STIFTUNG DATENSCHUTZ

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

Handlungsempfehlungen

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

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

Executive Summary

Die Preisgabe von persönlichen Daten gehört längst zum Alltag der Menschen in unserer vernetzten Welt. Ohne eine Einwilligung zur Datenverarbeitung kommen die Bürger allerdings 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. 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 der ausgeweiteten Verpflichtungen im Zuge der EU-Datenschutz-Grundverordnung haben zugleich auch die Unternehmen verstärkten Bedarf, mit nachvollziehbar dokumentierten und möglichst informiert erteilten Einwilligungserklärungen mehr Rechtssicherheit zu erlangen und Kundenvertrauen zu erhöhen. Die informierte Einwilligung bleibt dabei ein ganz entscheidendes Werkzeug der Informationsautonomie und letzten Endes eine Voraussetzung für die Ausübung des Grundrechts auf informationelle Selbstbestimmung.

Wie kann dieser Entwicklung Rechnung getragen werden? Welche Rolle spielt dabei die eingesetzte Technik? Inwiefern kann man den betroffenen Personen durch den Einsatz „intelligenter Technik“ die Verfügungsmacht über ihre Daten zurückgeben und eine verbesserte Einwilligungsmöglichkeit erzeugen? 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?

Eine große Chance bestünde dann, wenn es zukünftig gelänge, durch einen anwenderfreundlichen technischen Lösungsansatz die häufig inflationäre Erteilung von Einverständniserklärungen zu vermeiden und gleichzeitig mehr Rechtssicherheit herzustellen. So fordert auch der Grundsatz „Datenschutz durch Technik“ (Art. 25 DSGVO) bei der Sicherstellung der Transparenz und im Hinblick auf die Einwilligung technische Lösungsansätze. Es spricht vieles dafür, dass mehrere aktuelle Probleme im Bereich des Datenschutzes durch die sogenannten „Personal Information Management Services“ (PIMS) bzw. „Privacy Enhancing Technology“ (PET) gelöst werden könnten.

Die Idee hinter solchen 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. Damit könnten nicht nur die Anforderungen an eine „informierte Einwilligung“ erfüllt werden, sondern auch der Weg zu sogenanntem „Empowered Consent“ ermöglicht werden. So könnten die Nutzer in den Stand versetzt werden, Datenschutzpräferenzen selbstbestimmt zu setzen. Für die Wirtschaftsseite, insbesondere für den Mittelstand, würden gleichzeitig Rechtssicherheit geschaffen und Kosten für die notwendige Umsetzung der Datenschutzvorschriften gesenkt werden. Durch die kontrollierte Preisgabe von personenbezogenen Daten, verbunden mit der Möglichkeit, die Daten dynamisch zu aktualisieren, könnte außerdem die Qualität der Daten gesteigert werden (Smart Data).

Je nachdem, auf welchen Teilaspekt oder auf welche Reihe von Schwerpunkten sich die einzelnen Projekte konzentrieren, können durch den Einsatz von automatisierten Einwilligungsverfahren ebenso viele Anforderungen aus der Datenschutz-Grundverordnung umgesetzt werden – so etwa eine informierte Einwilligung (Art. 4 Abs. 11), die Zweckbindung und die Datensparsamkeit (Art. 5 Abs. 1), das Recht auf Datenübertragbarkeit in maschinenlesbarem Format (Art. 20 Abs. 1.) sowie die Sicherheit der Datenverarbeitung.

Die gemeinnützige Bundesstiftung für den Datenschutz hat im Rahmen eines vom Bundesministerium des Innern geförderten Projekts eine Reihe von unterschiedlichen Einwilligungsprojekten verglichen sowie die rechtlichen[1] und ökonomischen[2] Rahmenbedingungen für die Implementierung von Einwilligungsplattformen untersucht.[3] Im vorliegenden Papier 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.

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

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

3 Siehe Studie „Neue Wege bei der Einwilligung im Datenschutz – technische, rechtliche und ökonomische Herausforderungen“ der Bundesstiftung (beide o.g. Gutachten finden sich auch als Anhang der Studie): https://stiftungdatenschutz.org/themen/projekt-einwilligung-und-transparenz/

Inhaltsverzeichnis

I. Herausforderungen

1. Technische Ausgestaltung von Einwilligungsassistenten

1.1 Produktspezifische Herausforderungen

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? Welche Lösungsansätze – sowohl international als auch in Deutschland – existieren bereits und wo besteht weiterhin Forschungsbedarf?

Die Stiftung Datenschutz hat eine Reihe von sehr unterschiedlichen Projekten verglichen.[4] Die Evaluation von technischen Möglichkeiten und Lösungsansätzen im Bereich von PIMS zeigt, dass viele Ansätze Voraussetzungen für die legale Verarbeitung betroffener Daten schaffen und Auskunftsrechte oder Rechte zur Beschränkung der Verarbeitung, Löschung oder digitales Vergessen ermöglichen könnten, ohne stets erneut eine direkte Nutzerinteraktion zu erfordern. Auf diese Weise vereinfachen sie das Einwilligungsverfahren.

Die Ansätze wurden u. a. im Hinblick daraufhin untersucht, inwiefern sie Transparenz schaffen durch automatisierte Erstellung einer Übersicht über die Zugriffsrechte der verschiedenen Applikationen; inwiefern sie die Nutzer selbstbestimmt im Vorfeld entscheiden lassen, wer welche Daten zu welchem Zweck erhalten soll; auf welche Weise sie die Selbstkontrolle durch individuelle Nutzungsübersicht ermöglichen und inwieweit sie im Sinne des Selbstdatenschutzes die Verbraucher motivieren können, ihre Daten durch Wahrnehmung ihrer Auskunftsrechte zu kontrollieren.

Bei den untersuchten Projekten bestehen dabei erhebliche Unterschiede, sowohl im Hinblick auf die technische Herangehensweise als auch auf die wirtschaftliche Umsetzung. Sie unterscheiden sich auch im Hinblick darauf, wie breit die Anwendungen aufgestellt sind. So kann ein Lösungsansatz z. B. nur einen Schwerpunkt beinhalten (z. B. reine Nutzeraufklärung) oder aber auch mehrere unterschiedliche Angebote in sich vereinen.

Bei einigen Projekten wie PGuard oder auch MyPermissions steht die Nutzeraufklärung als Ziel im Vordergrund. Es wird jeweils davon ausgegangen, dass wenn die Nutzer 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 für diejenigen Daten, die ohnehin abgeschöpft werden, der Nutzer zumindest eine monetäre Kompensation erhält. Dies könnte einerseits als eine Art der Resignation vor dem zunehmenden Kontrollverlust gegenüber einer massenhaften Abschöpfung von personenbezogenen Daten betrachtet werden.

4 *Siehe Studie „Neue Wege bei der Einwilligung im Datenschutz – Technische, rechtliche und ökonomische Herausforderungen“: https://stiftungdatenschutz.org/themen/projekt-einwilligung-und-transparenz/*

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.

Für die Wiedergewinnung der Datensouveränität machen schließlich diejenigen Ansätze am meisten Hoffnung, welche durch eine einheitliche zentralisierte Datenkontrolle an einer Stelle („One-Stop-Shop“) dem Nutzer auf einfache und verständliche Art und Weise die Möglichkeit geben, seine Daten zu verwalten und bei mehreren Dienstanbietern die Weitergabepräferenzen gleichzeitig zu ändern. Auf diese Weise kann eine „informierte Einwilligung“ technisch ermöglicht und der „Einwilligungsüberforderung“ entgegengewirkt werden.

Bei den spezifischen technischen Erwägungen unterscheiden sich die einzelnen Ansätze unter anderem hinsichtlich des Standortes der Daten (zentral/cloud-basiert/lokal). 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). Das Vertrauen der Verbraucher in ein dezentrales System, bei dem die Daten in der Nutzersphäre bleiben, dürfte tendenziell größer sein als in ein zentrales.

