeln beheben. Eine pauschale Einwilligung ist unwirksam. Entwickler von Konzepten wie CoMaFeDS könnten jedoch die Möglichkeit einer „pauschalen Interessensbekundung“ prüfen. Wird wie hier eine Wissensplattform zentral erstellt, wäre auch denkbar, dass der Nutzer ein Interesse kundtut (etwa: „Ich möchte Informationen über günstige Kosmetikangebote während meines Einkaufs“ oder „Ich nehme an jedem Gewinnspiel teil, bei dem ich einen Fernseher gewinnen kann“). Die Einwilligung, die in Bezug auf einen konkreten Anbieter und ein konkretes Angebot erteilt wird, muss jedoch stets „für den bestimmten Fall in informierter Weise“ erfolgen. Der „Wissensgraph“ müsste daher eine dynamische Einwilligungsmöglichkeit bieten und beim Nutzer eine automatisierte Rückfrage stellen (können), ob dieser mit der konkreten Datenverarbeitung einverstanden ist. Der Nutzer muss auf der Grundlage der Datenschutzbestimmungen des einzelnen Anbieters eine freie und informierte Entscheidung treffen können.

! Bei einer solchen zentralen Datenspeicherung mit Zugriffsmöglichkeiten von unterschiedlichen Empfängern ist vor allem an die Sicherheit des „Wissensgraphen“ (CoMaFeDS) und ausreichende Verschlüsselung zu denken. Außerdem ist die Frage entscheidend, wer Verantwortlicher dieses „Wissensgraphen“ und ob sowie in welcher Form diesbezüglich eine zusätzliche Einwilligung des Nutzers vorliegen muss. Es empfiehlt sich außerdem eine Zertifizierung, da ein Nutzer die technischen Voraussetzungen, technische Sicherheit und die Vorgehensweise einer Datenverarbeitung nicht überblicken kann.[156] 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, seine Anonymität gegenüber potenziellen Empfängern gewahrt ist und keine Verknüpfungsmöglichkeiten bestehen, insbesondere da diese Plattform großes Potenzial für Big Data-Anwendungen bietet. Ob die erforderliche Sicherheit der Datenverarbeitung umsetzbar ist, muss einer gesonderten technischen Bewertung unterliegen (in dieser Stellungnahme werden lediglich rechtliche Anforderungen geprüft).

III. Freiwilligkeit und Kopplungsverbot

1. Voraussetzungen

Gemäß Artikel 4 Nr. 11 Datenschutz-Grundverordnung muss es sich bei einer Einwilligung um eine freiwillige Willensbekundung handeln. Artikel 7 Absatz 4 Datenschutz-Grundverordnung konkretisiert dies dadurch, dass „bei der Beurteilung, ob die Einwilligung freiwillig erteilt wurde, dem Umstand in größtmöglichem Umfang Rechnung getragen werden muss, ob unter anderem die Erfüllung eines Vertrags, einschließlich der Erbringung einer Dienstleistung, von der Einwilligung zu einer Verarbeitung von personenbezogenen Daten abhängig ist, die für die Erfüllung des Vertrags nicht erforderlich sind.“

Im Vergleich dazu muss im Sinne von Artikel 2h der Richtlinie 95/46/EG eine Willensbekundung ohne Zwang erfolgt sein. Hierzu wird vertreten, dass die Freiwilligkeit nicht mehr gegeben ist, wenn die betroffene Person die Willensbekundung in sozialer oder wirtschaftlicher Schwäche oder Unterordnung erteilt hat oder wenn sie einen Verstoß gegen zwingende Schutznormen darstellen würde.[157] Auch im Arbeitsverhältnis wird die Freiwilligkeit der Einwilligung kritisch gesehen.[158]

156 *Siehe jedoch unter E. Verantwortlichkeit (S. 50 ff.), dass auch bei dezentraler Speicherung beim Nutzer eine Zertifizierung des Systems von außerordentlicher Wichtigkeit sein kann.*

157 *Brühann: in Grabitz/Hilf, Das Recht der Europäischen Union, 40. Auflage, 2009, Loseblattsammlung, Stand: Mai 1999 Ergänzungslieferung 13, A30, Art. 2 Rn. 28.*

158 *Artikel-29-Datenschutzgruppe, Stellungnahme 8/2001 zur Verarbeitung personenbezogener Daten von Beschäftigten, 10. Siehe auch Däubler, Gläserne Belegschaften?, 5. Aufl. Frankfurt 2010, Rn. 150 ff., der unter Rn. 160 ausführt, dass die Freiwilligkeit nur gewahrt ist, wenn die Willensbildung des Betroffenen nicht in unangemessener Weise beeinflusst wurde („Überrumpelung“, zielgerichtete Beratung) und wenn keine vermeidbaren Nachteile oder übermäßigen Vorteile in Aussicht gestellt wurden. Außerdem: Gola, Die Einwilligung als Legitimation für die Verarbeitung von Arbeitnehmerdaten, RDV 2002, S. 109 ff.*

Im Verlaufe der Verhandlungen zur Datenschutz-Grundverordnung konnte sich die Benennung eines „Ungleichgewichts“ im unmittelbaren Verordnungstext nicht durchsetzen. Vielmehr wurde lediglich im Erwägungsgrund 43 formuliert, dass die Einwilligung in besonderen Fällen keine gültige Rechtsgrundlage liefern sollte, nämlich wenn zwischen der betroffenen Person und dem Verantwortlichen ein klares Ungleichgewicht besteht (insbesondere wenn es sich bei dem Verantwortlichen um eine Behörde handelt) und es deshalb in Anbetracht aller Umstände in dem speziellen Fall unwahrscheinlich ist, dass die Einwilligung freiwillig gegeben wurde. Allerdings wurde der Vorschlag nicht übernommen, die Marktmacht als einen Fall des Ungleichgewichts klar zu benennen[159].

Zum Kopplungsverbot etwa Gola/Schomerus, Bundesdatenschutzgesetz, 11. Auflage 2012, § 28 Rn. 46; Taeger in: Taeger/Gabel, Kommentar zum BDSG (2010), § 28 Rn. 180 ff.

Im deutschen Recht ist die Regelung in § 28 Absatz 3b BDSG zum Kopplungsverbot auf die Fälle der Einwilligung im Bereich Werbung und Adresshandel beschränkt. Außerdem ist diese Regelung sehr weit gefasst: Das Kopplungsverbot soll nur gelten, wenn dem Betroffenen ein anderer Zugang zu gleichwertigen vertraglichen Leistungen ohne die Einwilligung nicht oder nicht in zumutbarer Weise möglich ist. Dies bedeutet, dass die „Freiwilligkeit“ überall dort weiterhin bestehen würde, wo die betroffenen Personen entsprechende Leistungen bei anderen Unternehmen in Anspruch nehmen können. Letztendlich muss das Unternehmen nach überwiegender Meinung also eine Monopolstellung innehaben.[160] Im Sinne dieser Auslegung kann das Kopplungsverbot bei international vorhandenen Dienstleistungen kaum praktische Anwendung finden, da es unwahrscheinlich ist, kein als gleichwertig zu betrachtendes Angebote zu finden.

Der Bundesrat hatte aus diesem Grunde in der Vergangenheit vorgeschlagen,[161] dass die verantwortliche Stelle den Abschluss eines Vertrags nicht von einer Einwilligung des Betroffenen nach Absatz 3 Satz 1 abhängig machen dürfe. Eine solche Einwilligung sei unwirksam. Dies bedeutet, dass die betroffene Person den Dienst dennoch in Anspruch nehmen könnte, was ihr Recht auf informationelle Selbstbestimmung insgesamt stärken würde. Ein solches allgemeines Kopplungsverbot ist nunmehr auch in Artikel 7 Absatz 4 der Datenschutz-Grundverordnung enthalten, jedoch unter der Einschränkung, dass hier keine eindeutige Formulierung wie im Entwurf des Bundesrats vorgesehen ist, sondern lediglich ein Maßstab zur Beurteilung der Freiwilligkeit. Im Erwägungsgrund 43 wird näher präzisiert, dass die Einwilligung nicht als freiwillig erteilt gilt, wenn zu verschiedenen Verarbeitungsvorgängen von personenbezogenen Daten nicht gesondert eine Einwilligung erteilt werden kann, obwohl dies im Einzelfall angebracht ist, oder wenn die Erfüllung eines Vertrags, einschließlich der Erbringung einer Dienstleistung, von der Einwilligung abhängig ist, obwohl diese Einwilligung für die Erfüllung nicht erforderlich ist.

159 *Siehe Änderungsantrag 20 zu Erwägungsgrund 34 im Berichtsentwurf 2012/0011 (COD) vom 16.01.2013; Entwurf eines Berichts über den Vorschlag für eine Verordnung des Europäischen Parlaments und des Rates zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr (Datenschutz-Grundverordnung)*

160 *Zum Kopplungsverbot etwa Gola/Schomerus, Bundesdatenschutzgesetz, 11. Auflage 2012, § 28 Rn. 46; Taeger in: Taeger/Gabel, Kommentar zum BDSG (2010), § 28 Rn. 180 ff.*

161 *Bundesrat-Drucksache 55/1/15 vom 16.03.2015 „Entwurf eines Gesetzes zur Verbesserung der zivilrechtlichen Durchsetzung von verbraucherschützenden Vorschriften des Datenschutzrechts“; http://www.bundesrat.de/SharedDocs/drucksachen/2015/0001-0100/55-1-15.pdf?__blob=publicationFile&v=4. Siehe zum Kopplungsverbot auch die Ausführungen von Jan Albrecht unter https://www.janalbrecht.eu/fileadmin/material/Dokumente/Datenschutzreform_Stand_der_Dinge_10_Punkte_070115.pdf“Das Parlament hat ausdrücklich ein Kopplungsverbot vorgesehen, um zu verhindern, dass Dienste nur mit überschießenden Datensammlungen genutzt werden können.“*

2. Relevanz für den Einwilligungsassistenten

Der Einwilligungsassistent muss so gestaltet sein, dass die betroffene Person frei zwischen unterschiedlichen Daten, Zwecken und Empfängern wählen kann. In diesem Sinne kann der Einsatz eines solchen Assistenten eine Unterstützung für die betroffene Person darstellen, da dieser in übersichtlicher Weise die Datenverarbeitung auflistet und die betroffene Person sich zwischen den Verarbeitungstatbeständen frei entscheiden kann.

Bei Nichteinwilligung in einzelne Verarbeitungstatbestände dürfen ihr insbesondere ohne finanziellen Druck keine Nachteile entstehen. Die Einwilligung darf in diesem Zusammenhang nicht irreführend sein. Die Artikel-29-Datenschutzgruppe verweist etwa darauf, dass eine Einwilligung des Betreffenden nicht eingeholt werden darf, um die Verarbeitung zu legitimieren, wenn eine medizinische Fachkraft aus medizinisch indizierten Gründen in einer bestimmten Situation nicht anders kann als personenbezogene Daten in einer elektronischen Patientenakte zu verarbeiten. Eine Einwilligung sollte auf die Fälle beschränkt werden, in denen die betreffende Person tatsächlich frei entscheiden kann und anschließend die Einwilligung ohne irgendwelche Nachteile zurückziehen kann.[162]

Es sollte zudem keine Datenverarbeitung legitimiert werden, die bereits durch andere Rechtsgrundlagen abgedeckt ist.[163] In diesem Sinne würde es ebenso an der Freiwilligkeit fehlen. Dieser Umstand könnte nur „geheilt“ werden, wenn deutlich wird, dass sich der Datenverarbeiter bei einem etwaigen Widerruf der Einwilligung nicht zusätzlich auf diese Rechtsgrundlage beruft, um die Datenverarbeitung trotzdem weiter zu verfolgen. Ein solches Verhalten wäre aus datenschutzrechtlicher Sicht unzulässig.

Der Düsseldorfer Kreis hat bereits für Apps entschieden,[164] dass der Nutzer die Einwilligung jederzeit mit Wirkung für die Zukunft widerrufen können muss. Es handele sich nicht um eine wirksame Einwilligung, wenn der Nutzer entweder den Dienst „so nehmen müsse, wie er ist“ oder den Dienst nicht in Anspruch nehmen kann und ein Widerruf der „Einwilligung“ nur durch Beendigung des Nutzungsvertrags möglich ist.[165]

Für den Einwilligungsassistenten bedeutet dies, dass bereits bei der Entwicklung zu prüfen ist, inwieweit die Erbringung einer Dienstleistung von einer Einwilligung abhängig gemacht wird, obwohl diese Einwilligung für die Erfüllung nicht erforderlich ist (was auch dem Grundsatz „Datenschutz durch Technikgestaltung“ gemäß Artikel 25 Datenschutz-Grundverordnung entspricht).

Sofern der Nutzer wie bei einer App als Gegenleistung mit seinen Daten bezahlen soll, wäre fraglich, ob diese Daten für die Durchführung der Dienstleistung erforderlich sind.

162 *Artikel-29-Datenschutzgruppe, WP 131, Arbeitspapier Verarbeitung von Patientendaten in elektronischen Patientenakten (EPA), angenommen am 15. Februar 2007; S. 9.*

163 *Siehe Artikel 29-Datenschutz-Gruppe Fn. 122.*

164 *Düsseldorfer Kreis, S. 17 -Orientierungshilfe- Datenschutzanforderungen an App-Entwickler und App-Anbieter vom 16.06.2014: Eine App dürfe zudem nur die erforderlichen Berechtigungen vom Nutzer anfordern und es wird in diesem Zusammenhang dargestellt, dass einige Betriebssysteme Berechtigungen lediglich in festen Kombinationen anbieten, welche neben den erforderlichen auch nicht benötigte Datenzugriffe enthielten, so dass dies bei der Entwicklung zu berücksichtigen sei. Als Beispiel nennt der Düsseldorfer Kreis Android, welches bis zur Version 4.0 den Zugriff auf das Kontaktverzeichnis nicht zugelassen habe, ohne zugleich Zugriffsrechte auf den Anrufverlauf zu bekommen. Insgesamt sei ein Zugriff auf das gesamte Adressbuch des Geräts mit all den darin hinterlegten persönlichen Informationen des Nutzers und seiner Kontakte und deren Verwendung nicht zulässig, wenn lediglich z. B. eine Adresse für die Navigation mit einer App benötigt werde (siehe S. 17)*

165 *Düsseldorfer Kreis, S. 15 Fn. 26 - Orientierungshilfe- Datenschutzanforderungen an App-Entwickler und App-Anbieter vom 16.06.2014.*

Wie oben ausgeführt, hat der Düsseldorfer Kreis die Empfehlung gegeben, dass keine wirksame Einwilligung vorliegen soll, wenn eine wirksame Nutzung nur unter Beendigung des Nutzungsvertrages möglich ist.[166] Der Bundesrat hat in seinem Gesetzesentwurf zum Kopplungsverbot im Bundesdatenschutzgesetz zudem darauf hingewiesen, dass besondere Gefahren erheblicher Verletzungen des Persönlichkeitsrechts unterbunden werden, indem Unternehmen wirksam untersagt wird, Angebote von dem Einverständnis der Kunden in die Datennutzung abhängig zu machen oder auf einen anderen Erlaubnistatbestand zurückzugreifen. Dies gelte umso mehr, als dem Kunden oftmals nicht klar sein wird, welche der Angaben zu seiner Person und zu seinen persönlichen Verhältnissen zu Werbe-, Marketing-, Score- oder anderen erlaubten Zwecken verwendet wird. Wichtig sei, dass der Einwilligende in Kenntnis aller Umstände frei bestimmt, wenn er sich mit der Erhebung und Verwertung seiner persönlichen Daten einverstanden erklärt, also er selbstbestimmt entscheidet, ob er für das Angebot mit Daten oder Euro bezahlen will. Insoweit wird es für erforderlich gehalten, dass die Einwilligung in Datennutzungsrechte nicht mit Vorteilen, die Dritte einräumen, gekoppelt werden dürfe.[167]

Auch wenn dieses Gesetz nicht in Kraft getreten ist, können diese Ausführungen als Auslegungshilfe „für die Wahrung des Persönlichkeitsrechts“ dienen und sollten ebenso für Artikel 7 Absatz 4 Datenschutz-Grundverordnung herangezogen werden. In Bezug auf diesen Punkt könnten die deutschen Datenschutzaufsichtsbehörden bereits zum jetzigen Zeitpunkt Anforderungen festlegen und ihre Auffassung zur Auslegung kundtun, wobei zukünftig europaweit eine Verhaltensregel (soweit diese aufgrund einer Verarbeitungstätigkeit in mehreren Mitgliedstaaten ausgearbeitet werden kann) oder eine Leitlinie durch den Europäischen Datenschutzausschuss erstellt werden sollte, um ein einheitliches Schutzniveau sicherzustellen.

Für den Einwilligungsassistenten bedeutet dies, dass die Freiwilligkeit im Besonderen bei der Gestaltung des Systems zu berücksichtigen ist und bei kostenlosen Diensten, bei denen im Gegenzug Daten bereit gestellt werden sollen, besondere Vorsicht geboten ist. Diese werbefinanzierten Dienste kommen auch bei Smart-TV-Angeboten in Betracht.[168]

Sofern für die unterschiedlichen Zwecke eine Einwilligung eingeholt wird, muss darüber hinaus im besonderen Maße geprüft werden, ob es für die betroffene Person irreführend ist, sich darüber hinaus auf berechtigte Interessen gemäß Artikel 6 f Datenschutz-Grundverordnung zu stützen. Auch bezüglich der berechtigten Interessen obliegen dem Verantwortlichen Informationspflichten nach Artikel 13 Absatz 1 d Datenschutz-Grundverordnung, und zwar bei Erhebung der persönlichen Daten (wenn die Verarbeitung auf Artikel 6 Absatz 1 Buchstabe f beruht, die berechtigten Interessen, die von dem Verantwortlichen oder einem Dritten verfolgt werden).

166 *Düsseldorfer Kreis, S. 15 Fn. 26 - Orientierungshilfe- Datenschutzanforderungen an App-Entwickler und App-Anbieter vom 16.06.2014.*

167 *Bundesrat-Drucksache 55/1/15 vom 16.03.2015 „Entwurf eines Gesetzes zur Verbesserung der zivilrechtlichen Durchsetzung von verbraucherschützenden Vorschriften des Datenschutzrechts“; http://www.bundesrat.de/SharedDocs/drucksachen/2015/0001-0100/55-1-15.pdf?__blob=publicationFile&v=4*

168 *Siehe Düsseldorfer Kreis, S. 15 - Orientierungshilfe zu den Datenschutzanforderungen an Smart-TV-Dienste vom 15./16.09. 2015. https://www.datenschutz-hamburg.de/news/detail/article/orientierungshilfe-datenschutzanforderungen-an-smart-tv-dienste.html?tx_ttnews%5BbackPid%5D=203&cHash=ff2c5449bc0eba90ba131dbe32a19db1*

Daher ist der Verantwortliche angehalten, dies klar zu trennen:

- Es geht einerseits um die Verarbeitung, die auf der Einwilligung gemäß Artikel 6 Absatz 1 a Datenschutz-Grundverordnung beruht. Diese muss gemäß Artikel 4 Nr. 11, Artikel 7 und Artikel 13 Absatz 2 c Datenschutz-Grundverordnung in informierter Weise erfolgen (wenn die Verarbeitung auf Artikel 6 Absatz 1 Buchstabe a beruht, das Bestehen eines Rechts, die Einwilligung jederzeit zu widerrufen, ohne dass die Rechtmäßigkeit der aufgrund der Einwilligung bis zum Widerruf erfolgten Verarbeitung berührt wird).

- Plant der Verantwortliche die Datenverarbeitung darüber hinaus auf berechtigte Interessen gemäß Artikel 6 Absatz 1 f Datenschutz-Grundverordnung zu stützen, muss insbesondere beim Einholen einer Einwilligung darauf geachtet werden, dass nicht der Eindruck erweckt wird, dass die Datenverarbeitung sei durch die Einwilligung abschließend abgedeckt. Es muss vielmehr eine transparente Information erfolgen, welche Datenverarbeitung stattfinden soll und auf welcher Rechtsgrundlage diese erfolgt.

Insgesamt muss die Datenverarbeitung fair und nachvollziehbar bleiben (Artikel 5 Absatz 1 a Datenschutz-Grundverordnung).

! Fazit Nr. 8

Die betroffene Person muss darüber informiert werden, ob sie gesetzlich oder vertraglich verpflichtet ist, ihre personenbezogenen Daten preiszugeben oder ob die Bereitstellung für einen Vertragsschluss erforderlich ist. Darüber hinaus ist sie darüber in Kenntnis zu setzen, was die möglichen Folgen einer verweigerten Bereitstellung sind.

Ist die Rechtsgrundlage der Datenverarbeitung die Einwilligung, kann der Einwilligungsassistent durch Zusammenstellung und Auflistung klar beschriebener Zwecke, Empfänger und der verwendeten Daten zur Informiertheit und damit Transparenz bei der Einwilligung beitragen.

Es darf dennoch bei Verwendung eines Einwilligungsassistenten nicht der Eindruck entstehen, dass damit die Datenverarbeitung abschließend abgedeckt ist, wenn beispielsweise darüber hinaus eine Verarbeitung aufgrund berechtigter Interessen geplant ist. In diesem Falle muss besonders auf die Nachvollziehbarkeit für den Betroffenen geachtet werden und Einwilligung und Information über Datenverarbeitung aufgrund anderer Rechtsgrundlagen klar getrennt werden.

Bei der Auslegung des Kopplungsverbots ist im besonderen Maße auf die freie Bestimmung durch die betroffene Person zu achten. Es müssen die Gesamtumstände berücksichtigt werden, ob sie tatsächlich vollständig überblicken kann, für welche Marketing- und/oder Scoringzwecke ihre 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 den Betroffenen.

! Der Gesetzesvorschlag des Bundesrats hinsichtlich eines Kopplungsverbots beinhaltet Hinweise für mögliche Anforderungen zur Wahrung des Persönlichkeitsrechts. Die Ausführungen könnten daher bei der Auslegung von Artikel 7 Absatz 4 Datenschutz-Grundverordnung herangezogen werden. In Bezug auf diesen Punkt könnten die deutschen Datenschutzaufsichtsbehörden bereits zum jetzigen Zeitpunkt Anforderungen festlegen und ihre Auffassung kundtun, wobei zukünftig europaweit eine Verhaltensregel erstellt (soweit diese aufgrund einer Verarbeitungstätigkeit in mehreren Mitgliedstaaten ausgearbeitet werden kann) oder eine Leitlinie durch den Europäischen Datenschutzausschuss bereit gestellt werden sollte.

IV. Dauer der Einwilligung

1. Definition

In den Informationspflichten muss über die Dauer der Einwilligung transparent informiert werden (Artikel 13 Datenschutz-Grundverordnung). Insgesamt ist die Feststellung zu wiederholen, dass die Einwilligung vor Datenverarbeitung einzuholen ist, auch wenn dies weder in der Datenschutz-Grundverordnung noch in der Richtlinie 95/46/EG ausdrücklich fixiert wurde.[169] Damit ist eine Regelung ausgeschlossen, bei der sich eine Person erst gegen die Übermittlung aussprechen kann, nachdem sie bereits stattgefunden hat.[170] Daher darf das Widerspruchsrecht nicht mit der Einwilligung verwechselt werden.[171]

Die Artikel-29-Datenschutzgruppe verweist darauf, dass mit dem Verstreichen der Zeit möglicherweise Zweifel entstehen, ob die Einwilligung, die ursprünglich auf gültigen, ausreichenden Informationen beruhte, immer noch gültig ist, so dass die für die Datenverarbeitung Verantwortlichen den betroffenen Personen die Möglichkeit zur Überprüfung geben sollten.[172]

Hierzu könnten sie diese beispielsweise über ihre aktuelle Wahl informieren und ihnen die Möglichkeit anbieten, sie entweder zu bestätigen oder zu widerrufen, wobei der jeweilige Zeitraum vom Kontext und den Umständen des Falls abhänge.[173]

Die Entscheidungen von Landgerichten, die sich mit der Wirksamkeit von Werbeeinwilligungen befassen, verlangen vom Anbieter nach einer gewissen Zeit die Rückversicherung, dass die Ansprache per Email oder Telefonanruf weiterhin gewünscht ist.[174]

169 Artikel-29-Datenschutzgruppe, WP 187, Stellungnahme 15/2011 zur Definition von Einwilligung, angenommen am 13. Juli 2011, S.11 mit Verweis darauf, dass in deutschem Recht der Begriff „Einwilligung" verwendet werde, was im deutschen Zivilrecht als „vorherige Zustimmung" definiert werde. Siehe auch Überarbeitung von 2002/58/EG: „prior consent".

170 Artikel-29-Datenschutzgruppe, WP 114, Arbeitspapier der Artikel-29-Datenschutzgruppe über eine Gemeinsame Auslegung des Artikels 26 Absatz 1 der Richtlinie 95/46/EG vom 24. Oktober 1995, Arbeitspapier vom 25. November 2005, S. 12. Artikel-29-Datenschutzgruppe, WP 114, Arbeitspapier der Artikel-29-Datenschutzgruppe über eine Gemeinsame Auslegung des Artikels 26 Absatz 1 der Richtlinie 95/46/EG vom 24. Oktober 1995, Arbeitspapier vom 25. November 2005, S. 12.

171 Artikel-29-Datenschutzgruppe, WP 187, Stellungnahme 15/2011 zur Definition von Einwilligung, angenommen am 13. Juli 2011, S. 12.

172 Artikel-29-Datenschutzgruppe, WP 187, Stellungnahme 15/2011 zur Definition von Einwilligung, angenommen am 13. Juli 2011, S. 24: Aus einer Vielzahl von Gründen würden die Leute häufig ihre Meinung ändern, weil ihre ursprünglichen Entscheidungen schlecht waren oder aufgrund einer Änderung der Umstände, beispielsweise wenn ein Kind reifer wird.

173 Artikel-29-Datenschutzgruppe, WP 187, Stellungnahme 15/2011 zur Definition von Einwilligung, angenommen am 13. Juli 2011, S. 24.

174 Siehe LG München Urteil vom 08.04.2010, Az.: 17 HK O 138/10, 17 HKO 138/10 (zu § 7 Absatz 2 Nr. 3 UWG); LG Berlin Beschluss vom 02.07.2004, Az.: 15 O 653/03; LG Hamburg Urteil vom 17.02.2004, Az.: 312 O 645/02.

Wenn bei diesen gerichtlichen Entscheidungen im Werbekontext ein Zeitrahmen von 1,5 bis 2 Jahren angenommen wird, stellt sich in Bezug auf „andere“ Einwilligungen im Einzelfall die Frage, ob die Persönlichkeitsrechte der betroffenen Person stärker betroffen sein könnten als durch den Versand eines Newsletters oder Telefonanrufs, und daher die Überprüfung des Einverständnisses weitaus früher erfolgen muss.[175] In der Literatur wird die Befristung einer datenschutzrechtlichen Einwilligung auf zwei bis drei Jahre befürwortet.[176]

2. Relevanz für den Einwilligungsassistenten

Sofern die betroffene Personen durch entsprechende selbstständige und granulare Einstellungen ihre Einwilligung zu einer bestimmten Datenverarbeitung erteilt, muss sichergestellt sein, dass sie diese nach einer gewissen Zeit überprüfen können oder dass die Einwilligung nur einmalig gilt. Bei der Einwilligung in Verwendung von Standortdaten ist beispielsweise vorstellbar, dass diese für eine Restaurantsuche in einem bestimmten Ort nur einmalig verwendet wird. Ansonsten könnten die Entwickler prüfen, ob ein „technisches Warnsystem“ installiert werden kann, dass nach einem bestimmten Zeitablauf oder in regelmäßigen Abständen die Nutzer automatisiert über erteilte Einwilligungen informiert und die einfache Möglichkeit zur Korrektur bietet. Zu berücksichtigen ist jedoch, dass die Empfänger immer die Möglichkeit haben, Daten der Nutzer in ihr System zu kopieren bzw. zu übertragen, so dass insbesondere zu diesen Systemen eine Rückkopplung der Information erfolgen muss

! Fazit Nr. 9

Die Einwilligung ist auf die Dauer des jeweiligen konkreten Verwendungszwecks zu begrenzen. Konzepte wie LETsmart stellen die automatisierte Löschung nach Wegfall des Verwendungszwecks sicher. Die Empfänger müssen aber gleichermaßen den Widerruf oder die zeitlich befristete Einwilligung berücksichtigen, wenn sie die Daten der Nutzer in ihren eigenen Systemen erfasst haben.
Es sollte entwicklerseitig geprüft werden, ob automatisiert nach einer gewissen Zeitspanne oder regelmäßig eine Information der Nutzer über die erteilte Einwilligungen erfolgen kann, gekoppelt mit der Bereitstellung einer einfachen Widerrufsmöglichkeit.

E. Verantwortlichkeit

Eine besondere Problemstellung bei der Gestaltung eines Einwilligungsassistenten ergibt sich in Bezug auf Haftung und Verantwortlichkeit. Hier sind die technische Entwicklung und der geplante Einsatz zu berücksichtigen, da entschieden werden muss, ob es sich um „nur“ ein Software-Tool in Eigenverantwortung der betroffenen Person handelt und ob der Empfänger damit „nur“ für die im Anschluss folgende Datenverarbeitung nach den allgemeinen Grundsätzen und ohne besondere Verpflichtung für den Einwilligungsassistenten verantwortlich ist,[177] oder ob darüber hinaus eine Einordnung als eigenständiger Dienst, entweder im Sinne eines „Inhaltsdienstes“ gemäß der Richtlinie 2000/31/EG, „inhaltsneutral“ oder als Dienst mit Zusatznutzen in Betracht kommt.

175 *Dies gilt z. B. bei komplexen Datenverarbeitungen, wie sie auch in Zusammenhang mit Smart-TV oder Smart-Grid vorkommen könnten, wenn diese durch Einwilligung legitimiert sind und nicht durch „für zur Vertragserfüllung erforderliche Zwecke“.*

176 *Rogosch, Die Einwilligung im Datenschutzrecht, S. 148.*

177 *Siehe bereits hierzu S. 21.*

Die Frage ist, inwieweit zukünftig die Installation einer Software oder die technische Fortentwicklung des Einwilligungsassistenten als eigener Online-Dienst eingestuft werden kann, so dass der Empfänger der Daten zum Anbieter und damit ebenso zum Verantwortlichen für den Einwilligungsassistenten im Sinne eines Dienstanbieters wird. Möglich wäre ebenso ein zwischengeschalteter „weiterer Anbieter", etwa Anbieter von Telekommunikationsdiensten, der einen solchen Dienst zur Verfügung stellt. In Bezug auf den Empfänger der Daten wäre außerdem denkbar, dass die Verwendung des Einwilligungsassistenten als eine die Datenverarbeitung unterstützende Softwarelösung verstanden wird. In diesem Sinne wäre er zwar Verantwortlicher der ordnungsgemäßen Datenverarbeitung, aber nicht im Sinne eines (Online)Dienstanbieters.

I. Allgemein

Durch die Richtlinie 95/46/EG ist bislang eine generelle Meldepflicht bei den Aufsichtsbehörden vorgesehen, sofern personenbezogene Daten verarbeitet werden.[178]

Die Datenschutz-Grundverordnung geht nun insgesamt von einem risikobasierten Ansatz anstatt einer grundsätzlichen Meldepflicht aus, um zukünftig einen bürokratischen und finanziellen Aufwand zu verhindern. Gemäß Erwägungsgrund 89 der Datenschutz-Grundverordnung sollen die bestehenden unterschiedslosen Meldepflichten nunmehr durch wirksame Maßnahmen ersetzt werden, die sich mit denjenigen Verarbeitungsvorgängen befassen, die aufgrund

- ihrer Art
- ihres Umfangs
- ihrer Umstände
- ihrer Zwecke

wahrscheinlich ein hohes Risiko für die Rechte und Freiheiten natürlicher Personen mit sich bringen. Zu solchen Arten sollen insbesondere die Verarbeitungsvorgänge zählen, bei denen neue Technologien eingesetzt werden und die neuartig sind und bei denen der Verantwortliche noch keine Datenschutzfolgeabschätzung durchgeführt hat.

Dies bedeutet, dass ein Unternehmen zukünftig eine Risikobewertung vor Verarbeitungsvorgängen durchführen muss. Hierbei ist entscheidend, dass objektive Kriterien gefunden werden, die den Betroffenen in den Fokus der Bewertung stellen und anhand derer die Eintrittswahrscheinlichkeit und Schwere eines Risikos für dessen Rechte und Freiheiten ermittelt werden kann.

Wichtig ist hierbei, dass das Unternehmen gleichzeitig die Maßnahmen und Verfahren im Blick hat, mit denen dieses Risiko eingedämmt werden kann. Die Datenschutz-Grundverordnung nimmt etwa immer wieder Bezug auf die Pseudonymisierung als geeignete Garantie für die Betroffenenrechte.

178 *Bei der Umsetzung dieser Richtlinie in nationales Recht hat Deutschland gemäß § 4d Absatz 2 Bundesdatenschutzgesetz (BDSG) eine Ausnahme der Meldepflicht vorgesehen, wenn ein Beauftragter für den Datenschutz im Unternehmen bestellt ist. Aufgrund der unmittelbaren Geltung der Datenschutz-Grundverordnung in den Mitgliedstaaten der Europäischen Union entfällt damit auch die entsprechende Umsetzung der Richtlinie 95/46/EG in § 4d Absatz Bundesdatenschutzgesetz.*

Eine solche Pseudonymisierung kann nach der Datenschutz-Grundverordnung auch innerhalb der verantwortlichen Stelle (Unternehmen) stattfinden, wenn diese sicherstellt, dass die zusätzlichen Informationen, mit denen die personenbezogenen Daten einer betroffenen Person zugeordnet werden können, gesondert aufbewahrt werden.

Für das Unternehmen ist letztendlich entscheidend, dass die erforderliche Risikobewertung vor der Verarbeitung stattfindet, um zu Beginn der Verarbeitung nachweisen zu können, dass die durchgeführte Verarbeitung personenbezogener Daten rechtmäßig gemäß Artikel 5 Absatz 1a Datenschutz-Grundverordnung erfolgt. Eine solche Nachweispflicht bzw. Rechenschaftsverpflichtung ist in der Datenschutz-Grundverordnung in Artikel 5 Absatz 2 ausdrücklich benannt. An dieser Stelle werden zukünftig genehmigte Verhaltensregeln (Artikel 40 Datenschutz-Grundverordnung) und Zertifizierungen (Artikel 42 Datenschutz-Grundverordnung) eine wichtige Rolle einnehmen.

Die Risikobewertung vor Datenverarbeitung orientiert sich dabei an den Regelungen zur Datenschutz-Folgenabschätzung gemäß Artikel 35 und 36 Datenschutz-Grundverordnung. Die Aufsichtsbehörde muss von dem Unternehmen vor der geplanten Verarbeitung außerdem nur dann konsultiert werden, wenn eine Form der Verarbeitung, insbesondere die Verwendung neuer Technologien, aufgrund der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung voraussichtlich ein hohes Risiko für die Rechte und Freiheiten natürlicher Personen zur Folge hat.

Diese Risikobewertung liegt in der Hand des Unternehmens als Verantwortlichen.[179]

Gemäß Artikel 35 Absatz 7 Datenschutz-Grundverordnung muss eine Datenschutz-Folgenabschätzung zumindest Folgendes enthalten:

- Systematische Beschreibung der geplanten Verarbeitungsvorgänge und der Zwecke der Verarbeitung, gegebenenfalls einschließlich der von dem für die Verarbeitung Verantwortlichen verfolgten berechtigten Interessen.

- Bewertung der Notwendigkeit und Verhältnismäßigkeit der Verarbeitungsvorgänge in Bezug auf den Zweck.

- Bewertung der Risiken der Rechte und Freiheiten der betroffenen Personen.

179 *Gemäß der in Deutschland geltenden Regelungen ist bislang eine Vorabkontrolle gemäß § 4d Absatz 5 Bundesdatenschutzgesetz von dem betrieblichen Datenschutzbeauftragten durchzuführen, soweit besonders sensible Daten nach § 3 Absatz 9 Bundesdatenschutzgesetz betroffen sind oder die Datenverarbeitung dazu bestimmt ist, die Persönlichkeit des Betroffenen, einschließlich seiner Fähigkeiten, Leistungen oder seines Verhaltens zu bewerten. Zukünftig ist jedoch ein Datenschutzbeauftragter gemäß Artikel 37 Datenschutz-Grundverordnung nur noch in Ausnahmefällen zu bestellen. Artikel 37 regelt eine grundsätzliche Verpflichtung zur Bestellung eines Datenschutzbeauftragten für öffentliche Stellen, ansonsten nur, wenn*
- die Kerntätigkeit des Verantwortlichen oder des Auftragsverarbeiters in der Durchführung von Verarbeitungsvorgängen besteht, welche aufgrund ihrer Art, ihres Umfangs und/oder ihrer Zwecke eine umfangreiche regelmäßige und systematische Überwachung von betroffenen Personen erforderlich machen, oder
- die Kerntätigkeit des Verantwortlichen oder Auftragsverarbeiters in der umfangsreichen Verarbeitung besonderer Kategorien von Daten gemäß Artikel 9 oder von personenbezogenen Daten über strafrechtliche Verurteilungen und Straftaten gemäß Artikel 10 besteht.
Sofern die deutsche Gesetzgebung gemäß der Öffnungsklausel in Artikel 37 Absatz 4 von der Möglich Gebrauch macht und in einem Anpassungsgesetz zum Bundesdatenschutzgesetz (entsprechend den Vorgaben der Datenschutz-Grundverordnung) die Regelungen zur Bestellung eines Datenschutzbeauftragten beibehält, ist dieser bei einer Risikoabschätzung zwar um Rat zu fragen. Dies ist aber insoweit abweichend von einer Vorabkontrolle gemäß § 4d Absatz 5 Bundesdatenschutzgesetz, für die der Datenschutzbeauftragte zuständig ist.

