DYNAMIC CONSENT ALS WEG AUS DER EINWILLIGUNGSKRISE

Eva Schlehahn / Rigo Wenning

Juristin am Unabhängigen Landeszentrum für Datenschutz (ULD) Schleswig-Holstein in Kiel, Holstenstraße 98, 24103 Kiel, DE;
Email: uld67@datenschutzzentrum.de oder eschlehahn@gmx.de

Jurist am European Research Consortium for Informatics and Mathematics (ERCIM), Sophia Antipolis, 06410 Biot, FR;
Email: rigo@w3.org

Schlagworte: ***Big Data, Datenschutz, DSGVO, Transparenz, datenschutzfreundliche Technologien, dynamische Einwilligung, UI Design,***

Abstract: *Wer hat sie nicht schon verflucht, die Cookie – Banner? Vorausgefüllte Banner sind nach der Planet 49 – Entscheidung des EUGH[1] unzulässig. Manche Stimmen reden sogar vom Ende der Zustimmung im Datenschutz. Gleichzeitig werden die Anforderungen an die Information der Nutzer immer größer. Sie sind eine wichtige Voraussetzung dafür, dass die betroffenen Personen in der Lage sind, eine informierte Entscheidung zu treffen. Der Vortrag beschreibt einen Ausweg aus dem Dilemma mittels «computer-aided consent (CAC)» durch innovative und kontextuale Information. Die Innovation betrifft dabei nicht nur die technische, sondern auch die juristische Dimension und ist daher ein Thema im Zentrum der Rechtsinformatik.*

1. Die Probleme bei herkömmlichen Ansätzen des Einwilligungsmanagements bei Big Data

In jenen Fällen, in denen die Einwilligung Rechtsgrundlage für beabsichtigte personenbezogene Verarbeitungsvorgänge sein soll, verlangt Artikel 4 Abs. 11 DSGVO eine freiwillige, informierte, eindeutige und konkrete Willensbekundung der Betroffenen, die Verarbeitung ihrer personenbezogenen Daten durch eine Erklärung oder sonstig klare Zustimmungsmaßnahme zu akzeptieren. Aus diesem Grund ist erforderlich, dass Betroffene genau verstehen, welche Daten von welchen Stellen für welche Zwecke erhoben werden. Art. 13 DSGVO normiert entsprechende Informationspflichten. Eine entsprechende Datenschutzerklärung muss den gesamten Lebenszyklus der Verarbeitung der personenbezogenen Daten darstellen. Beschrieben wird deshalb alles, vom Zeitpunkt der ersten Datenerhebung über die einzelnen Phasen der Verarbeitung wie Speicherung oder Übermittlung bis hin zur Löschung der Daten.[2] Ziel war immer die informationelle Selbstbestimmung, um dem Betroffenen eine Wahl zu ermöglichen, Machtasymmetrien abzumildern und die Grundsätze der Fairness und Rechtmäßigkeit durch die Einräumung von Kontrolle zugunsten des Betroffenen zu wahren.[3] Viele Verantwortliche sind von der Bereitstellung der Information genauso überfordert wie die Nutzer, die diese Information dann verarbeiten sollen. Es kommt zu Fehlern.[4]

Auf Nutzerseite belegen zahlreiche Untersuchungen und Studien, dass statische, oft lange Datenschutzerklärungen und Nutzungsbedingungen entweder nicht gelesen, oder wenn doch, dann nicht mal ansatzweise von

1 EuGH Grand Chamber, ECLI:EU:C:2019:801 C-673/17.

2 Artikel-29-Datenschutzgruppe (jetzt Europäischer Datenschutzausschuss), Guidelines on transparency under Regulation 2016/679, WP260rev.01, vom 29. November 2017, in der zuletzt überarbeiteten und angenommenen Fassung vom 11. April 2018.

3 Dies wurde von der damaligen Artikel-29-Datenschutzgruppe gefordert; siehe WP259rev.01 vom 28. November 2017, in der überarbeiteten und angenommenen Version v. 10. April 2018.