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. Aus technischer Sicht ist entscheidend, wie die Abstufung von Kundenpräferenzen ausgestaltet sein muss, damit der Verbraucher einerseits seinen Datenweitergabe-Willen klar formulieren kann, andererseits jedoch nicht durch ständig neue Anfragen zu geänderten oder erweiterten Nutzungszwecken überfrachtet wird. Gerade Letzteres kann mittelfristig zur Abstumpfung des Nutzers beim Einwilligungsvorgang führen.

Gerade für den weder technisch noch juristisch vorgebildeten Nutzer ist es darüber hinaus wichtig, ein Mindestmaß an Verständnis über die technischen Vorgänge zu bekommen. Dazu gehört z. B. eine übersichtliche Datenschutzerklärung, die Nutzung von Symbolen, Übersichtsgrafiken oder der Einsatz einfacher und stimmiger Erläuterungen zur Funktionsweise.

Viele der untersuchten Ansätze befinden sich noch in einer Entwicklungs-, Test- oder Implementierungsphase. Es bleibt daher abzuwarten, inwiefern sich die technischen Lösungsansätze sowohl auf Anbieterseite 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 soll dem Nutzer an einer Stelle („One-Stop-Shop“) 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. 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 werden.

Abschließend muss festgestellt werden, dass sich die Auseinandersetzung mit automatisierten Einwilligungsverfahren und Einwilligungsassistenten in Deutschland noch in den Anfängen befindet, 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. 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]

1.2 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 der europaweiten, 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?

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*

- 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).

2. Rechtliche Herausforderungen

2.1 Anforderungen an den Einwilligungsassistenten[7]

Im Fokus der rechtlichen Betrachtung stehen technische Konzepte, die zum Ziel haben, Nutzer bei 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[8]. Es muss 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.

In Bezug auf die von der Stiftung Datenschutz betrachteten Ansätze 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 Funktionsweisen einzelner Konzepte können daher im Folgenden lediglich grundsätzliche Anforderungen an einen Einwilligungsassistenten benannt, nicht jedoch eine abschließende rechtliche Beurteilung einzelner Ansätze vorgenommen werden.

7 Dieser Abschnitt bezieht sich auf die Stellungnahme zu rechtlichen Aspekten eines Einwilligungsassistenten der Stiftungsstudie (Anhang 1) https://stiftungdatenschutz.org/themen/projekt-einwilligung-und-transparenz/
Die Stellungnahme ist ebenfalls einzeln abrufbar unter: https://stiftungdatenschutz.org/themen/projekt-einwilligung-und-transparenz/

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

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 DSGVO (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 Project) können bei der Umsetzung berücksichtigt werden.

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 möglich sein.[9] Einige Konzepte[10] könnten gleichwohl bei Forschungszwecken unterstützend eingesetzt werden. Gemäß Erwägungsgrund 33 DSGVO 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 überprüfbar sein. Schwierigkeiten können sich etwa dann ergeben, wenn in den Datenschutzhinweisen auf vertragsrelevante Zwecke verwiesen wird und daraus gemäß Nutzerpräferenz automatisiert eine Einwilligungserklärung generiert wird. Für vertragliche Zwecke ist jedoch keine Einwilligung erforderlich, lediglich 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.

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

10 Wie z. B. „Consent Management for Federated Data Sources”-Ansatz der TU Berlin. Zur Beschreibung des Ansatzes siehe Studie der Stiftung Datenschutz (a.a.O.), Kapitel II. 2.

Probleme, die sich im Zusammenhang mit dem Recht auf Datenübertragbarkeit (Artikel 20 DSGVO) ergeben könnten, wären damit ebenso umgangen.[11]

Die Richtigkeit der Daten (Artikel 5 Absatz 1d) DSGVO) kann systemseitig sichergestellt werden, wenn der Einwilligungsassistent in der Lage ist, diejenigen Datenzugriffe zu verhindern, bei welchen Empfänger, Zweck und Umfang der konkreten personenbezogenen Daten nicht übereinstimmen. Die möglichen Empfänger erhalten 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 anzufragen/einzuholen.[12]

Im Rahmen der Gestaltung des Einwilligungsassistenten muss im besonderen Maße auf das Kopplungsverbot und die freie Bestimmung durch den Betroffenen geachtet werden. Es müssen die Gesamtumstände berücksichtigt werden und 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. Es darf außerdem 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.

Der Einwilligungsassistent sollte automatisiert sicherstellen können, 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. 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) DSGVO fordert aber gerade die Sicherstellung der Transparenz.

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

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

Hier könnte geprüft werden, inwieweit der sogenannte „One-Pager“ als transparente Zusammenfassung der erteilten Einwilligung unterstützend in Betracht kommt.[13] 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 im Auftrag des Bundesministeriums der Justiz und für Verbraucherschutz untersucht werden[14]).

In diesem Zusammenhang sei angemerkt, dass die rechtlichen Anforderungen an eine informierte Einwilligung und Einwilligungsplattformen ohne zusätzliche verhaltensökonomische Einsichten schwerlich auskommen können. Die Bereitstellung transparenter Informationen ist zwar eine notwendige, aber keine hinreichende Bedingung für eine genaue Einschätzung von Datenschutzrisiken – die Emotionen und kognitiven Fähigkeiten des Nutzers sind in diesem Zusammenhang ebenso bedeutsam, wenn nicht bedeutsamer.[15] Mit anderen Worten: Die rechtlichen Rahmenbedingungen für eine informierte Einwilligung lassen sich nur angemessen bewerten und gestalten, wenn auch die tatsächliche Bereitschaft der Nutzer, sich mit dem Schutz ihrer eigenen Privatsphäre aktiv auseinanderzusetzen, in den Blick genommen wird.

Abschließend muss festgestellt werden, dass es stets entscheidend ist, 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. In diesem Zusammenhang ist besonders an einheitliche Verhaltensregeln oder Leitlinien zu denken. Bei der praktischen Umsetzung kann ein Einwilligungsassistent mit transparenten Gestaltungsmöglichkeiten 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.

2.2 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 Verantwortung der Hersteller/Entwickler.

13 *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*

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

15 *So: Hermstrüwer, Y., Informationelle Selbstgefährdung, Tübingen 2016, S. 236*

- 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.

- 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 jedoch die Möglichkeit einer „pauschalen Interessensbekundung“ prüfen. Die Umsetzung eines konkreten Anbieters kann jedoch nur dann „für den bestimmten Fall informiert“ erfolgen, wenn keine Daten übermittelt oder bekannt gegeben 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 nach 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.[16] 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?[17] Eine der wesentlichen Aufgaben bestünde dabei darin, die Komplexität der 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.[18]

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

17 *Hermstrüwer, Y., Informationelle Selbstgefährdung, Tübingen 2016, S. 237*

18 *Ebd., S. 312*

3. Ökonomische und verbraucherpolitische Herausforderungen[19]

3.1 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 es international in 2014-2015 rund 400 Unternehmen sein, schätzt die britische Unternehmensberatung Ctrl-Shift.[20]

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), 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.

19 *Dieser Abschnitt stellt die Zusammenfassung des von der Stiftung Datenschutz in Auftrag gegebenen gleichnamigen Gutachtens von Dr. Nicola Jentzsch dar (Deutsches Institut für Wirtschaftsforschung (DIW Berlin)). Das Gutachten findet sich als Anhang 2 der Stiftungsstudie https://stiftungdatenschutz.org/themen/projekt-einwilligung-und-transparenz/ Das Gutachten ist ebenfalls einzeln abrufbar unter: https://stiftungdatenschutz.org/themen/projekt-einwilligung-und-transparenz/*

20 *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*

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.[21] 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 müssen 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.[22]

Um sich am Markt durchzusetzen, müssen die PIMS einen deutlichen Mehrwert in der Datenaggregation generieren und bestenfalls Echtzeitdaten abbilden. Datenbasis und Datenqualität werden hier zu Schlüsselfaktoren, wenn die Plattformen sich in der Informationsintermediation durchsetzen sollen. 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.

