

PRIVACY NEWS



Aus Sicht der Stiftung Datenschutz – „Der Einwilligungsassistent und die Chancen eines personal data ecosystem“

Frederick Richter, LL. M.

Im vergangenen Jahr berichtete ich an dieser Stelle vom Start unserer Untersuchungen zu neuen Instrumenten für mehr Informiertheit und Kontrolle bei der Einwilligung im Datenschutz. Nun ist es Zeit für die Vorstellung des Befundes.¹

Die Stiftung Datenschutz beleuchtete in den zurückliegenden Monaten verschiedene Ansätze, die uns geeignet erschienen, mit einem anwenderfreundlichen technischen Lösungsansatz der inflationären Erteilung nicht-informierter Einverständniserklärungen zu begegnen. Ziel muss es nämlich aus unserer Sicht sein, dem Datensubjekt mehr Kontrolle über die Verwendung „seiner“ Daten zu ermöglichen und gleichzeitig dem die Daten verwendenden Unternehmen mehr Rechtssicherheit zu bieten, vor allem beim Nachweis der Einwilligung (Art. 7 Abs. 1 DSGVO). Es geht also darum, informationelle Selbstbestimmung umzusetzen, und das dazu praxistauglich; ein hochgestecktes Ziel. Dem Grundsatz „Datenschutz durch Technik“ (Art. 25 DSGVO) und den „Privacy Enhancing Technologies“ (PET) kommt dabei große Bedeutung zu.

Einwilligungsassistenz als Lösung?

Mit einer Idealvorstellung gingen wir in unser Vorhaben: Wäre es nicht probates Mittel gegen die zunehmende Fülle von

Zustimmungsersuchen, wenn Nutzerinnen und Nutzer digitale Werkzeuge bei der Hand hätten, denen sie nur einmal (oder bei Änderung ihrer grundsätzlichen Haltung) ihre Präferenzen zur Datenverwendung mitteilen müssten? Solche Privatsphäre-Assistenten könnten dann gemäß der nutzerbestimmten Voreinstellung die meisten Anfragen zur datenschutzbezogenen Einwilligung abwickeln. Ein Abgleich der vom designierten Vertragspartner vorgeschlagenen Verwendungszwecke mit den Festlegungen des Datensubjekts würde automatisch vorgenommen, und bei Kongruenz würde die erbetene Einwilligung erteilt. Der Nutzer müsste dann nicht jedes Mal erneut entscheiden; er hätte seine Zustimmung zum Datenumgang zuvor abstrakt erteilt; der Einwilligungsassistent würde im Einzelfall den Datenschutzwillen konkret exekutieren.

Schnell stellten wir fest, dass dieses Ideal noch keine Entsprechung in der Realität hat. Bei der rechtlichen Analyse² lernten wir zudem, welche erschwerenden oder gar hindernden Punkte auf dem Weg zu ihm liegen. So muss auch bei einer abstrakten Mandatierung von digitalen Assistenten zur Erteilung konkreter Einwilligungen im Einzelfall der Zweck stets eindeutig for-



Frederick Richter ist Ständiger Autor bei „Privacy in Germany“. Seit Anfang 2013 leitet er die in Leipzig ansässige Bundesstiftung für Privatheit und Datenschutz.
(Foto: Lorenz Becker)

muliert sein. Pauschale Einwilligungen sind unwirksam. Zu klären wären zunächst die Verantwortlichkeiten für das einzusetzende tool, welches die betroffene Person bei einem datenschutzrechtlich sehr relevanten Vorgang unterstützt. Wer soll haf-ten, wenn ein Einwilligungsassistent die Daten der ihn mandatierenden Person nicht im Sinne der Datenschutz-Grundverordnung ordnungsgemäß verarbeitet? Diese Fragen wiegen schwer – dennoch sollten aus unserer Sicht durchaus weitergehende Überlegungen in Richtung digitaler Datenschutz-Assistenten angestellt werden. Auch bei etablierten Unternehmen wächst anscheinend das Interesse an dem Bereich, wie ein erster Wettbewerb zu einem „privacy bot“ zeigt.³

¹ Abrufbar unter: <https://stiftungdatenschutz.org/themen/pims-studie>.

² Stellungnahme zu rechtlichen Aspekten eines Einwilligungsassistenten, A. Richter, 2016, abrufbar unter: https://stiftungdatenschutz.org/fileadmin/Redaktion/Bilder/Abschluss_Studie_30032017/stiftungdatenschutz_Stellungnahme_Rechtliche_Aspunkte_eines_Einwilligungsassistenten_Anhang_1_final.pdf.

³ Abrufbar unter: www.telekom.com/en/media/media-information/archive/deutsche-telekom-launches-competition-for-privacy-bots-481810.

Vielfältige Vorschläge für mehr Kontrolle

Ganz konkret ist dagegen bereits die Entwicklung im Bereich der Personal Information Management Services (PIMS). Die Europäische Datenschutzaufsicht⁴ befasst sich mit diesem Bereich mittlerweile ebenso wie die Europäische Kommission.⁵ Da das Thema in der deutschen Datenschutz-Community ersichtlich – wenn gleich unverständlich – noch keine Rolle spielt, holten wir einige PIMS-Protagonisten im März des Jahres nach Berlin.⁶ Besonders die Initiative MyData,⁷ unterstützt von der Open Knowledge Foundation in Finnland und Frankreich, ist sehr aktiv.⁸

Das Ziel der bei MyData aktiven PIMS-Anbieter und der Vordenker einer „personal data economy“⁹ liegt darin, den Datenbürger – den Ausgangspunkt aller personenbezogenen Daten – wieder in den Mittelpunkt zu stellen. Es soll nicht etwa unterbunden werden, dass Unternehmen und andere Stellen persönliche Informationen für eigene Geschäftsmodelle und Zwecke nutzen. Die betroffene Person aber soll zum einen besser im Bilde sein, was mit den sie betreffenden Daten passiert, und zum anderen auf diese Datenverwendungen mehr Einfluss haben. Schließlich soll das Datensubjekt Teil der persönlichen Datenwirtschaft werden und nicht deren bloßer Zuschauer bleiben. Gewerbliches Ziel und Geschäftsmodell der Unternehmen in der MyData-Community sind attraktive Plattformen für den Austausch und gegebenenfalls Handel mit Nutzerdaten. Ob sich die großen digitalen Plattformen und eine kritische Masse von Nutzerinnen und Nutzern darauf einlassen werden, ist offen.