4 Siehe auch Kamp/Rost, Kritik an der Einwilligung – ein Zwischenruf zu einer fiktiven Rechtsgrundlage in asymmetrischen Machtverhältnissen, veröffentlicht in Datenschutz und Datensicherheit (DuD) 2/2013, 80–83.

durchschnittlichen Nutzern verstanden werden.[5] Die hypothetischen volkswirtschaftlichen Kosten für den Fall, dass alle Datensubjekte alle Datenschutzerklärungen lesen würden, sind schon untersucht worden. Allein das Lesen der Erklärungen wurde mit 44,3 Milliarden Stunden veranschlagt.[6] Ferner werden diese statischen Datenschutzerklärungen stets dann zum Problem, wenn es um dynamische Datenverarbeitungsvorgänge geht. Wenn Datenkategorien, Empfänger, Zwecke sich ändern oder wegfallen können sollen, wenn neue Dienste hinzu kommen und weder von der bereits erteilten Einwilligung, noch von einer anderen Rechtsgrundlage gedeckt sind, dann wird es schwierig. Gerade in Bezug «data re-use», also auf die zweckändernde Datenverarbeitung für andere, ebenfalls vom Verantwortlichen bereit gestellte Dienste ist dies der Fall. Der Verantwortliche steht nun vor dem Problem, dass er sich für die Rechtmäßigkeit dieses Vorhabens von neuem an den Betroffenen wenden muss. Dies ist jedoch aufgrund der Art und Weise, wie der Dienst ursprünglich dem Betroffenen zur Verfügung gestellt wurde, oft nicht möglich oder möglicherweise vom Verantwortlichen nicht gewollt um Nutzer nicht mit zahlreichen Einwilligungsanfragen zu überhäufen. Doch genau in der innovativen weiteren Verwendung der Daten liegt das maßgebliche Innovationspotential von Big Data. Des Weiteren wird der Weg des sogenannten «Opt-Out» immer ungangbarer, wie sich auch durch die jüngste Rechtsprechung des Europäischen Gerichtshofes (EuGH) vom 1. Oktober 2019 zu der Setzung von Cookies auf den Endgeräten von Webseitenbenutzern zeigt.[7] Vielmehr zeichnet sich immer mehr ab, dass nur ein «Opt-In» des Betroffenen auf der Grundlage einer vollständig informierten Entscheidung geeignet erscheint, eine valide Einwilligung für die Verarbeitung von personenbezogenen Daten zu generieren. Und hier schließt sich der Kreis, denn dank «information overload» und der kaum erklärbaren Komplexität der Systeme willigen nur noch ganz wenige Leute ein. Der Drang nach Big Data Innovation wird daher den Datenschutz existentiell bedrohen, oder umgekehrt. Ziel muss also sein, Innovation zu ermöglichen und dennoch die Ziele des Datenschutzes einzuhalten. Unter Ziel des Datenschutzes ist dabei philosophisch die von Beate Rössler definierte Autonomie der eigenen Handlung zu verstehen. Die Zweckbindung z.B. dient diesem Ziel und muss in ihrem Lichte betrachtet werden.[8]

2. Dynamisches Einwilligungsmanagement als neuer Weg

Bereits in der Vergangenheit hat es Versuche gegeben, mit Hilfe von technischen Lösungen und verbesserten Benutzeroberflächen (Engl.: User Interfaces) Wege zu schaffen, auf Veränderungen des Verarbeitungsprozesses zu reagieren. Auch der Begriff «dynamic consent» wurde bereits zuvor aufgegriffen, um interaktiv personalisierte Schnittstellen zu beschreiben, die es Betroffenen ermöglichen, ihre Einwilligung in Echtzeit abzugeben, zu verändern oder zurück zu ziehen.[9]

2.1. Metadatensteuerung als Grundvoraussetzung

Grundvoraussetzung ist ein System, wie es von Kirrane/Wenning auf der IRIS 2017 und 2018 vorgestellt wurde. Es erlaubt eine Datensteuerung durch Metadaten.[10] Ein solches Metadatensystem kann auch die Interaktionen mit dem Nutzer aufzeichnen und im data lake verwalten. Dieses System ist aber so reich an Information, dass überlegt werden muss, wie man den Nutzer vor dieser Informationsflut bewahrt. Denn informationelle Selbstbestimmung zielt darauf ab, dass der Betroffene in die Lage versetzt wird, die für ihn relevanten

5 Vgl. hierzu beispielhaft Litman-Navarro, We Read 150 Privacy Policies. They Were an Incomprehensible Disaster. Artikel v. 12.06.2019 aus der NY Times, basierend auf einer Studie des New York Times Privacy Project.