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

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

3.2 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 Online-Einkäufen 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.[23]

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.[24] Hierzu gehören Effekte wie Status quo-Akzeptanz, Entscheidungskomplexität und Verlustaversion, um nur einige zu nennen, die erheblich die Entscheidung des Verbrauchers verzerren können.[25] Die Anwendung solcher und ähnlicher Erkenntnisse aus der ökonomischen Wirtschaftsforschung wird insbesondere dann unabdingbar sein, wenn Marktmechanismen aufgesetzt werden sollen.

23 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.

24 Siehe dazu: Jentzsch, N., Ökonomische Rahmenbedingungen innovativer Lösungen zu Datenschutz-Einwilligungen, S. 28 ff. https://stiftungdatenschutz.org/themen/projekt-einwilligung-und-transparenz/

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

3.3 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, welche 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 multi-homing 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.[26]

- 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.[27] 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.

26 Zu den Protokollen des sicheren Datenaustausches gehören bspw. das XDI Protokoll (s. http://xdi.org/).

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

II. 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.[28] Hier kann sich auch die Formulierung eines Negativkatalogs empfehlen.

Der Europäische Datenschutzausschuss sollte

- aufgrund der unterschiedlichen Auslegung in der Vergangenheit 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 Auslegungshilfe das Kartellrecht oder Markenrecht heranzuziehen ist. Bei Direktwerbung können sich im Rahmen der Datenverarbeitung Überschneidungen zum Wettbewerbsrecht ergeben. Datenschutzrechtlich muss die betroffene Person Verarbeitungstätigkeit oder Zweck vernünftigerweise erwarten dürfen, aber die Datenschutzgrundverordnung 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 diese aufgrund einer Verarbeitungstätigkeit in mehreren Mitgliedsstaaten ausgearbeitet werden können.

Die Europäische Kommission sollte

- noch vor Inkrafttreten der Datenschutzgrundverordnung 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 Auswirkung auf die Betroffenenrechte haben könnte. Bereits in der Vergangenheit wurde der Begriff „explicit“ von den Mitgliedsstaaten im Hinblick auf die Zwecke unterschiedlich übersetzt.[29]

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

29 *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.*

- im Sinne einer Vollharmonisierung und der Sicherstellung eines gleichwertigen Datenschutzniveaus in der Europäischen Union insgesamt frühzeitig kontrollieren, welche Auslegung des Wortlauts der Datenschutzgrundverordnung 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 96/46/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.

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 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. Bei dezentraler Speicherung und der Verantwortung des Nutzers für das System bzw. die Software stellt sich in gleichem Maße die Frage nach Sicherheit sowie Zertifizierung und nach der Verantwortung der Hersteller/Entwickler. Die Datenschutzaufsichtsbehörden könnten auch hier auf Erklärungen der Industrie hinwirken, dass diese als Hersteller datenschutzrechtliche Ansprechpartner sind.

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 zu 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 „DigiMe“ bieten[30], 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 standardisierungsbezogene 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 für das Experimentieren mit und das Testen von Beta-Versionen neuer Dienste mit Nutzern (Labor) genutzt werden kann.

30 *Siehe Studie der Stiftung Datenschutz (a.a.O.), Kapitel II. 2.*

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 können ein geeignetes Instrument darstellen, um potenzielle Anwender in den Entwicklungsprozess frühzeitig einzubinden und Lösungen mit einer konkreten Verwertungschance zu entwickeln.

- Finanzierung der Grundlagenforschung im Bereich des Ende-zu-Ende Privatsphären-Managements, insbesondere 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 Daten-Monetarisierung.

- Insbesondere die tatsächliche Nutzerbereitschaft, 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 beispielsweise durch ConPolicy im Auftrag des Bundesministeriums der Justiz und für Verbraucherschutz im Hinblick auf „informierte Entscheidungen“ durchgeführt werden[31], sind ausdrücklich zu begrüßen, da sie einen konkreten rechtspolitischen Vorschlag auf seine praktische Eignung durch valide empirische Forschung prüfen.

- Die Datenschutz-Folgenabschätzung muss bereits in die Entwicklungsphase von PIMS-Produkten miteinbezogen 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.

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

- Da die potenziellen 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 „informierter 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 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, 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 und 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, insbesondere für den Mittelstand, die Rechtssicherheit bei der Datenverarbeitung gestärkt und eine 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).

- 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 Multiplikatoren 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 o.ä. 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 Practice-Beispiel für den privaten Sektor dienen.

- Es sind europaweite, 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.

STIFTUNG DATENSCHUTZ

New ways of providing consent in data protection - technical, legal and economic challenges

Policy Paper

Foundation for Data Protection
Foundation with legal capacity under the civil code

Karl-Rothe-Straße 10–14
04105 Leipzig
Germany

Phone +49 341 / 5861 555-0
mail@stiftungdatenschutz.org
www.stiftungdatenschutz.org

Founded in 2013 by the German federal government

New ways of providing consent in data protection - technical, legal and economic challenges

Executive Summary

In our networked world the disclosure of personal information has long been a part of everyday life. People can‘t benefit from the digital services available without consenting to the use of personal details. However, the associated data protection policies are usually long and often remain unread because of their legal jargon, technical complexity and lack of time. As a result the content of such„ data protection terms and conditions “is more or less agreed to blindly. More and more requests for data protection consent also cause data owners to be overwhelmed by the need to make decisions, deadening them into a state of ‚rational ignorance‘ and finally to a devaluation of the significance of providing consent. In real life the ideal data protection situation of ‚informed consent‘ is a rarity.

Given the rising incidence of non-informed consent, uncertainty is growing on the part of consumers about how their personal data is actually handled. The situation also leads to asymmetries between what users know about themselves and what the data-processing services know. The trust that is placed in the industry using the data diminishes to the same extent. In view of the uncertainty on the part of consumers and the extended requirements of the EU‘s General Data Protection Regulation, companies at the same time have an increased need to gain more legal certainty and increase customer confidence by clearly documented and informed declarations of consent. Informed consent remains an absolutely crucial tool for information autonomy and ultimately a prerequisite for the exercise of the fundamental right to self-determination in terms of individual data.

How can the requirements of this development be satisfied? What role is played by the technology which is applied? To what extent can those who are affected be given back sovereignty over their data by the use of ‚smart technology‘, and how can an improved possibility for providing consent be created? To what extent will it be possible - by means of technical consent supports and consent platforms to strengthen and ensure rights to information, automation of the approval process - to ensure the clarity and intelligibility of the consent as well as the transparency of data processing purposes?

It would be a great opportunity if in future means of a user-friendly technical solution could avoid the frequent inflationary declarations of consent and could ensure more legal certainty at the same time. The principle of „Data protection through technology“ (Art. 25 of the General Data Protection Regulation - DSGVO) accordingly also stipulates technical solutions in order to ensure transparency and with regard to consent. There is a great deal in favour of solving several current problems in the field of data protection by so-called „Personal Information Management Services“ (PIMS) or ‚Privacy Enhancing Technology‘ (PET).

The idea behind such approaches is that it should be possible for users to decide when, to whom, for what purposes, to what extent and for how long they transmit their data, and track the use of this data and, if necessary, withdraw their consent to its use. This would not only meet the requirements for, informed consent‘ but also open up the way to so-called ‚empowered consent‘. So users could be put in a position to determine their own data protection preference settings. For business, especially for small and medium-sized companies, legal certainty would be created and costs for the necessary implementation of data protection regulations would simultaneously be reduced.

The controlled disclosure of personal information, coupled with the ability to update the data dynamically, would also increase the quality of the data (smart data).

Depending on what aspect or focal points the individual projects are concentrated on, the use of automated consent processes could also implement many requirements of the General Data Protection Regulation - for example informed consent (Article 4 para. 11.), the use of data for specific purposes, data minimisation (Art. 5 para. 1), the right to data portability in machine-readable format (Art. 20 para. 1) and the security of data processing.