- Abhilfemaßnahmen, einschließlich Garantien, Sicherheitsvorkehrungen und Verfahren, durch die der Schutz personenbezogener Daten sichergestellt und der Nachweis dafür erbracht werden soll, dass die Bestimmungen dieser Verordnung eingehalten werden, wobei den Rechten und berechtigten Interessen der betroffenen Personen und sonstiger Betroffener Rechnung getragen werden soll.

Bei der Risikobewertung sollen gemäß Erwägungsgrund 77 der Datenschutz-Grundverordnung mögliche physische, materielle und immaterielle Schäden berücksichtigt werden. Auch hier wird es zukünftig maßgeblich davon abhängen, ob genehmigte Verhaltensregeln, genehmigte Zertifizierungsverfahren oder Leitlinien des Ausschusses diesbezüglich eine Anleitung enthalten. Die Aufsichtsbehörde soll zudem Listen von Verarbeitungsvorgängen erstellen, für die Datenschutz-Folgenabschätzungen erforderlich oder gerade nicht erforderlich sind (Artikel 35 Absatz 4 und Absatz 5 Datenschutz-Grundverordnung). Dies bedeutet, dass die Intention der Datenschutz-Grundverordnung ist, Unternehmen - auch wenn sie zukünftig keinen Datenschutzbeauftragten bestellt haben – Orientierungshilfen bei der Durchführung der Datenschutz-Folgenabschätzungen von staatlicher Seite zur Verfügung zu stellen.

Gemäß Artikel 30 ist außerdem ein Verzeichnis der Verarbeitungstätigkeiten zu erstellen, und zwar ebenso von Auftragsverarbeitern, in schriftlicher oder elektronischer Form. Der Aufsichtsbehörde ist dieses Verzeichnis nur auf Anfrage zu Verfügung zu stellen. Eine Ausnahme soll hierbei für Unternehmen mit weniger als 250 Mitarbeitern gelten. Diese sind zunächst von der Verpflichtung befreit, ein Verzeichnis der Verarbeitungstätigkeiten zu führen (nicht aber von der Risikobewertung). Allerdings müssen ebenso Unternehmen mit einer Mitarbeiterzahl von weniger als 250 dennoch ein solches Verzeichnis führen, wenn die Verarbeitung ein Risiko für die Rechte und Freiheiten der betroffenen Personen birgt, ebenso wenn sie nicht nur gelegentlich erfolgt.

Da an dieser Stelle im Verordnungstext jedoch nicht ein hohes Risiko verlangt wird, kann unterstellt werden, dass zukünftig bei nahezu jeder dauerhaften Verarbeitung personenbezogener Daten ein Verzeichnis der Verarbeitungstätigkeiten zu führen ist (es sei denn dies würde durch eventuelle Verhaltensregeln gemäß Artikel 40 Datenschutz-Grundverordnung präzisiert).

Ein Verzeichnis der Verarbeitungstätigkeiten soll ebenso eine allgemeine Beschreibung der technischen und organisatorischen Maßnahmen gemäß Artikel 32 Datenschutz-Grundverordnung enthalten. Die dort genannten Schutzziele „Integrität, Vertraulichkeit, Verfügbarkeit“ entsprechen den Gewährleistungszielen des Datenschutz-Standard-Schutzmodells (als die drei Risiken der Informationssicherheit).[180] Neu ist der Begriff der Belastbarkeit, der zukünftig ebenso noch der Auslegung bedarf.

Artikel 4 Nr. 2 Datenschutz-Grundverordnung definiert die Verarbeitung als Vorgang oder Vorgangsreihe.[181] Für die Auslegung, was unter einer Verarbeitungstätigkeit zu verstehen ist, die in einem Verzeichnis zu führen ist, sind inhaltlich Artikel 30 Absatz 1 b, c und d Datenschutz-Grundverordnung entscheidend.

180 Siehe Konzept der Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder zur Datenschutzberatung und –prüfung auf der Basis einheitlicher Gewährleistungsziele vom 30.09./01.10.2015. https://www.baden-wuerttemberg.datenschutz.de/wp-content/uploads/2015/10/SDM-Handbuch_V09a.pdf

181 Artikel 4 Nr. 2 Datenschutz-Grundverordnung: Im Sinne dieser Verordnung bezeichnet der Ausdruck „Verarbeitung“ jeden mit oder ohne Hilfe automatisierter Verfahren ausgeführten Vorgang oder jede solche Vorgangsreihe im Zusammenhang mit personenbezogenen Daten wie das Erheben, das Erfassen, die Organisation, das Ordnen, die Speicherung, die Anpassung oder Veränderung, das Auslesen, das Abfragen, die Verwendung, die Offenlegung durch Übermittlung, Verbreitung oder eine andere Form der Bereitstellung, den Abgleich oder die Verknüpfung, die Einschränkung, das Löschen oder die Vernichtung

Danach sind neben einer Beschreibung der Kategorien betroffener Personen und der Kategorien personenbezogener Daten sowie der Kategorien von Empfängern, die Zwecke der Verarbeitung anzugeben. Die Frage ist daher, ob mehrere Zwecke einer Verarbeitung in einem Verarbeitungsvorgang oder einer Vorgangsreihe von Verarbeitungen nicht nur sinnvoll verbunden werden können, sondern ob diese Verbindung der Zwecke auch für die betroffene Person im Sinne der Sicherstellung der Transparenz in einer nachvollziehbaren Weise erfolgen und von ihr vernünftigerweise erwartet werden kann.[182]

II. Relevanz für den Einwilligungsassistenten

Eingangs wurde bereits die Problematik dargestellt, dass die Frage der Verantwortlichkeit im Hinblick auf den Einwilligungsassistenten zum jetzigen Zeitpunkt noch nicht abschließend entschieden werden kann. Der Empfänger der Daten ist zwar immer für die Datenverarbeitung verantwortlich. Aber hier geht es vielmehr um den Prozess davor, um die Verantwortung und Haftung für das eingesetzte Tool, welches die betroffene Person bei ihrer Einwilligung unterstützt. Wer führt für dieses System die Datenschutz-Folgenabschätzung durch und ist damit im Sinne der Datenschutz-Grundverordnung Verantwortlicher?

Verantwortlicher ist gemäß Artikel 4 Nr. 7 Datenschutz-Grundverordnung die natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die allein oder gemeinsam mit anderen über die Zwecke und Mittel der Verarbeitung personenbezogener Daten entscheidet.

Installiert der Nutzer das System als zusätzliche Software auf seinem Rechner, eigenverantwortlich und in seinem Herrschaftsbereich stellt sich die Frage, inwieweit ein Dritter (Empfänger) als Verantwortlicher angesehen werden kann und im Sinne des Gesetzes über die Verarbeitung zumindest mit entscheidet. Ist ein Softwareanbieter tatsächlich „Mitentscheider“? Fraglich ist auch, ob der Empfänger stets dadurch zum Mitentscheider wird, da die Technik auf beiden Seiten (Nutzer und Empfänger) kompatibel sein muss.

Sollte dem Nutzer eine (Mit-)Verantwortung für das eingesetzte System obliegen, muss in diesem Falle ebenso berücksichtigt werden, ob er in dem Sinne „alleingelassen“ werden der Software vertrauen kann? Wer haftet, wenn seine Daten nicht im Sinne der Datenschutz-Grundverordnung ordnungsgemäß verarbeitet werden?

Hier geht es um mehr als nur um die Installation eines technischen Werkzeuges, sondern es geht um die Nachvollziehbarkeit einer Entscheidungsfindung.

Das Forum Privatheit hat etwa auf die Möglichkeit einer wissenschaftlichen Datenschutz-Folgeabschätzung Bezug genommen. Eine wissenschaftlich orientierte Datenschutz-Folgeabschätzung könnte für den Bereich der Forschung und Entwicklung sinnvoll sein, auch wenn sie nicht unbedingt die Anforderungen an eine Datenschutz-Folgeabschätzung im Sinne der Datenschutz-Grundverordnung erfüllt. Dadurch könnten ebenso Fragen des Datenschutzes in das Risikomanagement der Hersteller und Systembetreiber integriert werden.[183] Müsste eine solche auch hier erfolgen, wenn der Nutzer alleine für das Management des Einwilligungsassistenten verantwortlich wäre?

182 Siehe hierzu bereits die Ausführungen zur Zweckbestimmung, S. 34 ff.

183 Siehe hierzu die Ausführungen des Forum Privatheit im White Paper Datenschutz-Folgeabschätzung https://www.forum-privatheit.de/forum-privatheit-de/texte/veroeffentlichungen-des-forums/themenpapiere-white-paper/Forum_Privatheit_White_Paper_Datenschutz-Folgenabschaetzung_2016.pdf, S. 35.

Eine konkrete Datenschutz-Folgeabschätzung der für die Datenverarbeitung Verantwortlichen (wie in Artikel 35 Datenschutz-Grundverordnung verlangt), könnte im Übrigen ebenso auf einer solchen generischen (wissenschaftlichen, forschungsorientierten) Datenschutz-Folgeabschätzung aufbauen.[184]

Bei einer zentralen Datenspeicherung mit mehreren zugriffsberechtigten Empfängern stellt sich gleichermaßen die Frage nach der Verantwortung sowie zusätzlich nach einer vertrauenswürdigen Instanz.[185] Sofern hier im Sinne einer Wissensplattform große Datenmengen vorhanden sind, ist zu überlegen, wer hier als zertifizierte Stelle die Verantwortung für diese Plattform übernimmt. Diese rechtliche Bewertung könnte sogar mit der Fragestellung verknüpft werden, welche Auswirkungen auf die Gesellschaft zu erwarten sind.[186]

Wenn der Einwilligungsassistent Teil eines Dienstleistungsangebots ist, müssen die Dienstanbieter eine solche Datenschutz-Folgenabschätzung gemäß Artikel 35 Datenschutz-Grundverordnung übernehmen. Wenn jedoch die betroffene Person das Tool in Eigenverantwortung installiert , um mehr Selbstbestimmung über die Daten zu erhalten, sind zwar in Bezug auf die übertragenen Daten die Empfänger die verantwortliche Stelle, in Bezug auf das Tool sind jedoch nur die Hersteller bzw. Entwickler Ansprechpartner. Es besteht einerseits nach der Datenschutz-Grundverordnung die Verpflichtung zur Entwicklung datenschutzfreundlicher Technik gemäß Erwägungsgrund 78, aber andererseits keine Haftung für die Hersteller oder Entwickler.[187] Hinsichtlich „vernetzter Autos“ gibt es allerdings eine gemeinsame Erklärung vom Verband der Autoindustrie und Datenschutzbehörden, dass die Hersteller Ansprechpartner für die Datenschutzbehörden bleiben.[188] Eine weitergehende Verantwortung der Hersteller wird jedoch nicht diskutiert.

Daher stellt sich die Frage, ob Zertifizierungen überhaupt ausreichend sind oder der Gesetzgeber für noch mehr Verantwortung der Hersteller sorgen muss.

Man könnte beispielsweise an eine Erweiterung des Produkthaftungsgesetzes denken. Nach diesem Gesetz können nicht nur Hersteller, sondern sogar Händler haftbar gemacht werden, sofern letztere den Vorlieferanten nicht innerhalb einer bestimmten Frist nennen können. Sofern Persönlichkeitsrechtsverletzungen durch fortschreitende Technik und Datenverknüpfungen zunehmen, könnte sich in entsprechender Ausgestaltung einer Schmerzensgeldtabelle für eingetretene Körperschäden ebenfalls eine Richtschnur für angemessene Beträge entwickeln.[189]

Ein Verbandsklagerecht für Verbraucherverbände ist nun in Artikel 80 Datenschutz-Grundverordnung sowie im deutschen Recht im Unterlassungsklagegesetz berücksichtigt.[190]

184 Siehe hierzu auch Ausführungen des Forum Privatheit im White Paper Datenschutz-Folgeabschätzung https://www.forum-privatheit.de/forum-privatheit-de/texte/veroeffentlichungen-des-forums/themenpapiere-white-paper/Forum_Privatheit_White_Paper_Datenschutz-Folgenabschaetzung_2016.pdf, S. 35.

185 Siehe hierzu die Beschreibung von CoMaFeDS in dieser Stellungnahme, S. 3 ff. und in der Studie der Stiftung Datenschutz, Kapitel II. 2. sowie den Dienst „DigiMe“ Kapitel II. 2. der Stiftungsstudie.

186 Siehe zum „Gefährdungsdiskurs“ in Bezug auf Privat und der Frage, warum Privatheit nicht allein als individueller, sondern auch als gesellschaftlicher Wert betrachtet werden sollte, insgesamt Seubert, Der gesellschaftliche Wert des Privaten, DuD 2012, S. 100 ff.

187 Ungeklärt ist, inwieweit ein Hersteller als „Verantwortlicher“ im Sinne von Artikel 4 Nr. 7 Datenschutz-Grundverordnung eingeordnet werden kann, wenn er Mittel der Verarbeitung bereitstellt.

188 Siehe https://www.vda.de/dam/vda/Medien/DE/Themen/Innovation-und-Technik/Vernetzung/Gemeinsame-Erkl-rung-VDA-und-Datenschutzbeh-rden-2016/Gemeinsame-Erklaerung-VDA-und-Datenschutzbehoerden-2016.pdf

189 Gemäß § 8 Produkthaftungsgesetz kann wegen des Schadens, der nicht Vermögensschaden ist, eine billige Entschädigung in Geld gefordert werden.

190 Siehe Verbraucherschutz in Zeiten von Big Data vom 12.3.2015, S. 28 https://www.bundestag.de/blob/371456/30e60f5f09a696b737bf65fece23afa4/vzbv-data.pdf sowie https://www.bundestag.de/blob/373540/dfa875e79c70deaa7c188933c2b5048b/caspar-data.pdf, S. 8.

Die Regelungen im Unterlassungsklagegesetz ermöglichen Verbraucherverbänden, Wirtschaftsverbänden, Industrie- und Handelskammern und Handwerkskammern Klagemöglichkeiten, die jedoch beschränkt sind auf die unzulässige Erhebung, Verarbeitung oder Nutzung von Verbraucherdaten zu Zwecken der Werbung, der Markt- und Meinungsforschung, des Betreibens von Auskunfteien, des Erstellens von Persönlichkeits- und Nutzungsprofilen, des Adresshandels, des sonstigen Datenhandels oder zu vergleichbaren kommerziellen Zwecken. Die Regelung des Artikel 80 Datenschutz-Grundverordnung geht darüber hinaus, da hiernach „die betroffene Person das Recht hat, eine Einrichtung, Organisationen oder Vereinigung ohne Gewinnerzielungsabsicht, die ordnungsgemäß nach dem Recht eines Mitgliedstaats gegründet ist, deren satzungsmäßige Ziele im öffentlichem Interesse liegen und die im Bereich des Schutzes der Rechte und Freiheiten von betroffenen Personen in Bezug auf den Schutz ihrer personenbezogenen Daten tätig ist, zu beauftragen, in ihrem Namen eine Beschwerde einzureichen, in ihrem Namen die in den Artikeln 77, 78 und 79 genannten Rechte wahrzunehmen und das Recht auf Schadensersatz gemäß Artikel 82 in Anspruch zu nehmen, sofern dieses im Recht der Mitgliedstaaten vorgesehen ist.“ Danach ist jede Datenverarbeitung betroffen, die nicht im Einklang mit der Verordnung besteht.

Im Sinne des umfassenden Persönlichkeitsschutzes wäre zu befürworten, wenn von diesen „Organisationen“ und „Vereinigungen“ des Artikel 80 Datenschutz-Grundverordnung ebenso Gewerkschaften und Betriebsräte umfasst wären und ein entsprechendes Verbandsklagerecht bestehen würde.

! Fazit Nr. 10

Die Entwickler des Einwilligungsassistenten sollen frühzeitig den konkreten Verwendungs- und Einsatzweck definieren, um die Verantwortlichkeiten in der praktischen Umsetzung ausreichend berücksichtigen zu können. Unklar ist, ob der Einwilligungsassistent selbst einen eigenständigen Dienst (z. B. Dienst der Informationsgesellschaft oder Dienst mit Zusatznutzen) darstellen kann.

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.

Liegt das System in der Verantwortung des Nutzers und gibt es im Sinne der Datenschutz-Grundverordnung keinen Verantwortlichen der Datenverarbeitung – ausgenommen dem Nutzer selbst -, ist zumindest ein Datenschutzsiegel (vgl. Erwägungsgrund 100) zu fordern. Unter Umständen könnte auch eine wissenschaftliche Datenschutz-Folgenabschätzung ein adäquates Mittel zur ordnungsgemäßen Prüfung und Wahrung der Betroffenenrechte darstellen.

Hersteller sind zwar angehalten, datenschutzgerechte Technik zu entwickeln, aber ohne konkrete rechtliche Verantwortlichkeit. Ungeklärt ist, inwieweit ein Hersteller als „Verantwortlicher“ im Sinne der Verordnung eingeordnet werden kann, wenn er Mittel der Verarbeitung bereitstellt. Hier könnte über die Erweiterung des Produkthaftungsgesetzes nachgedacht werden. Die Datenschutzaufsichtsbehörden haben mit dem Verband der Automobilindustrie eine gemeinsame Erklärung unterzeichnet, so dass Hersteller als Ansprechpartner zur Verfügung stehen sollen. Solche Erklärungen sollten zukünftig auch bei anderen technischen Entwicklungen in Betracht kommen.

Im Hinblick auf Artikel 80 Datenschutz-Grundverordnung könnte klargestellt werden, ob damit auch Arbeitnehmervertretungen/Gewerkschaften erfasst sind.

F. Zukünftige Fragestellungen

Die oben dargestellte Prüfung 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. Wenn das System jedoch über diese genannten Voraussetzungen hinaus eingesetzt wird, sollen kurz die beiden folgenden Fragen skizziert werden, ohne diese jedoch abschließend prüfen zu können.

I. Automatisierte Entscheidungsfindung

Relevant wäre datenschutzrechtlich, wie eine automatisierte Entscheidung zu werden ist. Hier ist Artikel 22 Datenschutz-Grundverordnung einschlägig.

Sofern der Einwilligungsassistent von einem Dienstleister oder einem Vertragspartner eingesetzt wird, stellt sich die Frage, ob der Einwilligungsassistent nicht bereits als solches die Voraussetzungen des Artikels 22 Datenschutz-Grundverordnung erfüllen muss.

Gemäß Artikel 22 Absatz 1 Datenschutz-Grundverordnung hat die betroffene Person das Recht, nicht einer ausschließlich auf einer automatisierten Verarbeitung – einschließlich Profiling – beruhenden Entscheidung unterworfen zu werden, die ihr gegenüber rechtliche Wirkung entfaltet oder sie in ähnlicher Weise erheblich beeinträchtigt.

Dies gilt jedoch nicht gemäß Absatz 2, wenn die Entscheidung

- für den Abschluss oder die Erfüllung eines Vertrages zwischen der betroffenen Person und dem Verantwortlichen erforderlich ist,

- aufgrund von Rechtsvorschriften der Union oder der Mitgliedstaaten, denen der Verantwortliche unterliegt, zulässig ist und diese Rechtsvorschriften angemessene Maßnahmen zur Wahrung der Rechte und Freiheiten sowie der berechtigten Interessen der betroffenen enthalten, oder

- mit ausdrücklicher Einwilligung der betroffenen Person erfolgt.

Für einen Einwilligungsassistenten, der automatisiert Entscheidungen trifft (unter der Voraussetzung, dass nicht der Nutzer als alleiniger Entscheider angesehen wird und sofern keine entsprechenden gesetzlichen Regelungen in den Mitgliedstaaten vorhanden sind), bedeutet dies:

⇢ 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 (so dass die automatisierte Entscheidungsfindung zur Vertragserfüllung erforderlich ist)

oder

⇢ Für die Nutzung des Einwilligungsassistenten ist eine 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. Die Artikel-29-Datenschutzgruppe hat wie oben ausgeführt dargelegt, dass eine Einwilligung nicht alle rechtmäßigen Zwecke abdecken kann, sondern sich auf die Verarbeitung beziehen muss, die in Bezug auf den Zweck angemessen und erforderlich ist. Daher ist dies aus datenschutzrechtlicher Sicht besonders kritisch zu sehen.

Zu berücksichtigen ist zudem, wer Verantwortlicher der Einwilligungsassistenten ist und ob ein eigenständiger Dienst in Betracht kommt oder dies dezentral in der alleinigen Verantwortung des Nutzers verbleibt.[191]

Besondere Kategorien personenbezogener Daten gemäß Artikel 9 dürfen im Rahmen einer automatisierten Entscheidungsfindung im Übrigen nur bei ausdrücklicher Einwilligung des Betroffenen verarbeitet werden oder wenn es entsprechende Rechtvorschriften auf der Grundlage des Unionsrechts oder des Rechts der Mitgliedstaaten gibt.

Zu beachten ist allerdings, dass die Bildung von Profilen als solche keinem besonderen Schutz unterliegt, sondern allein an den Voraussetzungen des Artikel 6 Datenschutz-Grundverordnung zu messen ist.

Insgesamt bleibt aber bei Anwendbarkeit des Artikel 22 Datenschutz-Grundverordnung 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.

Die Informationspflichten sowie das Auskunftsrecht der betroffenen Person würden sich zudem im Falle einer automatisierten Entscheidung, einschließlich Profiling, gemäß Artikel 13, 15 ebenso auf die Logik und Tragweite einer derartigen Verarbeitung beziehen. Es besteht außerdem ein Recht auf einer Kopie der Daten, die Gegenstand der Verarbeitung sind (Artikel 15 Absatz 4).

Nach der Datenschutz-Grundverordnung entfällt zwar der Grundsatz der Direkterhebung. Dennoch obliegen dem Verantwortlichen Informationspflichten gemäß Artikel 14 Datenschutz-Grundverordnung, wenn Daten nicht bei der betroffenen Person erhoben werden. Daher bleibt es notwendig, die betroffenen Personen zu informieren, wenn auch nicht unbedingt bei Erhebung.

II. Datenschutzrecht und Zivilrecht

Ohne vertiefend hierauf eingehen zu können, sollen folgende Überlegungen zum Zivilrecht kurz aufgegriffen werden:

Eine Einwilligung muss aus datenschutzrechtlicher Sicht nicht für die Übermittlung von Daten für vertragsrelevante Zwecke eingeholt werden. Sie spielt aber insoweit eine Rolle, wenn der Einwilligungsassistent selbstständig Tätigkeiten übernimmt, etwa durch Sprachsteuerung ein Hotel oder Taxi bucht. Dieses erweiterte Konzept ist nicht von den in dieser Stellungnahme untersuchten technischen Lösungen erfasst, soll aber hier bereits kurz erwähnt werden, da große Anbieter (wie etwa Deutsche Telekom AG) solche Lösungen planen.

191 Siehe oben S. 21 und S. 55.

Wenn ein solcher Einwilligungsassistent den „Auftrag“ hat, ein Taxi zum Flughafen zu bestellen, muss sichergestellt sein, dass zivilrechtlich Handlungswille und Erklärungsbewusstsein bestehen.[192] Ohne einen entsprechenden Handlungswillen liegt keine Willenserklärung vor[193] und insgesamt ist entscheidend, auf wessen Willen die Entscheidung basiert.[194] Datenschutzrechtlich muss sichergestellt sein, dass die entsprechenden Daten verarbeitet bzw. übermittelt werden dürfen. Dies ist nur der Fall, wenn der Vertrag auch geschlossen wurde. In diesem Fall wird datenschutzrechtlich keine Einwilligung benötigt. Dementsprechend muss die betroffene Person vorher nochmals eine Rückmeldung erhalten, die sie für jeden Einzelfall bestätigen muss, und zwar bevor die Daten an mögliche Empfänger weitergegeben werden.

Es müsste darüber hinaus geklärt werden, wer das Angebot abgibt und wer den Antrag annimmt. Ein Hotel muss wissen, mit wem es einen Vertrag abschließen möchte, so dass es für einen Hotelbetreiber wichtig sein kann, die persönlichen Angaben im Vorhinein zu erhalten. Der Bundesgerichtshof hat hierzu entschieden, dass nicht nur Privatleute, sondern auch Unternehmen ihr Hausrecht grundsätzlich frei ausüben können. Eingeschränkt wird dieses Recht jedoch bei Vorliegen von sachlichen Gründen, etwa wenn aufgrund einer vertraglichen Abrede ein Erfüllungsanspruch erworben wurde.[195] Bei einem Massengeschäft Taxi sind die Angaben zur Person dagegen weniger wichtig bzw. werden im Alltag regelmäßig nicht erfragt.

Aus zivilrechtlicher Sicht werden bei einer automatisierten Entscheidungsfindung nicht nur Handlungswille und Erklärungsbewusstsein und der Zeitpunkt des Vertragsschlusses relevant sein, sondern ebenso die Frage, unter welchen Gesichtspunkten ein Mangel oder eine Pflichtverletzung erheblich ist. Dies erhält bei einer automatisierten Entscheidungsfindung insoweit Relevanz, wenn nur wenige Angaben etwa zur Kategorie gemacht werden oder beispielsweise eine blaue Corvette gekauft werden soll, wenn sie endlich gefunden wurde, aber „automatisiert“ eine schwarze gekauft wird.[196] Hier wird es auch zivilrechtlich auf die Granularität ankommen.[197]

Zivilrecht und Datenschutzrecht sind daher strikt zu trennen. Aus datenschutzrechtlicher Sicht ist keine Willenserklärung in Form einer Einwilligung zusätzlich notwendig, um vertragsrelevante Daten verarbeiten zu dürfen.

Bei der Gestaltung des Einwilligungsassistenten ist somit darauf zu achten, dass für den Nutzer nicht der Eindruck entsteht, er würde nun ebenso seine Einwilligung für vertragsrelevante Zwecke erteilen, gleichwohl muss der Nutzer transparent über diese Zwecke informiert werden.

192 Siehe hierzu bereits oben S. 22 ff.

193 Siehe etwa Köhler, BGB, Allgemeiner Teil, 40. Auflage, München 2016, der auf den Handlungswillen als notwendiges Tatbestandsmerkmal einer Willenserklärung verweist und das Beispiel der Hypnose anführt; der Handlungswille fehle, wenn die äußerlich als Willenserklärung gewertete Handlung nicht gewollt war (§ 7 Rn. 4). Ebenso Rüthers/Stadler, Allgemeiner Teil des BGB, 17. Auflage, München 2011, § 17 Rn. 7: Handlungswille ist notwendige Voraussetzung für das Vorliegen einer Willenserklärung.

194 Köhler, BGB, Allgemeiner Teil, 40. Auflage, München 2016, § 6 Rn. 8 stellt klar, dass automatisierte Willenserklärungen echte Willenserklärungen sind, wenn die Datenverarbeitungsanlage keine autonomen Entscheidungen trifft, sondern nur logische Operationen aufgrund eines vorgegebenen Programms verwirklicht. Dahinter stehe der Wille des Anlagenbetreibers.

195 BGH Urteil vom 9. März 2012 -V ZR 115/11 ; http://juris.bundesgerichtshof.de/cgi-bin/rechtsprechung/document.py?Gericht=bgh&Art=en&nr=59967&pos=0&anz=1

196 BGH NJW-RR 2010, 1289 ff., 1292 mit Abkehr von der Vorinstanz, die noch eine unerhebliche Pflichtverletzung gemäß § 323 Absatz 5 BGB bei dieser Farbabweichung angenommen hatte.

197 Aus datenschutzrechtlicher Sicht würde es auf diese Frage nur ankommen, wenn die Verwendung des Einwilligungsassistenten selbst der Einwilligung bedarf.

Der Einwilligungsassistent müsste also insgesamt so konzipiert sein (inhaltlich und grafisch), dass dem Betroffenen im Einzelfall bewusst ist, eine Erklärungshandlung vorzunehmen.
Es müsste mindestens im Nachhinein nochmals die automatische Information über die Einwilligung im Einzelfall erfolgen. Allerdings ist damit ein im Vorfeld fehlender Handlungswille nicht ohne weiteres zu kompensieren. Um diesen Handlungswillen sicherzustellen, muss der betroffenen Person deutlich sein, dass eine Willenserklärung erfolgt. Aus zivilrechtlicher Hinsicht kann dies mit Schwierigkeiten behaftet sein, da gegebenenfalls immer unterstellt werden kann, dass bei einer automatisierten Entscheidung kein Handlungswille und damit keine Willenserklärung vorliegt. In diesem Fall müsste also zusätzlich diskutiert werden, wer (nach deutschem Recht) das Angebot gemäß § 145 BGB abgibt und wer dieses annimmt. Sofern man unterstellt, dass aus zivilrechtlicher Sicht kein verbindliches Angebot vorliegt, etwa da beim Buchen eines Taxis oder Hotels noch als essentialia negotii der Preis und/oder Empfänger noch nicht feststehen, müsste der Annehmende der Nutzer des Dienstes sein und der Dienstleister gibt das verbindliche Angebot ab (siehe Deutsche Telekom AG, die über Sprachsteuerung, die Möglichkeit per Assistent eröffnen möchten, etwa Hotels und Taxen selbstständig zu buchen).

G. Zusammenfassung der Anforderungen an den Einwilligungsassistenten

Die Entwickler der eingangs beschriebenen Systeme sollten berücksichtigen, dass die weitere technische Ausgestaltung des Systems 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.

Es muss daher zukünftig geklärt werden, ob der Einwilligungsassistent als Teil der Datenverarbeitung einen eigenständigen (Online)Dienst darstellt. Vorstellbar wäre ebenso, dass er von einem weiteren Anbieter als eigenständige Dienstleistung eingesetzt wird. Der Einwilligungsassistent (als Software) könnte aber ebenso an Nutzer zum Selbstmanagement veräußert werden.

Aufgrund der noch nicht näher beschriebenen und veröffentlichten technischen Details und Funktionsweise können daher lediglich die im Folgenden dargestellten grundsätzlichen Anforderungen benannt, aber keine abschließende rechtliche Beurteilung vorgenommen werden:

- Eine eindeutig bestätigende Handlung gemäß Artikel 4 Nr. 11 Datenschutz-Grundverordnung wird durch den Einwilligungsassistenten 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

- 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 ursprünglichen geplanten Datenschutz-Grundverordnung (Entwurf vom 25.01.2012) sowie der Vorgabe „Datenschutz durch Technikgestaltung“ gemäß Artikel 25 Datenschutz-Grundverordnung entsprechen. Die Erkenntnisse zu P3P (Platform for Privacy Preferences) können bei der Umsetzung berücksichtigt werden.

- Der Zweck muss eindeutig formuliert sein. Im Sinne einer datenschutzgerechten Auslegung sollte der Zweck 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) Datenschutz-Grundverordnung realisiert.

  Pauschale Einwilligungen sind unwirksam. Daher muss bei „Interessensbekundungen“ eine dynamische Einwilligungsmöglichkeit gegeben sein, wie sie aktuell bei CoMaFeDS geplant ist.[198]

  Konzepte wie CoMaFeDS könnten gleichwohl bei Forschungszwecken unterstützend eingesetzt werden. Gemäß Erwägungsgrund 33 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 der Form einer Liste, deren leere Felder der Nutzer aktivieren muss) muss im Einzelfall aus rechtlicher Sicht überprüfbar sein. Schwierigkeiten können sich etwa 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 keine Einwilligung erforderlich, wohl aber eine transparente Information.

- Soll der Einwilligungsassistent zukünftig daher zur Unterstützung bei Vertragsabschlüssen eingesetzt werden, müssen 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 zu achten, dass diese Trennung für den Nutzer deutlich wird. Die Einwilligung beinhaltet aus datenschutzrechtlicher Sicht stets ein Widerrufsrecht.

- Insgesamt ist daher zu berücksichtigen, dass die Zulässigkeit der Datenverarbeitung aus datenschutzrechtlicher Sicht auf unterschiedlichen Rechtsgrundlagen beruhen kann. Wird eine Einwilligung eingeholt, muss dem Betroffenen auch das Widerspruchsrecht zustehen. Der Verantwortliche kann sich im Nachhinein nicht auf andere Legitimationsgrundlagen (etwa berechtigte Interessen) berufen.

198 Die rechtlichen Voraussetzungen einer solchen „dynamischen Einwilligung“ müssen gesondert geprüft werden.

- Systeme wie LETsmart bieten dem Nutzer ein Selbstmanagement an, so dass er jederzeit seine Einwilligung ändern, berichtigen und löschen kann. Damit können die Anforderungen an einen jederzeitigen Widerruf gemäß Artikel 7 Absatz 3 Datenschutz-Grundverordnung erfüllt werden. Probleme, die sich im Zusammenhang mit dem Recht auf Datenübertragbarkeit (Artikel 20 Datenschutz-Grundverordnung) ergeben könnten, wären in diesem Zusammenhang ebenso umgangen.[199]

- Die Richtigkeit der Daten (Artikel 5 Absatz 1d) Datenschutz-Grundverordnung) 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, was bei dem System CoMaFeDS geplant ist.[200]

- 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 aufrecht erhalten möchte.[201] In diesem Falle werden die Gebote der Speicherbegrenzung (Artikel 5 Absatz 1e Datenschutz-Grundverordnung) sowie der Datenminimierung (Artikel 5 Absatz 1c Datenschutz-Grundverordnung) 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.

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

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

201 LETsmart plant, die Daten nach Wegfall des Verwendungszwecks automatisiert zu löschen.

- 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 Datenschutz-Grundverordnung) verwendet werden.

- Bei komplexer Datenverarbeitung mit unterschiedlichen Zwecken oder Empfängern könnte jedoch auch bei Verwendung eines Einwilligungsassistenten eine intransparente Darstellung vorliegen, die gemäß Artikel 5 Absatz 1 a Datenschutz-Grundverordnung gerade vermieden werden muss. Hier könnte geprüft werden, inwieweit der so genannte „One-Pager“ als transparente Zusammenfassung der erteilten Einwilligung unterstützend in Betracht kommen könnte.[202]

H. Fazit und Zusammenfassung der Handlungsempfehlungen

Entsprechend der in der Einführung dargestellten Zielsetzung wurde der Einwilligungsassistent 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 Mitgliedstaaten 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. Ein Indikator für diese Prüfung kann die Umsetzung der Richtlinie 96/46/EG in den einzelnen Mitgliedstaaten 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 Verhaltensregel könnte in zeitlicher Hinsicht langwierig sein. So muss sich die Verhaltensregel auf Verarbeitungstätigkeiten in mehreren Mitgliedstaaten beziehen und die zuständige Aufsichtsbehörde muss diese dem Europäischen Datenschutzausschuss vorlegen, bevor die Kommission erklären kann, dass diese in der Union allgemeine Gültigkeit besitzen.

202 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.

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.

⇢ 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.[203] 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 die Tatsache der Verarbeitungstätigkeit und deren Zweck vernünftigerweise erwarten dürfen, wobei sich die Datenschutz-Grundverordnung ebenso auf die Einwilligung „in einem Kontext“ bezieht. Fraglich ist, 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 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.

⇢ die Ausarbeitung von einheitlichen, europaweiten Verhaltensregeln in den genannten Bereichen fördern, soweit diese aufgrund einer Verarbeitungstätigkeit in mehreren Mitgliedstaaten ausgearbeitet werden können.

⇢ Durch Initiative der Europäischen Kommission
könnte sich ein aktueller Vergleich der Übersetzungen der Datenschutz-Grundverordnung durch die einzelnen Mitgliedstaaten noch vor deren Inkrafttreten dahingehend empfehlen, inwieweit ein einheitliches, europaweites Verständnis über die Auslegung der Begriffe „explicit“, „specified“ und „provide with“ besteht.[204] Dabei sollte berücksichtigt werden, ob unterschiedliche Auslegungen Auswirkung auf die Betroffenenrechte im Sinne eines einheitlichen Schutzniveaus haben könnten.

203 Siehe hierzu auch Düsseldorfer Kreis, „Orientierungshilfe zur datenschutzrechtlichen Einwilligungserklärung in Formularen“, März 2016.

204 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.

Bereits in der Vergangenheit wurde der Begriff „explicit“ von den Mitgliedstaaten im Hinblick auf die Zweckbestimmung unterschiedlich übersetzt.