6 McDonald/Cranor, The cost of reading privacy policies, A Journal of Law and Policy for the Information Society 4(3), 543–568, 2008.

7 Siehe Fn. 1, die «Planet49» Entscheidung des EuGH vom 1.10.2019 – C-673/17.

8 Beate Rössler, Der Wert des Privaten, Suhrkamp 2001.

9 Vgl. Kaye/Whitley/Lund/Morrison/Teare/Melham, Dynamic consent: a patient interface for twenty-first century research networks. European Journal of Human Genetics (2015) 23, 141–146. Aber auch das EU FP-7 Forschungsprojekt PrimeLife (Privacy and Identity Management in Europe for Life): https://primelife.ercim.eu/.

10 Wenning/Kirrane, Compliance mit Metadaten, IRIS 2017 (Datenschutz VIII) & GDPR compliance for Big Data, IRIS 2018.

Informationen zu erkennen und auf der Grundlage eine selbstbestimmte Entscheidung treffen zu können. Aus diesem Grund ist die reine Metadatensteuerung im Datenmanagement zwar eine notwendige, aber keine hinreichende Bedingung für die Herstellung von Verständnis beim Betroffenen. Ebenso hinzu kommen muss eine innovative Nutzung der Metadaten, um die richtige Information zum richtigen Zeitpunkt an den richtigen Ort zu bringen. Es wird also ein Informationssystem angenommenen, wie es vom SPECIAL-Projekt[11] konzipiert wurde, das Metadaten wie Policy-Informationen speichert und den Datenmanagement-Algorithmen zur Verfügung stellen kann. Metadaten umfassen unter anderem Datenschutzinformationen, Angaben zur Identität, zu Aufbewahrungsfristen, Zwecken und Weitergabe der Daten. Werden die Daten verarbeitet, dann wird diese Tatsache erneut in das System zurück geschrieben und gegebenenfalls mit Verschlüsselung oder Blockchain-Technologie gesichert. Mit der so gesicherten Liste der Verarbeitungen kann nun ein Compliance Check relativ schnell und einfach vorgenommen werden. Alle Verarbeitungen, Logs, Nutzerinteraktionen sind jetzt selbst neue Metadaten und werden so gespeichert, dass eine feste Verbindung zum Datum besteht, über das sie eine Aussage treffen. Wie schon 2018 vorgestellt, werden hierzu die Eigenschaften von Linked Data genutzt und eine volle Annotierbarkeit der Daten hergestellt.

Wenn aber aus der Nutzerinteraktion gewonnene Daten auch Metadaten sind, dann werden diese wie alle anderen kontextualen Informationen beim digitalen Austausch in den data lake geschrieben und annotieren das entsprechende Datum. Somit wird klar, dass eine Nutzerinteraktion hier ein zumindest pseudonymes Identitätsmanagement voraussetzt. Denn wenn personenbezogene Daten annotiert werden sollen, dann geht das nicht ohne eine Identität im Sinne der Informatik anzunehmen. Denn nur ein zustandsbehaftetes System braucht eine solche Steuerung um die datenschutzkonforme Profilbildung zu ermöglichen. Die Nutzerinteraktion ist dann Teil des Profils, was durchaus weitere datenschutzrechtliche Probleme bereiten kann. Ein System mit ausschließlich anonymen Daten dagegen braucht keine Identitäten. Der oben aufgeführte Aufwand ist überflüssig. Wie aber schon auf der IRIS 2018 nachgewiesen[12], ist die Deanonymisierung so weit fortgeschritten, dass wirklich anonymisierte Daten weitgehend ihren Wert verloren haben. Deswegen ist es auch nicht sehr sinnvoll für die Big Data Analyse, die ja neue Erkenntnisse bringen soll, auf rein anonyme Daten mit niedriger Entropie zu setzen.