In a project funded by the Federal Ministry of the Interior the non-profit Federal Association for Data Protection compared a number of different data consent projects. It also investigated the legal[1] and economic[2] conditions for the implementation of consent platforms.[3] This study looks at possible ways of using technology to facilitate the legal validity of the consent process in terms of greater self-determination and user control. Proposals are developed on how the process of consent in data protection law and practice can be made more practicable and provided with technical support.

1 See also: "Stellungnahme zu rechtlichen Aspekten eines Einwilligungsassistenten" (Opinion on legal aspects of the consent assistant), Prof. Anne Riechert, Foundation for Data Protection,https://stiftungdatenschutz.org/themen/projekt-einwilligung-und-transparenz/

2 See also: Report „Ökonomische Rahmenbedingungen innovativer Lösungen zu Datenschutz-Einwilligungen", Dr. Nicola Jentzsch, German Institute for EconomicResearch (DIW Berlin), https://stiftungdatenschutz.org/themen/projekt-einwilligung-und-transparenz/

3 See study: "Neue Wege bei der Einwilligung im Datenschutz - technische, rechtliche und ökonomische Herausforderungen (New approaches to consent in data protection - technical, legal and economic challenges) by the Federal Foundation (both of the above reports can also be found as an appendix to the study): https://stiftungdatenschutz.org/themen/projekt-einwilligung-und-transparenz/

Content

I. Challenges

1. Technical design of consent assistants

1.1 Product-specific challenges

To what extent will technical consent assistants and consent platforms ensure the strengthening of rights to information, the automation of the consent process, the clarity and intelligibility of the consent, and the transparency of data processing purposes? What solutions - both internationally and in Germany - already exist and where is further research needed?

Stiftung Datenschutz (the Foundation for Data Protection) has compared a number of very different projects.[4] The evaluation of technical possibilities and solutions in the field of PIMS shows that many approaches could create the preconditions for the legal processing of the relevant data and enable access rights or rights to restrict the processing, erasure or digital oblivion of data without requiring repeated direct user interaction. In this way they would simplify the consent process.

The approaches were analysed from the point of view of how they create transparency through automated creation of an overview of the access rights of various applications; how they let the user decide individually in advance who should receive what data and for what purpose; how they enable users to take control by providing an overview of usage and how - in terms of self-protection of their data - they can motivate consumers to control their data by exercising their rights to information.

The examined projects show significant differences, both in terms of their technical approach and economic implementation. They also differ in terms of how extensive the effect of the application is. For example a specific approach may only have one focus (e.g. pure user education), or can combine several different purposes.

For some projects, such as PGuard or MyPermissions the main focus is on user education. In each case it is assumed that giving users an insight into the personal information stored on them will provide them with an incentive to be more careful with their data when surfing. A prerequisite for the use of such approaches is that users should already have a minimum sensitivity, or even a certain lack of trust towards the data-processing industry, and are interested in obtaining an insight into the use of data by third parties.

Other projects seek to enable more checks on the handling of personal data or to simplify data control. Projects like Citizenme and Datacoup aim to ensure that users at least receive monetary compensation for data which is skimmed off anyway. On the one hand, this could be regarded as a kind of resignation relating to increasing loss of control over the mass skimming off of personal data. On the other hand - taking a very pessimistic approach - the monetization of data transfer could in future prove to be the only remaining pragmatic possibility for the user to counter the uncontrolled trade in data.

4 *See study "Neue Wege bei der Einwilligung im Datenschutz" (New approaches to consent in data protection - technical, legal and economic challenges):https://stiftungdatenschutz.org/themen/projekt-einwilligung-und-transparenz/*

In terms of the recovery of data sovereignty, the approaches which give the most hope are those which - using a single centralised data checkpoint at one location (‚one-stop-shop') - present users with a simple and understandable way of managing their data and of changing their transfer preferences simultaneously with several service providers. In this way ‚informed consent' can be made technically possible and ‚consent overwork' can be counteracted.

In the specific technical considerations, approaches differ among other factors with regard to the location of the data (central / cloud-based / local). Where and how personal data is stored is crucial not only for the evaluation of data protection safety but also with regard to other factors such as confidence in a platform and the security of the data. The various approaches range between two extremes: on the one hand, cloud-based solutions in which the data is stored on external servers and access to users is ensured via client applications. On the other hand, there are purely local applications in which data is stored locally with the user. Both of these methods have advantages and disadvantages: local data management can affect the compatibility with other systems and counteract a high level of market distribution. By contrast, cloud solutions can pose difficulties in terms of data security. For example, attacks on central storage locations are easier and - because of the quantity of data available for stealing - more attractive („honeypot") than stealing data from individual users (e.g by means of Trojans). Consumer confidence in a decentralised system, in which the data remains within the sphere of the user, tends to be greater than in a centralised system.

For the technical implementation, it is also important to consider how much influence users have on the transfer of their data and whether dynamic adjustment options and thus comprehensive user controls, are made possible to them by technical means. From a technical perspective it is crucial how the gradation of customer preferences is configured, so that consumers can on the one hand clearly formulate their intentions relating to the transfer of their data, and are not on the other hand overloaded by constantly new requests relating to amended or extended usage purposes. In the medium term the latter in particular can lead to the desensitising of users with regard to the consent procedure.

For users who are neither technically nor legally educated it is also important to obtain a basic level of understanding of the technical processes. This includes for example a clear data protection statement, the use of symbols, explanatory graphics or the use of simple and coherent explanations of the way the system functions.

Many of the examined approaches are still in the development, testing or implementation phase. It remains to be seen in what way the technical solutions will prevail both on the provider side as well as the user side, and how the technical methods can be adapted to the requirements of the EU's General Data Protection Regulation.

From the perspective of the Foundation for Data Protection a personal information management service must ideally meet the following criteria:

- A single centralised data checkpoint should enable users to manage their data at one location (‚one-stop-shop'), as well as to change their transfer preferences and delete shared data if necessary with multiple several service providers simultaneously.

- The product should ideally include the following three functions.

    1. Displaying transparency (automatically grouping the data processing operations desired by the data recipient in a standardised machine-readable declaration of consent);

    2. Conveyance of transparency (with the use of understandable standardised symbols and pictograms which convey the data protection declarations in a simplified way);

    3. Enabling an informed decision (instead of opt-in and opt-out options the decision should involve defining data protection preferences).

- The technical traceability of data use (‚sticky policies') and an automated right to information should be guaranteed.

- It should include the ability to make the disclosure of personal data granularly based on customer preference, combined with the possibility for users to dynamically update the data and the relevant scope of authorisation themselves. .

- The system must be simple, but designed in detail as required. The user may not be overwhelmed, but advanced users should have the ability to adjust their interests via ‚advanced settings' in detail. The balance between different user interests must be ensured.

Finally, it must be noted that the application of automated approval processes and consent assistants is still in its infancy in Germany, although these subjects have already been dealt with intensively at a European level. In September 2016, in an official statement by[5] the EDPS (European Data Protection Supervisor), the opportunities and challenges of PIMS were assessed and the specific justification of support for the development of such innovative approaches were highlighted to the Commission. The PIMS report of the European Commission published in November 2016 addressed the particular challenges of the implementation of PIMS platforms in detail.[6]

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*

1.2 General challenges

- It must be clarified whether the consent assistant should be available only for certain segments (social networking, health information, finance, etc.) or whether universal assistants are possible for all aspects of data handling. What requirements must be met to achieve this?

- To reach the greatest possible number of users, products must feature a user-friendly set of instructions, with pictograms and symbols to achieve a minimum level of clarity and intelligibility for the consent. For this purpose the need for the Europe-wide uniform standardisation of data protection instructions and icons is clear.

- For factors such as confidence in the platform and security of the data, the location of the data (cloud or local) is crucial. On the one hand, local storage might affect compatibility with other systems. On the other hand, the cloud solution can bring problems of data security or user trust.

- For the technical implementation it must be taken into account how much influence users have on the transfer of their data and whether dynamic adjustment possibilities and revocability are available. From a technical perspective it has to be investigated how the gradation of customer preferences is to be enabled.

- Possibilities must be explored for delegating the consent process to other people or computers if the data provider is not able, in certain situations, to give legal consent (especially significant for patients in the health / e-health sector).