Die von uns untersuchten Angebote wählen unterschiedliche Wege zu solchem Mehr an Nutzerkontrolle. Je nachdem, auf welchen Teilaspekt oder auf welche Schwerpunkte sich die einzelnen Projekte konzentrieren, kann ihr Einsatz die Umsetzung der Datenschutz-Grundverordnung erleichtern – etwa hinsichtlich der Informiertheit der Einwilligung (Art. 4 Abs. 11 DSGVO), bei Zweckbindung und Datensparsamkeit (Art. 5 Abs. 1 DSGVO), beim Recht auf Datenübertragbarkeit in maschinenlesbarem Format (Art. 20 Abs. 1 DSGVO) oder allgemein bei der Nachvollziehbarkeit der Datenverarbeitung und Belegbarkeit vorliegender Zustimmungserklärungen.

Bei den von uns betrachteten Projekten bestehen trotz des gemeinsamen Zieles einer „(Wieder-)Ermächtigung“ des Nutzers erhebliche Unterschiede in der Herangehensweise. So steht bei PGuard¹⁰ oder MyPermissions¹¹ die Nutzeraufklärung 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 Verhalten datensparsamer zu gestalten. Eine Voraussetzung für die Nutzung solcher Angebote besteht freilich darin, dass die Nutzer bereits über ein Mindestmaß an Sensibilität oder jedenfalls über ein gewisses Vertrauensdefizit gegenüber der datenverarbeitenden Industrie verfügen und interessiert sind, einen Einblick in die Datenverwendung durch Dritte zu bekommen. Andere Projekte wollen vor allem die Datenkontrolle vereinfachen oder den „Datenabfluss“ veranschaulichen. Projekte wie Citizenme¹² und Datacoup¹³ zielen dagegen darauf ab, dass für Daten, die ohnehin abgeschöpft werden, der Nutzer zumindest eine monetäre Kompensation erhält.

PIMS am Start

Viele der untersuchten Ansätze befinden sich noch in der Entwicklungs-, Test- oder Implementierungsphase. Sie stehen, wenn überhaupt, erst seit kurzer Zeit im Markt. Es bleibt daher abzuwarten, inwiefern sich diese neuartigen technischen Lösungsansätze für mehr Datenkontrolle auf Anbieterseite als auch bei den Nutzern durchsetzen können. Aus Sicht der Stiftung Datenschutz lässt sich festhalten, dass ein Personal-Information-Management-Service (PIMS) für beidseitige Akzeptanz verschiedene Elemente bieten sollte: Eine übersichtliche Datenkontrolle sollte dem Nutzer an einer Stelle – via dashboard o. ä., als „One-Stop-Shop“ – ermöglichen, seine Daten zentral zu verwalten. Es sollte möglich sein, bei mehreren Diensteanbietern die Nutzungspräferenzen gleichzeitig zu ändern. Die Nutzer sollten großen Einfluss auf die Weitergabe von Daten haben; ebenso sind dynamische Anpassungsmöglichkeiten (dynamic consent) und einfache Widerrufbarkeit (Art. 7 Abs. 3 S. 4 DSGVO) wichtig.

Abgesehen von den Details der Ausgestaltung wird es bei den innovativen Ansätzen zu einem „personal data ecosystem“ darauf ankommen, dass kritische Masse erreicht wird und sich auch große digitale Plattformen für das System der PIMS interessieren. Ansonsten besteht die Gefahr, dass eine gute Idee in der Nische bleibt. Aus Sicht der Stiftung Datenschutz sollte die öffentliche Hand die sich bietenden Chancen unterstützen und den Bereich fördern.

4 EDPS-Opinion 9/2016 – Opinion on Personal Information Management Systems – towards more user empowerment in managing and processing personal data; abrufbar unter: https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consultation/Opinions/2016/16-10-20_PIMS_opinion_EN.pdf.

5 Abrufbar unter: <https://ec.europa.eu/digital-single-market/en/news/emerging-offer-personal-information-management-services-current-state-service-offers-and>.

6 Abrufbar unter: https://stiftungdatenschutz.org/veranstaltungen/unsere-veranstaltungen-detailansicht/news/abschlussveranstaltung-studie-neue-wege-bei-der-einwilligung-im-datenschutz/?tx_news_pi1%5Bcontroller%5D=News&tx_news_pi1%5Baction%5D=detail&Hash=f5726067cbd82ab938eeb69f8990cb5a.

7 Abrufbar unter: <http://mydata.org/about>.

8 Abrufbar unter: <http://dataethicsconsulting.com/en/the-mydata-movement-has-bloomed>.

9 Abrufbar unter: <https://mobileecosystemforum.com/personal-data-economy-whitepaper>.

10 Abrufbar unter: <https://datenschutz-scanner.de/das-projekt>.

11 Abrufbar unter: <https://mypermissions.com/whoweare>.

12 Abrufbar unter: www.citizenme.com/public/wp/about.

13 Abrufbar unter: <https://datacoup.com/docs/how-it-works>.