2.2. Probleme der derzeitigen Interaktion (Why Johnny can't opt-in)

Durch die Verwaltung einer Identität kann ein Nutzer – auch pseudonymen – Zugang zu seinem Profil erhalten. Die Entwicklung solcher Interfaces stellt Juristen und Informatiker gleichermaßen vor große Herausforderungen. Welche Informationen müssen wann und wo abrufbar sein um eine Gesetzeskonformität herzustellen? Kann ein Interface die nach Art. 13 DSGVO geforderten Informationspflichten erfüllen? Wie muss es dazu gestaltet sein?

Klassischerweise werden die gesetzlich geforderten Informationen zum Zeitpunkt der Installation präsentiert, oder aber wenn eine Webseite zum ersten Mal aufgerufen wird. Bei Webseiten kommt hinzu, dass der Zustand des Systems, also die schon erfolgte Lieferung der Information, normalerweise als Referenz zu einer ID in einem Cookie abgelegt wird. Da Tracking und Missbrauch durch Cookies allerdings schlimme Formen angenommen haben, löschen Nutzer inzwischen regelmäßig alle Cookies. Eine Selektion wäre viel zu mühsam. Damit geht der Status verloren und es muss erneut die volle Information geliefert und der Status

[11] Dieser Vortrag basiert auf Forschungsergebnissen der Projekte SPECIAL (Scalable Policy-awarE linked data arChitecture for prIvacy, trAnsparency and compLiance) und dem Privacy&Us Innovative Training Network. Für das Projekt SPECIAL wurden im Rahmen der Finanzhilfevereinbarung Nr. 731601 Fördermittel aus dem Programm der Europäischen Union für Forschung und Innovation «Horizon 2020» bereitgestellt. Für das Projekt Privacy&Us wurden Fördermittel aus dem Programm der Europäischen Union für Forschung und Innovation «Horizon 2020» unter dem Marie Skłodowska-Curie Grant Agreement Nr. 675730 im Rahmenprogramm des Marie Skłodowska-Curie Innovative Training Networks (ITN-ETN) bereitgestellt. Mehr unter https://www.specialprivacy.eu/ und https://privacyus.eu/.

[12] Kirrane/Wenning, GDPR compliance for big data, IRIS Conference, Salzburg 2018.

in einem Cookie abgelegt werden. Das wiederholt sich dauernd auf allen Webseiten und die Internetnutzer werden überdrüssig, ständig irgendwelche OK-Buttons zu klicken. Auf den Inhalt, den die OK Buttons betreffen, schaut schon lange niemand mehr. Das kann durchaus gewollt sein, denn nunmehr hat beispielsweise eine Webseite die Möglichkeit, sich eine Einwilligung erteilen zu lassen, welche die bürokratischen Anforderungen erfüllt und dennoch eine eher unfaire und intransparente Datenerhebung legitimiert. Dazu wurde sogar mit «Dark Patterns» ein eigener Begriff eingeführt.[13] «Dark Patterns» gehen aber insofern über das hier gesagte hinaus, als nicht nur opportunistisch eine Situation genutzt wird, sondern bewusst verwirrende Interfaces erstellt werden. Damit ist die informationelle Selbstbestimmung ausgehebelt. Dazu passt dann, dass versucht wird, das Einverständnis vorausgefüllt zu präsentieren. Der lästige Formalismus wird bedient, die eigene Haftung minimiert, und der Nutzer nicht von der Wahrnehmung seiner Rechte gestört. Das ist allerdings rechtlich nicht mehr valide.[14] Es ist nun eindeutig eine informierte Entscheidung erforderlich; somit reicht gerade nicht mehr, nur einen «OK»-Button neben einem «Wir-benutzen-Cookies» Infotext anzubieten, und im besten Fall noch auf eine lange Datenschutzerklärung zu verweisen.