- The need for a clear determination of the identity of the party using the data also requires a technical solution. In addition, what happens with company acquisitions? Are the obligations of the company passed on the purchaser? Is data blocked if the company making the acquisition does not comply with the negotiated framework?

- For adaptive consent assistants it still has to be clarified how a change by the user is handled. Is the previous status (such as a default „no data to advertisers“) stored in a history, and where is this history stored (with all data holders or in an archive?), are changes implemented immediately, and is this technically possible at all? Real-time updates, especially with the amount of data records, could overwhelm the system. Where are data records temporarily cached for update in delayed updates?

- Can and should data records and consents be processed by third parties (such as correcting errors in the database)? Or should only the user have the possibility of correction, with the risk that the data is not error-free. Who informs, where necessary, the user of possible errors and checks for data validity?

- The core problem remains with how user confidence in the respective platform can be established with technical support. The use of solid cryptography can be a way (it may be necessary here to involve quantum cryptography research).

2. Legal challenges

2.1 What is required of the consent assistant?[7]

The focus of the legal considerations is on technical concepts which aim to support users in automated form when performing their consent. The reason for this is that not only the principle of ‚data protection by the design of technology' in accordance with Article 25 of the General Data Protection Regulation calls for the development of data protection compliant technical solutions, but Article 29 relating to data protection group also calls for the submission of technical means to comply with the legal framework for cookies[8]. It must be clarified, therefore, whether from May 2018 the PIMS approaches can comply with the legal requirements of the General Data Protection Regulation, what requirements need to be observed in the design of the relevant technology and whether the uniform legal framework is complied with in terms of the consent requirements. For this purpose, the conditions of consent in accordance with the General Data Protection Regulation have had to be interpreted in the light of current legal practice.

With regard to the approaches looked at by the Foundation for Data Protection, it must be considered that the further technical development of the systems, and in particular their planned concrete application, will have a significant impact on the question of the legal status of the consent assistant and the issues of responsibility and liability involved. Due to the present lack of detailed and published technical descriptions and functioning of individual concepts, in what follows only basic requirements of a consent assistant can be provided, and no final legal assessment of individual approaches can be made.

A clear confirmative action under Article 4 no. 11 GDPR is fulfilled by the consent assistant if it makes it possible in easily accessible and understandable language for a person to give consent to the use of personal data for different processing purposes, recipients or categories of recipients. The necessary granularity also needs to be taken into account. Location data must be examined separately, as the exact location has to be determined. If the person concerned in accordance with the provisions of Article 29 Data Protection Group can tick blank boxes with the desired processing purpose, a this would even mean that express consent has been provided. This would in turn correspond to the intention of the originally planned GDPR (draft dated 25.01.2012) as well as the specification of ‚privacy by the design of technology' in accordance with Article 25 GDPR. The findings on P3P (Platform for Privacy Preferences Project) can also be considered in the implementation.

In terms of a data protection-friendly interpretation of the regulation, the purpose of the data processing should also be explicitly stated, which can be achieved by means of a consent assistant. The context must be interpreted in a limited and strict way. In this way dedicated processing within the meaning of Article 5, paragraph 1b) GDPR will then be achieved. In contrast blanket consents are not valid.

7 This section refers to the opinion on the legal aspects of consent assistants in the foundation study (Appendix 1) https://stiftungdatenschutz.org/themen/projekt-einwilligung-und-transparenz/
The opinion is also available at:https://stiftungdatenschutz.org/themen/projekt-einwilligung-und-transparenz/

8 Article 29 Data Protection Working Group,WP 171 Opinion 2/2010 on advertising based on behavioural targeting, adopted on 22 June 2010, p 27

It is therefore necessary for ‚expressions of interest' to make a dynamic possibility of providing consent available.[9] Some concepts[10] could nevertheless be used in order to support research. According to GDPR Recital 33 the person concerned may give their consent for specific areas of scientific research, i.e. without a complete statement of purpose. This could (within the meaning of data recipients) also apply to recipients.

Automated translation of data protection instructions for a consent statement (for example, in the form of a list, whose empty fields must be activated by the user) must be subject to verification in each individual case. Difficulties might for instance arise if the data protection information references contract-related purposes and if a consent statement is generated from this on an automated basis according to user preferences. However, no consent is required for contractual purposes, only transparent information. If the consent assistant is used in future to assist in the conclusion of contracts, then civil law and data protection law must be separated. Under civil law, consensual statements of intent are required for the formation of a contract, and as essentialia negotii of a purchase contract this also includes the definition of the subject and the contracting parties. From a data protection perspective, data may be processed without consent if it is necessary for contractual purposes. Nevertheless, transparent information about the data processing (such as processing for contract-related purposes) must be provided. In designing the consent assistant care must be taken to ensure that this separation is clear to the user.

In addition, from a data protection perspective the consent always includes a right to revocation. With regard to the exercise of the right to revocation, for example, systems such as LETsmart offer users a self-management function, so that users can change, correct and delete their consent at any time. Thus, the requirements for a revocation in accordance with Article 7, paragraph 3 of the GDPR can be met at any time. Problems that could arise in connection with the right to data portability (Article 20 DGPR) would then be bypassed.[11]

The accuracy of the data (Article 5, paragraph 1d) GDPR) may be ensured by the system if the consent assistant is able to prevent the type of data access in which the recipient, purpose and scope of the specific personal data do not match. The potential recipients have access to the records of users only on the condition that the right combination of legitimate recipients and processing purposes are present. In cases of deviations, the consent assistant must also be able, in dynamic form, to request/obtain the consent of the user.[12]

As part of the design of the consent assistant the coupling prohibition and free consent by the relevant parties must be observed to a special degree. All the circumstances must be taken into account and whether the person actually can see in full for which marketing and / or scoring purposes the personal data is used. This self-determination can be difficult to determine in certain individual cases. But the more purposes are interrelated, or the more data reciepients are involved, the more likely is the confusion for the person concerned. When using a consent assistant the impression must also not be created that as a result the data processing is complete - especially if, for example, additional processing is planned for a legitimate reason.

9 The legal requirements of such 'dynamic consent' must be examined separately.

10 Such as: 'Consent Management for Federated Data Sources' - concept by TU Berlin. For a description of the approach see the Foundation for Data Protection study (ibid), Section II. 2.

11 This does not affect the fact that with regard to the copying and storage of user data in their own system, recipients of the data remain subject to data protection requirements.

12 The legal requirements of such 'dynamic consent' must be examined separately.

The consent assistant should be able to automatically ensure that consent is not granted for an indefinite period, but that data access will automatically be prevented - either when the purpose of use no longer applies, or if after an appropriate time the user is asked if he/she wants to maintain his/her the consent. In this case, the restrictions on data storage (Article 5 paragraph 1e) GDPR) and data minimization are fulfilled (Article 5 paragraph 1c) GDPR), since the person concerned decides what data is processed in that access is subject to the declaration of consent together with the category of recipients. The person responsible for the data processing must provide the consent on an informed basis. He must provide the information prior to collection of the data and must be able to show proof of consent. In future, however, it must be determined whether in cases of electronic consent the requirements of the Telecommunications Act and Telemedia Act with respect to logging and constant accessibility will still apply. It should be noted that logging can be used as a form of evidence, but in terms of a European harmonisation other methods could also be considered. For the obligation to provide proof, codes of practice will in future determine conduct.

To support the transparent design of the choices (purpose, recipient, data) and in the interests of an informed and unequivocal expression of will, a consent assistant could also apply visual elements (Recital 58 GDPR). For complex data processing with different purposes or recipients, the representation could well be anything but transparent even if a consent assistant were used. Article 5 paragraph 1a) GDPR, however, requires that transparency should be ensured. Here it could be examined to what extent the so-called ‚one-pager' would be useful as a transparent summary of the consent given.[13] In this context, behavioural science findings as to the net effect of the design and structuring of data protection information on the consumer are highly relevant (as they are being examined for example by ConPolicy on behalf of the Federal Ministry of Justice and Consumer Protection)[14]).