⇢ Die deutsche Politik und Gesetzgebung
sollten in Bezug auf die Einwilligung die Verpflichtung zur Protokollierung und jederzeitige 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 Mitgliedstaaten möglich ist.

⇢ könnten 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?

⇢ 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.

⇢ sollten außerdem die Anregungen der Artikel-29-Dateschutzgruppe 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.

⇢ ihre Konzepte zudem dahingehend analysieren, ob eine Kombination mit bereits bestehenden Diensten und Funktionen, wie sie beispielsweise „MyData“ oder „DigiMe“ bieten, möglich und sinnvoll sein könnte.[205]

⇢ 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, technische Sicherheit und die Vorgehensweise einer Datenverarbeitung nicht überblicken kann.

205 Siehe Studie der Stiftung Datenschutz, Kapitel II. 2.

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, 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. Software stellt in gleichem Maße die Frage nach Sicherheit sowie Zertifizierung und 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 bereitstellt.

sollten die Sicherheit der Datenverarbeitung aus technischer Sicht gesondert und besonders prüfen, vor allem unter Maßgabe, wer als Verantwortlicher des Systems einzustufen ist. Dies hängt auch von dem oben ausgeführten Verwendungszweck ab und von der Frage, ob es sich um einen eigenständigen Dienst handelt oder um Software, die der Verantwortung des Nutzers oder eines Dienstanbieters obliegt.

I. Zusatz zur rechtlichen Stellungnahme vom Dezember 2016

Prof. Dr. Anne Riechert, Stiftung Datenschutz / Frankfurt University of Applied Sciences
Stand: Januar 2017, begründet auf:

Proposal „Regulation on Privacy and Electronic Communications", (10.01.2017) – 2017/0003 (COD)

Allgemein

Der Vorschlag der EU-Kommission („Regulation on Privacy and Electronic Communications" – im Folgenden: „Vorschlag") beinhaltet Regelungen zum Schutz der Privatsphäre und der personenbezogenen Daten in der elektronischen Kommunikation und soll die Richtlinie 2002/58/EG ersetzen. Klarstellend wird darauf verwiesen, dass diese Richtlinie „lex specialis" zur Datenschutz-Grundverordnung darstellt (siehe 1.2). Dies entspricht insoweit der aktuellen Rechtslage im Hinblick auf das Verhältnis der Richtlinie 2002/58/EG zur Datenschutz-Richtlinie (95/46/EG). Unberührt bleiben gemäß dem Vorschlag die Regelungen der Richtlinie 2000/31/EG (siehe Artikel 2 Nr. 4). Darüber hinaus steht es den Mitgliedstaaten ebenfalls frei, Regelungen zur Vorratsdatenspeicherung zu erlassen (siehe 1.3 des Vorschlags)

In dem Vorschlag sind unter anderem die Ergebnisse einer öffentlichen Befragung (durch Beteiligung von Verbraucherorganisationen, Industrie und Behörden) umgesetzt. Außerdem wurden Workshops sowie eine Meinungsumfrage unter EU-Bürgern durchgeführt (siehe 3.2 des Vorschlags). Aufgrund letzterer wurde beispielsweise festgestellt, dass 78% der Befragten es sehr wichtig finden, dass ein Zugang zu den auf einem Computer, Smartphone oder Tablet gespeicherten persönlichen Informationen nur aufgrund ihrer Erlaubnis möglich ist, und dass 89% mit der vorgeschlagenen Möglichkeit einverstanden sind, aufgrund von Voreinstellungen im Browser das Teilen ihrer persönlichen Informationen zu verhindern.

Des Weiteren basiert der Vorschlag auf einer Folgenabschätzung unter Berücksichtigung von Effektivität und Wirtschaftlichkeit, wobei nach der Untersuchung von unterschiedlichen möglichen Maßnahmen die Option befürwortet wurde, die eine maßvolle bzw. gemäßigte Stärkung von Privatsphäre und Vereinfachung beinhaltet. Damit ist gemäß den Ausführungen in dem Vorschlag vor allem gemeint, die Vertraulichkeit der elektronischen Kommunikation durch geeignete technische Einstellungen zu verbessern sowie das Regelungsumfeld zu vereinfachen, indem der Handlungsspielraum für die Mitgliedstaaten verringert wird (siehe 3.4 des Vorschlags).

Cookies

In Bezug auf Cookies verweist der Vorschlag gemäß Erwägungsgrund 21 darauf, dass für erforderliche Cookies keine Einwilligung eingeholt werden muss (z. B. das Ausfüllen von Online-Formularen über mehrere Seiten, das Messen des Traffic der Webseite). In Erwägungsgrund 22 wird detailliert aufgeführt, dass technische Voreinstellungen in Bezug auf Tracking-Cookies für den Nutzer übersichtlicher sind als Anfragen hinsichtlich seiner Zustimmung, wobei in Erwägungsgrund 23 im Besonderen auf die damit verbundene Anforderung des Artikel 25 Datenschutz-Grundverordnung hingewiesen wird („Privacy by Design").

Die Umsetzung dieses Anspruch sollte danach durch unterschiedliche und für den Nutzer leicht erkennbare Privatsphäreeinstellungen erfolgen, die beispielsweise Funktionen wie „Cookies niemals akzeptieren" bis „Cookies immer akzeptieren" bieten, aber ebenso die Option „nur Erstanbieter Cookies akzeptieren" umfassen.

In Erwägungsgrund 24 und Artikel 9 Absatz 1 des Vorschlags wird sodann auf die Geltung der Einwilligungsvoraussetzungen gemäß Artikel 4 Nr. 11 sowie Artikel 7 Datenschutz-Grundverordnung verwiesen. Davon unberührt ist gemäß Artikel 9 Absatz 2 Datenschutz-Grundverordnung jedoch die Verpflichtung, dort wo es „technisch möglich und machbar ist", für die Zwecke von Artikel 8 Absatz 1b des Vorschlags (für Informationen, die im Endgerät des Nutzers gespeichert sind), die Einwilligung des Nutzers durch geeignete technische Einstellungen mittels einer Softwareapplikation einzuholen. Erwägungsgrund 24 regelt hierzu näher, dass im Falle von „Third-Party-Cookies" die Nutzer aktiv auswählen sollen, dass sie mit „Third-Party-Cookies" einverstanden sind und diese Einwilligung bestätigen sollen. Dies gilt unter der Maßgabe, dass sie die notwendigen Informationen erhalten haben, diese Auswahl treffen zu können.

Im Sinne der oben bereits genannten Option (=maßvolle bzw. gemäßigte Stärkung von Privatsphäre und Vereinfachung) bezieht sich der Vorschlag darauf, eine Dialogbox zwischen Nutzer und besuchten Webseiten einzurichten, die dem Nutzer die Ablehnung von „Third-Party-Cookies" ermöglicht (siehe 3.4 des Vorschlags). Gemäß den Ausführungen in dem Vorschlag könnten damit Cookie-Banner und Benachrichtigungen umgangen werden, was zur Vereinfachung, aber auch Kosteneinsparung führen würde. Klarstellend wird darauf verwiesen, dass Webseitenbetreiber jedoch nach wie vor das Recht haben, eine Einwilligung aufgrund einer individuellen Anfrage beim Endnutzer einzuholen (siehe 3.4 des Vorschlags).

Aus wirtschaftlicher Sicht wird auf eine geschätzte, aber nicht näher begründete Kosteneinsparung von 948.8 Million Euro verwiesen (siehe 3.4 des Vorschlags).

Als Verantwortliche für diese technische Umsetzung könnten Internet Browser, Drittanbieter (die das Tracking durchführen) und die Webseiten in Betracht kommen (siehe 3.4 des Vorschlags). Gemäß Artikel 10 in Verbindung mit Artikel 23 des Vorschlags müssen Anbieter von elektronischer Kommunikationssoftware die Möglichkeit bieten, „Third-Party-Cookies" zu verhindern und die Einwilligung der Nutzer einzuholen. Anderenfalls können Bußgelder bis zu 10.000.000 EURO, alternativ 2% des weltweiten Jahresumsatzes drohen.

Relevanz im Hinblick auf die rechtliche Stellungnahme zum Einwilligungsassistenten und Handlungsempfehlung

Insgesamt besteht die Intention des Vorschlags darin, eine Einwilligung durch Unterstützung von Software, im Besonderen durch Internet Browser, einzuholen. Internet Browser stellen aber nur eine Möglichkeit dar. In den Handlungsempfehlungen der rechtlichen Stellungnahme vom Dezember 2016 (siehe Studie) wurden die Entwickler bereits zur Prüfung aufgefordert, ob ihr Konzept ebenso auf Cookies erweitert werden könnte.

In Bezug auf Cookies stellen die Erwägungsgründe klar, dass eine Einwilligung durch eine bestätigende Handlung erteilt werden soll, beispielsweise dadurch, dass von den Nutzern verlangt wird, eine Einstellung „accept third party cookies“ aktiv auszuwählen (Erwägungsgrund 26). Daraus lässt sich die Absicht entnehmen, dass ausdrücklich (nicht konkludent) durch Auswahl und aktiver Bestätigung unterschiedlicher Optionen ein Dialog stattfinden soll. Aufgrund dessen, dass dies aber (nur) ein Ausführungsbeispiel darstellt und gemäß Artikel 9 Absatz 2 zudem der Vorbehalt der „technischen Möglichkeit und Machbarkeit“ enthalten ist sowie außerdem unter 3.4 darauf verwiesen wird, dass Webseitenbetreiber das Recht haben, eine Einwilligung aufgrund einer individuellen Anfrage beim Endnutzer einzuholen, kann sich eine weitere Klarstellung empfehlen. So könnten im Hinblick auf die „technische Machbarkeit“ klare Regelfälle definiert werden. Außerdem wäre eine Betonung dahingehend möglich, dass ausschließlich (und nicht nur beispielsweise) durch die aktive Auswahl des Nutzers (Checkbox) von unterschiedlichen Optionen eine Einwilligung zustande kommt, damit eine transparente Information unter Weiternutzung des Dienstes deutlich ausgeschlossen ist (siehe etwa Rechtspraxis auf der Webseite der unabhängigen Datenschutzaufsichtsbehörde (ICO) von Großbritannien – aufgeführt in der rechtlichen Stellungnahme zum Einwilligungsassistenten).

Hinsichtlich der Einwilligungsvoraussetzungen insgesamt verweist Artikel 9 Absatz 1 auf die Voraussetzungen der Datenschutz-Grundverordnung (Artikel 4 Nr. 11 und Artikel 7 Datenschutz-Grundverordnung), so dass auch hier auf die Ausführungen in der rechtlichen Stellungnahme verwiesen wird (siehe etwa die Problematik im Hinblick auf die konkludente Einwilligung oder der Auslegung der Begriffe „explicit“ und „specified“).

Die rechtliche Verantwortung wird aufgrund der Regelungen in Artikel 10 und 23 des Vorschlags ebenso auf den Softwareentwickler verlagert, was in der Datenschutz-Grundverordnung in einer solch namentlich benannten Formulierung nicht vorgesehen ist. In der Datenschutz-Grundverordnung ist zwar der Grundsatz „Datenschutz durch Technik“ gemäß Artikel 25 enthalten, aber im Vorschlag „Regulation on Privacy and Electronic Communications” wird ausdrücklich benannt, dass auch der Anbieter von Software zur Umsetzung verpflichtet ist und ihm Geldbußen auferlegt werden können. Im Hinblick auf die Datenschutz-Grundverordnung könnte daher der Begriff des Verantwortlichen gemäß Artikel 4 Nr. 7 präzisiert werden, inwieweit ein Softwareanbieter als „Verantwortlicher“ im Sinne der Verordnung eingeordnet werden kann, da er Mittel der Verarbeitung bereit stellt und daher mit entscheiden könnte. Insgesamt muss vermieden werden, dass ein Dienstanbieter sich auf die mangelnde Umsetzung oder Entwicklung der erforderlichen softwareseitig sicherzustellenden Einwilligungsvoraussetzungen eines Softwareanbieters beruft (siehe Artikel 9 Absatz 2 „technically possible and feasible“), da Browserlösungen unter Umständen Entwicklungszeit benötigen.

Klarstellend könnte daher geregelt werden, dass jeder Anbieter verpflichtet ist, eine ausdrückliche Einwilligung durch Bereitstellung von interaktiven Auswahlmöglichkeiten einzuholen. Damit wäre eine aktive Entscheidung der Nutzer sichergestellt, die nicht in der Weiternutzung des Dienstes (auch nicht durch transparente Information) bestehen kann. In diesem Zusammenhang sei ebenso darauf verwiesen, dass Konzepte wie P3P in der Vergangenheit vom Windows-Browser seit der Version Windows 10 nicht mehr unterstützt wurden. Externe Softwareentwickler und Browseranbieter müssen daher in Bezug auf „technische Machbarkeit“ eng zusammenarbeiten.

Darüber hinaus wäre als vertrauensbildende Maßnahme für die Nutzer an dieser Stelle zertifizierte Software hilfreich.
Empfehlenswert wäre bei einer Verlagerung des Datenschutzes auf die technische Seite außerdem, eine Bildungsoffensive zu starten. Es ist ganz entscheidend, dass Nutzer keine Vorbehalte oder Ressentiments gegenüber einem technischen Datenschutz haben, sich die Bedienung von vorneherein zutrauen und nachvollziehen können, aus welchem Grunde technische Maßnahmen wichtig sind. Hier geht es im Besonderen um die Nachvollziehbarkeit des Selbstdatenschutzes, da dadurch gleichermaßen ein verantwortungsvoller Umgang der Daten seitens des Nutzers erwartet wird. Im Hinblick auf „Big Data“ muss einem Nutzer bekannt sein, wo die Gefahren von Third-Party-Cookies liegen. Um überhaupt eine Entscheidung treffen zu können, darf ihm die Entscheidung, welche Arten von Cookies er akzeptiert, nicht aus Unwissenheit „egal sein“.

Daher ist sowohl die Schul- als auch Erwachsenenbildung über (technischen) Datenschutz sehr bedeutsam.

DIW BERLIN

GUTACHTEN

„Die persönliche Datenökonomie: Plattformen, Datentresore und persönliche Clouds“

– Ökonomische Rahmenbedingungen innovativer Lösungen zu Einwilligungen im Datenschutz –

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

Berlin, den 31. Januar 2017

Kontakt:
Dr. Nicola Jentzsch
Deutsches Institut für Wirtschaftsforschung Berlin (DIW Berlin)
Abteilung Wettbewerb und Verbraucher
Mohrenstraße 58 | 10117 Berlin
Tel.: 030 89789-230 | Fax: 030-89789-103
E-Mail: njentzsch@diw.de

Inhaltsverzeichnis

Anhang 2 – Seite

1. Einleitung 4

2. Abgrenzung des Forschungsgegenstands 7
- 2.1 Marktabgrenzung 7
- 2.2 Begrifflichkeiten 8

3. Klassifikation der Akteure und Geschäftsmodelle 9
- 3.1 Verschiedene Modelle der Informationsintermediation 11
- 3.2 Taxonomie der Persönlichen Informationsmanagement-Systeme (PIMS) 14
  - 3.2.1 Hub-Modelle 16
  - 3.2.2 Verteilte Systeme 17
- 3.3 Nutzer-zentrierte Intermediation als mehrseitiger Markt 18
- 3.4 Anreize für Nutzer und Unternehmen 19
  - 3.4.1 Anreize für Plattform-Nutzer 19
  - 3.4.2 Anreize für Unternehmen als Datennachfrager 21
  - 3.4.3 Anreize für andere Teilnehmer 22
- 3.5 Selbstselektion und Datenqualität 22
- 3.6 Einwilligungsmanagement in vertikalen Wertschöpfungsketten 24

4. Dynamiken in Märkten der persönlichen Datenökonomie 25
- 4.1 Wettbewerb der Plattformen in der persönlichen Datenökonomie 25
- 4.2 Persönliche Informationen als handelbares Gut 26
- 4.3 Monetarisierung persönlicher Informationen 27
- 4.4 Verhaltensökonomische Forschung zur Einwilligungserklärung 28
  - 4.4.1 Privatsphären-Kalküle und Affektentscheidungen 29
  - 4.4.2 Erkenntnisse aus der empirischen Forschung zu Einwilligungen 30
- 4.5 Signalökonomie und Prozesse des Unraveling 31

5. Zusammenfassung 33

6. Empfehlungen 34

Anhang 2 – Seite

Tabellenverzeichnis

Tabelle 1 Überblickstabelle Taxonomie (Entwurf) 15
Tabelle 2 Privatsphären-Kalkül und Affektentscheidung 29

Abbildungsverzeichnis

Abbildung 1 Überblick über das ‚Ökosystem' der persönlichen Datenökonomie 10
Abbildung 2 Informationsintermediation über Kreditauskunfteien 11
Abbildung 3 Informationsintermediation bei Google 11
Abbildung 4 Persönliche Datenplattformen 12
Abbildung 5 Nutzung von PIMS-Diensten 22
Abbildung 6 Wertschöpfungsketten im Einwilligungsmanagement 24

Abkürzungsverzeichnis

API	Application Programming Interface
BVerfG	Bundesverfassungsgericht
CRM	Customer Relationship Management
DLT	Distributed Ledger Technology
EU-DSGVO	Europäische Datenschutzgrundverordnung
EDPS	European Data Protection Supervisor
IPACSO	Innovation Framework for Privacy and Cyber Security Market Opportunities
IP	Internet-Protokoll
ISO	Internationale Organisation für Normung
M2M	Machine-to-machine
NACE	Nomenclature statistique des activités économiques dans la Communauté européenne
OASIS	Organization for the Advancement of Structured Information Standards
OAuth 2.0	Open Authentication 2.0
PIMS	Persönliche Informationsmanagement-Systeme
UMA	User Managed Access
VRM	Vendor Relationship Management
W3C	World Wide Web Consortium
XDI	XRI Data Interchange

Disclaimer

Das Gutachten reflektiert die Ansichten der Autorin und ist nicht als offizieller Standpunkt des DIW Berlin zu verstehen.

Danksagung

Die Autorin dieser Studie bedankt sich für den fachlichen Austausch mit einer Reihe von Personen. Besonderer Dank gilt Katryna Dow (Meeco), Florian Götz (Digitando), Daniel Kaplan (MesInfos), Joachim Lohkamp (Jolocom), Gunnar Hempel (LETSmart), Frank Ingenrieth (PGuard Projekt, SRIW), Julian Ranger (Digi.me), Claus Dieter Ulmer (Deutsche Telekom) und Sebastian Wolfsteiner (Personiq, EmVolution).

1. Einleitung

Durch die Nutzung digitaler Technologien werden massive Datenvolumina produziert, auf deren ökonomische Verwertung sich eine Vielzahl unterschiedlicher Akteure spezialisiert hat. Persönliche Daten gelten derzeit als ‚neues Vermögen' oder vierter Produktionsfaktor, neben Arbeit, Kapital und Boden (s. auch Khosrow-Pour 2015 und World Economic Forum 2011). Eine Grundlage für die ökonomische Verwertung von persönlichen Daten ist die informierte Einwilligung in die elektronische Datenverarbeitung durch den Verbraucher als Subjekt der Daten.

Durch die Digitalisierung kommt der Einwilligung zunehmend eine strategische Bedeutung in der Datenerschließung für die im Wettbewerb stehenden Unternehmen zu. Zum einen bestimmt sie den rechts- und gerichtssicheren Handlungsspielraum bezüglich der Daten – also ihr ökonomisches Verwertungspotential. Zum anderen wird über die Einwilligungserklärung der Kunde potentiell zum ‚strategischen Spieler', der seine Zustimmung zur Datenverarbeitung – im Idealfall – von den Bedingungen des Daten-Handels abhängig machen kann.

Neben ihrer ökonomischen Bedeutung ist die Einwilligung zugleich ein wichtiges Instrument der Ausübung des Rechts auf informationelle Selbstbestimmung (Volkszählungsurteil des BVerfG vom 15. Dezember 1983, Az. 1 BvR 209/83). Sie ist damit Teil eines Bündels von Rechtsbindungen und -positionen, welche die Partizipations- und Einflussrechte des Einzelnen absichern.

Die Effektivität von Einwilligungserklärungen wird in Fachkreisen angezweifelt. So haben Verbraucher längst den Überblick verloren, wer welche Daten sammelt und zu welchen Zwecken diese ausgewertet werden. Aufgrund der Intransparenz kann ein Verbraucher nicht immer die für ihn optimale Entscheidung fällen, was die Verarbeitung und Analyse seiner Daten angeht. Rechtsprofessor Daniel J. Solove, zitiert in Custers (2016), konstatiert, dass Datenschutzversprechen ihr Ziel des Datenschutzes verfehlen. Sie würden, erstens, nicht gelesen, und in dem Falle, dass Verbraucher sie lesen würden, würden sie oft nicht verstanden. Zusätzlich fehle meist das Hintergrundwissen für eine informierte Entscheidung. Sollte letzteres vorliegen, würden die offerierten Entscheidungsoptionen meist nicht die Präferenzen des Verbrauchers widerspiegeln.

Es drängt sich also die Frage auf, ob Einwilligungserklärungen noch als Instrument der informierten Entscheidung gesehen werden können, über welches der Verbraucher seine Souveränität ausübt. Wie es scheint, bestehen jetzt günstige Voraussetzungen für eine potentielle Umorganisation der Informationsintermediation in digitalen Märkten. Eine Reihe von Projekten, Partnerschaften und Start-ups setzen dem Mangel an Transparenz und Kontrollmöglichkeiten innovative Alternativen entgegen. Hierbei hat sich bereits ein ganzes ‚Ökosystem' mit verschiedenen Stakeholdern entwickelt, darunter Industrie-Kooperationen, Standardisierungsinitiativen und Fachkonferenzen.

Die Neuentwicklungen des technischen Einwilligungsmanagements lassen sich hierbei unter einer Vielzahl von Fachbegriffen fassen, darunter persönliche Informationsmanagement-Systeme (PIMS), Datentresore oder persönliche Clouds. Diese werden allesamt der ‚persönlichen Datenökonomie' zugeordnet. Im Zentrum steht der Nutzer, der eigenverantwortlich das Einwilligungs- sowie Autorisierungsmanagement übernimmt.

Besondere Vorteile entstehen durch die Automatisierung und Dynamisierung der Einwilligung, sowie maschinenlesbare Übersetzung von Datenschutz-Politiken. Ein Haupttreiber dieser Entwicklung ist die Umsetzung der Datenschutzgrundverordnung (EU-DSGVO) mit ihrer Stärkung der Einwilligung, sowie den Vorgaben des privacy by default und privacy by design. Die neuen Plattformen könnten es Nutzern erlauben, ihre Privatsphären- und Vertrauenseinstellungen optimal ihren Präferenzen anzupassen. Die Präferenzen der Informationspreisgabe könnten dann mit den Wahlhandlungen konvergieren.

Makroökonomisch gesehen handelt es sich bei datenintensiven Branchen um Wachstumstreiber, wie die Boston Consulting Group (2012) beschreibt. Sie schätzt, dass diese Branchen, für welche digitale Identität eine erhebliche Rolle spielt, zwischen 2008 und 2011 stark gewachsen sind. Der generierte Wert der datenintensiven Branchen inclusive des für den Verbraucher produzierten Wertes könnte 2020 schon bei 8% des Bruttoinlandsproduktes der EU-27 liegen.

Es herrscht Aufbruchsstimmung: viele der Unternehmensgründer wollen die angestammte Intermediation von Nutzerdaten über Datenhändler revolutionieren. Die zentralisierte Erhebung und Speicherung von Daten in Digitalkonzernen soll ersetzt werden durch eine Zentralisierung der Daten beim Verbraucher und einer dortigen Verankerung der Zugriffs- und Verwertungsrechte.

Solche Plattformen würden nicht nur eine bessere Durchsetzung von Privatsphären-Präferenzen der Nutzer, sondern unter Umständen auch eine Neuorganisation der Kunden-Unternehmensbeziehungen implizieren. Gleichzeitig würden sich Innovationspotentiale für neue Anwendungen bei peer-to-peer Diensten, Anwendungen für die Jobsuche oder der digitalen Selbstvermessung (Selbstanalyse oder persönliche Vorhersagen) ergeben.

Die junge Branche ist aber auch von schnellen Veränderungen geprägt, Markteintritten sowie -austritten. Wie es scheint mangelt es den vielen Start-ups an relevanten Nutzerzahlen und robusten Geschäftsmodellen. Zurecht ist diese Branche als in derzeit embryonalen Zustand bezeichnet worden (Juniper Research 2016). Die Plattformen befinden sich außerdem in einem herausfordernden Wettbewerbsumfeld: als zweiseitige Plattform müssen sie mindestens zwei Kundengruppen (Datenanbieter und -nachfrager) gleichzeitig anziehen, neue Daten-Monetarisierungsmechanismen entwickeln und technische sowie protokollarische Ende-zu-Ende-Sicherheit einsetzen, um bei Nutzern Vertrauen zu generieren.

Auf der Seite der Unternehmen, welche Daten nachfragen könnten, können Initiativen der Datenrückgabe (‚share back') komplexe Umorganisations- und Standardisierungsprozesse, sowie neue Datenmanagement-Architekturen erfordern. Gleichzeitig ermöglichen die Plattformen eine Zulieferung von Echtzeit-Informationen und damit eine Just-in-time-Integration in Produktionsprozesse der Unternehmen.

Referenzrahmen des Gutachtens

Aus dem rechtlichen Kontext und der aktuellen technologischen Entwicklung (Big Data, Distributed Ledger Technology) ergeben sich Spielräume für innovative Geschäftsmodelle des (technischen) Einwilligungsmanagements. Diese Lösungen, sowie die Rahmenbedingungen für eine förderliche Entwicklung derselben sollen Gegenstand dieses Gutachtens sein.

Hauptziele des Gutachtens

Ein Hauptziel des Gutachtens ist die Analyse von Geschäftsmodellen und Initiativen im Bereich des selbstbestimmten Einwilligungsmanagements. Diese werden in eine neue Typologie eingeordnet, welche die Funktion des besseren Überblicks erfüllen soll. In die Analyse sollen Mehrwertschaffung, Anreizsysteme, sowie Erlösmechanismen (Daten-Monetarisierung) einbezogen werden. Die Typologie bietet auch die Grundlage für eine bessere Beurteilung, welchen Marktdynamiken diese Angebote unterliegen. Sie wird aufgrund des eng gesetzten Zeitrahmens des Gutachtens allerdings nur exemplarisch auf einige Unternehmen angewandt.

Diese Geschäftsmodelle und Projekte sollen – auf abstrakter Ebene – in eine vertikale Betrachtung der Wertschöpfungsketten eingeordnet werden (s. auch Jentzsch 2015). Persönliche Daten sind als ein Input in verschiedenen Online-Dienste zu betrachten. Eine Veränderung der Konditionen der Inputerschließung kann sich auf die nachgelagerten Produktionsstufen auswirken, indem sie eine Reorganisation der gängigen Prozessabläufe nach sich zieht.

Schlussendlich sollen die Betrachtungen in eine Diskussion der ökonomischen Rahmenbedingungen münden, innerhalb derer innovative Lösungsansätze im Bereich der datenschutzbezogenen Einwilligung erfolgreich sein können.

Dieser Diskussion schließt sich die Analyse potentieller Markt- und Preisbildungsmechanismen an. Da es sich bei der vorliegenden Publikation um ein Kurzgutachten handelt, kann letzteres nur auf abstrakter Ebene stattfinden, basierend auf Erkenntnissen der theoretischen und verhaltensökonomischen Forschung. In Gänze erlaubt diese Vorgehensweise die Diskussion förderlicher ökonomischer Rahmenbedingungen, eines der Hauptziele der vorliegenden Expertise.

Methodik

Methodisch basiert das Gutachten auf einer Kombination von Erkenntnissen aus der wirtschaftswissenschaftlichen Forschung und der Politikberatung in den Bereichen Ökonomie der Privatsphäre sowie Wettbewerb in Märkten für persönliche Informationen. Zum einen wird dabei auf die Erkenntnisse des FP-7 finanzierten Projektes „Innovation Framework for Privacy and Cyber Security Market Opportunities“ (IPACSO) zurückgegriffen, wo bereits eine ähnliche Klassifikation entwickelt wurde. Zum anderen soll auf Marktstudien wie Ctrl-SHIFT (2014) zurückgegriffen werden. Dieses Gutachten wurde innerhalb des Zeitrahmens von drei Wochen im Januar 2017 verfasst. Aufgrund des knapp bemessenen Zeitrahmens ist es deskriptivanalytisch und nicht quantitativ.

2. Abgrenzung des Forschungsgegenstands

2.1 Marktabgrenzung

Im Zentrum dieses Gutachtens sollen insbesondere solche Lösungen, Pilotprojekte und Unternehmen stehen, deren Hauptzweck oder -aktivität das selbstbestimmte Einwilligungsmanagement ist.[1] Die Innovationsleistung durch technisches Einwilligungsmanagement bildet zugleich ihren Mehrwert (value proposition). Es geht also grundsätzlich um Angebote, die das Erschließen, die Nutzung und Weitergabe von personenbezogenen Daten durch bzw. unter Kontrolle von Verbrauchern (Nutzern) erlauben.[2]

Märkte im artverwandten Bereich der Cybersicherheit werden hinlänglich in die Segmente Hardware, Software und Dienstleistungen unterteilt (Jentzsch 2015). Diese Segmentierung rekurriert auf die in Industrieklassifikationssystemen[3] angewandte Systematik. Das NACE-System ist allerdings nicht detailliert genug, um innovative Anbieter in diesem Bereich identifizieren zu können. Eine Recherche innerhalb des IPACSO-Verbundes über die Orbis-Firmendatenbank ergab sehr geringe Fallzahlen in Deutschland, sowie im EU-Ausland in den domänenspezifischen Bereichen der Einwilligung oder der Privatsphäre.

Im Bereich des Einwilligungs- und Privatsphären-Managements sind insbesondere die Segmente Software und Dienstleistungen wichtig. Hier geht es insbesondere um Angebote der business-to-consumer Linie und weniger der business-to-business Linie.

Es gibt Unternehmensberatungen, die andere Markt-Taxonomien aufgesetzt haben (Smith und Mitchell 2014), die weniger gut den Zwecken dieses Gutachtens dienen. Dies wird in Abschnitt 3.2 diskutiert und eine eigenständige Taxonomie entsprechend entwickelt.

In diesem Gutachten werden Angebote der Selbstanalyse nicht betrachtet. Informationskontrolle spielt bei solchen Angeboten ebenfalls eine Rolle, diese Angebote dienen aber primär dem Zweck der Selbstanalyse, Beispiele sind Wolfram|Alpha Personal Analytics für Facebook, JawBone oder Digifit. Selbstanalytik wird jedoch in manchen, hier aufgenommenen Angeboten integriert (z. B. My Data Store oder CitizenMe).

Um einen Überblick zu erlangen, wird hier auch das ‚Ökosystem' kartographiert, also eine Einordung von Forschungsprojekten, Unternehmen, und Standardisierungsunterfangen vorgenommen.

1 Als ‚primäre Geschäftsaktivität' wird innerhalb der Industrieklassifikationssysteme jene gesehen, welche für den überwiegenden Anteil der Einnahmen des Unternehmens verantwortlich ist.

2 Festgehalten wird dieser Zweck unter anderem auch von Projektpartnern der MyData-Konferenz (http://mydata2016.org/2016/08/01/empowering-individuals-with-their-personal-data-the-self-data-charter/); der hier zugrunde liegende Begriff der ‚persönlichen Information' bezieht sich auf die in der EU-DSGVO verwandten Definition. Die Begriffe ‚Verbraucher', ‚Nutzer' und ‚Datensubjekt' werden synonym verwendet.

3 Ein Beispiel hierfür ist das in Europa verwandte NACE-System (Nomenclature statistique des activités économiques dans la Communauté européenne).

2.2 Begrifflichkeiten

Die britische Unternehmensberatung Ctrl-SHIFT schätzt, dass es international rund 400 Unternehmen gibt, die im Markt für persönliche Datendienste tätig sind (Ctrl-SHIFT 2014). Die Bezeichnung ‚persönliche Datendienste' subsumiert hierbei persönliche Informationsmanagement-Systeme (personal information management systems, PIMS), Daten-Banken (personal data banks), Datentresore (personal data vaults), persönliche Datenspeicher (personal data stores), sowie persönliche Clouds oder Entscheidungsmaschinen (decision machines).

Andere Autoren verwenden Begriffe wie den Nutzervermittelten Zugang (user-managed access, UMA), siehe auch Catalano und Machulak (2014) oder MyData Architecture (1.2.1). Neben der bereits genannten Begrifflichkeit werden solche Dienste manchmal auch als authorization-as-a-service oder analytics-as-a-service bezeichnet.

Bei vielen dieser Anwendungen geht es um die Bereitstellung eines virtuellen Marktplatzes für den Kauf- und Verkauf von persönlichen Datenprofilen oder für den Tausch derselben. Deshalb finden sich in der Literatur auch Begriffe wie ‚persönliche Datenökonomie' oder ‚Märkte für persönliche Informationen'. Einige der Anwendungen basieren auf oder integrieren Funktionen des sozialen Tauschs (MyDataCan oder Di.me) aus denen sich eine soziale Allokation der persönlichen Daten ergibt.

Einbezogen werden sollen hier auch Systeme des Vendor Relationship Management (VRM), welches das Komplementär zum Customer Relationship Management (CRM) bildet. Zusätzlich werden die genannten persönlichen Clouds aufgenommen und Systeme, welche die Distributed Ledger Technology (DLT) verwenden.

Eine Klassifikation der Geschäftsmodelle sowie der Projekte in diesem Bereich soll aussagekräftig sein und die wichtigsten Merkmale mit Trenngüte aufnehmen.

3. Klassifikation der Akteure und Geschäftsmodelle

Marktplätze für Produkte und Dienstleistungen des Managements von Verbraucherdaten unterliegen zwar grundsätzlich gemeinsamen Tendenzen, wie beispielsweise der Tendenz zu starker Marktkonzentration. Im Einzelfall aber sind sie unterschiedlich organisiert, was die Informationsintermediation angeht (Bundeskartellamt 2005; Federal Trade Commission 2014; Jentzsch 2007).

Die hier vorgestellten Innovationen sollen die Zentralisierung der Daten in Unternehmen wie Amazon, Apple, Google oder Facebook durch eine Zentralisation und Verankerung der Verfügungsrechte beim Verbraucher ersetzen. Unter anderem argumentieren die Befürworter der neuen Modelle, dass persönliche Daten derzeit in separierten Datenbanken gespeichert sind und kein komplettes Profil ermöglichen (World Economic Forum 2013). Abgesehen davon, dass ein umfassendes digitales Persönlichkeitsprofil datenschutzrechtlich durchaus bedenklich sein kann,[4] bewerben Unternehmen wie Clario oder Experian seit längerem die 360°-Sicht von Verbrauchern zumindest im US-amerikanischen Markt (Jentzsch 2016a).

Ein Silo-Ansatz ist für Unternehmen wie Google kaum mehr feststellbar, seit das Unternehmen im Jahr 2012 seine globale Datenschutzpolitik verändert hat und Diensteübergreifend Daten zusammenführt (s.a. Gutachten der Dutch Data Protection Authority 2013). Selbst Facebook kauft zunehmend Daten von Datenbrokern, also Drittquellen, ein und versuchte eine Zusammenführung bestimmter Datenkategorien von WhatsApp.[5]

Hauptaugenmerk liegt hier auf den PIMS, also Datendiensten, durch die Zentralisation und Kontrolle auf Verbraucher übergehen sollen, auch unter dem Aspekt, dass dies meistens eine Replikation der Einzeldatensätze bedeutet. Viele dieser Dienste sind als mehrseitige Plattformen gestaltet, was in Kapitel 4 diskutiert wird.

Eine erste Annäherung an die Akteure kann gelingen, indem man das bereits existierende domänenspezifische ‚Ökosystem' kartographiert, wie dies in Abbildung 1 unternommen wird. Diese Abbildung zeigt in den vier Quadranten Regierungsinitiativen, Unternehmen, Standardisierungsinitiativen sowie Forschungsprojekte.[6]

Zunächst ist auffällig, dass es im Bereich der persönlichen Datenökonomie nur wenig Regierungsinitiativen gibt. Hier scheint vor allem Großbritannien führend zu sein.[7] Dem stehen vereinzelte Forschungsprojekte auf EU-Ebene, sowie auf der Ebene der Nationalstaaten gegenüber. Die Forschungsprojekte können derzeit hinsichtlich ihrer Erfolgswahrscheinlichkeit nicht abschließend beurteilt werden, da sich diese zumeist in der Frühphase der Implementierung befinden.