Es gibt einen zweiten Grund, warum «Notice and Choice» nicht funktioniert hat.[15] Die nach Art. 13 DSGVO verlangte Information kann kaum verständlich gemacht werden. Denn um die Praxis der Verarbeitung personenbezogener Daten darzustellen, muss erst einmal die gesamte Datenverarbeitung selbst erklärt werden. Ein Service muss also seine gesamte Dienstleistung beschreiben um dann die Punkte der Datenerhebung und die anschließende Verarbeitung der personenbezogenen Daten zu beschreiben. Das führt dann regelmäßig zu über 20 Seiten unverständlicher Melange aus technischem Jargon und Juristendeutsch. Und das ist zwangsläufig so. Alle Versuche, mit semiotischen Zeichen und anderen Icons eine Vereinfachung zu erreichen, sind an der komplexen Realität der heutigen Datenverarbeitungssysteme gescheitert. Auch das Marketing der betroffenen Unternehmen und die Werbeindustrie sind nicht glücklich über diesen Zustand, denn eine Einwilligung wird so immer schwieriger. Es gibt auch schon Stimmen, die die Einwilligung für überholt halten.[16] Die Anwälte der Werbebranche hatten daraufhin ein Konzept rund um Tracking und Profiling als «legitimes Interesse» gesetzt und dies sogar durch Lobbybemühungen im Erwägungsgrund 47 der DSGVO niederlegen können. Danach kann Direktmarketing ein legitimes Interesse sein. Mit der schon erwähnten Planet49 – Entscheidung des EuGH[17] ist dieses Schlupfloch geschlossen worden.

Damit wird die einwilligungsbasierte Verarbeitung personenbezogener Daten zunächst sehr schwierig. Im Wettbewerb dominieren deswegen die Firmen, die das Datenschutzproblem ignorieren oder aussitzen können, weil sie nur schwer erreichbar sind. Die Versprechungen von Big Data drohen in Europa auf rein technische Daten ohne Personenbezug beschränkt zu werden. Das derzeitige System der Einwilligungen ist zu schwierig um vom Nutzer wirklich beherrscht oder akzeptiert werden zu können. Eine valide, wirklich informierte Einwilligung wird unter diesen Umständen dann nur noch in unter einem Prozent der Fälle erreicht.[18] Die Gesellschaft und die Forschung müsste nun ohne Big Personal Data auskommen. Das wird sie nicht tun.

Die Frage ist also, wie eine elegante, verständliche Einwilligung erreicht werden kann um auf fairem Wege mehr personenbezogene Daten für gesellschaftlich nützliche Anwendungen zu erhalten und dem Nutzer wieder Vertrauen in diese Systeme geben zu können.

---

13 Luguri/Strahilevitz, Shining a Light on Dark Patterns (August 1, 2019). University of Chicago, Public Law Working Paper No. 719; University of Chicago Coase-Sandor Institute for Law & Economics Research Paper No. 879.

14 Siehe Fn. 1.

15 Siehe dazu den Cartoon von Daniel Solove: https://teachprivacy.com/cartoon-notice-choice-avoid-creepy/.

16 Statt vieler, Hildebrandt, Primitives of legal protection in the era of data-driven Platforms. Georgetown Law Technology Review (2) Rev. 252 (2018); dagegen, Wenning, Quo vadis Datenschutz, Artikel für die Berliner Datenschutzrunde vom 14.08.2014.

17 Siehe FN 1.

18 Utz/Degling/Fahl/Schaub/Holz, (Un)informed Consent: Studying GDPR Consent Notices in the Field.ACM SIGSAC Conference on Computer and Communications Security (CCS'19), November 11–15, 2019, London, United Kingdom.