In this context, it should be noted that the legal requirements of informed consent and consent platforms would be difficult to establish without the additional insights of economic behaviour. Providing transparent information is a necessary but not a sufficient condition for an accurate assessment of data protection risks - in this respect the emotions and cognitive abilities of the user are just as important, if not more important.[15] In other words: the legal framework for informed consent can only be assessed and structured appropriately if the actual willingness of users to actively deal with the protection of their privacy is taken into account.

Finally, it must be noted that it is always crucial to ensure the future achievement of the aim of the General Data Protection Regulation of putting in place a uniform and high level of protection for natural persons by applying an equivalent level of protection for the rights and freedoms of natural persons with regard to the processing of their personal data in all member states. In this context, it is particularly useful to consider uniform codes of conduct or guidelines. In practical application a consent assistant with transparent design possibilities can contribute to the level of protection. Users have more control over their options, since data can be collected directly from them, with their active participation and can be limited in time. However, technical developments must constantly be critically examined against a background of ‚automated decisions', the possibilities of profiling and a change of purpose.

13 On the 'one-pager' see the instructions of the Federal Ministry of Justice and Consumer

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

15 E.g.: Hermstrüwer, Y., " Informationelle Selbstgefährdung" (Informational self-endangerment), Tübingen 2016, p 236

2.2 Clarification requirements

- The developer should consider at an early stage whether a decentralised or centralised system is to be applied. In the case of centralised data storage with possible access by multiple recipients, IT security has to be considered above all, together with the question of who is responsible for the data and in what form additional user consent is necessary in this respect. In decentralised storage and where the user is responsible for the system and the software, this also poses the equivalent question of security and the responsibility of the manufacturer / developer.

- In connection with the prohibition on coupling it has to be asked how the consent assistant needs be designed to ensure that the person involved is free to choose between different data, purposes and recipients, without disadvantages arising in the processing of individual elements in the case of non-consent. Consent should not be misleading in this context. The use of such assistants can be a support for the persons concerned if it clearly lists the data processing and the person involved can freely decide between the elements to be processed. When using a consent assistant the impression must also not be created that as a result the data processing is complete - especially if, for example, additional processing is planned for a legitimate reason.

- It must be determined whether in cases of electronic consent the requirements of the Telecommunications Act and Telemedia Act with respect to logging and constant accessibility will still apply. With regard to the obligation to provide proof, codes of practice will in future determine conduct. It should be noted that logging can be used as a form of evidence, but in terms of a European harmonisation other methods could also be considered.

- Blanket consent is not valid. However, developers could consider the possibility of a ‚general expression of interest'. However, the implementation of a concrete provider can only be carried out ‚with information for the specific case' if no data is to be received or disclosed, and instead users receive automated feedback from the system in individual cases, on the basis of which they can decide freely, and if they have (also) agreed to such a procedure previously.

- The information requirements should contain transparent information about the duration of the consent (Article 13 DSGVO). It must be examined by the developer to what extent it can be ensured that after a certain time the consent can be reviewed, or that the agreement is valid only on a one-off basis. It should also be checked by the developer whether users could be notified automatically after a certain time or on a regular basis about the consents they have provided, coupled with the provision of a simple revocation option.

- Although manufacturers are encouraged to develop data protection-compliant technology, but without specific legal responsibility it is unclear how a manufacturer providing a means of processing can be classified as a ‚responsible party' within the meaning of the regulation. This raises the question of security and responsibility on the part of the manufacturer / developer. The data protection authorities could also work towards declarations by the industry, that as manufacturers they will also act as data protection contact partners (see joint statement with the Association of the Automotive Industry). Moreover, on the basis of the draft ‚Regulation on Privacy and Electronic Communications' dated 10.01.2017 it could be examined (in this case for software developers) to what extent a manufacturer can influence the means of data processing.

- It should be clarified to what extent the future installation of software under a consent assistant or its technological advancement can be classified as a separate online service, so that the recipient of the data becomes a provider and accordingly responsible for the consent assistant within the meaning of a service provider (such as an information society service or service with additional benefits). The legal classification of the service also largely depends on the planned functions and the purpose of use.

- In future the question may also be raised whether as such the consent assistant has not already fulfilled the conditions of Article 22 GDPR.[16] For a consent assistant which makes automated decisions this means: either a contract has to be implemented in advance for the ‚application of the consent assistant in itself' between users and the responsible party to regulate the functions of the consent assistant. The automated decision-making would be necessary to fulfil the contract Or the explicit consent of the user would be required for the use of the consent assistant. Here again it is crucial to see if this is feasible on an informed basis and in full knowledge of the facts of a well-defined situation.

- Overall with the applicability of Article 22 GDPR the question remains open if such a regulation is to be interpreted to the effect that a person concerned has the right not to be subjected to a decision based exclusively on an automated process. If the user continues to have the opportunity to lay down specific requirements for the use of the consent assistant, the feature of ‚exclusivity' could be omitted here.

- Last but not least there is the question of whether PIMS can convey to consumers the necessary basic knowledge about the data processing, so that they can anticipate the consequences of data disclosure?[17] One of the main tasks would involve the reduction of the complexity of the regulatory content of data protection statements, so that the actual decision-making information is perceived and the simplified representation format means that the information provided is not dismissed as unimportant.[18]

16 The legal opinion of the study assumes that the consent assistant converts the provided consent in the interests of the granular requirements of the user. The system is not applied on a self-learning basis and therefore does not make its own decisions.

17 E.g.: Hermstrüwer, Y., " Informationelle Selbstgefährdung" (Informational self-endangerment), Tübingen 2016, p 237

18 Ibid., P 312

3. Economic and consumer policy challenges[19]

3.1 General economic conditions for innovative solutions to data protection consent

The main objective of the economic report was to develop a taxonomy that allows an overview of the protagonists in the ‚ecosystem' of innovative consent management, as well as to analyse the market dynamics and supporting economic framework conditions. This should particularly include such projects whose main purpose or activity is self-determined consent management. The innovation provided by technical consent management also constitutes its added value. Therefore, in principle it is a matter of solutions which enable the accessing, use and transfer of personal data by or under the control of consumers (users).

In this case the ‚ecosystem' includes not only governmental and standardisation initiatives but also research projects and both profit-oriented and socially-oriented companies. Overall, the British business consultancy Ctrl-Shift estimates internationally around 400 companies could be involved in 2014-2015.[20]

Initially supplier-centric intermediation platforms can be identified with and without a direct customer relationship can be differentiated from user-centred intermediation platforms. The main difference is that in the latter case the user autonomously assumes the consent management. In many of the traditional intermediation forms (e.g. direct marketing, credit reports) users have no active role or have no direct relationship with the company which aggregates the data.

Within user-centric platforms there is a variety of business models; mostly, however, dealing with bilateral or multilateral platforms which bring together data providers (users) and data consumers (companies, app developers, researchers). Many of the PIMS offer several services, including consent assistants, overview functions, search functions, marketplace functions or preference information (so-called intent casting)).

At the top level, the companies can be divided into hub models and distributed systems. Hub models store user data using cloud solutions (private / public), data centres, or hybrid solutions. Architecturally, data records can be stored centrally with the provider or decentralised (with the respective user). Distributed systems on the other hand store the data in block chain applications or modifications of these.

The revenue models also differ from company to company. While some platforms require transaction-based fees, other pursue subscription or licensing approaches.

19 *This section presents the summary of the study by Dr. Nicola Jentzsch (German Institute for Economic Research (DIW Berlin) commissioned by the Foundation for Data Protection. The report can be found as an Appendix 2 of the Foundation study https://stiftungdatenschutz.org/themen/projekt-einwilligung-und-transparenz/*
The opinion is also available at:https://stiftungdatenschutz.org/themen/projekt-einwilligung-und-transparenz/

20 *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*

In particular platforms are characterised by direct and in particular indirect network effects. Direct network effects arise on the same side of the market, especially if value is created by the use of the service by others. With PIMS this could be a secure data exchange with other PIMS users compared to the use of other technologies.[21] Indirect network effects arise from influences across different parties, for example if more companies request data because users offer it and so the probability of a ‚good data deal' for users is increased (so-called liquidity).