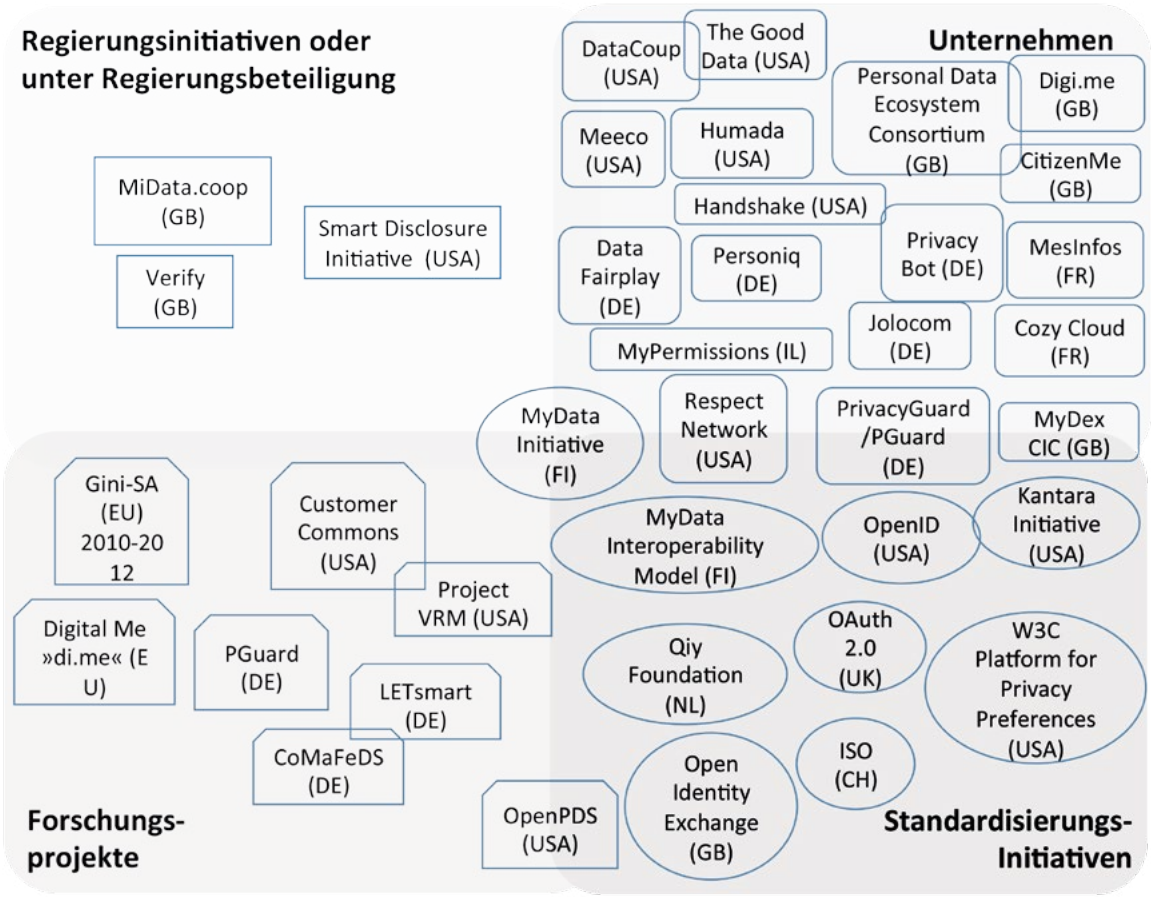
4 Regelung zur Profilbildung sowie Nutzung für automatisierte Einzelentscheidungen, DSGVO, Art. 22.

5 Reilly, M. (2016). How Facebook Learns About Your Offline Life, MIT Technology Review, https://www.technologyreview.com/s/603283/how-facebook-learns-about-your-offline-life/

6 Aufgrund des sehr kurzen Untersuchungszeitraumes basiert das Schaubild auf Recherchen der Autorin, da – wie beschrieben – eine systematische Analyse aufgrund der geringen Fallzahlen in Orbis nicht möglich war.

7 Gegenstand dieses Gutachtens ist keine detaillierte Betrachtung aller im ‚Ökosystem' vorhandener Institutionen und Akteure. Vielmehr konzentrieren wir uns auf die Unternehmen und Forschungsprojekte.

Abbildung 1 Überblick über das ‚Ökosystem' der persönlichen Datenökonomie



Anmerkung: Überlappung von Formen impliziert keine Kooperation.

Im Quadranten der Unternehmen existiert eine große Vielfalt, was die Geschäftsmodelle anbetrifft, die Gewinnorientierung oder die entwickelten und angebotenen Technologien (z. B. Apps, DLT-Anwendungen oder persönliche Clouds). Und schließlich sind auch verschiedene Initiativen im Bereich der Standardisierung zu nennen. Diese betreffen einerseits die Entwicklung maschinenlesbarer Datenschutz-Versprechen, sowie deren Um- und Durchsetzung, aber auch die Entwicklung von Protokollen oder harmonisierten semantischen Standards (z. B. XDI).[8] Interoperabilität und Portabilität von Datenprofilen sind für den Wettbewerb zwischen den Anbietern persönlicher Datenlösungen eine unabdingbare Grundlage. Ähnlich wie bei einem Bankkonto-Umzugsdienst könnte dies für eine erleichterte Mitnahme eines Profils von einer Plattform zur anderen ermöglichen.

Im Gebiet der Standardisierung spielt die Internationale Organisation für Normung (ISO) eine gewichtige Rolle, die globale Standards der Datenqualität, des Identitätsmanagements sowie der Cybersicherheit setzt. Es kann an dieser Stelle allerdings keine Diskussion geleistet werden, inwiefern sich Standards aufeinander beziehen – dies wäre eine separate Untersuchung.

8 *Definitionen für Formate und Protokolle für semantischen Datenaustausch werden durch das OASIS Semantic Data Exchange bereitgestellt. XDI ist ein Standard für den domänenübergreifenden Austausch, das Verlinken und die Synchronisierung von maschinenlesbaren Informationen (u. a. ID-Attribute).*

3.1 Verschiedene Modelle der Informationsintermediation

Der Hauptunterschied der PIMS – im Vergleich etablierten Modellen der Informationsintermediation – ist das aktive Eingreifen des Datensubjektes in diese Intermediation. Dies soll anhand der folgenden Beispiele generisch dargestellt werden (s. Abbildung 2 und Abbildung 3). Diese Darstellungen sind stark vereinfacht und erheben keinen Anspruch auf Vollständigkeit.

Abbildung 2 Informationsintermediation über Kreditauskunfteien

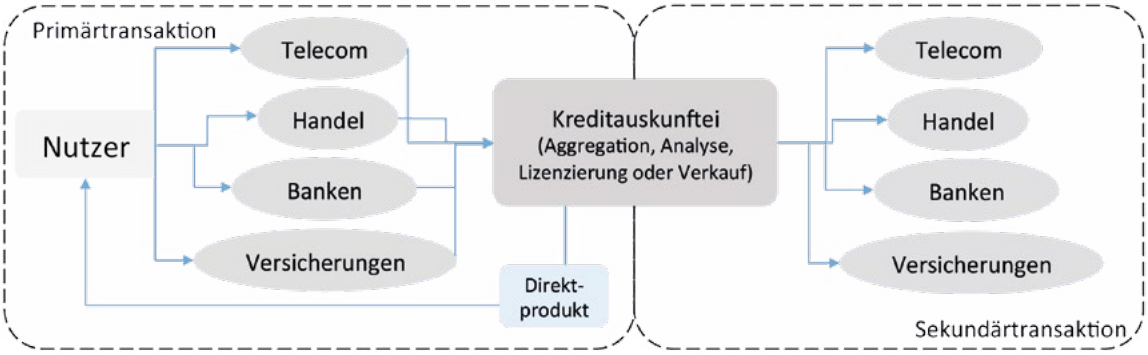


Abbildung 2 stellt den Datenhandel dar, wie er sich im Bereich der Wirtschaftsauskünfte in den letzten Jahren entwickelt hat. Augenscheinlich ist der Nutzer über seine Einwilligung in der Primärtransaktion hinaus quasi nicht aktiv am Datenhandel beteiligt.[9] Die Plattform hat hierbei keinen direkten Bezug zum Verbraucher außerhalb der u.U. angebotenen „Direktprodukte“ (consumer direct products).[10] Hierzu gehören Angebote wie MeineSchufa.de, myFICO oder VantageScore. Diese sollen nicht Gegenstand der vorliegenden Expertise sein. Eine ähnliche Intermediationsart wird auch von Unternehmen wie BlueKai (Oracle) und Acxiom eingesetzt.

Abbildung 3 Informationsintermediation bei Google

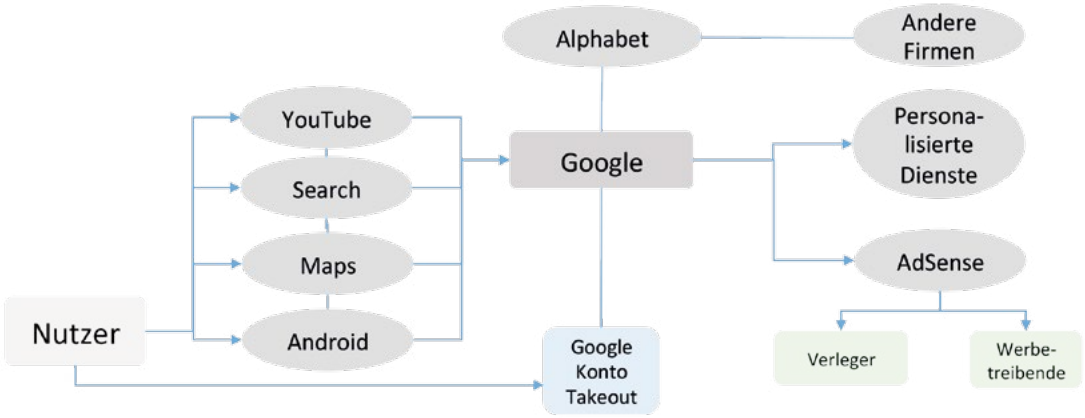


Abbildung 3 zeigt, modellhaft am Beispiel von Google, wie die Intermediationsfunktion verlaufen kann,

9 *Dies gilt mit Einschränkungen, da der Kunde in einem gewissen Maß Verfügungs- und Kontrollrechte hat. So kann er auf Basis des geltenden Bundesdatenschutzgesetzes in Deutschland seine Daten einsehen und diese korrigieren (s.a. Jentzsch 2007).*

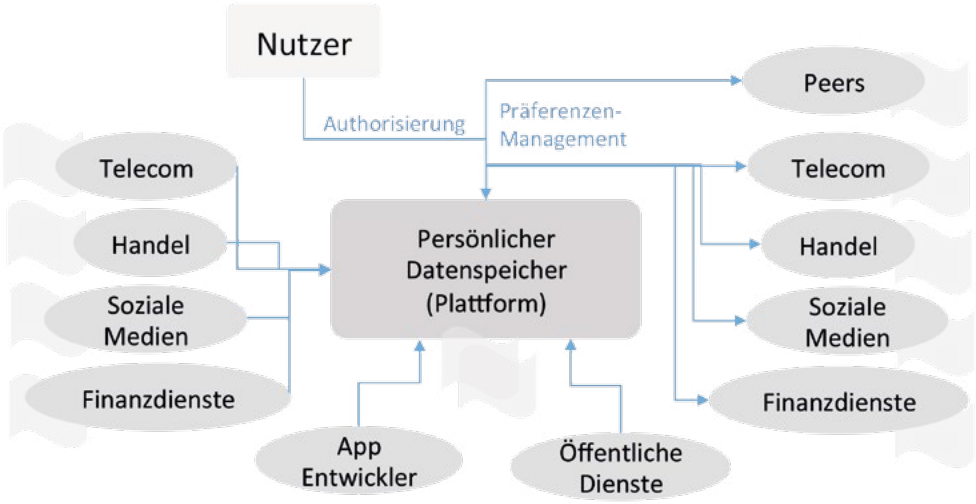
10 *Dieser Ausdruck wird in der Industrie verwandt, es handelt sich aber genau genommen um Dienstleistungen.*

wenn das Unternehmen einen direkten Bezug zum Kunden hat und Daten über ihn sammelt, auch wenn dies in pseudonymisierter Art und Weise passiert (IP-Nummern) und Nutzerprofile an sich nicht transferiert werden.

Die Abbildung zeigt auch, dass ein Nutzer verschiedener Google-Dienste Einsichts- und Kontrollrechte über sein Google-Konto ausüben kann. In diesem kann er auch Privatsphären-Einstellungen vornehmen. Nach Angaben des Unternehmens haben über 100 Millionen Nutzer bei Google bereits ihre Datenschutz-Einstellungen verändert.[11] Die Diensteübergreifende Zusammenführung der Daten bei Google erlaubt die Personalisierung von Gütern und Dienstleistungen. Über AdSense wiederum interagieren Verleger und Werbetreibende bezüglich der Schaltung von Online-Werbung miteinander. Für eine detaillierte Analyse, siehe auch European Commission (2008).

Es können also auch Produkte und Dienste identifiziert werden, die von etablierten Unternehmen für eine verbesserte Einsicht und Transparenz der gespeicherten Daten bereitgestellt werden. Beispiele dafür sind das Google Dashboard und der genannte Google Takeout, der mit einem Google-Konto genutzt werden kann. Hierbei stellt Google ein Zip-File der Daten zur Verfügung.

Abbildung 4 Persönliche Datenplattformen



Schließlich zeigt Abbildung 4 schematisch die von verschiedenen Akteuren ersonnene Neuorganisation der Intermediation durch die Einführung von PIMS. Nutzer sollen hier aktiv in die Informationsintermediation eingreifen können. So können sie Vertrauens- und Privatsphären-Einstellungen vornehmen, sowie Konditionen von unentgeltlichem Datentransfer oder -verkäufen festsetzen.

Die Abbildung zeigt auch, dass die Datenprofile (hellgrau dargestellt) sich durch solche Systeme in erster Linie zunächst replizieren. Über Schnittstellen erlaubt der Nutzer bei den meisten PIMS Daten aus Drittquellen, sozialen Medien, Banken, öffentlichen Versorgern, Wearables, etc. über ihn abzufragen.

11 *Angabe von Thoralf Schwanitz (Google Public Policy and Government Relations) auf der Berliner Konferenz „Der Datenmensch“ im Jahr 2016.*

Sie können – je nach Modell – in einem persönlichen Datenspeicher oder Konto zusammengeführt werden. Die ursprünglichen Profile bei Dritten bleiben aber erhalten und werden dort bei weiterer Nutzung des Dienstes fortgeführt. Es handelt sich also grundsätzlich um eine Replikation des Datensatzes. Viele der Systeme erlauben nicht eine Veränderung der Privatsphären-Einstellungen in laufenden Verträgen mit Dritten.

Mit der Zusammenführung soll dem Datensubjekt die Verfügungshoheit über die Daten zurückgegeben werden. Dies kann beispielsweise über die Implementierung eines Dashboards sowie die Visualisierung von Datenströmen oder Datenschutzpraktiken passieren. Dies soll außerdem Probleme der Inversion der Privatsphäre reduzieren, wenn Unternehmen Zugang zu persönlichen Informationen haben zu welchen das Datenschutzsubjekt keinen Zugang besitzt (Gurevich et al. 2016).

Der wohl wichtigste Unterschied zu den gängigen Intermediationsmodellen ist die nutzerseitig veranlasste Datenzentralisation im Gegensatz zur anbieterseitig induzierten Datenzentralisation. Beides könnte künftig unter Umständen sogar koexistieren. Ein Spannungsverhältnis entsteht aber vor allem dann, wenn PIMS-Modelle, durch die Entstehung von Datensätzen, die einen echten Mehrwert darstellen, in unmittelbare Konkurrenz zum gängigen Geschäftsmodell der Drittquellen (soziale Medien, unentgeltlichen Suchmaschinen, etc.) treten.

Es soll auch erwähnt werden, dass manche der neuen Plattformen sich auf der Ebene des Einwilligungsmanagements als reine „Infrastrukturunternehmen“ verstehen (z. B. Digi.me), welche die technischen Applikationen entwickeln und vertreiben, selbst aber weder Daten halten noch Einblick in sie nehmen. Bei einem solchen Modell entstehen Fragen nach anwendbaren Gesetzen oder Regulierungen, wenn beispielsweise das Unternehmen selbst Daten nicht hält (ähnlich wie bei Uber, ein Unternehmen, welches keinen Fuhrpark unterhält).

Standardisierung ist eine wichtige Grundlage für das Funktionieren dieser neuen Plattformen. Zum einen müssen Protokolle, Datenschutzpolitiken und Einwilligungserklärungen maschinenlesbar werden, damit sich Automatisierungspotentiale realisieren lassen. Erwähnt seien hier maschinenlesbare Privatsphären-Präferenzen, die mit Daten reisen können (‚sticky policies‘) oder andere entsprechende Protokolle für den Datenaustausch (EDPS 2016: 9). Eine wichtige Frage in diesem Zusammenhang betrifft auch die Interoperabilität, sowie Standards des vertrauenswürdigen, sicheren Datenaustausches, wie durch das XDI Protokoll der XDI Public Trust Organisation anvisiert.[12]

12 Siehe auch http://xdi.org/

3.2 Taxonomie der Persönlichen Informations-management-Systeme (PIMS)

Die Suche nach trennscharfen Kriterien für die Taxonomie gestaltet sich schwierig. Für die Entwicklung einer Taxonomie böte sich eine Übertragung bekannter Intermediationsmodelle aus der Finanz- und Versicherungswelt an, beispielsweise eine Unterteilung in Informations-Broker, Dealer oder Agent, je nachdem welche Rolle ein Unternehmen in der Verwertungskette einnimmt. Gerade der Begriff des Brokers ist in diesem Zusammenhang schon gängig (Federal Trade Commission 2014).

Beispielsweise führt ein Broker die Vorgaben der Auftraggeber aus, z. B. in Bezug auf Kauf und Verkauf von Daten, wofür Kommission berechnet wird (andere Abrechnungsarten sind ebenfalls möglich). Ein Dealer kauft und verkauft auch aus eigenem (Daten-)Inventar, während ein Agent im Auftrag von nur einer Firma handelt. Letztere ließe sich auf manche Bot-Systeme übertragen. Eine solche Unterteilung zieht eine detaillierte Analyse des Intermediationsmechanismus der jeweiligen Anbieter nach sich – dies kann in der Kürze der Zeit nicht vollständig geleistet werden. Ein exemplarischer Überblick über Firmen wird im Anhang gegeben.

Eine Unterteilung nach Tauschmechanismus (entgeltlich oder unentgeltlich) bietet sich ebenfalls nicht an, da es Systeme gibt, die beides integrieren (z. B. MyDataCan). Außerdem bieten fast alle Plattformen Freemium-Dienste an, da auf der Nutzerseite das Herunterladen einer App oder das Nutzerkonto kostenlos ist (sozialer Tausch). Auf manchen Plattformen kann der Nutzer danach seine Daten verkaufen (ökonomische Transaktion).

Andere Typologien werden von Bründl et al. (2015), Smith und Mitchell (2014) und Young (2015) vorgestellt. Bründl et al. (2015) entwickeln ein Schema, das an Wertschöpfungsketten im deutschen Datenmarkt für echtzeitbasierte Online-Werbung orientiert ist. Dieses Schema eignet nur beschränkt für den Gegenstand dieser Studie, da im Augenblick nicht gesagt werden kann, wie sich Verleger, Datensammler, und Werbetreibende um die neuen Dienste organisieren werden.

In Smith und Mitchell (2014) wird die Branche in Systeme des persönlichen Datenmanagements, Entscheidungsunterstützende Systeme und Lebensmanagement-Systeme unterteilt. Young (2015) unterteilt in VRM, Infomediär-Dienste und Daten-Aggregationsdienste. Viele der analysierten Plattformen integrieren mehrere dieser Funktionen, so dass wir diese nicht als separierende Klassifikationsmerkmale nutzen können.

Dieselbe Überlegung lässt sich auf die vom World Economic Forum (2014: 11) vorgeschlagene Klassifikation in persönliche Analysedienste (personal analytics services), Datengenerierungs-Werkzeuge (datagenerating tools), Datentransfer-Dienste (data sharing tools and services), Profil- oder Persona-Management Systeme (profile/persona management systeme), Datenzugangs- und Löschungsdienste (data access and delention services) anwenden. Das World Economic Forum schlägt dies als „Kartographie des Marktes“ vor. Die Begriffe beschreiben zwar einzelne Mehrwertgenerierende Dienste der Anbieter, sie scheinen aber weniger als Grundlage der Unternehmensklassifikation geeignet, da diese in Mehrheit mehrere dieser Lösungen anbieten.

Der Ausdruck der Plattform scheint zutreffend, da dieser Begriff einen Ort des Austausches beschreibt. Mit dem Begriff ist allerdings noch keine Aussage über den Typus des Anbieters dieser neuen Plattformen getroffen. Der Plattform-Anbieter könnte in einer weitergehenden Untersuchung durchaus mit Agent, Broker oder Dealer beschrieben werden.

Zusammen mit einer Charakterisierung des angewandten Intermediationsmechanismus würde dies ein exakteres Bild ergeben. Diese Typologie kann aber in dieser Kurzanalyse aufgrund des Zeitrahmens nicht geleistet werden. Tabelle 1 präsentiert einen Überblick über die vorgeschlagene Taxonomie.

Tabelle 1 Überblickstabelle Taxonomie (Entwurf)

Anbieter-zentrierte Intermediations-Plattformen	**Nutzer-zentrierte Intermediations-Plattformen**
Mit direkter Kundenbeziehung	**Hub-Modelle**
Google	Data Fairplay
FaceBook	Meeco
Amazon	Digi.me
Ohne direkte Kundenbeziehung	DataCoup
Experian	**Verteilte Systeme**
Schufa	Jolocom
Acxiom	Evernym
BlueKai	KYC-Chain

Der folgende Vorschlag ist angelehnt an die Typologisierung, die in EDPS (2016: 6) vorgeschlagen wird, unterscheidet sich aber in der Feinunterteilung aufgrund des Einbezugs von Technologien. Angesichts der bestehenden Vielfalt soll auf der obersten Ebene folgende Unterscheidung eingeführt werden:

Anbieter-zentrierte Intermediations-Plattformen: Hierbei handelt es sich um die Datenzentralisation wie sie von Unternehmen wie Google, Experian, Acxiom oder Facebook betrieben wird. Diese Intermediationsmodelle können direkten Bezug zum Datenanbieter (Nutzer) aufweisen oder nicht.

Nutzer-zentrierte Intermediations-Plattformen: Hierbei handelt es sich um eigenverantwortliches Nutzer-zentriertes Datenmanagement basierend auf einer technischen Infrastruktur sowie einem vertrauensvollen Rahmen (trust framework). Diese Kategorie lässt sich weiterhin in folgende Subkategorien unterteilen:

- Hub-Modelle: Speicherung der Nutzerdaten auf Basis der Inanspruchnahme privater/öffentlicher Cloud-Dienste, sogenannter on-premises Datencentern oder hybrider Lösungen
    - Zentralisierende Hub-Modelle: Speicherung der Nutzerdaten, Anwendungen oder Daten-Auswertungen auf sicherem Server oder einem Netz an Servern zum Management von Einwilligungen, Autorisierungen, sowie für das Loggen des Datenflusses
    - Lokale, dezentralisierende Hub-Modelle: Speicherung der Nutzerdaten, Anwendungen oder Daten-Auswertungen lokal beim Nutzer auf dessen Endgerät (Handy, Laptop, Tablet, PC, etc.)
- Verteilte Systeme: Speicherung der Daten des Nutzers auf Basis der Distributed Ledger Technology, das heißt in Abwandlungen der Blockchain oder der Blockchain[13]

Plattformen können außerdem in Transaktionsplattformen und Nicht-Transaktionsplattformen unterteilt werden (Filistrucchi et al. 2014). Bei ersterem interagieren die zwei Kundengruppen der Plattform direkt miteinander. PIMS würden hierzu zählen. Bei zweitem besteht keine direkte Interaktion. Dies gilt für viele der Geschäftsmodelle im Marketing, Online-Handel oder der Kreditbeauskunftung.

3.2.1 Hub-Modelle

Viele der hier untersuchten Geschäftsmodelle sind Lösungen, die unterschiedliche Funktionalitäten verbinden, darunter Plattformfunktionen (Marktplatz), Selbstanalyse-Tools, persönliche Clouds oder Komponenten sozialer Netze. Die meist offerierten Funktionen umfassen dabei die Verbindung aller Datensätze und Kuratierungsfunktionen (Aktualisierung, Zufügung und Löschung von Informationen).

Die Modelle in diesem Bereich sind sehr unterschiedlich und können in der Kürze der Zeit nur grob selektiert werden. In den zentralisierenden Hub-Modellen kann eine Speicherung der Nutzerdaten, Anwendungen oder Daten-Auswertungen auf sicheren Servern oder Server-Netzwerken stattfinden. Der Nutzer kann Datenquellen und Datendienste über die Plattform durch Einwilligung und Autorisierung miteinander verbinden. So kann er beispielsweise die Abfrage seiner Daten durch eine App über API-Interfaces (kompatible Dienste) erlauben und die Konditionen hierfür festlegen.
Bei den dezentralisierenden Hub-Modellen soll die Speicherung der Nutzerdaten, Anwendungen oder Daten-Auswertungen dezentral, also lokal beim Nutzer stattfinden. Teilweise können sogar Algorithmen zur Ausführung auf dem Endgerät des Nutzers importiert werden (EDPS 2016: 6). Bei diesen Modellen entstehen Fragen bezüglich der technischen Sicherheit, wenn der Nutzer eigenverantwortlich das Datenmanagement übernimmt.

In allen Modellen jedoch entstehen die sogenannten Metadaten, also Informationen über Parteien, Arten, Zeiten, Dauer und Richtungen von Transaktionen, die über die Plattform abgewickelt werden. Diese werden in Audit-logs gespeichert. Auch hier bestehen Fragen hinsichtlich der Sicherheit und Privatheit dieser Daten, da auch sie Identifikationspotential aufweisen.

13 ‚Distributed Ledger' wird mit dem Begriff des ‚verteilten Kontobuches' übersetzt. Hier soll der englische Fachbegriff benutzt werden. Es gibt in Fachkreisen eine Diskussion darüber ob ‚verteilt' gleichgesetzt werden kann mit ‚dezentral'. Die Autorin bedankt sich bei Joachim Lohkamp für diesen Hinweis. Auf die Diskussion kann hier nicht weiter eingegangen werden.

3.2.2 Verteilte Systeme

Bei der Distributed Ledger Technology (DLT) handelt es sich – stark vereinfach dargestellt – um ein dezentral geführtes Kontobuch oder dezentral geführtes Register von Transaktionen. Es wurde im Zuge der Digitalwährung BitCoin entwickelt. Damit sollte das Problem der potentiellen Mehrfachausgabe einer Einheit der Währung eliminiert werden. Gleichzeitig sollte eine Einheit einem Eigentümer eindeutig zugeordnet werden können. Mittlerweile gilt die Erkenntnis, dass die Anwendung der DLT weit über die der digitalen Währung hinausgeht (Shrier et al. 2016: 4).[14]

Verkürzt dargestellt funktioniert die Technologie wie folgt (s. Jentzsch 2016c): Daten über eine Transaktion, beispielsweise die Bezahlung mit einem BitCoin, werden in einem Datenblock gespeichert. Die im Netzwerk angeschlossenen Rechner prüfen die Transaktion auf Authentizität und Legitimität, bspw. ob der rechtmäßige Eigentümer der Währungseinheit hier agiert. Sollte dies der Fall sein, wird die Transaktion freigegeben und als Block codiert der Kette angehängt (BlockChain). Da jeder Datenblock Informationen über den vorherigen Block beinhält, gilt die Verkettung als kaum manipulierbar. Die Blöcke können rückwirkend nicht gelöscht werden.

Trotz der derzeit kritischen Diskussionen über Schnelligkeit, Energieeffizienz oder Kosten der DLT (vgl. Ali et al. 2014: 7), lässt sich feststellen, dass diese Technologie für sichere Dokumentation, also Notariatsfunktionen, sowie zur selbstständigen Ausführung von Verträgen (sog. smart contracts) eingesetzt werden kann (s. Rosenberg 2016: 2). Diese Möglichkeiten machen die Technologie attraktiv für Anwendungen im Bereich des Identitätsmanagements inklusive des Einwilligungsmanagements. Die Technologie erlaubt es, unter bestimmten Bedingungen auf Mittelsmänner zu verzichten, die Information verifizierende Funktionen übernehmen.

Identitätsattribute wie Name, Geburtsdatum, biometrische Daten oder digitale Signaturen können künftig in der DLT gespeichert und damit dem Datensubjekt eindeutig überantwortet werden. Der Dateneigentümer könnte diese für sichere Authentifizierung einsetzen (Shrier et al. 2016: 5). Der Vorgang würde auch eine Verankerung der Eigentumsrechte an den Identitätsdaten bedeuten.

Manche der hier interviewten Partner waren der Ansicht, dass DLT-basierte Anwendungen sich nicht für hochfrequente Transaktionsdaten eignen. Ihre Hauptanwendung bestünde in der Speicherung sowie der Abfrage von Stammdaten (sog. identity grid). Andere Akteure sind allerdings der Ansicht, dass diese Technologie auch für Anwendungen, bei denen Einwilligungserklärungen dynamisch verändert werden, eingesetzt werden können.

Unternehmen in diesem Segment bieten beispielsweise ein dezentralisierte Datentransfer- und Kollaborationstools an, bei denen der Nutzer eine Web ID, benutzt, die mit seinen persönlichen Daten verbunden ist (z. B. Jolocom). Die Informationen können dann direkt mit den anderen im Netzwerk ausgetauscht werden. Die Firma gibt an, dass Nutzerdaten aus allen möglichen Quellen verlinkt werden können.[15]

14 *Es gibt Systeme, die BlockChain-basiert sind sowie eigene DLT-Systeme. Auf Kosten der Präzision und zur Vereinfachung wird hier nur DLT benutzt.*

15 *Siehe Webseite: http://jolocom.com/#about*

Andere sehen sich als Online-Konto sowie eine Plattform mit API-Anbindung zu Dienstleistern im Bereich des Identitätsmanagements. Die Nutzer besitzen hierbei die Schlüssel zu ihren persönlichen Daten und Identitätszertifikaten. Nach Angaben der Firma sind die Nutzer die einzigen, die entscheiden, mit wem die Informationen geteilt werden und unter welchen Konditionen dies geschehen soll.[16] Andere sind als ‚Identity Grid' (Identitätsnetz) aufgesetzt, so entwickelt Evernym ein DLT-System, das als Open Source Network zu einem globalen Identitätsnetzwerk werden soll.[17] Zweck des Netzes ist die Generierung einer „selbstsouveränen" Identität durch Eigentum am Identitätsgraphen inklusiver der Kontrolle über Produktion, Modifikation, Speicherung, Verbreitung und Löschung der assoziierten Identitätsattribute. Der Zeitrahmen des Gutachtens erlaubt keine detaillierte Analyse der ökonomischen Erfolgschancen, Auswirkungen und Risiken, die mit dieser Technologie verbunden sind. Dies müsste künftige Forschung leisten.

3.3 Nutzer-zentrierte Intermediation als mehrseitiger Markt

Nahezu alle Akteure des im Ökosystem abgebildeten Quadranten für Unternehmen (siehe Abbildung 1) sind als zwei- oder mehrseitige Märkte aufgestellt. Ein Intermediär stellt dabei die Plattform zur Verfügung über welche zwei oder mehrere Kundengruppen interagieren. Auch wenn die Abgrenzung im Einzelnen umstritten sein kann,[18] gelten Plattformen als mehrseitige Märkte, wenn zwei oder mehr Seiten zur Produkterstellung notwendig sind. Bei den hier analysierten Plattformen wären das die Datenanbieter auf der einen Seite (d.h. die Nutzer), sowie die Datennachfrager auf der anderen Seite (Werbetreibende, App-Entwickler, Forschungseinrichtungen, etc.).

Vereinfachend soll ab jetzt von mehrseitigen Märkten die Rede sein. Diese sind im Regelfall durch wechselseitige indirekte Netzwerkeffekte sowie eine nicht-neutrale Preisstruktur gekennzeichnet. Zunächst soll erklärt werden, was Netzwerkeffekte sind, um dann kurz auf die Nicht-Neutralität der Preisstruktur einzugehen.

Direkte Netzwerkeffekte entstehen auf derselben Marktseite, insbesondere dann, wenn ein Nutzenzuwachs aus der Nutzung des Dienstes durch andere entsteht. Bei PIMS könnte das ein sicherer Datenaustausch mit anderen PIMS-Nutzern sein gegenüber der Nutzung anderer Technologien.[19]

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.

Die Nicht-Neutralität der Preisstruktur ergibt sich, wenn das Transaktionsvolumen der Plattform maßgeblich durch die Preissetzung nach beiden Seiten beeinflusst wird (Rochet und Tirole 2003). Dies soll hier nicht weiter vertieft werden.

16 Siehe Webseite: http://kyc-chain.com/#about

17 Siehe Webseite: http://www.evernym.com/

18 Siehe unter anderem: Filistrucchi et al. (2014) und Luchetta (2014).

19 Für ein entsprechendes Beispiel sei der Leser auf die Darstellung der persönlichen Clouds in Reed (2013: 15 ff.) verwiesen.

Die Plattform könnte sich – wie an anderer Stelle in diesem Bericht genannt – über Lizenzen, Teilnahmegebühren oder Transaktionsgebühren finanzieren. Werbefinanzierte Angebote, wie dies bei vielen Freemium-Diensten derzeit der Fall ist, werden in dieser Domäne nach derzeitigem Kenntnisstand eher nicht angestrebt.

Wie später noch ausführlicher erläutert wird, unterliegen Märkte, in welchen die Plattform das dominante Geschäftsmodell darstellt, starken Konzentrationstendenzen. Es scheint einen Punkt oder eine kritische Masse an Nutzern zu geben, ab welcher eine solche Plattform nonlineares Wachstum aufweist (sog. tipping point). Dies kann in stark asymmetrische Marktanteile münden, wobei ein dominanter Anbieter existiert, während andere Plattformen keine bedeutende Rolle spielen. Diese Art der Wettbewerbsdynamik wird aller Voraussicht nach auch in den PIMS-Märkten entstehen.

3.4 Anreize für Nutzer und Unternehmen

Mehrseitige Märkte unterliegen fast ausschließlich dem Problem, dass sie zwei oder mehr Kundengruppen gleichzeitig anziehen müssen, um attraktiv zu werden. Um sich am Markt durchsetzen zu können muss eine Plattform Nutzer, welche Daten einlegen, und Unternehmen, welche die Daten abfragen, gleichzeitig anbinden. Der Nutzen für die Kundengruppen hängt indirekt voneinander ab, was ein mehrseitiges Start-up-Problem generieren kann. Im Folgenden sollen die Vor- und Nachteile der Nutzung solcher Plattformen für Nutzer wie auch Unternehmen dargestellt werden.

Wichtig ist auch anzumerken, dass eine Plattform nennenswerte Nutzerzahlen erreichen muss, um ihren Mehrwert gegenüber den momentan existierenden Intermediationsmodellen zu beweisen.

3.4.1 Anreize für Plattform-Nutzer

Auf der Nutzerseite basiert die Entscheidung über die Nutzung einer solchen Plattform auf Erwägungen in Bezug auf ihren erwarteten Nutzen. Diese Erwägung lässt sich als Kosten/Nutzen-Kalkül darstellen: Der erwartete Nutzen aus der Teilnahme an der Plattform muss den erwarteten Aufwand übersteigen. Vorteile für Kunden sind unter anderem die übersichtliche Darstellung der verteilten Daten sowie die Übernahme vermehrter Kontroll- und besserer Durchsetzungsmöglichkeiten von Verfügungsrechten u. a. über eine Dashboard-Applikation. Große Vorteile bestehen auch in der Ermöglichung von automatisierten Einwilligungserklärungen machine-to-machine (M2M) Kommunikation. Kunden können außerdem den Zugang zu neuen Apps erhalten, z. B. Selbstanalyse-Tools oder Entscheidungsmaschinen für die Produktsuche. Letzteres wird möglich durch ein automatisiertes Matching von Kunden-Präferenzen mit Produkteigenschaften. Sollten Kunden weitere Daten in ihre Profile einpflegen können (sog. intent casting), könnte dies zu passgenaueren Angeboten führen, da diese zusätzlichen Informationen unter Umständen ihre Präferenzen besser abbilden.

Es sind auch Dienste denkbar, bei welchen ein persönlicher Assistent dem Nutzer behilflich ist, die Datenströme aus dessen ‚persönlichen Big Data Speicher' zu verwalten (EDPS 2016: 7). Künftig könnten dann auch neue, peer-to-peer Dienste möglich sein, bei denen sich Handelspartner gegenseitig Vertrauenswürdigkeit signalisieren können.

Die Plattformen könnten einen vermehrten Schutz vor Tracking, Personalisierung oder Preisdiskriminierung implizieren – müssen sie aber nicht. Dies wird ganz maßgeblich von der technischen Umsetzung abhängen. Außerdem könnten sie Dienste erlauben, die beispielsweise die Datenschutzpolitiken von Apps vergleichen.