2.3. Interaktion mit einem Metadatensystem

Das SPECIAL Projekt hat drei Fallbeispiele bearbeitet, von denen insbesondere der geolokalisierte Dienst von besonderem Interesse ist. Die Idee setzt am oben beschriebenen Problem an. Eine Datenschutzerklärung selbst ist wegen der Abstraktion der Aussagen unverständlich. «Location based services» (LBS) haben ein großes, interessantes Potenzial. Denn was nützt zum Beispiel die Möglichkeit, eine Pizza in Palo-Alto bestellen zu können, nur weil die Suchmaschine nicht begreifen kann, dass ich in Lyon bin? Vielmehr kann mir ein LBS wirklich sehr nützliche Dinge vorschlagen, die gerade um mich herum stattfinden. Zum Teil gibt es bereits Dienste, die daran ansetzen, jedoch sind diese bisher in keiner Weise datenschutzkonform. Viele andere Services hingegen bieten noch keine eigene Geolokalisierung an, auf die man zugreifen könnte. Des Weiteren ist in Europa die Angst vor der Datenschutzhaftung zu groß geworden. LBS sind auch deshalb nicht akzeptiert, weil das System ja alle möglichen Daten sammeln und auch Dinge vorschlagen kann, die ich gar nicht sehen will, z.B. Werbung mit Hochglanzbildern, welche die Bandbreite verbrauchen und das Smartphone blockieren. Man braucht ein Profil mit den Dingen, die man sehen will. Nur so kann der Computer auf der anderen Seite die ungewollten Dinge weglassen. In der klassischen Datenschutzerklärung müssen jetzt alle potentiellen Datenpunkte und alle Möglichkeiten der Kommunikation und Interaktion mit der Cloud-basierten Anwendung zur Auswertung und Steuerung beschrieben werden, inklusive der Möglichkeit, die so gesammelten Daten in sozialen Netzwerken zu teilen. Wer das liest ist zuerst überfordert, dann sehr besorgt und versucht möglichst, alles abzudrehen, was er oder sie findet.

In SPECIAL hingegen wurde die Idee verfolgt, aus vielen kleinen Einwilligungen ein lernfähiges System entstehen zu lassen, das den Nutzer bei seiner informationellen Selbstbestimmung unterstützt ohne zu nerven. Die Summe aller kleinen gegebenen Einwilligungen bietet die Basis und den Rechtsgrund für die Verarbeitung der personenbezogenen Daten. Es entsteht ein Datenschutzprofil, welches schon erkannte Entscheidungen automatisiert an den Dienst weitergibt. Wir nutzen dabei die Tatsache, dass der Nutzer kontextual oft sehr genau weiß, was gerade passiert und auch sehr genau weiß, was er erwartet. Je nach Uhrzeit sucht der Nutzer ein Restaurant oder eine lohnende Veranstaltung und hat deshalb das GPS aktiviert. Er will die Daten vielleicht auch in sein Cloudprofil speichern um die Qualität der Empfehlungen zu verbessern.

Die Idee besteht darin, ein nicht-invasives interaktives Banner im Interface erscheinen zu lassen.[19] Damit es nicht invasiv wird, verschwindet das Banner nach ca. 5 – 7 Sekunden wieder. Das Banner hat drei Schalter: «Jetzt, Immer, Mehr Information». Interagiert der Nutzer, wird das Ergebnis dem System als Metadatum übergeben. Interagiert der Nutzer nicht mit dem Banner, wird die bei der Installation getroffene Default-Nachricht übergeben. So können besonders besorgte Nutzer den Default auf «Nein» setzen, während andere lieber akzeptieren und später nachkorrigieren wollen. Wie schon gesehen ist die Entscheidung des Nutzers ein weiteres Metadatum, das im SPECIAL System oder einem anderen Metadatensystem verwaltet werden kann. Zu diesem System gehört auch ein interaktives Dashboard.[20] Dort kann der Nutzer die Metadaten in einem Interface betrachten und editieren. Vielleicht will er eine im Banner falsch getroffene Entscheidung revidieren oder eine Veranstaltung oder ein Restaurant aus seinem Profil löschen.

Wenn also die Applikation ein neues personenbezogenes Datum oder eine Kategorie personenbezogener Daten erheben will, taucht das Banner auf und schreibt die Entscheidung zurück ins System. Mit der Zeit kennt das System die Entscheidungen des Nutzers, weil wir nur eine begrenzte Menge neue Dinge im Jahr tun. Es werden immer weniger Anfragen notwendig. Es bleibt Aufgabe zukünftiger Forschung herauszufinden, ab wann gar keine Interaktion mehr notwendig ist, weil das System keine neuen Verhaltensweisen mehr abfragen

[19] Die Idee stammt ursprünglich aus einer Kooperation zwischen Dave Raggett und Rigo Wenning zum Primelife Privacy Dashboard. Siehe http://primelife.ercim.eu/.