The platforms are in a challenging competitive environment. They have to attract at least two customer groups (data providers and requesters) simultaneously. Many of the platforms present themselves as ‚ecosystems' which want to bring several user groups together. With the users, confidence thresholds need to be overcome and they must be prepared to participate actively in consent management. However, this can only be achieved through credible technical and documented end-to-end security.

PIMS must on the one hand compete with academic free offers (e.g. MyDataCan or OpenPDS). Secondly, they have to compete with traditional information intermediation in order to generate more data demand. Especially the big corporations can also enter the market for innovative consent management at any time.[22]

In order to prevail on the market, PIMS must generate significant added value in data aggregation and at best represent real-time data. The database and data quality are key factors here, if the platforms are to prevail in information intermediation. A greater depth of data per user can be achieved, but the dynamics in the self-selection and in the information disclosure on the platform can cause the distortion of the information base.

Companies that wish to use PIMS on the one hand have to deal with complex reorganisation and standardisation processes arising from the new data management architectures, including potential data return initiatives (so-called share back). At the same time PIMS potentially enable the supply and just-in-time integration of real-time customer information in production processes. An automation of the consent process by machine-readable consent declarations also presents great potential for savings.

Overall, it can be said that a significant mass of people and businesses need to reorient their attitudes for these platforms to have long-term viability.

21 *For a relevant example please see the treatment of personal clouds in Reed (2013: 15 ff.) .*

22 *Although many of these solutions do not provide users with complete control over their data, they provide increased control options; Examples include Oracle Data Cloud Registry (BlueKai & Datalogix cookies), Google Dashboard and Take-out as well as Facebook's 'App Settings'.*

3.2 Economic behavioural challenges in terms of the provision of consent

Consent is an expression of the intention of a consumer to disclose information in a contractual relationship. In many of today's transactions the consumer is, however, not actively engaged with the consent. Many of the decisions relating to information disclosure - for example when making online purchases - can be characterised as a subconscious emotional decision and not as a deliberate and concrete cost-benefit calculation. In addition, the consumer is neither informed about the price for his data profile nor with the revenues third parties make with this data profile.[23]

It will be one of the main challenges for PIMS to design decision-making architectures in such a way that the indicated consumer preferences for privacy (so-called stated preferences) converge more and more with the actions they actually take (so-called revealed preferences). It is therefore important to clarify what factors influence the decision to learn about data processing, and to make the provision of consent dependent on this information. In future legal policy proposals should be examined in terms of their practical suitability in the light of the empirical findings of behavioural research.

Consumers will only opt for a PIMS solution if the benefits exceed the work involved in its use. Its added value will however not be based solely on consent management. The reason is that it is very difficult to persuade users to invest time, cognitive effort and money in something that was previously ‚free' or a kind of incidental function.

In future, the new platforms should allow users to align the privacy and trust settings of their applications with their preferences. There is therefore potential for improving the decision-making options in data processing, especially if the new providers include insights from behavioural economics in decision-making design.[24] This includes effects like accepting the status quo, decision-making complexity and loss aversion, to name but a few factors that can seriously distort the consumer's decision.[25] The application of these and other findings from economic research will be essential in particular if market mechanisms are to be put into place.

3.3 Points requiring clarification

- Since the aggregation and evaluation of personal data can cause the same privacy concerns, platforms first have to gain the confidence of the user. This raises the question of an optimal mix of decision-making design and protocol and technical security.

- To gain acceptance in the market, a platform has to connect - as simultaneously as possible - users who provide the requested data, and the companies which request the data. The benefits for the customer groups depend indirectly on each other, which could generate a multi-sided startup problem.

23 It varies from market to market, whether data is handled in personalised form (with real names) or whether an aggregation of data subjects into micro-groups takes place.

24 See also: Jentzsch, N., "Ökonomische Rahmenbedingungen innovativer Lösungen zu Datenschutz-Einwilligungen", (Economic framework for innovative solutions to data protection consents) P. 28 ff. https://stiftungdatenschutz.org/themen/projekt-einwilligung-und-transparenz/

25 Deviations from optimal behaviour (e.g. maximisation of the expected benefits) are referred to as 'distortions'.

- Under certain circumstances conflicts of interest arise directly between users and companies requesting data. This happens when customers clearly define the intended purpose and prohibit certain data evaluations in which companies have a great interest. For example a customer could allow product personalisation, but prohibit the estimate of willingness to pay by the company on the basis of the data.

- It raises the question as to whether PIMS markets will be characterised by a high number of exclusive users or if users will operate so-called multi-homing, i.e. place data with multiple platforms.

- Standardisation is an important basis for the functioning of these new platforms and - as in the field of interoperability - the question of what standards should be applied is raised.[26]

- A direct sale during the monetisation of personal information would imply the question of what mechanism market participants (should) use in order to set a price for the personal data involved. This is particularly important for platforms which wish to attract users by a sales or marketplace function and / or aim to generate revenues from transaction fees.

- Unravelling - data disclosure due to the self-interest of the data subjects - can cover everyone as a result of the privacy externalities which are generated.[27] While consumers with a good track record (sporting activities, creditworthiness etc.) have incentives to disclose information, consumers who don‘t not actively want to divulge their data arouse negative expectations on the part of companies. The unravelling process raises ethical and normative questions of distribution and fairness which can only be answered by a broad political and social debate.

II. Recommendations for action

1. Policy and practice

The German regulatory authorities should already at this stage be sensitised

⇢ to the issue of the ‚automated consent process and consent assistant‘, and enter into a cross-sectoral, international discourse

⇢ and start promoting the development of codes of conduct and formulate clear requirements with regard to the design of a declaration of consent.[28] The formulation of a negative catalogue can also be recommended here.

The European Data Protection Committee should,

⇢ due to the different interpretations in the past by the member states and supervisory authorities, in future formulate guidelines regarding consent criteria in order to ensure uniform application of the General Data Protection Regulation. Even if consent is subject to an obligation to prove consent and attended penalties, it should be ensured that identical criteria apply uniformly and Europe-wide.

26 *The protocols for secure data exchange include e.g. the XDI protocol (s.Http://xdi.org/).*

27 *Peppet, S.R. (2011). Unravelling privacy: The Personal Prospectus and the Threat of a Full Disclosure Future. Northwestern University Law Review 105: 1153-1204.*

28 *See also the Düsseldorf Circle, "Orientierungshilfe zur datenschutzrechtlichen Einwilligungserklärung in Formularen" (guide to data protection consent forms) March 2016.*

- Guidelines should be established as to what extent antitrust laws or trademark laws are be used as an aid to interpretation. In direct advertising there could be an overlap with competition law in the context of data processing. According to data protection law the person concerned must be reasonably entitled to expect privacy in relation to the processing activity or purpose, but the privacy regulation also relates to consent ‚in a context'. But it is questionable whether this is always to be understood as synonymous with ‚similar services' in a Europe-wide comparison, which could not be examined further in this study.

- In relation to the concept of the ‚responsible party', it needs to be clarified with a guideline to what extent a manufacturer can - on the basis of the draft ‚Regulation on Privacy and Electronic Communications' dated 10.01.2017 (in this case for software developers) - decide on means of data processing.

- The development of uniform EU-wide rules of conduct within the named areas should be promoted, provided these can be worked out on the basis of processing activity in multiple member states.

The European Commission should

- initiate, before the General Data Protection Regulation comes into effect, a review of the extent - in the context of translations by the member states - there is a uniform European-wide understanding of the interpretation of ‚explicit', ‚specified' and ‚provide with' which could have an impact on the rights of those concerned. In the past, the term ‚explicit' was translated differently by the member states with regard to purposes. [29]

- In the interests of full harmonisation and ensuring an equivalent level of data protection in the European Union as a whole, it should be checked at an early stage what interpretation of the wording of the GDPR by member states could affect these objectives and establish what approach is reasonably practicable. One indicator for this review could be the implementation of Directive 96/46/EC in each member state.