Nachteile für Nutzer ergeben sich in diesem Zusammenhang aus den Einstellungen, die ein Nutzer vornehmen muss.[20] Dazu gehört – je nach Plattform – das Runterladen und Installieren von Software, einer App oder das Aufsetzen einer persönlichen virtuellen Maschine. Nutzer sollen – so das Argument der Plattformen – ihre Privatsphäre besser durch Datenkonzentration und -replikation schützen. Dafür werden Informationsgewinnung (z. B. Selbstanalyse) sowie monetäre Anreize gesetzt.

Die Plattformen müssen also zunächst eine erhebliche Vertrauensschwelle beim Nutzer überwinden. Das Geschäftsmodell sowie bestimmte Selbstverpflichtungen, beispielsweise der Plattform keinen Zugang zu den Daten zu gewähren, kann dem durchaus zuträglich sein (s. bspw. MesInfos, Digi.me). Eine Reihe von weiteren Maßnahmen kann dafür sorgen, dass Vertrauen geschaffen werden kann: dezentralisierte Speicherung, lokale Speicherung beim Nutzer oder Depersonalisierung der Daten gegenüber interessierten Unternehmen.

Nichtsdestotrotz werden Daten u.U. in sehr viel größerem Ausmaß zur Verfügung gestellt.

Trotzdem bestehen Fragen der beim Nutzerverankerten Sicherheit, sowie der Verantwortlichkeit durch die komplette Überantwortung von Einwilligungsprozessen, die den Nutzer sogar zum ‚self-operator' (My Data Architecture 1.2.1: 13) werden lassen könnten.

Bei der Einwilligung wäre zu fragen, wie detailliert diese wird, auch im Hinblick auf M2M-Kommunikation. Eine unklare Sprache oder ungenaue Kategorisierung könnte auch hier zu einer Fehlabbildung der Nutzerpräferenzen führen, wenn er beispielsweise nicht versteht, was mit ‚Personalisierung' gemeint ist.

Nutzern ist es wohl kaum zu untersagen, ihre Daten bei mehreren Plattformen gleichzeitig einzulegen. Bei einer angestrebten Standardisierung und Datenportabilität zwischen den Plattformen wird dies sogar vereinfacht (s.a. MyData Initiative). Während dies einerseits Einschlusseffekte für Nutzer verhindern kann, führt es zu vermehrtem Wettbewerbsdruck unter den gewinnorientiert arbeitenden Plattformen. Der Nutzer müsste dann nicht mehr wählen, bei welcher Plattform er den besten Daten-Deal bekommt, sondern könnte alle Plattformen dieser Art nutzen, weil dies seinen Gewinn aus dem Verkauf immer erhöht. Dies würde den Differenzierungsdruck unter den Plattformen erhöhen.

20 Dies steht im Vergleich zum automatischen Einlesen von Einstellungen, die ein Nutzer auf Diensten bereits vorgenommen hat.

3.4.2 Anreize für Unternehmen als Datennachfrager

Unternehmen können künftig theoretisch zwischen mehreren Intermediationsmechanismen wählen. Zum einen könnten sie eine eigene Plattform starten (z. B. Gruppo Telecom Italia, Deutsche Telekom), zum anderen auf traditionelle Datenaggregatoren zugreifen (z. B. Experian) oder die neuen Plattformen nutzen. Unter Umständen bestehen die drei Optionen sogar nebeneinander, insbesondere dann wenn sich die Datenprofile qualitativ unterscheiden.

Vorteile für Unternehmen: Für Unternehmen, die persönliche Daten nachfragen, werden die neuen Plattformen nur dann interessant, wenn dort Daten und Dienste entstehen, welche einen echten Mehrwert darstellen. Dieser Mehrwert könnte tatsächlich in der anvisierten Verknüpfung der Daten liegen, was einen Zugang zu sehr viel detaillierteren Profilen ermöglichen würde.

Zusätzlich erlauben manche Plattformen Nutzern die Einmeldung eigener Daten (z. B. Citizen.me). Dies könnte eine bessere Identifizierung der Kunden-Präferenzen sowie anderer Faktoren, Preissensitivität und Transaktionsrisiko, ermöglichen. Der Vorteil wäre hier die Entstehung von Echtzeit-Daten über Kaufabsichten und Kundenpräferenzen, die momentan als besonders wertvoll angesehen werden.

Ein Interviewpartner betonte, dass Unternehmen die Möglichkeit sehen, das gesamte Management der Datenerschließung und –weitergabe zu outsourcen.

Es ist offen, ob sich im Zuge der Corporate Responsibility für Unternehmen durch die Teilnahme an einer solchen Plattform ein Differenzierungsmerkmal im Wettbewerb ergibt. Schließlich wurden solche Plattformen in der Vergangenheit auch schon als „ethische Marktmodelle“ bezeichnet (Young 2015). Unter Umständen würde dies Unternehmen ermöglichen, eine neue Art des Vertrauensverhältnisses mit den Kunden aufzubauen.

Nachteile für Unternehmen: Derzeit besteht unter Unternehmen Unsicherheit, was die Umsetzung der EU-DSGVO angeht. Hier könnten Plattformen EU-DSGVO konformes Einwilligungsmanagement ermöglichen. Nach Erfahrung mancher hier interviewten Personen, gibt es Unternehmen in verschiedenen Branchen, die eine grundsätzliche Neuordnung von IT-Strukturen mit Implementierung der EU-DSGVO für notwendig halten.

Andere Unternehmen scheinen da zurückhaltender und dritte wiederum halten die neuen Plattformen für nicht mehr als eine technologische Modeerscheinung.

Sollten Nutzer ihre Profile über die Plattform konkurrierenden Unternehmen verkaufen, dann erhöht dies den Wettbewerbsdruck unter diesen Unternehmen. Sollten konkurrierende Unternehmen Zugriff auf dieselben Daten haben, erbringen diese kaum einen Wissensvorsprung.[21] Die Wettbewerbsdynamiken in einem solchen Umfeld sind komplex und von mehreren Faktoren abhängig, s. hierzu Jentzsch (2017).

Es bestehen auch Fragen nach den Sorgfaltspflichten der Plattformen im Hinblick auch die Identitätsfeststellung der Nutzer (due diligence). So müsste verhindert werden, dass sich eine Plattform einen Wettbewerbsvorteil durch synthetische Profilbildung von Nutzern verschafft oder sich nicht vertrauenswürdige Dienste anmelden, die Nutzerdaten abfragen.

21 Dies gilt nur unter der vereinfachten Annahme, dass sich die Unternehmen in ihren Analysetechnologien nicht stark unterscheiden.

Von einem analytischen Standpunkt aus gesehen, könnten sich die erwähnten Selektionseffekte (s. Abschnitt 3.5) und eine inhomogene Datenbasis nachteilig auf die Qualität der Daten auswirken. Sollte die Plattform den Nutzern Feineinstellungen bei den Vertrauens-Ebenen und Privatsphären-Settings ermöglichen, würden die Daten granulierter und unter Umständen weniger umfassend.

Ein Interessenskonflikt zwischen Nutzern und Unternehmen ergibt sich dann, wenn Kunden die Zweckbindung klar definieren und bestimmte Datenauswertungen komplett 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. Dies könnte dazu führen, dass sich Unternehmen über Zertifikate auf bestimmte Zweckbindungen verpflichten müssen. Insgesamt lässt sich festhalten, dass eine signifikante Masse von Kunden und Unternehmen sich umorientieren muss, damit diese Plattformen langfristig rentabel sind.

3.4.3 Anreize für andere Teilnehmer

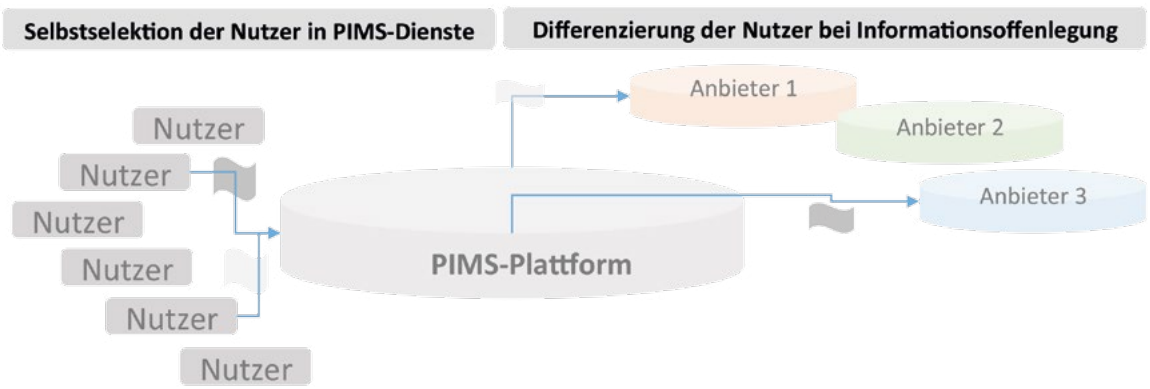
Unternehmen und Einzelpersonen, die Apps entwickeln können über so eine Datenbank u.U. auch auf bessere, vielfältigere und detaillierte Datensätze zugreifen, wie dies momentan der Fall ist. Diese Entwickler und Zugriffe können in einem Dienste-Register aufgeführt werden (MyData Architecture 1.2.1: 14).

Auch für andere Stakeholder ergeben sich Potentiale aus der Teilnahme an solchen Plattformen. So könnten Forschungsunternehmen auf die Datensätze zugreifen. Manche Plattformen implementieren dies quasi ähnlich einer ‚Spende', wobei es sich hier um eine ‚Datenspende' handelt. Schlussendlich hat ein Interviewpartner auch erwähnt, dass selbst zumindest ein großes IT-Unternehmen Interesse an der Kooperation mit einer solchen Plattform angemeldet hat. Das Interesse speist sich aus dem Bedürfnis auf weitere Datensätze der Nutzer aus der Offline-Welt zugreifen zu können.

3.5 Selbstselektion und Datenqualität

Abbildung 5 zeigt die generische Darstellung einer PIMS-Plattform. Auf der Datenangebotsseite befinden sich die Nutzer, welche ihre persönlichen Informationen direkt bzw. durch Autorisierung Dritter einlegen (hier nicht dargestellt, s. Abbildung 4).

Abbildung 5 Nutzung von PIMS-Diensten



Selbstselektion der Nutzer in PIMS-Dienste: In einem ersten Schritt kann davon ausgegangen werden, dass bei Freiwilligkeit sich nur bestimmte Nutzer für solche Systeme entscheiden werden. Dabei handelt es sich um jene für die der Nutzen den Aufwand übersteigt. Auf der Nutzerseite handelt es sich also zunächst um eine präselektierte Auswahl von Individuen, die ihre Daten einlegen. Dies ist keine repräsentative Auswahl aus der Bevölkerung, ein Phänomen, das in Bezug auf Social Media Plattformen bereits bekannt ist (Ruths und Pfeffer 2014).

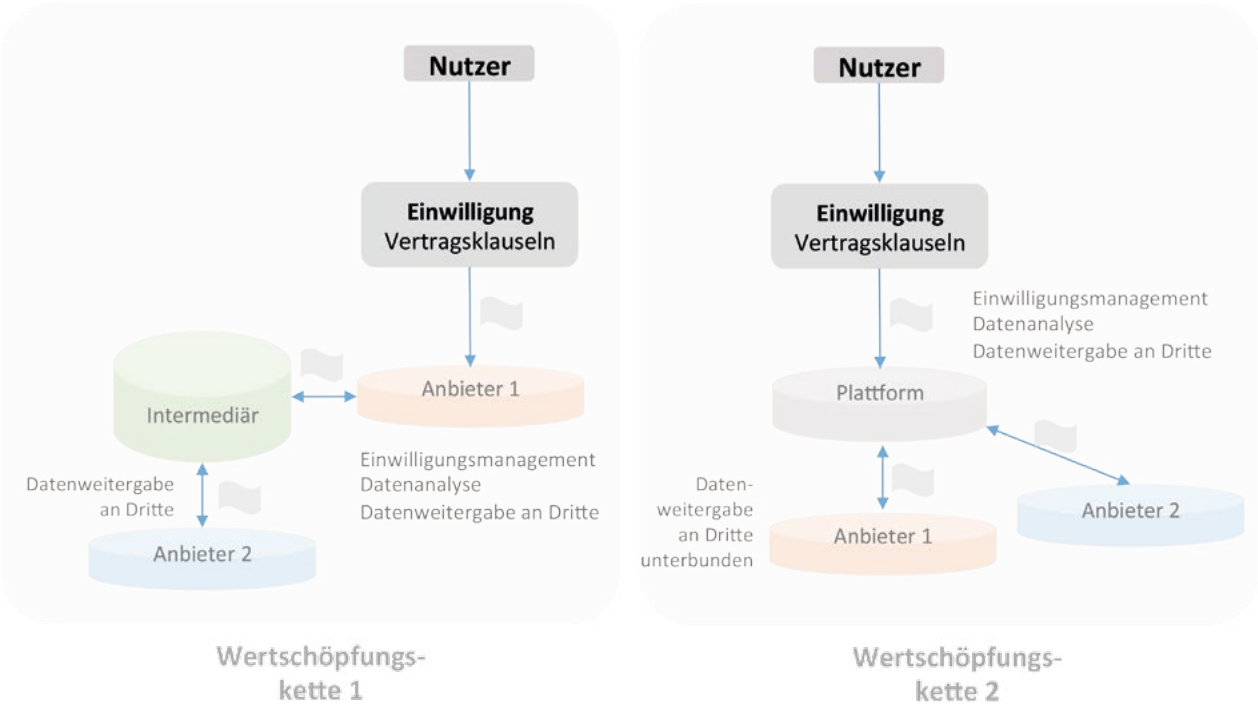
Differenzierung der Nutzer bei Informationsoffenlegung: In einem zweiten Schritt kann davon ausgegangen werden, dass nur ausgewählte Nutzer bestimmte persönliche Informationen offenlegen werden, um diese beispielsweise zu verkaufen (Peppet 2011). Es ist in ökonomischen Experimenten gezeigt worden, dass Probanden, die in einem sozialen Vergleich schlecht abschneiden (z. B. schlechtes Testresultat) diese Informationen entweder zu einem höheren Preis oder mit geringerer Wahrscheinlichkeit verkaufen (Feri et al. 2016, Huberman et al. 2005, Jentzsch 2014). Die Ausprägung einer Variablen ist also in manchen Umständen mit ihrer Bewertung durch den Träger der Eigenschaft korreliert. Die Teilnahme am Handel oder die Preissetzung kann dann als Signal gelesen werden.

Gleichzeitig können Nutzer unter Umständen ihre Einwilligung jederzeit entziehen. Auch hier können sich intertemporale Selektionseffekte ergeben, die sich auf die Datenqualität und Verfügbarkeit der Datenbasis auswirken.

3.6 Einwilligungsmanagement in vertikalen Wertschöpfungsketten

Im Folgenden soll eruiert werden, welche Wertschöpfungsketten im Bereich des Einwilligungsmanagements existieren. Dies findet grob vereinfacht statt und dient lediglich der schematischen Darstellung der Unterschiede der Modelle, siehe Abbildung 6. In der Abbildung (Wertschöpfungskette 1) zeigt sich, dass im derzeit gängigen Intermediationsmodell der Nutzer bei Anbieter 1 vertragliche Bedingungen eingeht und mit ihnen die Einwilligung in die Datenverarbeitung akzeptiert. Je nach Bündelung der Klauseln kann dies eine Datenweitergabe an Dritte beinhalten. Beispiele hierfür sind die Märkte für Wirtschaftsauskünfte, inklusive Kreditauskünfte.

Abbildung 6 Wertschöpfungsketten im Einwilligungsmanagement



In dem Schaubild zeigt die Wertschöpfungskette 2 die anvisierte Neuorganisation dieser Intermediation in der vertikalen Wertschöpfungskette der Datenverarbeitung. Hier würde der Nutzer über die Plattform qua Konto, Software (Bot) oder ähnlichem seine Einwilligung in maschinenlesbarer Form Anbietern übermitteln. Eine weitere Weitergabe an Dritte (hier: Anbieter 2) könnte durch entsprechende Privatsphären-Einstellungen unterbunden werden, hier beispielshaft dargestellt. Falls viele Nutzer eine Zweitverwertung untersagen, könnte Daten-Brokern tatsächlich das Geschäftsfeld entzogen werden.

In diesem Zusammenhang soll nicht unerwähnt bleiben, dass viele der Akteure in diesen Wertschöpfungsketten Zusagen über Anonymisierung und Pseudonymisierung der Daten machen. Wie schwierig eine solche Depersonalisierung ist wurde in anderen Zusammenhängen gezeigt, z. B. für Mobilfunk- und andere Datensätze (s. de Mulder et al. 2008; de Montjoye et al. 2013, 2015; Narayanan und Shmatikov 2008) und werden aktuell kontrovers diskutiert.[22]

22 *Siehe auch Brussels Privacy Forum 2016 (https://fpf.org/brussels-privacy-symposium/)*

4. Dynamiken in Märkten der persönlichen Datenökonomie

Im Folgenden sollen in Kürze grundlegende Dynamiken aus dem Bereich der Intermediation in digitalen Märkten dargestellt werden, in welchen Informationsgüter bestehend aus persönlichen Daten gehandelt werden. Diese Märkte sind durch komplexe Wettbewerbsdynamiken gekennzeichnet, welche gerade junge Unternehmen vor große Herausforderungen stellen können.

Die wichtigsten Aspekte des Wettbewerbs sollen hier diskutiert werden. Es ist bereits konstatiert worden, dass sich die neuen Anbieter im Wettbewerb mehrseitiger Plattformen befinden. Sie müssen beispielsweise gleichzeitig Nutzer, Unternehmen und API-Entwickler anziehen. Sie bieten darüber hinaus ein personalisiertes Informationsgut an und in den meisten Fällen wird eine Freemium-Strategie eingesetzt – die Nutzung der Plattform ist für Datenanbieter unentgeltlich. Die Differenzierung der Plattformen im Wettbewerb findet über die angebotene Technologie, die Funktionalitäten sowie die Datensicherheit statt. Derzeit kann jedoch noch nicht von intensivem Wettbewerb ausgegangen werden, zu Recht ist die Entwicklung der persönlichen Datenökonomie als ‚embryonal' bezeichnet worden (Juniper Research 2016: 4). Zusätzliche Herausforderungen für die neuen Anbieter entstehen durch die rechtlichen Rahmenbedingungen (Riechert 2017), die nicht Gegenstand dieser Untersuchung sind.

4.1 Wettbewerb der Plattformen in der persönlichen Datenökonomie

Eine Plattform steht unter dem Druck, schnell hohe Nutzerzahlen erreichen zu müssen, da sich durch direkte und indirekte Externalitäten positive Effekte ergeben, die nonlineares Wachstum implizieren sobald eine kritische Masse an Nutzern überschritten wird (Economides 1996). Bei diesen Märkten resultieren aus den Wettbewerbsdynamiken extreme Asymmetrien der Marktanteile und Gewinne (Economides 2001).

Im Bereich der PIMS müssen sich die neuen Anbieter auf der einen Seite gegen akademische Gratisangebote (MyDataCan oder OpenPDS) durchsetzen. Zum anderen müssten sie sich gegen traditionelle Informationsintermediation (Direktmarketing, etc.) durchsetzen, um mehr Datennachfrage zu generieren. Gerade die großen Konzerne können jederzeit in den Markt des innovativen Einwilligungsmanagements eintreten.[23]

Sollten die Anbieter in der ‚traditionellen' Informationsintermediation weiterhin dritte Datenquellen nutzen können wird in der Datenanalyse gegenüber dem Individuum auch künftig eine Informationsasymmetrie existieren. Nutzer der PIMS wissen in diesem Fall nicht, ob das von ihnen genutzte soziale Netz auch andere Daten zukauft und wie es diese analysiert.[24]

23 *Auch wenn viele dieser Offerten nicht die vollständige Datenhoheit den Kunden überanworten, erlauben sie erhöhte Kontrollmöglichkeiten. Ein Beispiel hierzu ist Oracle Data Cloud Registry, die Anwendung zeigt dem Kunden seine mit BlueKai & Datalogix Cookies verbundenen Interessen. Diese kann er löschen. Dies ist zwar ein Beispiel aus dem US-amerikanischen Raum, es zeigt aber, dass Unternehmen Zugriffs- und Kontrollwünsche von Kunden zunehmend wahrnehmen.*

24 *Reilly, M. (2016). How Facebook Learns About Your Offline Life, MIT Technology Review, https://www.technologyreview.com/s/603283/how-facebook-learns-about-your-offline-life/*

Aus der ökonomischen Theorie ist bekannt, dass die Wettbewerbsintensität zunimmt und Industriegewinne abnehmen, wenn im Modell zwei Firmen anfangen, Produkte zu personalisieren (Syam et al. 2005, Zhang 2011). Sollten sie dies bei gleichzeitiger Setzung von Standard-Preisen tun, landen sie im Gefangenen-Dilemma. Dies können sie verhindern, wenn sie auch Preise personalisieren (Ghose und Huang 2009). Diese Option ist allerdings dann nicht vorhanden, wenn es sich um Märkte handelt, in denen eine Gratisdienstleistung bereitgestellt wird (s.a. Evans 2011). Hier entfällt der Preis als Wettbewerbs- und Personalisierungsparameter.

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.

Zusätzliche Herausforderungen für die jungen Unternehmen entstehen durch die Kommodifikation von persönlichen Informationen als handelbarem Gut, die im nachfolgenden Abschnitt besprochen wird.

4.2 Persönliche Informationen als handelbares Gut

Um persönliche Informationen zu kommodifizieren, also in ein handelbares Gut zu überführen, müssen Eigentumseigenschaften über vertragliche Verfügungs- und Kontrollrechte hergestellt werden. Durch die originären Eigenschaften von Informationen kann dies die Vertragsparteien vor große Herausforderungen stellen. Zum einen sind Informationen ‚immateriell' also nicht an ein bestimmtes Medium gebunden (Jentzsch 2016b). Durch die Preisgabe seitens des Individuums reduziert sich kein Budget,[25] dies bedeutet, dass bestimmte Anreizbeschränkungen entfallen. Es besteht daneben Nicht-Rivalität im Konsum – Informationen verbrauchen sich nicht durch ihren Konsum. Im Bereich der PIMS bedeutet dies, dass mehrere Marktteilnehmer die Datenprofile nutzen können. Gleichzeitig könnte der Nutzer aber seine Datenprofile auch bei mehreren PIMS-Anbietern einlegen, um so den Datenverkauf und dadurch den Verdienst zu steigern.

Sobald Informationen kompiliert werden, ist es schwierig, bisweilen unmöglich andere von ihrer Nutzung auszuschließen. Dies wird mit Nicht-Ausschließbarkeit bezeichnet. Im Bereich der PIMS müssten Drittparteien (abfragende Unternehmen) vertraglich zu bestimmten Zweckbindungen angehalten werden und Vertragsabweichungen sanktionierbar sein. Ohne ein ausgereiftes System der Sorgfaltspflicht für gerade kleinere Drittparteien wird dies ein schwieriges Unterfangen.

Die Eigenschaften der Nicht-Rivalität sowie der Nicht-Ausschließbarkeit ergeben zusammengenommen das, was in der Wirtschaftswissenschaft unter dem Begriff der öffentlichen Güter verstanden wird. Bestehen Nicht-Rivalität und Ausschließbarkeit, so spricht man von einem Club-Gut.

Es bestehen außerdem Informations-Externalitäten. Externalitäten sind Einflüsse auf den Nutzen anderer im Marktgeschehen, die nicht über den Preis kompensiert werden. Sie treten besonders deutlich im Unraveling-Prozess hervor (s. Abschnitt 4.5). Externalitäten entstehen auch durch Datenanalyse. Beispielsweise erlaubt die Kombination von Variablen (z. B. Alter, Wohnort, Geschlecht, Automarke) das Extrahieren zusätzlicher Informationen (z. B. geschätztes Einkommen).

25 *Durch Informationspreisgabe kann sich die Privatsphäre reduzieren, diese stellt aber kein Budget im ökonomischen Sinne dar.*

Aufgrund dieser Externalitäten und der Möglichkeit Daten mehrfach für verschiedene Zwecke zu verwenden, ist ihre ökonomische Bewertung komplex.

Handelt es sich bei Informationen um persönliche Daten, sind zwei weitere Eigenschaften qua definitionem die der Differenzierung und Identitätsbezogenheit. Ökonomische Handlungsweisen verändern sich durch die psychologischen Effekte der Identifizierbarkeit. Dies evoziert unter anderem soziale Präferenzen (Charness und Gneezy 2008, Feri et al. 2016, Haley et al. 2005). Gleichzeitig gelten Informationsgüter auch als Erfahrungsgüter, da ihre Qualität erst durch Konsum ersichtlich wird. Die Eigenschaft des Erfahrungsgutes gilt für die von den PIMS angebotenen Dienste – im Hinblick auf deren Cybersicherheit.

Da die Aggregation persönlicher Daten und Auswertungen derselben Privatsphären-Bedenken hervorrufen können, müssen Plattformen zunächst eine Vertrauensschwelle beim Nutzer überwinden. Diese Vertrauensbildung kann unter anderem über Datenschutzfreundlichkeit sowie technische und protokollarischer Sicherheit in der Wertschöpfungskette erreicht werden.

4.3 Monetarisierung persönlicher Informationen

Unter Monetarisierung persönlicher Informationen soll hier der Verkauf persönlicher Daten durch eine Marktpartei verstanden werden. Andere Methoden und Arten der quantitativen Datenbewertung sollen hier nicht diskutiert werden (s. dazu Jentzsch 2016b; OECD 2013). Bislang wird ein großer Teil des Datenverkaufs in verschiedenen Märkten (z. B. durch Direktmarketing) ohne direkte Beteiligung des Datensubjekts an der Transaktion durchgeführt. Die Informationen an sich werden auch nicht transferiert, vielmehr wird der potentielle Zugang zu Kundengruppen mit bestimmten Merkmalen bereitgestellt. Neu ist, dass durch die Plattformen das Datensubjekt direkt als Datenverkäufer seiner Datensätze auftreten kann, was die Verhandlungsmacht stärken kann.

Ein direkter Verkauf impliziert die Frage, 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.

Die Plattform bringt über den eingesetzten Mechanismus Datenangebot und Datennachfrage zum Ausgleich. Auf der einen Marktseite werden Datenanbieter (Nutzer) den höchsten Preis für ihre Daten erzielen wollen. Auf der anderen Marktseite wollen Datennachfrager (Unternehmen) qualitativ hochwertige Informationen zum niedrigsten Preis kaufen. Daher ist ein Mechanismus wünschenswert, der eine anreizkompatible Wertschätzung des gehandelten Informationsgutes impliziert. Käufer sollten einen Anreiz haben, die individuelle Wertschätzung des Informationsgutes wahrheitsgemäß offenzulegen.

Gleichzeitig müsste der Mechanismus oder Begleitmaßnahmen desselben die wahrheitsgemäße Offenlegung der persönlichen Daten absichern.[26] Sollte dies nicht der Fall sein, könnten Nutzer verschiedene, auch teils unrichtige Profile verkaufen, um ihren Payoff zu maximieren.

26 Sollte dies nicht der Fall sein, könnten qualitativ schlechtere Informationen bessere aus dem Markt treiben, wie dies im Zitronenmodell bei Autos unterschiedlicher Qualitäten der Fall ist (Akerlof 1970).

Sie könnten auch Interesse falsch darstellen, um strategisch die Nachfrage nach den Datenprofilen zu erhöhen. An dieser Stelle muss konstatiert werden, dass die Frage des Marktmechanismus in die komplexe Literatur des sogenannten Mechanism Design führt. Darunter fallen auch Preisbildungsmechanismen in Auktionen und ähnliches. Der Umfang und Zeitrahmen des Gutachtens lässt keine detaillierte Diskussion dieser Fragen zu. Dasselbe gilt auch für die Frage, ob und wie Individuen für Privatsphären-Bedenken kompensiert werden sollen (s. u. a. Aperjis und Huberman 2012, Chellappa und Shivendu 2010, Jentzsch 2014 und Nissim et al. 2015).

Auch wenn im Rahmen dieser Kurzexpertise kein tiefer Einstieg in die Diskussion um Anreizkompatibilität des Auktionierens persönlicher Daten geleistet werden kann, kann dennoch festgestellt werden, dass für die Implementierung anreizkompatibler Auktionen in Online-Plattformen die Datenschutz-Protokolle von maßgeblicher Bedeutung sind (vgl. hierzu Huberman et al. 2005; Horowitz 2006; Jentzsch 2014, Joshi et al. 2005).

Zusammenfassend lässt sich festhalten, dass es für die neuen Marktspieler wichtig sein wird, Mechanismen zu implementieren, die Privatsphäre sicher- und Anreizkompatibilität herstellen und dies unter Anwendung kryptographischer Protokolle tun. Eine Stärkung der Forschung in diesem Bereich wäre unbedingt notwendig.

4.4 Verhaltensökonomische Forschung zur Einwilligungserklärung

Die Einwilligung ist der Ausdruck der Willenserklärung zur Informationspreisgabe eines Verbrauchers im vertraglichen Verhältnis. In diesem Kontext ist es wichtig zu verstehen, dass unterschiedliche Arten der Transaktionen (so entgeltliche vs. unentgeltliche) unterschiedliche Kalküle im Verbraucher evozieren. Neben dieser Feststellung kann davon ausgegangen werden, dass ein besserer Transfer von verhaltensökonomischen Erkenntnissen tatsächlich förderlich für die Entwicklung der PIMS-Plattformen sein könnte.

Zum einen könnte eine automatisierte Abbildung von Privatsphären-Präferenzen zu einer erhöhten Entscheidungszufriedenheit der PIMS-Nutzer führen. Zum anderen können PIMS-Anbieter durch den Einsatz von Nudges (Methoden der Verhaltensbeeinflussung) ebenfalls für eine höhere Entscheidungsqualität sorgen. Ein Beispiel wäre das effektive Timing von DatenschutzInformationen in einer Kaufentscheidung (Kelley et al. 2013). Hier bieten die PIMS-Dienste große Potentiale. Unter Umständen könnte es durch die Automatisierung der Einwilligungsentscheidung möglich sein, Verhaltensverzerrungen vorzubeugen und die Entscheidungen des Nutzers auf einen rationaleren Entscheidungspfad zu lenken.

4.4.1 Privatsphären-Kalküle und Affektentscheidungen

Im ökonomischen Kalkül würde ein rationaler Entscheider die Kosten der Informationspreisgabe gegen ihren Nutzen abwägen. Unter Bedingungen vollständiger Information würde er – theoretisch gesehen – seinen erwarteten Nutzen maximieren. Die Kontextualisierung oder Art der Entscheidungsdarstellung dürfte keine Rolle spielen: der Entscheider würde immer die optimale Wahl treffen. Bei Vorliegen von Intransparenz, systematischen Verhaltensanomalien oder Präferenz-Unsicherheit kann man allerdings nicht automatisch von einer optimalen Wahl ausgehen. Dies wird detaillierter in Abschnitt 4.4.2 diskutiert.

Zuerst soll festgehalten werden, dass bei Verbrauchern nicht immer ein Kosten-Nutzen-Kalkül über die Informationspreisgabe abläuft. Einer der Gründe hierfür ist, dass bei vielen Transaktionen, welche persönliche Daten involvieren, keine spürbaren Kosten entstehen.[27] Durch die Angabe wird kein ‚Budget' reduziert, stattdessen kann der Verbraucher seine Daten vielfach preisgeben (s. Abschnitt 4.2).

In diesem Kontext gilt es, die verschiedenen Arten der Transaktionen voneinander zu unterscheiden, wie in Tabelle 2 dargestellt. Es muss an dieser Stelle festgehalten werden, dass auch Kombinationsformen dieser Transaktionsarten vorliegen können. Dies ist zum Beispiel der Fall, wenn durch den Kauf eines Gutes die Informationspreisgabe quasi als Beifang des Kaufs auftritt, wie dies bei Online-Käufen üblicherweise der Fall ist. Hier bildet ist der Preis oder die Qualität des Produkts den Fokuspunkt des Verbrauchers – dies lenkt ihn unter Umständen von den Bestimmungen des Datentransfers ab. Wie bereits erwähnt, kann durch effektives Timing (Kelley et al. 2013) oder Visualisierung (Egelman et al. 2009) ein stärkerer Einbezug der Datenschutzfaktoren in die Entscheidung des Nutzers evoziert werden.

Tabelle 2 Privatsphären-Kalkül und Affektentscheidung

Sozialer Tausch (a)	Ökonomischer Tausch (b)
Preis als Numéraire ist entfernt Gratisgüter	Preis ist Numéraire
Preisvergleiche nicht möglich	Preisvergleiche möglich
Keine Reduktion Budget	Reduktion Budget (Anreizbeschränkung)
Affektentscheidung (Affekt überlagert Ratio) Akzeptanzschwelle geringer im Vgl. zu (b)	**Kosten-Nutzen-Kalkül** Akzeptanzschwelle höher im Vgl. zu (a)
Beispiele: Suchmaschinen, soziale Netzwerke, Freemium-Software	**Beispiele:** Datenverkauf auf PIMS-Plattform, Preisreduktionen bei Kundenkarten

27 *Ausgenommen sind hier Kosten der Privatsphäre. Kosten der Privatsphäre können in manchen Situationen, z. B. bei Preisdiskriminierung, approximativ quantifiziert werden (Jentzsch 2016d).*

4.4.2 Erkenntnisse aus der empirischen Forschung zu Einwilligungen

Aus der empirischen Verhaltensökonomik sowie der Marktforschung ist bekannt, dass konstatierte Präferenzen (stated preferences) nicht oder nur schwach mit offenbarten Präferenzen (revealed preferences), also Wahlhandlungen, zusammenhängen. Es ist wenig überraschend, dass dieses Phänomen auch in der Forschung zur Privatsphäre gefunden wird. Dort wird es unter dem Begriff des Privatsphären-Paradoxon diskutiert (Norberg et al. 2007).[28]

Künftig sollen die neuen Plattformen es Nutzern erlauben, die Privatsphären- und Vertrauenseinstellungen ihrer Anwendungen optimal ihren Präferenzen anzupassen. Die Präferenzen der Informationspreisgabe könnten dann mit den Wahlhandlungen konvergieren. Es besteht also das Potential die Entscheidungsoptionen über Datenverarbeitung zu verbessern, vor allem wenn die Anbieter der Plattformen Erkenntnisse aus der Verhaltensökonomie ins Entscheidungsdesign einbeziehen.

Im Rahmen dieses Gutachtens können nur einige wenige dieser Erkenntnisse diskutiert werden, da sie nicht Hauptgegenstand der Studie sind:

Status quo-Akzeptanz: Voreinstellungen werden von Verbrauchern meistens akzeptiert, da diese für die sozial erwünschte Handlung gehalten werden und/oder sich dadurch Handlungskosten reduzieren lassen (Johnson et al. 2002). Die Art der Frage beeinflusst die Raten der Zustimmung zur Einwilligung in die Datenverarbeitung. Eine Opt-out-Fragestellung evoziert beispielsweise erhöhte Zustimmungsraten (Bellman et al. 2001).

Anzahl der Optionen: Eine zunehmende Anzahl von Optionen, die einen differenzierteren Willensausdruck erlauben, führt zu einer Abnahme der Zufriedenheit mit der Entscheidung. Dies bedeutet, dass ein Anstieg der Entscheidungskomplexität mit Entscheidungsunzufriedenheit korreliert (Korff und Böhme 2014).[29]

Verlustaversion: Durch Betonung des Nutzens der Einwilligung kann Verlustaversion im Entscheider hervorgerufen werden. Dieser Nutzen wird als Gewinn für den Nutzer dargestellt und damit zum Referenzpunkt (Sakshaug et al. 2015)

Auch wenn die Plattformen einen verbesserten Ausdruck der Präferenzen erlauben, bedeutet dies nicht automatisch, dass Nutzer eine optimale Entscheidung fällen. Die Güte der Entscheidung hängt maßgeblich von einer Reihe von Faktoren ab, wie die verhaltensökonomischen Arbeiten zeigen. Ein besserer Transfer dieser Erkenntnisse in die Community der Startup-Unternehmen wäre wahrscheinlich als sinnvoll anzusehen.

28 Die Diskussion, ob das Paradoxon existiert und welche Erklärungen es dafür gibt, kann aufgrund des Umfangs des Gutachtens hier nicht geführt werden.

29 Über maschinenlesbare Konfiguration der Einwilligung kann der Einwilligungsprozess künftig automatisiert werden (ein Beispiel hierfür ist das hier genannte CoMaFEDs-Projekt).

4.5 Signalökonomie und Prozesse des Unraveling

Es ist mittlerweile bekannt, dass Verbesserungen des Einwilligungsmanagements nicht unbedingt zu mehr Datenschutz und mehr Privatsphäre führen müssen. Grund hierfür ist das ökonomische Eigeninteresse von Individuen, welches zur kompletten Offenlegung der privaten Informationen aller führen kann – zumindest im ökonomischen Modell (Hermalin und Katz 2006; Peppet 2011). Der Unraveling-Effekt geht ursprünglich auf Grossmann und Hart (1980) zurück.

Die Erosion der Privatsphäre entsteht nach Peppet (2011) mit der Signalökonomie. Sie geht einher mit der Reduktion der Kosten der Informationspreisgabe sowie der beim Individuum verankerten Kontrolle der persönlichen Daten. Unternehmen können in einem solchen Umfeld anreizkompatible Verträge aufsetzen, die – theoretisch gesehen – zu einer kompletten Offenlegung der Informationen aller im Gleichgewicht führen werden (sog. unraveling equilibrium oder Auflösungsgleichgewicht). Gleichzeitig werden Effizienzverluste aufgrund von Informationsasymmetrien reduziert.

Unter bestimmten Voraussetzungen kommt dieser Prozess nach Peppet (2011) ins Rollen: (i) geringe Kosten der Informationsoffenlegung; (ii) verifizierbare Informationen;[30] und (iii) die Unmöglichkeit Mimikry zu betreiben (also die Daten zu manipulieren).

Wie eingehend dargestellt ermöglichen PIMS den Nutzern, verifizierte Daten über Sozialverhalten, Lifestyle, Finanzverhalten oder Gesundheit auf einer Plattform zu zentralisieren. Damit könnte das entstehen, was Peppet (2011) als ‚personal prospectus' (Persönlichkeitsprospekt) bezeichnet. Dabei handelt es sich um ein Dossier, welches umfangreicher ist als die verteilten unvollständigen Profile, die derzeit in verschiedenen Organisationen existieren.

Der Unraveling-Prozess soll an einem Beispiel erläutert werden: Eine Versicherung kann durch einen Discount für einen besonders sportlichen Lebensstil die Freigabe von Tracker-Daten incentivieren. Angenommen der Sportlichste im Pool der Versicherten legt seine Daten offen. Der ‚Zweitsportlichste' antizipiert dies und hätte nun ebenfalls einen Anreiz dies zu tun, um nicht mit Unsportlichen in einen Topf geworfen zu werden. Dies wiederum antizipiert der Drittsportlichste, usw., usf. Der Unsportlichste ist indifferent zwischen Preisgabe und Nicht-Preisgabe, denn er wird automatisch als Unsportlichster durch die Handlungen der anderen identifiziert.

Unraveling – die Preisgabe aufgrund des Selbstinteresses der Datensubjekte – wird über die entstehenden Privatsphären-Externalitäten alle erfassen. Grundsätzlich lässt sich festhalten, dass in einer solchen Umgebung die Nicht-Preisgabe ebenfalls als Signal interpretiert wird. Unternehmen bilden dann Erwartungen darüber, warum ein Verbraucher seine Daten nicht offenlegt.

30 Die Verifizierbarkeit wird unter anderem von Mydex Data Services (2015: 7) stark betont. Das Unternehmen sieht sich als Plattform für den Austausch verifizierter Attribute, die nicht manipulierbar sind.

Das Argument, welches von Peppet hier angeführt wird ist, dass diese Aufdeckungsprozesse zu einer sozialen Norm der Offenlegung führen könnten. Jeder, der dieser Norm nicht folgt, wird ‚stigmatisiert'. Die Verankerung von Verfügungsrechten beim Individuum hat in diesem Szenario genau den gegenläufigen des erwarteten Effekts: Sie löst die Privatsphäre auf. Dies erhöht allerdings auch die allokative Effizienz.

Peppet sieht auch Grenzen des Prozesses, so wird er nicht gleichermaßen in allen Märkten entstehen. Transaktionskosten, Unkenntnis der Information oder deren Nicht-Existenz, sowie die Unfähigkeit Negativinferenzen über Nicht-Preisgabe zu bilden könnten werden den Prozess behindern (Peppet 2011: 1191 ff.). Schließlich sind es auch Privatsphären-Bedenken, die den Prozess unterminieren könnten.

Benndorf et al. (2015) zeigen, dass unraveling zum einen im Zusammenhang mit den Kosten der Offenlegung gesehen werden muss[31] und zum anderen im Zusammenhang mit der Verteilung des Merkmals in der Population. Die Autoren prüfen, inwiefern die Experimentalteilnehmer Entscheidungen fällen, welche den theoretischen Vorhersagen entsprechen. Die Laborergebnisse zeigen, dass der Unraveling-Prozess tatsächlich in Gang kommt. Die Rate der Offenlegung durch die Experimentalteilnehmer ist aber geringer als vorhergesagt. Insbesondere, wenn es sich um einen bestimmten Kontext wie Gesundheit handelt, reduzieren sich die Effekte. Die Rate der Offenlegung liegt zwischen rund 40 bis 60 Prozent.

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.

31 Diese sind in dem vorgestellten Modell aufgrund der Verifikation der Daten durch Zertifikat signifikant. Diese Kosten würden sich im Kontext von Big Data, in welchem es schwierig bis unmöglich ist, Daten zu manipulieren, erheblich senken.

5. Zusammenfassung

Bei den Plattformen der persönlichen Datenökonomie handelt es sich um neue Modelle des Nutzerzentrierten Einwilligungsmanagements, die in einem momentan entstehenden Markt aktiv sind. Aufgrund der Vielfalt der Geschäftsmodelle, ist die hier vorgeschlagene Klassifikation als nur vorläufig anzusehen, vor allem, wenn sich in Zukunft neue Kombinationsformen entwickeln.

Nahezu alle analysierten Modelle sind mehrseitige Plattformen, die sich von angestammten Intermediationsformen darin unterscheiden, dass der Nutzer eine aktive Rolle im Einwilligungsmanagement übernimmt. Innerhalb dieser Modelle, lassen sich Hub-Modelle (mit zentralisierender und dezentralisierter Datenspeicherung auf Nutzer-Endgeräten) von verteilten Systemen, die DLT-basiert sind, unterscheiden. Aber auch hier ist mit der technologischen Entwicklung die Unsicherheit verbunden, inwiefern eine solche Taxonomie künftig noch Trenngüte besitzt.

Die Plattformen sind in einem herausfordernden Marktumfeld tätig, als mehrseitige Plattformen müssen sie unterschiedliche Teilnehmergruppen anziehen. Bei den Nutzern müssen Vertrauensschwellen überwunden werden. Sie müssen außerdem einen deutlichen Mehrwert in der Datenaggregation darstellen. Zu den wichtigsten Herausforderungen gehört die Entwicklung von robusten und nachhaltigen Kommodifikations- und Monetarisierungsmodellen.

Bei den Unternehmen implizieren die neuen Modelle Umorganisationsprozesse. Ob die Plattformen künftig einen zusätzlichen Mechanismus darstellen oder transformative Wirkung entfalten, ist kaum abzuschätzen.

Da die neuen Plattformen wahrscheinlich weniger zu einer neuen Eigentumsordnung als mehr zu einer neuen Daten-Nutzungsordnung führen werden, ist es wichtig, dass künftig ein besserer Transfer von Forschungsergebnissen aus der verhaltensökonomischen Forschung in die Gemeinschaft der Unternehmensgründer stattfindet. Dasselbe wird gelten, wenn Privatsphärenschonende Marktplätze entstehen sollen, auf welchen Nutzer ihre Daten verkaufen sollen.

6. Empfehlungen

Empfehlungen können auf mehreren Ebenen ausgesprochen werden. Diese umfassen ökonomische Rahmenbedingungen ebenso wie institutionelle und forschungsorientierte Maßnahmen.

Förderliche ökonomische Rahmenbedingungen und Standardisierung

Derzeit befinden sich die Europäischen Staaten in der Umsetzungsphase der EU-DSGVO. Dies bedeutet, dass die gesetzlichen Rahmen der Datenerhebung und -verarbeitung novelliert werden. Innovative Geschäftsmodelle im Bereich des Einwilligungsmanagements könnten in diesem Zusammenhang von folgenden Maßnahmen profitieren:

- 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 standardisierten Vereinbarungen, die dem Einwilligungsmanagement zuträglich sind
- Pilotierung von Projekten, die eine technische Implementation sowie die rechtskonforme Automatisierung von Einwilligungserklärungen zum Gegenstand haben

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 der Politik, Industrie und Forschung

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

Forschungsmaßnahmen

- Finanzierung Grundlagenforschung im Bereich des Ende-zu-Ende Privatsphären-Managements insbesondere Förderung von interdisziplinären Forschungsprojekten im Bereich Verhaltensökonomie, Kryptographie und De-Personalisierungsmethoden

- Finanzierung von verhaltensökonomischen Arbeiten im Bereich des aktiven Einwilligungsmanagements sowie der Daten-Monetarisierung

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

Im Folgenden sollen die Bedingungen für Unternehmen ihre Software-Schnittstellen (API) bezüglich notwendiger Standardisierungen für persönlich verwaltetem Datenaustausch öffnen zusammengefasst dargestellt werden:

- Klar umrissener Mehrwert durch die vorgeschlagene Lösung sowie klar erkennbare Rechtskonformität

- Politische Unterstützung der rechtskonformen, automatisierten Einwilligung, sowie entsprechender Standardisierungsmaßnahmen

- Unternehmensintern werden Kostenreduktion durch die Öffnung sowie Teilnahme an Plattform bei gleichbleibender Datenqualität ein Treiber sein

- Ein Anreize für die Nutzung solcher Systeme könnte ganz maßgeblich die erhöhte Rechtssicherheit durch M2M-Kommunikation standardisierter Einwilligungserklärungen sein

Anhang

Name	Sitz	Typus	Gewinn-orientiert	Mehrwertdienste				Architektur/ Konfiguration
					Nutzer-Funktionalitäten	Monetari-sierung der Daten durch Nutzer?	Unternehmens-Funktionalitäten	
Data Fairplay	DE	Firma	Ja	- Einwilligungs-manager - Verbindung Datensätze - Datenverkauf - Datenzugabe-funktion	- Verkauf der Daten - Erhöhte Transparenz	Ökonomische Trans-aktion	- Datenabfrage	- Plattform (Online-Portal)
Digi.Me	GB	Firma	Ja	- Einwilligungs-manager - Verbindung Daten - Suchfunktion - Datenweiter-gabe	- Kostenlose Anwendung - Zentralisierung der Daten - Recherche-möglichkeit	Nicht geplant	- Datenabfrage - App-Entwick-lung	- Plattform - App in App-Stores - Desktop Version
Digitando	DE	Firma	Ja	- Archivierung von Rechnun-gen, Bestellun-gen - Transparenz Datenströme - Cashback bei Einkäufen	- Kostenlose Anwendung - Zentralisierung der Daten - Recherche-möglichkeit	N/a	- Datenabfra-ge über API geplant	- App und Webportal
LETSmart	DE	Projekt	Geplant	- Einwilligungs-manager - Erhöhte Trans-parenz	- Einwilligungs-manager - Erhöhte Transparenz	Transaktions-basiert	- Einwilligungs-manager - Rechtskonfor-me Einwilli-gung - Automatisierte Umsetzung Datenschutz	- Soft-ware-Modul - Integration in andere Dienste Drit-ter möglich
Meeco	AU	Firma	Ja	- Einwilligungs-manager - Verbindung Datensätze - Intent casting - Marktplatzfunk-tionen - Kuratierungs-funktion	- Kostenlose Anwendung - Zentralisierung Daten - Kuratierung und Aktuali-sierung	Künftig ökonomische Transaktionen geplant	- Datenabfrage - Abgabe Gebote	- Plattform - App - Do-not-track plugins - Auflis-tung von Kauf-wün-schen - Selbstana-lyse
MesInfos/ Cozy Cloud	FR	Projekt	Nein	- Verbindung Datensätze - Personal Virtual Machine auf Cozy Cloud	- Zentralisierung Daten - Download Apps von Dritten	Sozialer Tausch	- Datenabfrage - App-Entwick-lung	- Plattform (keine Markt-platz-funktiona-lität) - Persönliche Cloud mit Hosting auf Cozy Cloud Servern (oderSer-vern von Dritten)

Anhang

MyDataCan	USA	Projekt	Nein	- Verbindung Datensätze - Kuratierungs-funktion (inkl. Zugabe) - Datenweiter-gabe	- Kostenlose Anwendung - Zentralisierung Daten - Download Apps von Dritten	Wählbar	- Kostenlose Datenbank-dienste - Datenabfrage - App-Entwicklung	- Online-Daten-dienst-Plattform - Living Lab - API für APP-Entwickler
Personiq / EmVolution	DE	Plug-in für Browser	Ja	- Erhöhte Transparenz Webverhalten - Personalisierte Nachrichten	- Kostenlose Anwendung - Erhöhung Transparenz und Kontrolle	Künftig ökonomische Transaktionen geplant	N/a	- Plug-in für Firefox und Google Chrome Browser
PrivacyGuard (Pguard)	DE	App und Web-portal	N/a	- Erhöhte Transparenz über Zugriffe, Datentransfers, etc. von Apps des Nutzers	- Erhöhung Transparenz und Kontrolle über Daten-verarbeitung durch Apps, Visualisierung	Nicht geplant	N/a	- App und Webportal
Jolocom	DE	Firma	Ja	- Einwilligungs manager - Verbindung Datensätze - Daten-weitergabe	- Kostenlose Anwendung (App) - Erhöhte Trans-parenz - Übernahme Kontrolle	Wählbar	- Datenabfrage und Datennut-zung - Abgabe Gebote	- App kreiert persönliche Web ID, die mit persön-lichen Daten verbunden wird, Block-Chain-An-wendung
Telecom Italia/ My Data Store	IT	Firma	Ja	- Verbindung Datensätze - Cloud und Hosting - Kuratierung - Analyse & Visualisierung	- Zentralisierung Daten - Cloud und Hosting - Kuratierung - Analyse & Visualisierung - Datan-qualitäts-analyse	Datenverkauf geplant	- Datenabfrage - App-Entwicklung	- Persönliche Datenplatt-form - Persönliche Cloud - Datenmarkt-platz - Website - App und zertifizierte Apps

Literaturverzeichnis

Ali, R., J. Barrdear, R. Clews, und J. Southgate (2014). The Economics of Digital Currencies, Bank of England Quarterly Bulletin 54(3): 276-286.

Akerlof, G.A. (1980). The Market for 'Lemons': Quality Uncertainty and the Market Mechanism, The Quarterly Journal of Economics 84 (3): 488-500.

Aperjis, C. und B. Huberman (2012). A Market for Private Data: Paying Individuals According to their Privacy Attitudes, First Monday 17 (5), http://firstmonday.org/ojs/index.php/fm/article/view/4013/3209

Bellman, S., E. J. Johnson, G. L. Lohse (2001) On site: to opt-in or opt-out? It depends on the question, Commu-nications of the ACM 44 (2): 25-27.

Benndorf, V., D. Kübler und H.-T. Normann (2015). Privacy concerns, voluntary disclosure of information, and unraveling: An experiment, European Economic Review 75 (April): 43–59.

Boston Consulting Group (2012). The Value of Our Digital Identity, Liberty Global Policy Series, http://www.libertyglobal.com/pdf/public-policy/the-value-of-our-digital-identity.pdf

Bründl, S., C. Matt und T. Hess (2015). Wertschöpfung in Datenmärkten – Eine explorative Untersuchung am Beispiel des deutschen Marktes für persönliche Daten, http://www.forum-privatheit.de/forum-privatheit-de/texte/veroeffentlichungen-des-forums/Forschungsbericht-LMU-Wertschoepfung-in-Datenmaerkten_FP_3Sept15.pdf

Bundeskartellamt (2005). Beschlussabteilung B9 – 32/05 (2005), http://www.bundeskartellamt.de/SharedDocs/Entscheidung/DE/Entscheidungen/Fusionskontrolle/2005/B9-32-05.html

Catalano, D. und M. Machulak (2014). Protecting Personal Data in an IoT Network with UMA – A Patient Centric Use Case, Präsentation, Kantara Initiative Workshop, November 2014, http://de.slideshare.net/kantarainitiative/uma-auth-ziotirmdublinv06

Charness, G. and Gneezy, U. (2008) 'What's in a Name? Anonymity and Social Distance in Dictator and Ultima-tum Games', Journal of Economic Behavior & Organization 68(1): 29–35.

Chellappa, R. K. und Shivendu, S. (2010). Mechanism Design for „Free" but „No Free Disposal Services": The Economics of Personalization under Privacy Concerns, Management Science: 56 (10): 1766-1780.

Custers, B. (2016). Click here to consent forever: Expiry dates for informed consent, Big Data & Society (Janu-ary-June): 1-6.

Ctrl-Shift (2014) Personal Information Management Services: An analysis of an emerging market, Report, http://www.nesta.org.uk/publications/personal-information-management-services-analysis-emerging-market

de Fortuny, E.J., D. Martens und F. Provost (2013). Predictive Modeling with Big Data: Is Bigger Really Better? Big Data 1 (4): 215 – 226.

de Mulder, Y., G. Danezis, L. Batina und B. Preneel (2008). Identification via location-profiling in GSM networks (WPES'08), // researchmicrosoft.com/en-us/um/people/gdane/papers/GSMLocation-profile.pdf

de Montjoye, Y.-A., C.A. Hidalgo, M. Verleysen und V.D. Blondel (2013). Unique in the Crowd: The privacy bounds of human mobility. Nature 3, 1376; DOI:10.1038/srepo1376.

de Montjoye Y.-A., Radaelli L., Singh V. K., Pentland A. S., (2015). Unique in the shopping mall: On the reidenti-fiability of credit card metadata, Science 347 (6221): 536-539.

Dutch Data Protection Authority (2013). Investigation into the combining of personal data by Google - Re-port of Definitive Findings, November, z2013-00194, https://autoriteitpersoonsgegevens.nl/sites/default/files/downloads/mijn_privacy/en_rap_2013-google-privacypolicy.pdf

Economides, N. (1996). The Economics of Networks, International Journal of Industrial Organisation 14: 673-699.

Economides, N. (2001). The Impact of the Internet on Financial Markets, Journal of Financial Transformation 1 (1): 8-13.

Egelman, S., J. Tsai, L.F. Cranor, and A. Acquisti (2009). Timing is Everything? The Effects of Timing and Placement of Online Privacy Indicators, http://www.guanotronic.com/~serge/papers/chio9a.pdf.

EDPS (2016). EDPS Opinion on Personal Information Management Systems, Opinion 9/2016 (20 October 2016), https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consultation/Opinions/2016/16-10-20_PIMS_opinion_EN.pdf

European Commission (2008). Case No COMP/M.4731 – Google/ DoubleClick, http://ec.europa.eu/competition/mergers/cases/decisions/m4731_20080311_20682_en.pdf
Evans, D. E. (2011). Antitrust Economics of Free, Global Economics Group; University of Chicago Law School; University College London (17. April 2011),

Federal Trade Commission (2014). Data Brokers - A Call for Transparency and Accountability, A Report of the Federal Trade Commission, https://www.ftc.gov/news-events/press-releases/2014/05/ftc-recommends-congress-require-data-broker-industry-be-more

Feri, F., C. Giannetti, N. Jentzsch (2016). Disclosure of personal information under risk of privacy shocks, Journal of Economic Behavior & Organization 123: 138-148

Filistrucchi, L., D. Geradin, E. van Damme und P. Affeldt (2014). Market Definition in Two-sided Markets: Theory and Practice, Journal of Competition Law and Economics 10(2): 293-339.

Ghose, A. und K.-W. Huang (2009). Personalized Pricing and Quality Customization, Journal of Management and Strategy 18 (4): 1095-1135.

Gurevich, Y., E. Hudis und J.M. Wing (2016). Inverse Privacy, Communications of the ACM 59 (7): 38-42.
Grossman, S.J. und O.D. Hart (1980). Disclosure Laws and Takeover Bids, The Journal of Finance 35 (2): 323-334.

Haley, K.J., M. Daniel und T. Fessler (2005). Nobody's watching? Subtle Cues Affect Generosity in an Anony-mous Economic Game, Evolution of Human Behavior 26(3): 245–56.

Hermalin, B.E. und M.L. Katz (2006). Privacy, Property Rights and Efficiency: The Economics of Privacy as Secre-cy. Quantitative Marketing and Economics 4 (3): 209–39.

Horowitz, John K. (2006). The Becker-DeGroot-Marschak mechanism is not necessarily incentive compatible, even for non-random goods, Economics Letters 93 (1): 6–11.

Huberman, B., Adar, E., Fine, L. (2005). Valuating privacy. Security & Privacy IEEE 3 (5), 22–25.

Jentzsch, N. (2017). Wohlfahrts- und Verteilungseffekte personalisierter Preise und Produkte, Friedrich-Ebert-Stiftung, Vergabe-Nr.: 2016106.

Jentzsch, N. (2016a). Kreditwürdigkeitsanalysen im Zeitalter von Big Data: Innovation oder Revolution? Wirtschaftsdienst, Heft 9 (2016): 644-647.

Jentzsch, N. (2016b). State-of-the-Art of the Economics of Cyber-Security and Privacy, IPACSO- Innovation Framework for ICT Security, Deliverable No. 4.1., http://hdl.handle.net/10419/126223

Jentzsch, N. (2016c). Blockchain: Revolution der Finanzwelt? Kommentar, DIW Wochenbericht, DIW Berlin, Vol. 83 (29): 656.

Jentzsch, N. (2016d). Quantification of Privacy Harm, Presentation to Harvard SEAS Privacy Tools De-Identification Group, erhältlich auf Anfrage bei Autorin.

Jentzsch, N. (2015). The Marketplace for Privacy-Related Products and Services. IPACSO White Paper No. 1, http://econpapers.repec.org/paper/zbwesrepo/126226.htm

Jentzsch, N. (2014). Auctioning Privacy-Sensitive Goods: A note on Incentive-Compatibility, in B. Preneel and D. Ikonomou (eds.), Privacy Technologies and Policy, Lecture Notes in Computer Science, Vol. 8450, S. 133-142.

Jentzsch, N. (2007). Financial privacy: an international comparison of credit reporting systems (Springer-Verlag, Heidelberg).

Johnson, E.J., Bellman, S. and Lohse, G.L. (2002) Defaults, framing and privacy: Why opting in-opting out, Mar-keting Letters, 13 (1): 5-15.

Joshi, S. Y.-A. Sun and P.L. Vora (2005). The Influence of Privacy Cost on Threshold Strategies in Sealed-bid First and Second-price Auctions, http://www.seas.gwu.edu/~poorvi/auctions.pdf

Juniper Research (2016). Understanding the Personal Data Economy – The Emergence of a New Data Value-Exchange, Whitepaper, http://mobileecosystemforum.com/personal-data-economy-whitepaper/

Kelley, P. G., L.F. Cranor und N. Sadeh (2013). Privacy as part of the app decision-making process, Working Paper, https://www.cylab.cmu.edu/files/pdfs/tech_reports/CMUCyLab13003.pdf

Khosrow-Pour, M. (2015). Encyclopedia of Information Science and Technology, Information Science Refer-ence, Hershey, PA, USA

Korff, S., & Böhme, R. (2014). Too Much Choice: End-User Privacy Decisions in the Context of Choice Prolif-eration. In Proceedings of the Symposium on Usable Privacy and Security (SOUPS), https://www.usenix.org/system/files/soups14-paper-korff.pdf

Luchetta, G. (2014). Is the Google Platform a Two-sided Market? Journal of Competition Law & Economics 10 (1): 185-207.

MyData Architecture (1.2.1). Consent Based Approach for Personal Data Management, Release 1.2.1 (ohne Datum), http://hiit.github.io/mydata-stack/
Mydex Data Services CIC (2015). Your data, your way, http://www.openidentityexchange.org/wp-content/uploads/2016/11/MydexCIC-TheopportunityofAttributeexchange.pdf

Narayanan, A. und V. Shmatikov (2008). Robust De-anonymization of Large Sparse Datasets, https://www.cs.utexas.edu/~shmat/shmat_oako8netflix.pdf

Nissim, K., R. Smorodinsky und M. Tennenholtz (2015). Segmentation, Incentives and Privacy, Working Paper, https://www.researchgate.net/publication/280527559_Segmentation_Incentives_and_Privacy

Norberg P.A., D.R. Horne und D.A. Horne (2007). The Privacy Paradox: Personal Information Disclosure In-tentions versus Behaviors, The Journal of Consumer Affairs 41(1), 100-126.

OECD (2013). Exploring the Economics of Personal Data: A Survey of Methodologies for Measuring Mone-tary Value, OECD Digital Economy Papers, No. 220, OECD Publishing. http://dx.doi.org/10.1787/5k486qtxldmq-en

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

Reed, D. (2013). Why Personal Clouds Need a Network, Präsentation - Personal Cloud Community Meetup (2013-01-29), http://www.slideshare.net/evanwolf/respect-networkpcloudmeetup20130129

Riechert, A. (2017). Stellungnahme zu rechtlichen Aspekten eines Einwilligungsassistenten, Gutachten für die Stiftung Datenschutz.

Rochet, J.-C., J. Tirole (2003). Platform competition in two-sided markets, Journal of the European Economic Association 1(4): 990-1029.

Rosenberg, M. (2016). Von BitCoin zum Smart Contract, Schlaglichter der Wirtschaftspolitik, BMWi Monats-bericht Oktober 2016, http://www.bmwi.de/DE/Mediathek/monatsbericht,did=781534.html

Ruths, D. und J. Pfeffer (2014). Social Media for Large Studies of Behavior, Science 346 (6213): 1063–1064.

Sakshaug J.W., Wolter S. und Kreuter F. (2015). Obtaining Record Linkage Consent: Results from a Wording Experiment in Germany. Survey Insights: Methods from the Field, http://surveyinsights.org/?p=7288

Shrier, D., W. Wu, A. Pentland (2016). BlockChain & Infrastructure (Identity, Data Security), Massachusetts Institute of Technology (MIT), Part 3 (May 2016), http://cdn.resources.getsmarter.ac/wp-content/uploads/2016/05/MIT_Blockchain_Infrastructure_Report_Part_Three_May_2016.pdf

Smith, J. und A. Mitchell (2014). Personal Information Management Services Methodology Working Paper, Nesta Working Paper Series, Paper No. 14/08.

Syam, N.B., R. Ruan und J.D. Hess (2005). Customized Products: A Competitive Analysis. Marketing Science 24: 4, 569-584.

World Economic Forum (2014). Rethinking Personal Data: A New Lens for Strengthening Trust, Prepared in collaboration with A.T. Kearney, http://www3.weforum.org/docs/WEF_RethinkingPersonalData_ANewLens_Report_2014.pdf

World Economic Forum (2013) Unlocking the Value of Personal Data: From Collection to Usage, Prepared in collaboration with The Boston Consulting Group, http://www3.weforum.org/docs/WEF_IT_UnlockingValuePersonalData_CollectionUsage_Report_2013.pdf

World Economic Forum (2011). Personal Data: The Emergence of a New Asset Class, World Economic Forum, Geneva, http://www.weforum.org/reports/personal-data-emergence-new-asset-class

Young, K. (2015). Ethical Market Models in the Personal Data Ecosystem, Presentation – Personal Data Ecosystem Consortium, http://de.slideshare.net/Kaliya/ethical-market-models-in-the-personal-data-ecosystem

Zhang, J. (2011). The Perils of Behavior-Based Personalization, Marketing Science 30(1): 170-186.

DIW Berlin (Deutsches Institut für Wirtschaftsforschung)

Das DIW Berlin (Deutsches Institut für Wirtschaftsforschung) ist seit 1925 eines der führenden Wirtschaftsforschungsinstitute in Deutschland. Es erforscht wirtschafts- und sozialwissenschaftliche Zusammenhänge in gesellschaftlich relevanten Themenfeldern und berät auf dieser Grundlage Politik und Gesellschaft. Das Institut ist national und international vernetzt, stellt weltweit genutzte Forschungsinfrastruktur bereit und fördert den wissenschaftlichen Nachwuchs. Das DIW Berlin ist unabhängig und wird als Mitglied der Leibniz-Gemeinschaft überwiegend aus öffentlichen Mitteln finanziert.

Die Autorin Dr. Nicola Jentzsch

Dr. Nicola Jentzsch ist promovierte Volkswirtin und arbeitet am DIW Berlin. Sie forscht seit mehr als 15 Jahren im Gebiet der Ökonomie der Privatsphäre. Frau Jentzsch ist Experimental- und Wettbewerbsökonomin und verbindet Verhaltens- und Wettbewerbsfragen in digitalen Märkten mit Themen wie Big Data und technische Privatsphären-Garantien.

Vor dem DIW Berlin lehrte Frau Jentzsch an der Fakultät für Wirtschaftswissenschaften der Freien Universität und war Research Fellow an der Yale University. Sie hat in der Vergangenheit als Beraterin für die Europäische Kommission, die Europäische Agentur für Netz- und Informationssicherheit (ENISA), die Weltbank sowie mehrere Zentralbanken in afrikanischen und asiatischen Ländern gearbeitet. Frau Jentzsch wurde mit einem Google Research Award ausgezeichnet und veröffentlicht ihre Forschung in internationalen Wirtschaftsjournals der SSCI-Liste.

Inhaltsverzeichnis

	Anhang 3 – Seite
I. Einwilligung und Transparenz unter dem BDSG	2
1. Einwilligung	2
2. Transparenz	3
3. Zusammenfassung	5
II. Einwilligung und Transparenz unter der EU-Datenschutz-Grundverordnung	6
1. Einführung	6
2. Einwilligung	9
3. Transparenz	16
4. Zusammenfassung	20
III. „Informiertheit der Verbraucher“ als Regulierungsherausforderung	22

Abrufdatum der Internetlinks in Teil D: 24. Februar 2017

I. Einwilligung und Transparenz unter dem BDSG

1. Einwilligung

In frühen Entwürfen zum Bundesdatenschutzgesetz (BDSG) von 1971 war der Begriff der Einwilligung noch nicht enthalten, der Fokus wurde eher auf die Transparenz und auf die Einsichtsrechte der Bürger in die von ihnen erhobene Daten gelegt[1]. Spätere Gesetzesentwürfe im Jahre 1973[2] enthielten in §3 II Nr. 1 die Möglichkeit der Einwilligung in die Datenverarbeitung. Die Umänderung des Begriffs der „Zustimmung" in den der „Einwilligung" diente dabei dazu, dass nachträgliche Zustimmungen des Betroffenen zur Datenverarbeitung rechtlich wirkungslos blieben[3]. Die Einwilligung des Betroffenen wurde damit als Alternative zu rechtlichen Vorgaben bzw. Zwangsregelungen angelegt. Somit kann die Einwilligung als Auffangregelung betrachtet werden. Dem Betroffenen wurde unter gewissen Voraussetzungen, etwa wenn kein gesetzlicher Zwang vorlag, die Möglichkeit gegeben, eigenverantwortlich zu handeln und in Schriftform der Datenverarbeitung bei der betreffenden Stelle zuzustimmen.

Auch wenn der Begriff der „informationellen Selbstbestimmung" erst im Verlauf des Volkszählungsurteils von 1983 geprägt wurde, so zeigt die Urfassung des BDSG von 1977 erste Ansätze, welche das Selbstbestimmungsrecht der Betroffenen in den Vordergrund rücken. Das Schriftformerfordernis stellt dabei den erhöhten Anspruch an die Einwilligung dar[4]. Es wird die Protokollierungs- und Nachweisfunktion der Einwilligung deutlich. Jedoch wurde schon hier mit der Ausnahme bei „besonderen Umständen" das Schriftformerfordernis nicht als unabdingbar festgehalten. Allerdings wird, neben diesen Schutzwirkungen für den Bürger, für die nicht-öffentlichen Stellen auch ein weiter Spielraum für die Datenverarbeitung geschaffen, auch ohne die Einwilligung des Betroffenen. So lautet etwa §32 Nr.1 BDSG (1977): „(1) Das Speichern personenbezogener Daten ist zulässig, soweit kein Grund zur Annahme besteht, dass dadurch schutzwürdige Belange des Betroffenen beeinträchtigt werden. Abweichend von Satz 1 ist das Speichern zulässig, soweit die Daten unmittelbar aus allgemein zugänglichen Quellen entnommen sind." Hier wird also auf eine reine Annahme der schutzwürdigen Belange durch die verarbeitende Stelle vertraut, welche durch gerichtliche Entscheidungen bzw. die Praxis ausgefüllt werden mussten. Weiterhin ist festzuhalten, dass eine Entnahme von Daten aus öffentlichen Drittquellen als zulässig festgehalten wird. So können Privatunternehmen rechtmäßig öffentliche Daten drittverwerten. Zusammenfassend wird im ersten BDSG der Fokus auf Datensicherung mit den vier Umgangsformen Speichern, Übermitteln, Verändern und Löschen[5] gelegt.

Die spätere Gesetzesänderung im Jahre 1990 ist vor allem durch das Volkszählungsurteil und den dadurch geprägten Begriff der „Informationellen Selbstbestimmung", das Recht auf selbige und die Konkretisierung des Begriffes beeinflusst. Das BDSG behält dabei das Modell des Verbots mit Erlaubnisvorbehalt bei. Die Änderungen befassen sich vor allem mit Detailfragen und Konkretisierungen (etwa im Zusammenhang mit der Forschung in § 4 Nr.3 BDSG). So werden etwa Einwilligungsfiktionen ermöglicht – wie etwa die in § 14 Abs. 3 BDSG alter Fassung – wenn nicht anzunehmen ist, dass eine Einwilligung verweigert wurde. Auch unbestimmte Rechtsbegriffe wie das „überwiegende Interesse" werden aufgenommen, um das BDSG auf unvorhersehbare zukünftige Rechtskonstellationen vorzubereiten.

1 vgl. Drucksache VI/2885, http://dipbt.bundestag.de/doc/btd/06/028/0602885.pdf

2 vgl. Drucksache VII/1027, http://dipbt.bundestag.de/doc/btd/07/010/0701027.pdf

3 vgl. dazu Ausführungen zu §3 in Drucksache VII/5277 (1976), http://dipbt.bundestag.de/doc/btd/07/052/0705277.pdf

4 vgl. Drucksache VII/1027 S.23, http://dipbt.bundestag.de/doc/btd/07/010/0701027.pdf

5 Wolff, H. A./Brink, S., Beck'scher Online-Kommentar Datenschutzrecht, Rn. 43.

Tragend in der Änderung des BDSG war das Hinzufügen der Begriffe der „Erhebung“ und „Nutzung“ personenbezogener Daten, welche den Schutz der Daten auch auf den Erhebungszeitpunkt ausdehnten. Die „Nutzung“ war als Auffangtatbestand vorgesehen, um unvorhergesehene Probleme außerhalb der anderen Kategorien auszuschließen.

Die Gesetzesänderung im Jahr 2001 (basierend auf Umsetzung der EU-Datenschutz-Richtlinie) betraf im Zusammenhang mit der Einwilligung etwa die direkte Datenerhebung beim Betroffenen. So soll dem Betroffenen, neben der Transparenz, auch die Möglichkeit eingeräumt werden, Kenntnis von den ihn betreffenden Datenverarbeitungen zu erlangen und diesen ggf. zustimmen zu können. Auch die datenverarbeitenden Stellen wurden dazu bewegt, bei der Datenerhebung frühzeitig auf fehlerhafte Datensätze zu achten. Weiterhin wurden Möglichkeiten eingeräumt, mit denen etwaige Melde- oder Prüfpflichten durch vorhandenen Einwilligungen der Betroffenen ausgeschlossen werden können.

Eine wichtige Änderung stellt weiterhin § 4a des BDSG dar, welcher einerseits das Prinzip der Verhandlung auf Augenhöhe einführt und andererseits das Schriftformerfordernis aufweicht. Besonders das Prinzip der Freiwilligkeit der Einwilligung stellt in diesem Kontext eine der wichtigsten Neuerungen dar. Gerade wenn es sich um Über- und Unterordnungsverhältnisse (wie sie etwa in einem Arbeitgeber- und Arbeitnehmerverhältnis bestehen) handelt, kann eine solche „freiwillige Einwilligung“ faktisch nicht vorhanden sein. Hier ist die Einsicht des Gesetzgebers zu erkennen, dass Einwilligungen häufig immer mehr als Randformalität betrachtet werden und ihre vom Gesetzgeber gewünschte Kontrollfunktion verlieren. Das Schriftformerfordernis wurde dabei auch mit Blick auf die neuen Medien und das Internet immer weiter aufgeweicht.

Auch neue Prinzipien wie die der „Datenvermeidung“, des „Datenschutzes durch Technik“, des „Datenschutz-Audits“ und eine Lösung der Problematik der Videoüberwachung fanden Einzug in das BDSG.

Die Änderungen in der Fassung von 2009 betreffen vorrangig bereichsspezifische Regelungen. So sind gerade Sonderregelungen zu Auskunfteien, dem Adresshandel oder der Werbung in dieser Gesetzesänderung zu finden. Weiterhin ist hervorzuheben, dass in § 28 BDSG eine Konkretisierung des Schriftformerfordernisses aufgenommen wurde, welche gerade für die elektronische Einwilligung äußerst relevant ist. So wird es ermöglicht, dass – sofern dies auf Anbieterseite protokolliert wird – eine Einwilligung auch ohne eine Schriftform wirksam ist. Hier wird durch den Gesetzgeber dem Umstand Rechnung getragen, dass es bei der intensiven Internetnutzung für den Betroffenen einfacher ist, die Einwilligung in elektronischer Form zu erteilen.