Germany's policy-makers and legislators should examine

- to what extent an extension of the product liability law could be applied with regard to ensuring the protection of privacy and whether over time a compensation table corresponding to injury through physical harm could be developed here.

The member states, the data protection authorities and the European Data Protection Committee should

- encourage the adoption of data protection specific certification procedures and privacy seals. In the case of centralised data storage with possible access by multiple recipients, IT security has to be considered above all, together with the question of who is responsible for the data and in what form additional user consent is necessary in this respect. For such a central platform certification is recommended, because users are unable to understand all the technical conditions, the technical security and the procedure of data processing. In decentralised storage and where the user is responsible for the system and the software, this also poses the equivalent question of security and the responsibility of the manufacturer / developer. The data protection authorities could also work towards declarations by the industry, that as manufacturers they will also act as as data protection contact partners.

29 *See also the study on the implementation of Directive 95/46 /EC athttp://ec.europa.eu/justice/policies/privacy/docs/lawreport/consultation/technical-annex_en.pdf("Analysis and impact study on the implementation of Directive 95/46 EC in member states ") and Article 29 Working party" Opinion 03/2013 on purpose limitation ", WP 203 adopted 2 April, 2013.*

The developers

- should develop proposals for the translation of data protection policies in a machine-readable form. In any form of consent request they must also ensure that active user confirmation is required, e.g. by the use of empty boxes that the user actively has to tick. This will exclude implied consent. The findings relating to P3P (Platform for Privacy Preferences Project) should be considered in the implementation.

- With regard to the design of a consent assistant to be used in the context of a civil contract, care should be taken to ensure that users are not given the impression that they are providing their data protection consent for contract-related purposes. From a data protection point of view there is no need for consent for any purpose that is required to fulfil the contract. Nevertheless, the user must be informed about these purposes in a transparent way. Civil law and data protection law must be separated and this separation must be transparent.

- The suggestions of Article 29 Data Protection Group on the design of technical systems for ‚consent to cookies' should be included in the considerations and a check should be made on whether their concept could be extended accordingly - always with the proviso that with third-party cookies prior consent is required.

- Their concepts should be analysed to check whether a combination with existing services and features such as those offered, for example, by ‚MyData' or ‚DigiMe'[30] might be possible and useful.

- It should be considered at an early stage whether a decentralised or centralised system is to be applied.

2. Economic conditions

- Drawing up of guidelines to clarify the language applied in consent forms in a machine-readable manner (among other purpose for secondary use of data).

- Promotion of the exchange via existing interoperability and portability standards, and support for semantic clarification of concepts.

- Promotion of the exchange of existing standardisation systems (incl. ISO standards), APIs and standardised agreements which are conducive to consent management.

- Piloting of projects which aim at technical implementation as well as legally compliant automation of consent declarations.

30 See Foundation on Data Protection study (ibid), Section II. 2.

3. Institutional funding

- Formation of a public-private partnership (hub) to exchange views on important legal, technical and standardisation-related conditions for the development of innovative consent systems modelled on Finland's MyData initiative. Data protection authorities and independent research institutes should be explicitly included here.

- Connection of the above-mentioned hub with the resources of European research projects in this or related fields (e.g. IPACSO, FIDIS, GINI-SA).

- Development of a plan for the more efficient transfer of research results from economic research (especially empirical behavioural research) in the start-up scene or the above-mentioned hub.

- The organisation or promotion of an annual conference or workshop in Germany for protagonists from politics, industry and research.

- Development of a testbed that can be used by startups for experimenting with and testing beta versions of new services with users (laboratory).

4. Research activities

- In the promotion of research on consumer protection, greater focus should be placed on the relationship between data providers and data recipients. The application scenarios of privacy-friendly information technology solutions should be evaluated more intensively in terms of the interests and needs of companies receiving data. However, this demand should not just concentrate on technical security aspects, but must at the same time take into account the economic perspective, the practical applications and the willingness of companies to implement privacy-friendly approaches in their business models. A closer look at both perspectives will enable solutions for dealing with the issue of data protection in a way which not only promotes self-determination and adds benefits, but also increases social perception of the subject.

- Start-up funding or a targeted support programme for validating solutions in specific scenarios may constitute an appropriate instrument to involve potential users in the development process at an early stage and help to develop solutions which offer a concrete commercial opportunity.

- Funding of basic research in the field of end-to-end privacy management, in particular by promoting interdisciplinary research projects in the field of behavioural economics, privacy and choice architectures.

- Promotion of interdisciplinary research in the field of dissolution equilibria (unravelling) and the implementation of the principles and mechanisms of fairness in data markets.

- Financing of behavioural economic work in the field of active consent management and data monetization.

- In particular actual user readiness to use the technical consent assistant must be examined. The consumer policy proposals for the design of decision-making situations relating to consent need to be examined on the basis of the findings of behavioural science on the effects of the design and structuring of choices in the online context. Such studies, which have been carried out for example by ConPolicy on behalf of the Federal Ministry of Justice and Consumer Protection with regard to ‚informed decisions', [31] are to be warmly welcomed, as they review a specific legal policy proposal for its practical suitability by means of valid empirical research.

- The privacy impact assessment must already be included in the development phase of PIMS products. Business and science should develop generic privacy impact assessments for new technologies together. These can also represent a basis for the specific data protection impact assessments of the General Data Protection Regulation.

- Since the potential users and therefore potential partners in the development process are unevenly distributed throughout various federal states, the promotion of information technology solutions at the federal and European level is urgently necessary.

5. Cross-sector activities

- Data protection by means of the design of technology (Art. 25 GDPR) could not only meet the requirements of ‚informed consent', but also the transition from ‚informed consent' to an ‚empowered consent', thereby enabling users to set their own privacy preferences. Privacy preferences can accordingly be set dynamically, context-specifically and graduated. Especially worthy of promotion are the approaches which - using a single centralised data checkpoint at one location (‚one-stop-shop') - present users with a simple and understandable way of managing their data and of changing their transfer preferences or deleting shared data simultaneously with several service providers. Such approaches are particularly suited to enabling ‚informed consent' technically and counteracting ‚consent overload'.

- The special eligibility of automated approval processes for promotion is the result not least of the fact that they have the potential to strengthen self-determination opportunities for consumers in terms of information and at the same time to meet the interests of the data processing industry and to strengthen the capacity for innovation. On the one hand users could be put in a position where they can set their privacy preferences independently. At the same time this would strengthen the economic aspects, especially for mid-sized companies, the legal security of data processing and the possibility of economical implementation of data protection regulations. In addition the granular disclosure of personal information, coupled with the ability to update data dynamically, could also increase the quality of the data (smart data).

- The subject of ‚automated approval processes and consent assistants' is still in its infancy in Germany, although these subjects have already been dealt with intensively at a European level. The awareness of such approaches is at present rather limited in Germany. The need for political and public discussion on the PIMS approaches at the national level is therefore urgent.

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

- Education campaigns and a public debate on technical approaches like PIMS for strengthening informational self-determination are urgently needed in order to sensitise potential users and users for the topic at an early stage. An international discourse between developers, regulators, relevant stakeholders, NGOs, policy makers and potential users requires intensified practical political support (coordination and participation in the discourse, provision of the organisational infrastructure, work as multipliers, etc.).

- An international platform should be set up (along the lines of MyData), on which experiences can be exchanged on a regular basis between developers, regulators and data processing companies. Independent institutions such as the Foundation for Data Protection can form a suitable interface for this.

- Public institutions such as authorities and universities would be particularly suitable as ‚early adopters' of PIMS approaches. The implementation of the consent assistant by the public sector could increase both the acceptance and market entry opportunities, as well as serving as an example of best practice for the private sector.

- Pan-European uniform technical standards are urgently needed. To achieve the greatest possible number of users, products must include user-friendly operation, which uses pictograms and symbols to enable a minimum level of clarity and intelligibility for the consent process. In particular, European standardisation of visual consent assistants is highly desirable.