2. Transparenz

In der Urfassung des BDSG aus dem Jahr 1977 ist eine besondere (optische) Hervorhebung der Einwilligung festgelegt (§ 3). Bei der Entstehung des Gesetzes wurde dabei besonders auf das Problem des sogenannten „Kleingedruckten“ im Rechtsverkehr Rücksicht genommen[6]. So soll die Einwilligung in Verarbeitung von personenbezogenen Daten für den Betroffenen deutlich erkennbar (transparent) und von anderen Aspekten eines Vertragsabschlusses gezielt hervorgehoben sein.

6 vgl. Drucksache 7/1027 S. 23; zu § 2, http://dipbt.bundestag.de/doc/btd/07/010/0701027.pdf

Dies bedeutete einen weitreichenden Transparenzgewinn für die Betroffenen, informierter in die Datenverarbeitung zustimmen zu können. Weiterhin wurde in § 4 insbesondere auf die Auskunfts- und Informationsrechte der Betroffenen Rücksicht genommen. Es wurden umfangreiche Auskunfts- und Berichtigungsrechte eingeräumt. Auch die Freiwilligkeit der Angaben (§ 9) spielte eine bedeutende Rolle. Gerade wenn es sich um Über- und Unterordnungsverhältnisse bei staatlichen Stellen handelte, war – sofern Rechtsvorschriften keine Zwangsangaben anordneten – eine durchaus spezifische Information des Betroffenen über die Freiwilligkeit der Angaben notwendig, was die Transparenz der Datenschutzerklärungen erhöhen sollte. § 12 machte es dem Betroffenen außerdem möglich, die Übersicht über die datenverarbeitenden und -erhebenden öffentlichen Stellen zu behalten und ggf. (§ 13) einen Antrag auf die Auskunft über die gespeicherten Daten zu stellen. Schließlich wies § 26 die Auskunftspflicht über gespeicherte personenbezogene Daten der erstmalig speichernden Institution zu. Dies erhöhte die Transparenz der Datenverarbeitung erheblich. Eine Ausnahme stellte dabei jedoch schon damals die Datenerhebung aus allgemein zugänglichen Quellen dar, was bei der Debatte um die Regelungen zu heftigen Diskussionen führte[7].

In der BDSG-Fassung aus dem Jahr 1990 wurden die Informationspflichten der Datenverarbeiter erweitert und konkretisiert sowie die Auskunftsrechte der Betroffenen gestärkt. So wurde es beispielsweise für die Betroffene durch § 6 deutlich einfacher, Informationen über die gespeicherten personenbezogenen Daten zu erhalten, auch dann, wenn die zuständige Stelle nicht eindeutig festzustellen ist. Der Erhöhung der Transparenz diente es auch, dass die Betroffenen in den Datenerhebungsprozess weitgehend miteinbezogen wurden (vgl. § 13). Eine Erhebung ohne die Mitwirkung des Datensubjekts wurde nur unter der Güterabwägung (und deren Protokollierung) von schutzwürdigen Interessen möglich. Mit § 16 wurde weiterhin die Informationspflicht bei der Datenübermittlung an nicht-öffentliche Stellen geregelt. Gerade wenn es sich um eine Übermittlung von öffentlichen Stellen an nicht-öffentliche handelte, wurde durch die Informationspflichten für die Betroffenen eine umfangreich Transparenz geschaffen sowie die Möglichkeit eröffnet, ggf. der Datenübermittlung zu widersprechen. Weitere Auskunftsrechte wurden in § 19 konkretisiert (mitunter auch die Antragsform sowie der Inhalt der Rückinformation geregelt). Außerdem wurde zwischen Benachrichtigungspflichten und den Auskunftspflichten differenziert und der Unterschied zwischen einer Benachrichtigung und einer Auskunft näher konkretisiert (§ 33). In § 34 wurden zwar vorwiegend Ausnahmen für die Benachrichtigung aufgenommen, welche die Transparenz für Betroffene verringerten. Es handelte sich aber dabei vorwiegend um Sachverhalte, bei denen meist eine Auskunft aus überwiegenden anderen Interessen nicht zweckmäßig erschien und welche im Grundsatz eine Fortführung der Ausnahmen aus § 26 BDSG-1977 darstellten.

Auch durch die Stärkung der Institution des Bundesbeauftragten für Datenschutz (§ 21) wurde die Transparenz der Datenspeicherung indirekt bestärkt. Informationen, welche vorher möglicherweise nicht freigegeben werden konnten, konnten nunmehr unter der Mitwirkung des Bundesbeauftragten weit einfacher freigegeben werden. Mit der Einführung des Datenregisters (§ 26) wurde außerdem die Möglichkeit zur Einsicht über die von öffentlichen Stellen gespeicherten personenbezogenen Daten eröffnet. Eine wesentliche Neuerung in der Fassung von 1990 stellte schließlich die Unterscheidung von Regelungen für öffentliche und nicht-öffentliche Stellen dar (§ 27 ff.). Hier wurde eine deutlich striktere Regelungsdichte für die nicht-öffentlichen Stellen aufgebaut.

7 vgl. BT-Drs. 7/5277, S. 3ff., http://dipbt.bundestag.de/doc/btd/07/052/0705277.pdf

In der BDSG-Fassung von 2001 wurden erstmals die Benachrichtigungspflichten breiter gefasst und auch für öffentliche Institutionen im Allgemeinen als notwendig ausgewiesen. Es verblieb jedoch auch hier die weit gefasste Ausnahme im Falle eines „unverhältnismäßigen Aufwandes“ bzw. dem weit wahrscheinlicheren Fall, dass ein Gesetz die Speicherung vorsah[8]. In der Neufassung wurde außerdem mit Nachdruck darauf verwiesen, dass die Daten bei den Betroffenen erhoben werden müssen (§ 4). Indirekt wurde so die Transparenz erhöht, da die Betroffenen durch die Anfrage der Institution direkte Kenntnis über die von ihnen erhobenen Daten erlangen. Die Paragraphen §§ 4d-4g wurden mit Blick auf ihre Wichtigkeit vorgezogen. Gerade die Meldepflichten an den Bundesbeauftragten für den Datenschutz leisteten einen wichtigen Beitrag zur Kontrollfähigkeit und damit auch zur Transparenz von Datenerhebungen.

In der Neufassung des BDSG wurde schließlich dem Umstand der immer weitreichenderen Videoüberwachung von öffentlichen Stellen Rechnung getragen (§ 6b). Der Erhöhung der Transparenz sollte dabei die Pflicht zum Hinweis auf Videoüberwachungsanlagen dienen. Auch weitere Konkretisierungen und erhöhte Anforderungen für Werbe- und Meinungsforschungsunternehmen wurden in die Neufassung aufgenommen (§ 28). §§ 33 & 34 BDSG 2001 enthielten außerdem weitere Konkretisierungen, wie etwa den Ausschluss einer Auskunftspflicht zur Herkunft von Daten im Falle einer Berührung von Geschäftsgeheimnissen. Im Jahr 2009 wurde schließlich mit § 28b zum Scoring eine weitere bereichsspezifische Regelung ins BDSG aufgenommen.

3. Zusammenfassung

Im Laufe der Änderungen des BDSG unterlagen die Regelungen zur Einwilligung einer stetigen Konkretisierung. Es wurde zwar schon sehr früh darauf geachtet, dass Einwilligungen als solche für den Betroffenen zu erkennen sind und die Einwilligung in die Verarbeitung von personenbezogenen Daten freiwillig erteilt wird. Die Einwilligung verlor jedoch gleichzeitig auch immer mehr an faktischem Gewicht. So etwa durch den Wegfall des Schriftformerfordernisses bei der elektronischen Kommunikation. Dies ist sicherlich nachvollziehbar gerade wegen der Hürde für die Unternehmen, die Einwilligung schriftlich anzufordern (und der hohen Hemmschwelle der Nutzer, diese zu versenden). Es muss jedoch auch gefragt werden, ob die Einwilligung bei den Nutzern noch dieselbe Aufmerksamkeit erhält, wie sie diese noch vor wenigen Jahrzehnten hatte. Gerade vor dem Hintergrund, dass die AGB und Datenschutzerklärungen faktisch nicht mehr gelesen werden. So wird die Einwilligung immer mehr zum einfachen ungelesenen „Klick“ und verliert ihr gesamtes Wirkungsspektrum durch die sozialpsychologische Überlastung des Nutzers, sich mit den Datenverarbeitungsbedingungen auseinanderzusetzen. Bei den Änderungen des BDSG ist weiterhin die Tendenz zu immer spezifischeren Teilbereichsregelungen zu erkennen. Dies zeigt, dass die Datenschutzregelungen immer wieder auf gesellschaftliche, technische und wirtschaftlicher Entwicklungen reagieren und weiterhin reagieren werden müssen. Zunehmend problematischer wird außerdem das Prinzip der „Freiwilligkeit“ der Einwilligung. Bei den Regelungen zum BDSG wurde vom Gesetzgeber immer wieder der Wert auf die Beibehaltung dieses Prinzips gelegt, wobei es immer schwieriger wurde, das Prinzip der Freiwilligkeit in der Praxis umzusetzen.

8 vgl. § 19a II Nr. 3 BDSG-2001

Das Gebot der Transparenz war von Beginn an eines der Hauptanliegen des Gesetzgebers. Vorrangig sollten die von der Datenerhebung und Datenverarbeitung Betroffenen ihre Rechte kennen und umfangreiche Einflussmöglichkeiten erhalten, um ggf. gegen eine fehlerhafte oder eine unrechtmäßige Datenspeicherung vorzugehen. Besonders die in den neueren Änderungen aufgenommene Vorgabe zur Datenersterhebung schaffte den Betroffenen Transparenz über die gespeicherten personenbezogenen Daten. Während anfänglich noch versucht wurde, die Betroffenen über Bekanntmachungen in öffentlichen Druckwerken zu informieren, wurde schon bald damit begonnen, eine aktive Informationspflicht und umfangreiche Auskunftsrechte im BDSG zu verankern. Auch die zunehmend wichtig gewordene Institution des/der Bundesbeauftragten für den Datenschutz und (nach Inkrafttreten des Gesetzes zur Regelung des Zugangs zu Informationen des Bundes am 1. Januar 2006) der Informationssicherheit hat zur Ermöglichung der Transparenz erheblich beigetragen. Dies gilt auch für das Melderegister. Kernpunkt der Regelungen zur Transparenz war schließlich das Auskunftsrecht, welches immer weiter fortentwickelt wurde.

II. Einwilligung und Transparenz unter der EU-Datenschutz-Grundverordnung

1. Einführung

Unter dem Einfluss der sich rasant entwickelnden Technologien und der Globalisierung auf die Verarbeitung von personenbezogenen Daten, nehmen die Faktoren „Einwilligung und Transparenz“ an Bedeutung stetig zu. Die damit verbundenen Anforderungen an eine Datenverarbeitung konnte die EU-Richtlinie 95/46/EG nicht mehr ausreichend abdecken. Bezüglich Einwilligung und Transparenz war das Bedürfnis insgesamt groß, einen einheitlich anwendbaren Rechtsrahmen zu schaffen.

So waren ausdrückliche Regelungen zur Transparenz bzw. transparenten Datenverarbeitung, wie etwa die leichte Zugänglichkeit von Informationen in einfacher und verständlicher Sprache, in der EU-Richtlinie 95/46/EG gar nicht enthalten. Dies tangiert in einer digitalisierten Welt im besonderen Maße das Grundrecht auf informationelle Selbstbestimmung.

Hinsichtlich der Bedingungen einer Einwilligung regelte die EU-Richtlinie 95/46/EG, dass eine Einwilligung ohne Zwang, für den konkreten Fall und in Kenntnis der Sachlage erfolgt, dass die betroffene Person durch diese Einwilligung akzeptiert, dass personenbezogene Daten, die sie betreffen, verarbeitet werden. Allerdings haben die einzelnen Nationalstaaten diese Vorgabe sehr unterschiedlich ausgelegt und damit ebenso die jeweiligen gesetzlichen Regelungen unterschiedlich gestaltet. In einigen EU-Mitgliedstaaten musste die „Einwilligung“ ausdrücklich, in anderen schriftlich erteilt werden, während andere sogar eine konkludente Einwilligung für ausreichend erachtet haben. Dies wiederum hatte zur Folge, dass Einwilligungserklärungen nicht in allen Mitgliedstaaten gleichermaßen Gültigkeit hatten.[9]

9 http://ec.europa.eu/justice/news/consulting_public/0006/com_2010_609_en.pdf

Die Europäische Kommission hat bereits im November 2010 ein Dokument zu einer öffentlichen Befragung veröffentlicht. Darin sind unterschiedliche Meinungen über einen zukünftigen Rechtsrahmen in Europa hinsichtlich des Schutzes von personenbezogenen Daten zusammengefasst.[10]

Die Artikel-29-Gruppe hat etwa eine Stärkung Rechte der betroffenen Personen hervorgehoben, einschließlich einer „Purification" der Einwilligungsbedingungen:

! "Greater empowerment of data subjects, including a 'purification' of the consent requirement, as it is currently often used dubiously (e.g. internet 'opt-out') and more easily accessible means of redress for data subjects;"

Ebenso haben die befragten Bürger zum einen angeregt, die Wichtigkeit der Einwilligung nochmals zu bekräftigen, und zwar unter Berücksichtigung der zunehmenden Selbstbestimmungsmöglichkeiten, die mit einer wachsenden Nutzung von Internetdiensten und Sozialen Netzwerken verbunden sind. Zum anderen wurde vorgeschlagen, rechtliche Rahmenbedingungen über Mechanismen zur Aufhebung der erteilten Einwilligung zu schaffen.

Ein Entwurf der Datenschutz-Grundverordnung wurde am 25.1.2012 von der EU-Kommission vorgestellt.[11] In der Folgezeit wurde eine Vielzahl von Änderungsanträgen eingearbeitet und dazu zunächst ein Berichtsentwurf des Europäischen Parlaments am 16.01.2013 vorgelegt.[12] Am 21.10.2013 hat daraufhin der Ausschuss für Bürgerliche Freiheiten, Justiz und Inneres (LIBE) über das Verhandlungsmandat des Europäischen Parlaments zur Datenschutz-Grundverordnung mit 49 Ja-Stimmen, 1 Gegenstimme und 3 Enthaltungen abgestimmt[13] und einen ersten Entwurf unter Berücksichtigung der mittlerweile über 3000 Änderungsanträge des Europäischen Parlaments verabschiedet.[14] Weiterhin wurde die Aufnahme von Verhandlungen mit dem Rat der Europäischen Union (Ministerrat) gemäß Art. 70 GO beschlossen.[15]

10 http://ec.europa.eu/justice/news/consulting_public/0003/summary_replies_en.pdf

11 Datenschutz-Grundverordnung der EU-Kommission vom 25.1.2012, KOM(2012) 11 endgültig 2012/0011 (COD) - Vorschlag für Verordnung des Europäischen Parlaments und des Rates zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr (Datenschutz-Grundverordnung): http://ec.europa.eu/justice/data-protection/document/review2012/com_2012_11_en.pdf

12 Berichtsentwurf 2012/0011 (COD) vom 16.01.2013; Entwurf eines Berichts über den Vorschlag für eine Verordnung des Europäischen Parlaments und des Rates zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr (Datenschutz-Grundverordnung) (COM(2012)0011 – C7-0025/2012 – 2012/0011(COD); http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-%2F%2FEP%2F%2FNONSGML%2BCOMPARL%2BPE-501.927%2B04%2BDOC%2BPDF%2BV0%2F%2FDE)

13 https://www.janalbrecht.eu/themen/datenschutz-digitalisierung-netzpolitik/alles-wichtige-zur-datenschutzreform.html

14 https://www.janalbrecht.eu/themen/datenschutz-digitalisierung-netzpolitik/alles-wichtige-zur-datenschutzreform.html mit Verweis auf die inoffizielle Fassung nach der Abstimmung des LIBE-Ausschusses unter https://www.janalbrecht.eu/fileadmin/material/Dokumente/DPR-Regulation-inofficial-consolidated-LIBE.pdf - Außerdem Mester, EU-Datenschutz-Grundverordnung, DuD 12/2015, 822.

15 Vgl. Mester, EU-Datenschutz-Grundverordnung, DuD 12/2015, 822.

Der Bericht des LIBE-Ausschusses über den Vorschlag für eine Verordnung des Europäischen Parlaments und des Rates zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr (allgemeine Datenschutzverordnung) folgte sodann am 22.11.2013. Dieser enthielt den Entwurf einer legislativen Entschließung des Europäischen Parlaments.[16]

Das Europäische Parlament hat im darauffolgenden Jahr am 12.03.2014 einen Vorschlag zur Datenschutz-Grundverordnung in erster Lesung verabschiedet.[17] Eine Entscheidung des Ministerrats über eine gemeinsame Herangehensweise bei der Datenschutzreform erfolgte hat am 11.06.2015, so dass in Trilogverhandlungen mit dem Europäischen Parlament eingetreten werden konnte.[18]

Die abschließenden Verhandlungen (Trilog) zwischen EU-Parlament, Ministerrat und EU-Kommission begannen schließlich am 24. Juni 2015. Ein erstes Dokument hierzu wurde am 15.12.2015 veröffentlicht,[19] ein konsolidierter Text folgte am 28.01.2016.[20]

Am 27.04.2016 wurde die endgültige Fassung der Datenschutz-Grundverordnung verabschiedet.[21]

Unter Bezugnahme auf diese gerade genannten Zeitpunkte sind nun im Folgenden die im Verlaufe der Verhandlung der Datenschutz-Grundverordnung vorgeschlagenen Änderungen sowie Auffassungen bezüglich der Anforderungen an eine wirksame Einwilligung (siehe b)) und an die Transparenz (siehe c)) näher dargestellt.

16 *Bericht über den Vorschlag für eine Verordnung des Europäischen Parlaments und des Rates zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr (allgemeine Datenschutz-Grundverordnung)(COM(2012)0011 – C7-0025/2012 – 2012/0011(COD), - dieser Vorschlag erfolgte in Kenntnis des Berichts des Ausschusses für bürgerliche Freiheiten, Justiz und Inneres sowie der Stellungnahmen des Ausschusses für Beschäftigung und soziale Angelegenheiten, des Ausschusses für Industrie, Forschung und Energie, des Ausschusses für Binnenmarkt und Verbraucherschutz und des Rechtsausschusses - http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//NONSGML+REPORT+A7-2013-0402+0+DOC+PDF+V0//DE*

17 *Legislative Entschließung des Europäischen Parlaments vom 12. März 2014 zum Vorschlag für eine Verordnung des Europäischen Parlaments und des Rates zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr (allgemeine Datenschutz-Grundverordnung) (COM(2012)0011 – C7-0025/2012 – 2012/0011(COD)) (Ordentliches Gesetzgebungsverfahren: erste Lesung; http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+TA+P7-TA-2014-0212+0+DOC+XML+V0//DE*

18 *Vorschlag für eine Verordnung des Europäischen Parlaments und des Rates zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr (Datenschutz-Grundverordnung); https://www.datenschutz-grundverordnung.eu/wp-content/uploads/2015/12/Entwurf_der_Ratspr%C3%A4sidentschaft_ST_9565_2015_INIT_DE.pdf*

19 *Council of the European Union, Brussels, 15 December 2015 (OR. en) 15039/15 https://www.datenschutz-grundverordnung.eu/wp-content/uploads/2015/12/proposal-eudatap-regulation-final-compromise-151216.pdf*

20 *Rat der Europäischen Union, Brüssel, 28.01.2016 (OR.en) 5455/16, Interinstitutionelles Dossier: 2012/0011 (COD) http://eur-lex.europa.eu/legalcontent/DE/TXT/PDF/?uri=CONSIL:ST_5455_2016_INIT&from=EN*

21 *Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung) http://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=CELEX:32016R0679&from=DE*

2. Einwilligung

a) Erster Entwurf der EU-Kommission zur Datenschutz-Grundverordnung vom 25.01.2012

Im ersten Entwurf der Datenschutz-Grundverordnung[22] vom 25.01.2012 war vorgesehen, dass die Einwilligung explizit und ohne Zwang in Form einer Erklärung oder sonstigen eindeutigen Handlung erfolgen sollte.

! Artikel 4 Nr. 8 Begriffsbestimmungen
„Einwilligung der betroffenen Person“ jede ohne Zwang, für den konkreten Fall und in Kenntnis der Sachlage erfolgte explizite Willensbekundung in Form einer Erklärung oder einer sonstigen eindeutigen Handlung, mit der die betroffene Person zu verstehen gibt, dass sie mit der Verarbeitung der sie betreffenden personenbezogenen Daten einverstanden ist;

Ohne Zwang bedeutete gemäß Erwägungsgrund (33) die Klarstellung, dass die Einwilligung keine rechtswirksame Grundlage für die Verarbeitung liefert, wenn die betreffende Person keine echte Wahlfreiheit hat. Die Beweislast sollte der Verantwortliche der Verarbeitung tragen (Erwägungsgrund 32 und Artikel 7 Nr. 1).

Erwägungsgrund (25) hat insoweit präzisiert, dass die Einwilligung mittels geeigneter Methode erfolgen sollte, die

- eine für den konkreten Fall und in Kenntnis der Sachlage abgegebene Willensbekundung der betroffenen Person in Form einer Erklärung oder einer eindeutigen Handlung ermöglicht,
- sicherstellt, dass der betreffenden Person bewusst ist, dass sie ihre Einwilligung in die Verarbeitung personenbezogener Daten gibt,
- etwa durch Anklicken eines Kästchens beim Besuch einer Internetseite und durch jede sonstige Erklärung oder Verhaltensweise, mit der die betroffene Person in dem jeweiligen Kontext klar und deutlich ihr Einverständnis mit der beabsichtigten Verarbeitung ihrer personenbezogenen Daten signalisiert.

22 *Datenschutz-Grundverordnung der EU-Kommission vom 25.1.2012, KOM(2012) 11 endgültig 2012/0011 (COD) - Vorschlag für Verordnung des Europäischen Parlaments und des Rates zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr (Datenschutz-Grundverordnung): http://ec.europa.eu/justice/data-protection/document/review2012/com_2012_11_en.pdf.*

b) Stellungnahme des Deutschen Bundestages vom 06.11. 2012 zum ersten Entwurf der EU-Kommission zur Datenschutz-Grundverordnung

Zu diesem Entwurf der Datenschutz-Grundverordnung erfolgte eine Stellungnahme des Deutschen Bundestags im November 2012. Bezüglich der Einwilligung hob der Deutsche Bundestag die große Bedeutung der Freiwilligkeit nochmals hervor, forderte die Bundesregierung gleichzeitig ebenso auf, auf praxisgerechte Regelungen zur Einwilligung und zum Widerspruch zu achten.[23]

! Der Deutsche Bundestag nimmt zu den Vorlagen gemäß § 9 des Gesetzes über die Zusammenarbeit von Bundesregierung und Deutschem Bundestag in Angelegenheiten der Europäischen Union wie folgt Stellung:
Der Deutsche Bundestag fordert die Bundesregierung auf,
...

8. unter Beachtung der großen Bedeutung der Freiwilligkeit der Einwilligung auf praxisgerechte Regelungen zur Einwilligung und zum Widerspruch zu achten und dabei ebenfalls zu berücksichtigen, dass auch in Fällen eines Ungleichgewichts zwischen den Vertragspartnern, die wirksame Einwilligung nicht zwingend ausgeschlossen ist,
...

c) Berichtsentwurf des Europäischen Parlaments zur Datenschutz-Grundverordnung vom 16.01.2013

Außerdem gab es zahlreiche Änderungsanträge zum Kommissionsentwurf der Datenschutz-Grundverordnung vom 25.01.2012, die zunächst in einem Berichtsentwurf des Europäischen Parlaments vom 16.01.2013 zusammengefasst wurden.[24]

Hinsichtlich der Einwilligung bezogen sich diese Änderungsanträge im Bericht vom 16.01.2013 zum einen auf die Definition gemäß Artikel 4 (8), die in Änderungsantrag 89 dahingehend ergänzt wurde, dass der Betroffene mit der Datenverarbeitung für einen oder mehrere spezifische Zwecke einverstanden sein kann sowie auf Erwägungsgrund 31 (Änderungsantrag 17), in dem „Einwilligung“ durch „konkrete und ausdrückliche Zustimmung in Kenntnis der Sachlage“ ersetzt werden sollte.

! Änderungsantrag 89
Artikel 4 (8)
„Einwilligung der betroffenen Person“ jede ohne Zwang, für den konkreten Fall und in Kenntnis der Sachlage erfolgte explizite Willensbekundung in Form einer Erklärung oder einer sonstigen eindeutigen Handlung, mit der die betroffene Person zu verstehen gibt, dass sie mit der Verarbeitung der sie betreffenden personenbezogenen Daten für einen oder mehrere spezifische Zwecke einverstanden ist;

23 *Drucksache 17/11325 vom 06.11.2012.*

24 *Berichtsentwurf 2012/0011 (COD) vom 16.01.2013; Entwurf eines Berichts über den Vorschlag für eine Verordnung des Europäischen Parlaments und des Rates zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr (Datenschutz-Grundverordnung) (COM(2012)0011 – C7-0025/2012 – 2012/0011(COD); http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-%2F%2FEP%2F%2FNONSGML%2BCOMPARL%2BPE-501.927%2B04%2BDOC%2BPDF%2BV0%2F%2FDE).*

Zum anderen wurde in Erwägungsgrund (33) klargestellt (Änderungsantrag 19), dass die Verwendung von Voreinstellungen, die die betroffene Person verändern muss, keine freie Zustimmung ausdrückt. Bezüglich der Beweislast (Erwägungsgrund 32 und Änderungsantrag 18) wurde der Grundsatz der Datenminimierung betont, indem regelmäßig keine positive Identifizierung der betroffenen Person erforderlich sein soll.

Das Ungleichgewicht zwischen Verantwortlichem und Betroffenem sollte gemäß Änderungsantrag 20 (Erwägungsgrund 34) ebenso in einer beträchtlichen Marktmacht bestehen können.

d) Interinstitutionelles Dossier des Rats der Europäischen Union vom 31.05.2013

In einem interinstitutionellen Dossier des Rats der Europäischen Union vom 31.05.2013 wurde zwischenzeitlich sogar vorgeschlagen, bei der Definition des Begriffs „Einwilligung“ vom Erfordernis einer expliziten Einwilligung abzusehen und „explizit“ durch „ohne jeden Zweifel“ zu ersetzen, da eine explizite Einwilligung als unrealistisch betrachtet wurde.[25]

!

...
Definition des Begriffs „Einwilligung“
14. Die Einwilligung der betroffenen Person ist ein wichtiges Kriterium für eine rechtmäßige Datenverarbeitung (Artikel 6 Absatz 1 Buchstabe a). Die Mehrheit der Mitgliedstaaten ist sich darin einig, dass das Erfordernis einer „expliziten“ Einwilligung in allen Fällen – das von den Anforderungen der Datenschutzrichtlinie von 1995 abweicht – als unrealistisch anzusehen ist. Der Vorsitz schlägt daher vor, „explizit“ durch „ohne jeden Zweifel erteilt“ im Falle der Verarbeitung personenbezogener Daten zu ersetzen, bei denen es sich nicht um die in Artikel 9 genannten besonderen Kategorien handelt, für die an dem Ausdruck „explizit“ festgehalten wird.
15. Im Einklang mit der überwiegenden Mehrheit der Mitgliedstaaten ist Artikel 7 Absatz 4 gestrichen worden. In dem überarbeiteten Erwägungsgrund 34 wird präzisiert, dass die Einwilligung möglicherweise dann nicht gültig ist, wenn im Einzelfall eindeutig ein Ungleichgewicht zwischen den Parteien besteht und es dadurch unwahrscheinlich ist, dass die Einwilligung aus freien Stücken erfolgt ist.

e) Bericht des Ausschusses für Bürgerliche Freiheiten, Justiz und Inneres des Europäischen Parlaments (LIBE) vom 22.11.2013

Der gerade genannte Vorschlag im interinstitutionellen Dossier vom 31.05.2013 war bereits insoweit richtungsweisend, da im endgültigen Bericht des Ausschusses für Bürgerliche Freiheiten, Justiz und Inneres des Europäischen Parlaments (LIBE) vom 22.11.2013 von einer expliziten Einwilligung abgesehen wurde und explizit“ durch „ausdrücklich“ ersetzt wurde, und zwar sowohl in Artikel 4 Nr. 8 als auch in Erwägungsgrund 25.[26]

25 *Rat der Europäischen Union 31.Mai 2013 10227/13 Interinstitutionelles Dossier 2012/0011 (COD) ; Betr.: Vorschlag für eine Verordnung des Europäischen Parlaments und des Rates zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr (Datenschutz-Grundverordnung) – Kernfragen zu den Kapiteln I-IV.*

26 *Siehe zum LIBE-Ausschuss die Ausführungen in der Einführung: Am 21.10.2013 hat der Ausschuss für Bürgerliche Freiheiten, Justiz und Inneres (LIBE) über das Verhandlungsmandat des Europäischen Parlaments zur Datenschutz-Grundverordnung abgestimmt und am 22.11.2013 einen Bericht über den Vorschlag für eine Verordnung des Europäischen Parlaments und des Rates zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr (allgemeine Datenschutzverordnung)(COM(2012)0011 – C7-0025/2012 – 2012/0011(COD) erstellt. http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//NONSGML+REPORT+A7-2013-0402+0+DOC+PDF+V0//DE*

! Änderungsantrag 98
Artikel 4 Nr. 8
„Einwilligung der betroffenen Person“ jede ohne Zwang, für den konkreten Fall und in Kenntnis der Sachlage erfolgte ausdrückliche Willensbekundung in Form einer Erklärung oder einer sonstigen eindeutigen Handlung, mit der die betroffene Person zu verstehen gibt, dass sie mit der Verarbeitung der sie betreffenden personenbezogenen Daten einverstanden ist

Darüber hinaus wurde Artikel 7 Absatz 4 („Ungleichgewicht“) gestrichen und durch eine Regelung ersetzt, die sich auf die Zweckgebundenheit der Einwilligung und das Kopplungsverbot bezieht.

Insgesamt soll nunmehr für eine Einwilligung eine Entscheidung der betroffenen Person erforderlich sein. Erwägungsgrund 25 stellt dazu klar, dass eine ausdrückliche Einwilligung in einer bestätigenden Handlung liegen kann und Schweigen oder bloße Nutzung des Dienstes keine Einwilligung darstellen. Die Verwendung von Voreinstellungen, welche die betroffene Person verändern muss, stellt keine freiwillige Einwilligung dar (Erwägungsgrund 33).

In Erwägungsgrund 32 wird zudem der Verbraucherschutz unter Verweis auf die Anwendung der Richtlinie 93/13/EWG[27] stärker einbezogen, indem zum einen Klarheit und Transparenz der Datenschutzregelungen gefordert wird, zum anderen die Einwilligung in die Verarbeitung von Daten Dritter untersagt ist.

Im Hinblick auf den Widerruf soll gelten, dass dieser so einfach wie die Erteilung der Einwilligung sein muss und die betroffene Person von dem für die Verarbeitung Verantwortlichen zu informieren ist, wenn der Widerruf der Einwilligung zu einer Einstellung der erbrachten Dienstleistungen oder der Beendigung der Beziehungen zu dem für die Verarbeitung Verantwortlichen führen kann (Artikel 7 Absatz 3 und Erwägungsgrund 33).

f) Entschließung des Europäischen Parlaments vom 12.03.2014

Nachdem der LIBE-Ausschuss die Änderungsvorschläge in seinem Bericht vom 22.11.2013 aufgenommen hatte, stimmte am 12.03.2014 das Plenum des Europäischen Parlaments über die Datenschutzreform ab. Insgesamt stimmten 653 Abgeordnete ab, davon 621 für den ausgehandelten Text, 10 Abgeordnete waren dagegen und 22 Abgeordnete enthielten sich.[28]

Das Europäische Parlament hat somit am 12.03.2014 in erster Lesung bezüglich der Einwilligungsvoraussetzungen die Änderungen übernommen, die bereits vom LIBE-Ausschuss am 22.11.2013 angenommen wurden.[29]

27 *Richtlinie des Rates vom 5. April 1993 über missbräuchliche Klauseln in Verbraucherverträgen (ABl. L 95 vom 21.4.1993, S. 29).*

28 *https://www.janalbrecht.eu/themen/datenschutz-digitalisierung-netzpolitik/alles-wichtige-zur-datenschutzreform.html*

29 *Legislative Entschließung des Europäischen Parlaments vom 12. März 2014 zum Vorschlag für eine Verordnung des Europäischen Parlaments und des Rates zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr (allgemeine Datenschutzverordnung) (COM(2012)0011 – C7-0025/2012 – 2012/0011(COD)) Ordentliches Gesetzgebungsverfahren: erste Lesung; http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+TA+P7-TA-2014-0212+0+DOC+XML+V0//DE*

! Artikel 4 Nr. 8 Begriffsbestimmungen
„Einwilligung der betroffenen Person" jede ohne Zwang, für den konkreten Fall und in Kenntnis der Sachlage erfolgte explizite ausdrückliche Willensbekundung in Form einer Erklärung oder einer sonstigen eindeutigen Handlung, mit der die betroffene Person zu verstehen gibt, dass sie mit der Verarbeitung der sie betreffenden personenbezogenen Daten einverstanden ist;

g) Vorschlag des Rats der Europäischen Union vom 11.06.2015

Der Rat der Europäischen Union hat hingegen in seinem Vorschlag vom 11.06.2015 formuliert,[30] dass die Einwilligung weder explizit noch ausdrücklich erfolgen muss, sondern eindeutig auf beliebige geeignete Weise erfolgen kann (Artikel 4 Nr. 8 und Erwägungsgrund 25).

! Artikel 4 Nr. 8 Begriffsbestimmungen
„Einwilligung der betroffenen Person" jede ohne Zwang, für den konkreten Fall und in Kenntnis der Sachlage abgegebene (...) Willensbekundung in Form einer Erklärung oder einer sonstigen eindeutigen Handlung, mit der die betroffene Person zu verstehen gibt, dass sie mit der Verarbeitung der sie betreffenden personenbezogenen Daten einverstanden ist;

h) Weitere Änderungen des Ministerrats im Vergleich zu den Vorschlägen des LIBE-Ausschusses vom 22.11.2013 und des Europäischen Parlaments

- Erwägungsgrund 25 wurde insoweit ergänzt, dass die Einwilligung der betroffenen Person auch durch die Benutzung der entsprechenden Einstellungen eines Browsers oder einer anderen Anwendung erfolgen kann, sofern die betroffene Person zu Beginn des Nutzungsvorgangs die Informationen erhält, die für eine ohne Zwang und in Kenntnis der Sachlage erteilte Einwilligung für den konkreten Fall erforderlich sind.

- Während in den Änderungsvorschlägen des LIBE-Ausschusses vom 22.11.2013 und im Vorschlag des Europäischen Parlament konkret angegeben wird, dass „Schweigen, die bloße Nutzung eines Dienstes oder Untätigkeit" keine Einwilligung darstellen, formuliert der Rat, dass ein stillschweigendes Einverständnis ohne Zutun der betroffenen Person daher keine Einwilligung darstellen sollte.

- Der Rat hat außerdem im Rahmen der Einwilligung die Sicherstellung von Verbraucherschutz im Sinne der Richtlinie 93/13/EWG des Rates vom 5. April 1993 über missbräuchliche Klauseln in Verbraucherverträgen nicht ausdrücklich betont (Vgl. Artikel 7 Absatz 2 und Erwägungsgründe 32, 33). Vielmehr sollten vorformulierte Einwilligungserklärungen in verständlicher und leicht zugänglicher Form in einer klaren und einfachen Sprache zur Verfügung gestellt werden; der Inhalt der Erklärung sollte im Gesamtkontext nicht unüblich sein. Damit sie in Kenntnis der Sachlage ihre Einwilligung geben kann, sollte die betroffene Person mindestens wissen, wer der für die Verarbeitung Verantwortliche ist und für welche Zwecke ihre personenbezogenen Daten verarbeitet werden sollen.

30 *Vorschlag für eine Verordnung des Europäischen Parlaments und des Rates zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr (Datenschutz-Grundverordnung); https://www.datenschutz-grundverordnung.eu/wp-content/uploads/2015/12/Entwurf_der_Ratspr%C3%A4sidentschaft_ST_9565_2015_INIT_DE.pdf und http://data.consilium.europa.eu/doc/document/ST-9565-2015-INIT/en/pdf*

- Bezüglich der Beweislast wurde in Artikel 6 und Artikel 7 ergänzt (Artikel 6 Nr. 1a, Artikel 7 Absatz 1), dass der Verantwortliche beweisen muss, dass der Betroffene eine im Sinne von Artikel 6 Nr. 1a unmissverständliche Einwilligung erteilt hat.

- Im Hinblick auf den Widerruf hat der Rat ansonsten (anders als im Bericht des LIBE-Ausschusses von 22.11.2013 und vom Europäischen Parlament vorgesehen) keine besonderen Anforderungen aufgestellt und es gemäß Artikel 7 Absatz 3 als ausreichend angesehen, wenn die betroffene Person vor Abgabe der Einwilligung über die Widerrufsmöglichkeit in Kenntnis gesetzt wird.

Allerdings verbleibt es im Vorschlag des Rats – entsprechend der Änderungsvorschläge des LIBE-Ausschusses vom 22.11.2013 und dem Vorschlag des Europäischen Parlaments – bei der Streichung von Artikel 7 Absatz 4 („Ungleichgewicht"), wobei dennoch Erwägungsgrund 34 erneut aufgenommen und darin das klare Ungleichgewicht zwischen den Parteien als besonderer Fall formuliert wurde.

i) Trilogverhandlungen zwischen Europäischer Kommission, Europäischem Parlament und Rat der Europäischen Union vom 15.12.2015

Diese zuletzt genannte Ausrichtung der Datenschutz-Grundverordnung durch den Ministerrat wurde ab dem 24.06.2015 im Trilog (EU-Kommission, EU-Parlament und Ministerrat) verhandelt und am 15.12.2015 wurde ein erster Text dieser Trilogverhandlungen veröffentlicht.[31] Der konsolidierte Text folgte am 28.01.2016.[32]

Es sollte nun eine unmissverständlich abgegebene Willensbekundung in Form einer Erklärung oder einer sonstigen eindeutigen Handlung ausreichend sein, eine explizite Einwilligung nur für sensible Daten. Das Ungleichgewicht zwischen betroffener Person und Verantwortlicher wurde in Erwägungsgründen als spezieller Fall gehandhabt, während seine ausdrückliche Erwähnung in Artikel 7 Absatz 4 weiterhin unterblieb. Hinsichtlich der Ausübung des Widerrufsrechts wurden keine besonderen Anforderungen dahingehend gestellt, dass der für die Verarbeitung Verantwortliche zusätzlich zur Information über Einstellung der Dienstleistung verpflichtet ist. Die Möglichkeit des Widerrufs sollte jedoch jederzeit und einfach möglich sein.

Der Vorschlag des Europäischen Parlaments, dass „Schweigen, bloße Nutzung des Dienstes oder Untätigkeit" keine Einwilligung darstellen, wurde geändert in „Schweigen, voreingestellte Kästchen oder Untätigkeit" (Erwägungsgrund 25).

Der Bezug auf die Regelungen des Zivilrechts, Richtlinie 93/13 EWG über missbräuchliche Klauseln in Verbraucherverträgen, wurde beibehalten (Erwägungsgrund 32).

31 *Council of the European Union, Brussels, 15 December 2015 (OR. en) 15039/15 https://www.datenschutz-grundverordnung.eu/wp-content/uploads/2015/12/proposal-eudatap-regulation-final-compromise-151216.pdf*

32 *Rat der Europäischen Union, Brüssel, 28.01.2016 (OR.en) 5455/16, Interinstitutionelles Dossier: 2012/0011 (COD) http://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=CONSIL:ST_5455_2016_INIT&from=EN*

j) endgültige Fassung der Datenschutz-Grundverordnung vom 27.04.2016

In der endgültigen Fassung der Datenschutz-Grundverordnung vom 27.04.2016 ist in der Einwilligungsregelung weder „explizit“ noch „ausdrücklich“ enthalten, sondern „eine eindeutig bestätigende Handlung“ erforderlich.[33]

! Artikel 4 Nr. 11 Begriffsbestimmungen
„Einwilligung“ der betroffenen Person jede freiwillig für den bestimmten Fall, in informierter Weise und unmissverständlich abgegebene Willensbekundung in Form einer Erklärung oder einer sonstigen eindeutigen bestätigenden Handlung, mit der die betroffene Person zu verstehen gibt, dass sie mit der Verarbeitung der sie betreffenden personenbezogenen Daten einverstanden ist;

Danach ist eine Einwilligung eine freiwillige Willensbekundung, die informiert und unmissverständlich abgegeben wurde, entweder durch (schriftliche, elektronische oder mündliche) Erklärung oder durch eine sonstige eindeutig bestätigende Handlung (Artikel 4 Nr. 11 und Erwägungsgrund 32).

Letzteres kann ebenso beim Besuch einer Internetseite, durch die Auswahl technischer Einstellungen für Dienste der Informationsgesellschaft oder durch eine andere Erklärung oder Verhaltensweise geschehen, mit der die betroffene Person in dem jeweiligen Kontext eindeutig ihr Einverständnis mit der beabsichtigten Verarbeitung ihrer personenbezogenen Daten signalisiert (Erwägungsgrund 32).

Außerdem wird durch den Verweis auf die Richtlinie über missbräuchliche Klauseln in Verbraucherverträgen (93/13/EWG) ebenso der Verbraucherschutz einbezogen (Erwägungsgrund 42). Eine vom Verantwortlichen vorformulierte Einwilligungserklärung muss dementsprechend in verständlicher und leicht zugänglicher Form in einer klaren und einfachen Sprache zur Verfügung gestellt werden und darf keine missbräuchlichen Klauseln beinhalten (Artikel 7 Absatz 2).

Die Beweislast für die Abgabe trifft den Verantwortlichen (Artikel 7 Absatz 1), wobei der Widerruf der Einwilligung jederzeit und so einfach möglich sein muss wie die Erteilung (Artikel 7 Absatz 3 und Erwägungsgrund 42).

33 *Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung) http://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=CELEX:32016R0679&from=DE*

3. Transparenz

a) Erster Entwurf der EU-Kommission zur Datenschutz-Grundverordnung vom 25.01.2012

Artikel 11 (Transparenz und Modalitäten) des ersten Entwurfs der Datenschutz-Grundverordnung vom 25.01.2012[34] führte eine Verpflichtung zur Bereitstellung transparenter, leicht zugänglicher und verständlicher Informationen ein, die sich insbesondere an die Madrider Entschließung zu internationalen Standards zum Schutz der Privatsphäre anlehnt.

Erwägungsgrund (38) regelt, dass aus Transparenzgründen der für die Verarbeitung Verantwortliche verpflichtet werden sollte, seine berechtigten Interessen gegenüber der betroffenen Person ausdrücklich darzulegen und diese außerdem zu dokumentieren und die betroffene Person über ihr Widerspruchsrecht zu belehren. Erwägungsgrund (46) sowie Artikel 11 Absatz 2 regeln dazu näher, dass der Grundsatz der Transparenz voraussetzt, dass eine für die Öffentlichkeit oder die betroffene Person bestimmte Information leicht zugänglich sowie in einfacher und verständlicher Sprache abgefasst sein muss, wobei die betroffene Person (Erwägungsgrund (48)) insbesondere über die Existenz des Verarbeitungsvorgangs und seine Zwecke, die Speicherfrist, das Recht auf Auskunft sowie das Recht auf Berichtigung und Löschung der Daten und das Beschwerderecht zu informieren ist. Dies ist in Artikel 12 unter Bezug auf Artikel 13, 14 und 15 bis 19 ausdrücklich geregelt.

Zur Erhöhung der Transparenz wird in Erwägungsgrund (77) außerdem vorgeschlagen, die Einführung von Zertifizierungsmechanismen sowie Datenschutzsiegel und –prüfzeichen anzuregen, die den betroffenen Personen einen raschen Überblick über das Datenschutzniveau einschlägiger Erzeugnisse und Dienstleistungen ermöglichen.

b) Berichtsentwurf des Europäischen Parlaments zur Datenschutz-Grundverordnung vom 16.01.2013

Im Berichtsentwurf vom 16.01.2013[35] heißt es bezüglich der Transparenz (Änderungsantrag 51), dass Zertifizierungsmechanismen sowie Datenschutzsiegeln und -prüfzeichen den betroffenen Personen einen raschen, zuverlässigen und überprüfbaren Überblick über das Datenschutzniveau einschlägiger Erzeugnisse und Dienstleistungen ermöglichen sollen.

34 *Datenschutz-Grundverordnung der EU-Kommission vom 25.1.2012, KOM(2012) 11 endgültig 2012/0011 (COD) - Vorschlag für Verordnung des Europäischen Parlaments und des Rates zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr (Datenschutz-Grundverordnung): http://ec.europa.eu/justice/data-protection/document/review2012/com_2012_11_en.pdf*

35 *Berichtsentwurf 2012/0011 (COD) vom 16.01.2013; Entwurf eines Berichts über den Vorschlag für eine Verordnung des Europäischen Parlaments und des Rates zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr (Datenschutz-Grundverordnung) (COM(2012)0011 – C7-0025/2012 – 2012/0011(COD)); http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-%2F%2FEP%2F%2FNONSGML%2BCOMPARL%2BPE-501.927%2B04%2BDOC%2BPDF%2BV0%2F%2FDE*

Weiterhin wurde in Artikel 5 Absatz 1(a) klarstellend der Begriff „Transparenz“ aufgenommen.

! Änderungsantrag 91
Vorschlag für eine Verordnung
Artikel 5 – Absatz 1 - Buchstabe a
1. Personenbezogene Daten müssen (a) auf rechtmäßige Weise, nach dem Grundsatz von Treu und Glauben und in einer für die betroffene Person nachvollziehbaren Weise verarbeitet werden (Transparenz)

c) Interinstitutionelles Dossier des Rats der Europäischen Union vom 31.05.2013

Vor dem endgültigen Bericht des LIBE-Ausschusses vom 22.11.2013 wurde zwischenzeitlich, in einem interinstitutionellen Dossier des Rates der Europäischen Union vom 31.05.2013, vom Vorsitz des Rates die Bedeutung von verbesserten Transparenzstandards hervorgehoben. Die betroffenen Personen sollten eine Handhabe über die Verarbeitung der sie betreffenden personenbezogenen Daten haben und die ihnen zustehenden Rechte effektiv ausüben können.[36]

! ...
III. Zentrale Fragen – Kapitel III und IV

29. Was die Rechte der betroffenen Personen nach Kapitel III anbelangt, so hebt der Vorsitz die Bedeutung von verbesserten Transparenzstandards hervor; diese sind erforderlich, damit die betroffenen Personen eine Handhabe über die Verarbeitung der sie betreffenden personenbezogenen Daten haben und die ihnen zustehenden Rechte effektiv ausüben können. Diese Standards und Modalitäten für die Ausübung der Rechte der betroffenen Personen sind in Artikel 12 festgelegt. Zur Gewährleistung einer fairen und transparenten Verarbeitung wurden die Verfahren bezüglich der der betroffenen Person zur Verfügung gestellten Informationen angepasst und gestrafft.

IV. Schlussfolgerungen

30. Unter irischem Vorsitz sind erhebliche Fortschritte bei den Verhandlungen über diesen Verordnungsentwurf erzielt worden ...
In Anbetracht des Vorstehenden wird der Rat gebeten, Folgendes generell zu befürworten:
...
5) hinsichtlich der Rechte der betroffenen Personen: den Grundsatz, dass höhere Transparenzstandards gelten sollen, wodurch die Handhabe der betroffenen Personen über die sie betreffenden personenbezogenen Daten verstärkt und eine effektivere Ausübung ihrer Rechte nach Kapitel III erleichtert wird;
...

36 Rat der Europäischen Union 31.Mai 2013 10227/13 Interinstitutionelles Dossier 2012/0011 (COD) ; Betr.: Vorschlag für eine Verordnung des Europäischen Parlaments und des Rates zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr (Datenschutz-Grundverordnung) – Kernfragen zu den Kapiteln I-IV.

d) Bericht des Ausschusses für Bürgerliche Freiheiten, Justiz und Inneres des Europäischen Parlaments (LIBE) vom 22.11.2013

Letztendlich wurden im Bericht vom 22.11.2013[37] die Anforderungen an die Transparenz dahingehend verbessert, dass in Artikel 13a und Anhang 1 Regelungen zu standardisierten Informationsmaßnahmen unter Verwendung von Piktogrammen ergänzt wurden.

In Änderungsantrag 24 zu Erwägung 48 wurde dazu erstmals eine Informationsmöglichkeit durch Icons vorgeschlagen. Neu ist ebenso der Vorschlag, standardisierte Datenschutzprüfzeichen sowie ein „Europäisches Datenschutzsiegel" auf europäischer Ebene einzuführen (Änderungsantrag 52 zu Erwägung 77).

Eingefügt wurde außerdem Artikel 10a mit allgemeinen Grundsätzen für die Rechte der betroffenen Person und mit der Betonung, dass Grundlage des Datenschutzes klare und eindeutige Rechte der betroffenen Person bilden, die von dem für die Verarbeitung Verantwortlichen zu achten sind. Zu diesen Rechten gehören unter anderem die Bereitstellung klarer und leicht verständlicher Informationen.

Zudem wurde Erwägungsgrund 38 präzisiert und bezüglich der Dokumentationspflicht des Verantwortlichen im Hinblick auf seine berechtigten Interessen dahingehend ergänzt, dass das berechtigte Interesse der betroffenen Personen dann überwiegen kann, wenn personenbezogene Daten in Situationen verarbeitet werden, in denen eine betroffene Person vernünftigerweise nicht mit einer weiteren Verarbeitung rechnen muss.

e) Vorschlag des Rats der Europäischen Union vom 11.06.2015

Der Rat der Europäischen Union hat in seinem Vorschlag für eine Datenschutz-Grundverordnung am 11.06.2015[38] die Artikel 11 und Artikel 13 gestrichen, dafür Artikel 12 um „Transparente Information, Kommunikation und Modalitäten" für die Ausübung der Rechte der betroffenen Person ergänzt. Danach muss der für die Verarbeitung Verantwortliche geeignete Maßnahmen treffen, um der betroffenen Person alle Informationen gemäß den Artikeln 14 und 14a sowie alle Mitteilungen gemäß den Artikeln 15 bis 19 und Artikel 32, die sich auf die Verarbeitung personenbezogener Daten beziehen, in verständlicher und leicht zugänglicher Form in einer klaren und einfachen Sprache zu übermitteln. Möglich ist diese Übermittlung in schriftlicher, elektronischer oder mündlicher Form, wenn letzteres von der betroffenen Person (deren Identität nachgewiesen ist) verlangt wird.

In Erwägungsgrund 46 wurde zur Sicherstellung der Transparenz ebenso auf die Verwendung von visuellen Elementen Bezug genommen.

37 *Bericht über den Vorschlag für eine Verordnung des Europäischen Parlaments und des Rates zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr (allgemeine Datenschutzverordnung)(COM(2012)0011 – C7-0025/2012 – 2012/0011(COD), - dieser Vorschlag erfolgte in Kenntnis des Berichts des Ausschusses für bürgerliche Freiheiten, Justiz und Inneres sowie der Stellungnahmen des Ausschusses für Beschäftigung und soziale Angelegenheiten, des Ausschusses für Industrie, Forschung und Energie, des Ausschusses für Binnenmarkt und Verbraucherschutz und des Rechtsausschusses - http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//NONSGML+REPORT+A7-2013-0402+0+DOC+PDF+V0//DE*

38 *Vorschlag für eine Verordnung des Europäischen Parlaments und des Rates zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr (Datenschutz-Grundverordnung); https://www.datenschutz-grundverordnung.eu/wp-content/uploads/2015/12/Entwurf_der_Ratspräsidentschaft_ST_9565_2015_INIT_DE.pdf*

Im Hinblick auf den Grundsatz „Datenschutz durch Technik“ wurde als Umsetzungsmaßnahme unter anderem die Herstellung von Transparenz in Bezug auf die Funktionen und die Verarbeitung personenbezogener Daten vorgeschlagen (Erwägungsgrund 61).

Erwägungsgründe 38 (Dokumentationspflicht bezüglich berechtigter Interessen) sowie Erwägungsgrund 77 (Datenschutzsiegel) hat der Rat hingegen unverändert gelassen.

f) Trilogverhandlungen zwischen Europäischer Kommission, Europäischem Parlament und Rat der Europäischen Union vom 15.12.2015

Die Trilogverhandlungen (zwischen EU-Kommission, EU-Parlament und Ministerrat) begannen am 24.06.2015. Ein erstes Dokument dazu wurde am 15.12.2015 veröffentlicht, der konsolidierte Text folgte am 28.01.2016[39].

Danach setzt der Grundsatz der Transparenz gemäß Erwägungsgrund 30 voraus, dass alle Informationen und Mitteilungen zur Verarbeitung dieser Daten leicht zugänglich und verständlich und in klarer und einfacher Sprache abgefasst sind (insbesondere für die Informationen über die Identität des für die Verarbeitung Verantwortlichen und die Zwecke der Verarbeitung sowie für sonstige Informationen, die eine faire und transparente Verarbeitung gewährleisten).

Artikel 11 und 13 sind hinsichtlich der dort ursprünglich verankerten Transparenzgrundsätze gestrichen, dafür jedoch ist Artikel 12 um Regelungen für „Transparente Information, Kommunikation und Modalitäten für die Ausübung der Rechte der betroffenen Person“ ergänzt worden.

Der Verantwortliche muss dementsprechend geeignete Maßnahmen treffen, um der betroffenen Person alle Informationen gemäß den Artikeln 14 und 14a sowie alle Mitteilungen gemäß den Artikeln 15 bis 20 und Artikel 32, die sich auf die Verarbeitung personenbezogener Daten beziehen, in präziser, transparenter, verständlicher und leicht zugänglicher Form in einer klaren und einfachen Sprache zur Verfügung zu stellen (Artikel 12). Außerdem können die Informationen, die den betroffenen Personen gemäß den Artikeln 14 und 14a bereitzustellen sind, in Kombination mit standardisierten Bildsymbolen bereitgestellt werden, um in leicht wahrnehmbarer, verständlicher und klar nachvollziehbarer Form einen aussagekräftigen Überblick über die beabsichtigte Verarbeitung zu vermitteln.

Diese Anforderung und Möglichkeit der visuellen Elemente ist bereits in Erwägungsgrund 46 erwähnt. Die Kommission hat darüber hinaus die Befugnis, delegierte Rechtsakte zur Bestimmung der Informationen, die durch Bildsymbole darzustellen sind, und der Verfahren für die Bereitstellung standardisierter Bildsymbole zu erlassen.

Bei der Umsetzung des Grundsatzes „Datenschutz durch Technik“ ist die Transparenz in Bezug auf die Funktionen herzustellen (Erwägungsgrund 61). Bezüglich der Erhöhung der Transparenz bleibt es gemäß Erwägungsgrund 77 bei der bereits im ursprünglichen Entwurf enthaltenen Anregung, Zertifizierungsverfahren sowie Datenschutzsiegel und -prüfzeichen einzuführen.

39 Rat der Europäischen Union, Brüssel, 28.01.2016 (OR.en) 5455/16, Interinstitutionelles Dossier: 2012/0011 (COD) http://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=CONSIL:ST_5455_2016_INIT&from=EN

g) endgültige Fassung der Datenschutz-Grundverordnung vom 27.04.2016

In der endgültigen Fassung der Datenschutz-Grundverordnung vom 27.04.2016 ist gemäß Artikel 5 als Grundsatz für die Verarbeitung personenbezogener Daten verankert, dass diese auf rechtmäßige Weise, nach Treu und Glauben und in einer für die betroffene Person nachvollziehbaren Weise verarbeitet werden („Rechtmäßigkeit, Verarbeitung nach Treu und Glauben, Transparenz“).[40]

! Artikel 5 Grundsätze für die Verarbeitung personenbezogener Daten
(1) Personenbezogene Daten müssen
a) auf rechtmäßige Weise, nach Treu und Glauben und in einer für die betroffene Person nachvollziehbaren Weise verarbeitet werden („Rechtmäßigkeit, Verarbeitung nach Treu und Glauben, Transparenz“);

Dieser Grundsatz entspricht weitgehend dem Grundsatz im ursprünglichen Entwurf der Datenschutz-Grundverordnung vom 25.01.2012.

Gemäß Artikel 12 können die Informationen nach Artikel 13 und Auskunftsrechte nach Artikel 14 mit standardisierten Bildsymbolen kombiniert werden. Die Kommission kann hierfür delegierte Rechtsakte zur Bestimmung der Informationen, die durch Bildsymbole darzustellen sind, sowie der Verfahren für die Bereitstellung standardisierter Bildsymbole erlassen.

Der Grundsatz der Transparenz setzt insgesamt voraus, dass eine für die Öffentlichkeit oder die betroffene Person bestimmte Information präzise, leicht zugänglich und verständlich sowie in klarer und einfacher Sprache abgefasst ist und gegebenenfalls zusätzlich visuelle Elemente verwendet werden, wobei diese Information ebenso in elektronischer Form bereitgestellt werden kann, beispielsweise auf einer Webseite (Erwägungsgrund 58 und Erwägungsgrund 39).

Bei der Umsetzung des Grundsatzes „Datenschutz durch Technik“ ist die Transparenz in Bezug auf die Funktionen herzustellen (Erwägungsgrund 78).

Bezüglich der Erhöhung der Transparenz bleibt es gemäß Erwägungsgrund 100 bei der bereits im ursprünglichen Entwurf vom 25.01.2012 enthaltenen Anregung, Zertifizierungsverfahren sowie Datenschutzsiegel und - prüfzeichen einzuführen.

4. Zusammenfassung

Nach der Datenschutz-Grundverordnung ist eine Einwilligung eine freiwillige Willensbekundung, die informiert und unmissverständlich abzugeben ist, entweder durch (schriftliche, elektronische oder mündliche) Erklärung oder durch eine sonstige eindeutig bestätigende Handlung (Artikel 4 Nr. 11 und Erwägungsgrund 32). Letzteres kann spwohl beim Besuch einer Internetseite, durch die Auswahl technischer Einstellungen für Dienste der Informationsgesellschaft, als auch durch eine andere Erklärung oder Verhaltensweise geschehen, mit der die betroffene Person in dem jeweiligen Kontext eindeutig ihr Einverständnis mit der beabsichtigten Verarbeitung ihrer personenbezogenen Daten signalisiert (Erwägungsgrund 32).

40 *Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung) http://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=CELEX:32016R0679&from=DE*

! „Einwilligung“ der betroffenen Person jede freiwillig für den bestimmten Fall, in informierter Weise und unmissverständlich abgegebene Willensbekundung in Form einer Erklärung oder einer sonstigen eindeutigen bestätigenden Handlung, mit der die betroffene Person zu verstehen gibt, dass sie mit der Verarbeitung der sie betreffenden personenbezogenen Daten einverstanden ist;

Zudem wurde in der Datenschutz-Grundverordnung das Transparenzgebot klar formuliert: Personenbezogene Daten müssen gemäß Artikel 5 Absatz 1 a) auf rechtmäßige Weise, nach Treu und Glauben und in einer für die betroffene Person nachvollziehbaren Weise verarbeitet werden („Rechtmäßigkeit, Verarbeitung nach Treu und Glauben, Transparenz“). Der Grundsatz der Transparenz setzt insgesamt voraus, dass eine für die Öffentlichkeit oder die betroffene Person bestimmte Information präzise, leicht zugänglich und verständlich sowie in klarer und einfacher Sprache abgefasst ist und gegebenenfalls zusätzlich visuelle Elemente verwendet werden, wobei diese Information ebenso in elektronischer Form bereitgestellt werden kann, beispielsweise auf einer Webseite (Erwägungsgrund 58 und Erwägungsgrund 39).

Transparenz beginnt bereits bei der Gestaltung des technischen Systems (Grundsatz „Datenschutz durch Technik“), die in Bezug auf die Funktionen hergestellt werden soll (Erwägungsgrund 78). Unterstützend wird die Einführung von Zertifizierungsverfahren sowie Datenschutzsiegeln und -prüfzeichen angeregt (Erwägungsgrund 100). Darüber hinaus wird die konkrete Umsetzung von Transparenz jedoch gleichermaßen im Hinblick auf die Betroffenenrechte erweitert. Gemäß Artikel 12 sind Informationen über personenbezogene Daten, unabhängig davon, ob sie bei der betroffenen Person erhoben werden oder nicht (Artikel 13 und Artikel 14), in präziser, transparenter, verständlicher und leicht zugänglicher Form in einer klaren und einfachen Sprache zu übermitteln. Diese Informationen können mit standardisierten Bildsymbolen kombiniert werden. Die Kommission kann hierfür delegierte Rechtsakte zur Bestimmung der Informationen, die durch Bildsymbole darzustellen sind, sowie der Verfahren für die Bereitstellung standardisierter Bildsymbole erlassen.

III. „Informiertheit der Verbraucher“ als Regulierungsherausforderung

„Rationale Apathie“ oder „Privacy-Paradox“ – es gibt mittlerweile viele Bezeichnungen für das Phänomen, dass Nutzer zwar den Wert ihrer personenbezogenen Daten schätzen, jedoch nicht bereit bzw. nicht im Stande sind, ihre digitalen Rechte aktiv wahrzunehmen und einzufordern. Sie werden zwar ständig um Zustimmung zur Nutzung persönlicher Daten gebeten, diese Zustimmung erfolgt aber regelmäßig ohne eine genaue Kenntnis davon, worin man eigentlich einwilligt. Denn würde man sich tatsächlich Zeit für das Lesen von seitenlangen Datenschutzerklärungen nehmen, würde man diese als juristischer Laie nicht verstehen. Würde man sie doch verstehen, könnte man sie nicht ändern, da die Nutzung eines Produkts meist von der Akzeptanz aller Datenverarbeitungsoptionen durch den Datennehmer abhängt. Die Datenschutzerklärungen sind also meist lang und werden wegen juristischer Anforderungen, technischer Komplexität und Zeitmangels fast nie gelesen, sodass dem Inhalt dieser »Daten-AGB« für gewöhnlich mehr oder minder blind zugestimmt wird. Immer mehr Anfragen nach datenschutzrechtlichen Einwilligung führen beim Dateninhaber außerdem zu einer Entscheidungsüberforderung, Abstumpfung im Sinne einer „rationalen Apathie“ und schließlich zu einer Entwertung der Einwilligung. Und obwohl bei der Zustimmung zu den Datenverarbeitungs-AGB der Schein der Freiwilligkeit entsteht, findet sich die datenschutzrechtliche Idealvorstellung einer „informierten Einwilligung“ im realen Leben der Menschen somit faktisch kaum wieder.

Freilich gehört zur informationellen Selbstbestimmung aber auch die Freiheit zur Verwertung personenbezogener Daten und zur „informationellen Selbstgefährdung“[41]. Wenn der Nutzer sich wissentlich „digital entblößt“ und die Gefahr einer möglichen, für ihn nachteilhaften Verwendung seiner personenbezogenen Daten bei der Einwilligung billigend in Kauf nimmt, so ist dies letzten Endes auch ein Ausdruck seiner Freiheitsausübung. Aber kann eine Freiheitsausübung ohne genaue Kenntnis der möglicherweise eingegangenen Risiken überhaupt erfolgen? Wo liegt die Grenze zwischen der Entscheidungsherrschaft des Einzelnen und der nicht mehr legitimierbaren Selbstgefährdung?

Aus der Verbraucherperspektive muss daher gefragt werden, wie man in der Praxis die Nutzer dazu bringt, sich mit der Einwilligungsthematik auseinanderzusetzen. Auch wenn den Nutzern mit den Einwilligungsassistenten ein technisches Instrument zur Berücksichtigung der individuellen Datenschutzpräferenzen zur Verfügung stünde, bliebe trotzdem die Frage offen, wo für die Verbraucher überhaupt die Anreize liegen sollen, sich der technischen Lösungsansätze beim Einwilligungsverfahren zu bedienen? Müssen die Einwilligungsanreize rechtlich gesteuert werden, und wenn ja, wie?

Exemplarisch für diese Fragestellungen ist die gängige verbraucherpolitische Diskussion über die Informiertheit der Nutzer. Hier wird oft (mit einer gewissen Selbstverständlichkeit) davon ausgegangen, dass eine gesetzlich vorgeschriebene Vereinfachung der Darstellung von AGB zur Verarbeitung von personenbezogenen Daten automatisch zur besseren Informiertheit der Nutzer und damit in Konsequenz zu einem bewussten und souveränen Umgang mit persönlichen Daten führt. So wird beispielsweise in der Ausschussempfehlung des Bundesrates zur Verbesserung der Verbraucherfreundlichkeit von Allgemeinen Geschäftsbedingungen[42] u. a. die Übersichtlichkeit von Datenschutzhinweisen, eine erleichterte Lesbarkeit und die Hervorhebung von Änderungen empfohlen, „um damit dem tatsächlichen ‚Nicht-zur-Kenntnisnehmen‘ von AGB entgegenzuwirken“[43].

41 Dazu grundlegend: Hermstrüwer, Y., Informationelle Selbstgefährdung, Tübingen 2016.

42 Bundesrat, Drucksache 577/1/16 vom 21.10.2016.

43 Ebd., S. 2

Hervorhebungen wesentlicher Punkte sowie die Kürzung und Straffung von AGB sollen demnach den Nutzern ein zeitaufwändiges Lesen ersparen und ein höheres Maß an Rechtssicherheit gewährleisten, was letztendlich die Transparenz erhöhen und dem Empfänger einen schnellen Überblick über die wesentlichen Änderungen der Vertragsbeziehung ermöglichen soll. In die gleiche Richtung gehen auch Vorschläge wie die Verpflichtung zur Verwendung vorformulierter Datenschutzbestimmungen, wodurch der Betroffene sich mit den einzelnen Bestimmungen eines Geschäftsbereiches bereits vor dem Einwilligungsprozess vertraut machen und anschließend verschiedene Online-Verträge abschließen kann, ohne sich um eine zu weitreichend erteilte Einwilligungserklärung sorgen zu müssen.[44] Auch der Vorschlag eines „One-Pagers" durch den Nationalen IT-Gipfel im Jahr 2015 geht in diese Richtung: Mit dem „One-Pager" sollen die Informationen zur Datenverarbeitung bei digitalen Angeboten so aufbereitet werden, dass die Verbraucher schnell, einfach und umfassend alle wesentlichen Informationen zur Datenverarbeitung bekommen.[45]

Aber sind solche rechtspolitischen Forderungen tatsächlich dazu geeignet, eine datenschutzbewusste Haltung der Verbraucher herbeizuführen? Die Annahme, dass allein transparent gestaltete AGB die Informiertheit der Nutzer zu fördern vermögen, muss jedenfalls hinterfragt werden: Die Bereitstellung transparenter Informationen ist „allenfalls eine notwendige, aber keine hinreichende Bedingung für die akkurate Einschätzung von Datenschutzrisiken"[46]. Die Emotionen und kognitiven Fähigkeiten des Nutzers sind in diesem Zusammenhang ebenso bedeutsam, wenn nicht bedeutsamer.

Zum einen stehen den mittel- bis langfristigen Risiken und Nebenwirkungen der Datenpreisgabe stets kurzfristige Vorteile bzw. geldwerte Vergünstigungen gegenüber, welche die Einwilligungsbereitschaft emotional verstärken. „Oft werden die zeitlich früheren Folgen einer Einwilligung recht konkrete Vorteile darstellen, während spätere Folgen meist weniger wohldefiniert oder greifbar sind."[47] Zusätzliche Informationen dürften die damit verbundene Neigung zur impulsiven oder „kurzsichtigen" Datenpreisgabe nur bedingt abfedern. Dies wirft die Frage auf, ob die Nutzer ihre Einschätzung der Risiken und ihre Einwilligungsbereitschaft schon allein deswegen überdenken würden, wenn sie darüber informiert würden, dass eine (Preis-)Vergünstigung in der Gegenwart zu Nachteilen in der Zukunft führen könnte, etwa höheren Preisen oder datenbasierter Diskriminierung.[48]

Zum anderen muss hinterfragt werden, ob eine komprimierte Darstellung von AGB bisweilen nicht gerade das Gegenteil von Informiertheit bewirkt – und zwar, wenn sie die dargestellten Informationen dem Nutzer als irrelevant erscheinen lässt. So könnten die Diensteanbieter ihre Datenschutzerklärungen theoretisch auch so umfassend gestalten, dass die entscheidenden Informationen unterhalb der Wahrnehmungsschwelle der Nutzer bleiben.[49] Yoan Hermstrüwer stellt in diesem Zusammenhang treffend fest: „Das Datenschutzrecht steht insoweit vor der schwierigen Aufgabe, die Komplexität der Regelungsinhalte von Datenschutzerklärungen dergestalt zu reduzieren, dass die tatsächlich entscheidungsrelevanten Informationen wahrgenommen werden, ohne dass die bereitgestellten Informationen aufgrund ihrer unterkomplexen Darstellung als irrelevant abgetan werden."[50]

44 Pollmann, M. /Kipker, D.-K., IGMR, Eingeschränkte Selbstbestimmung im Onlineverkehr; Stärkung der Einwilligungserklärung durch Einführung vorformulierter Datenschutzbestimmungen, 2016, S. 10 ff., https://www.jura.uni-bremen.de/uploads/IGMR/Pollmann_Kipker_Working-Paper_Eingeschrankte_Selbstbestimmung_im_Onlineverkehr_2016.pdf

45 https://www.bmjv.de/SharedDocs/Artikel/DE/2015/11192015_OnePager_Nationaler_IT_Gipfel.html

46 Hermstrüwer, Y., Informationelle Selbstgefährdung, Tübingen, 2016, S. 236.

47 Ebd., S. 299 (m.w.N.).

48 Vgl., ebd., S. 299.

49 Ebd., S. 312 (m.w.N.).

50 Ebd., S. 312.

Des Weiteren könnten transparent dargestellte Informationen über die Datenpreisgabe den Nutzern ein Gefühl der Kontrollierbarkeit der Datenverwendung suggerieren, ohne dass dieses Gefühl die tatsächlichen Einflussmöglichkeiten auf die Datenverwendung durch Dritte widerspiegelt. Dies könnte unter Umständen zu einer Unterschätzung von Risiken führen: „Das Gefühl der Kontrolle über die Informationspreisgabe [kann] in eine Illusion der Kontrolle über die Informationsverwendung umschlagen.“[51] Die transparenten Datenschutzerklärungen dürfen jedoch nicht als Zusicherung von Schutz fehlinterpretiert werden. In Wirklichkeit liefern sie Informationen zur Aufklärung, auch über eine möglicherweise riskante Datenverarbeitung, und gerade keine „Garantie für Datenschutz“. Bei den rechtspolitischen Forderungen nach transparent gestalteten AGB muss jedenfalls bedacht werden, dass die übersichtlich gestalteten „One-Pager“ – entgegen der häufigen Annahme – bloß ein Informiertheitsgefühl statt tatsächlicher Informiertheit zur Folge haben könnten.

Es muss schließlich hinterfragt werden, inwiefern transparent gestaltete AGB die tatsächliche Bereitschaft der Nutzer steigern, sich mit den Bedingungen der Datenverarbeitung auseinanderzusetzen. So entwickelt beispielsweise ConPolicy im Rahmen eines durch das Bundesministerium der Justiz und für Verbraucherschutz geförderten Forschungsvorhabens konkrete Vorschläge, wie die Entscheidungssituation bei der Einwilligung ausgestaltet sein sollte, damit Verbraucherinnen und Verbraucher informierte Entscheidungen treffen und somit ihre Datensouveränität möglichst gut ausüben können[52]. In Bezug auf das oben bereits aufgeführte Beispiel des „One-Pagers“ des Nationalen IT-Gipfels, wird dort empirisch untersucht, wie Entscheidungssituationen bei Einwilligungen gestaltet sein müssen, um den Verbrauchern eine informierte Einwilligung zu erleichtern und die bestehenden Missstände zu beheben. Diese Vorschläge basieren auf verhaltenswissenschaftlichen Erkenntnissen zu den Auswirkungen der Gestaltung und Strukturierung von Wahlentscheidungen im Online-Kontext. Eine solche Herangehensweise ist jedenfalls zu begrüßen, da sie einen konkreten rechtspolitischen Vorschlag auf seine praktische Geeignetheit durch valide empirische Forschung prüft.

Im Zusammenhang mit PIMS muss an dieser Stelle angemerkt werden, dass die Einwilligungsassistenten einige der dargestellten Herausforderungen durchaus zu bewältigen im Stande wären – etwa durch die automatisierte Kontrolle der zweckmäßigen Datenverwendung oder auch durch eine automatisierte Zusammenstellung von tatsächlich abgefragten Daten anhand einer technischen Erkennung des Datenzugriffs. Aber auch hier müssten die tatsächlichen Entscheidungen der Nutzer und ihre Bereitschaft zur Nutzung technischer Einwilligungsassistenten verhaltensökonomisch untersucht werden.

Die oben dargestellten Aspekte am Beispiel der „Informiertheit“ zeigen, dass die rechtlichen Anforderungen an eine informierte Einwilligung und Einwilligungsplattformen ohne zusätzliche verhaltensökonomische Einsichten schwerlich auskommen können. 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.“[53] 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. Es ist daher wichtig zu klären, welche Faktoren die Entscheidung der Nutzer beeinflussen, sich über die Datenverarbeitung zu informieren und die Einwilligung von den so gewonnenen Informationen abhängig zu machen.

51 Ebd., S. 318.

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

53 Hermstrüwer, Y., Informationelle Selbstgefährdung, Tübingen 2016, S. 249.

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