[20] Raschke/Drozd/Bos, D4.3 Transparency dashboard and control panel release V2. SPECIAL public deliverable 31. Januar 2019. DOI https://doi.org/10.5281/zenodo.2554207.

muss. Wie im Schlaraffenland muss sich der Nutzer also durch eine interaktive Phase fressen bis das System kaum noch Fragen stellt. Das Tolle ist nun, dass nach dieser ersten Lernphase nur noch wirklich relevante neue Begebenheiten abgefragt werden. Der Nutzer wird also nicht zugemüllt mit Datenschutzbürokratie, sondern bekommt die relevante Information zur rechten Zeit. Da das wenige Fragen sind, hat der Nutzer Zeit, sich damit zu beschäftigen. Und weil die Frage nach der Datenerhebung im zeitlichen Kontext der Nutzung eines bestimmten Dienstes erfolgt, kann der Nutzer auch den Zweck der Datenerhebung verstehen und eine gut informierte Entscheidung treffen. Durch die kontextuale Information und das Verständnis des gerade stattfindenden Vorgangs wird auch «Dark Patterns»[21] entgegengewirkt, jedoch ohne sie gänzlich ausschließen zu können.

Juristisch ist ein solches System sehr schwierig umzusetzen. Denn die DSGVO sieht Informationspflichten nach Art. 13 und 14 vor. Eine klassische Herangehensweise würde diese Information entweder bei der Installation oder anlässlich der ersten Datensammlung vollumfänglich auf dem Bildschirm darstellen. Das oben dargestellte Problem der Informationsüberlastung bei der Einwilligung wäre verschoben, aber nicht gelöst. Um dem zu begegnen nutzt der hier vorgestellte Ansatz eine Kombination aus Einwilligung und «layered approach». Anstatt alles in eine Datenschutzerklärung zu schreiben, kann man die Information mittels Verweisen, am besten mit Hypertext, in verständliche Häppchen teilen. Gezeigt und verständlich gemacht werden muss dann nur der Einstieg in dieses System.

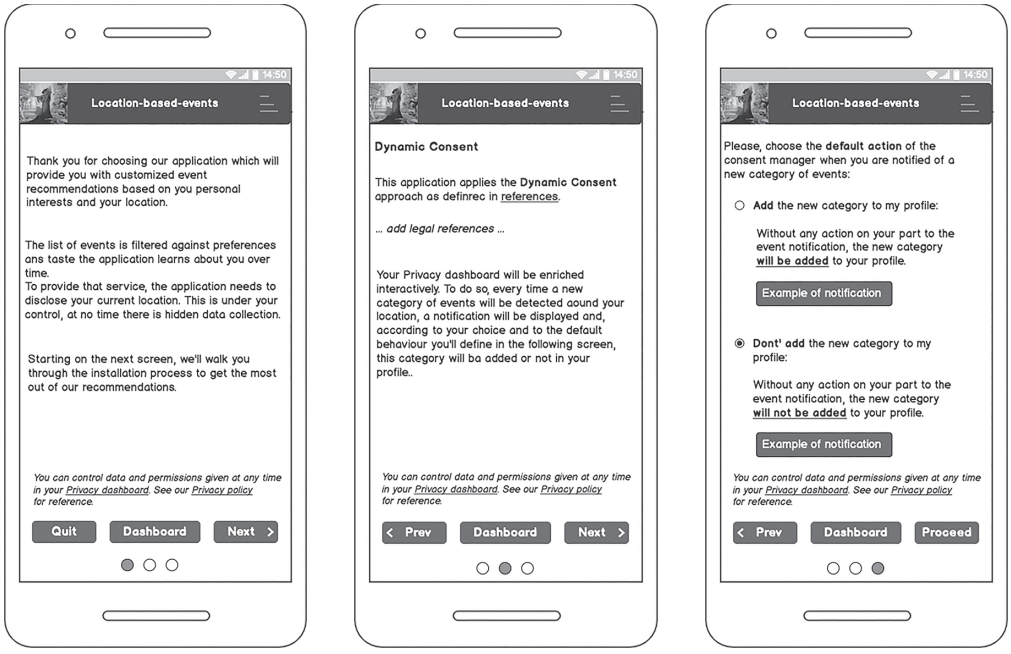
Mit dem Banner ist ein solcher Einstieg gegeben. Allerdings hat die Art. 29 Working Party in einem Dokument festgelegt, welche Informationen beim «layered approach» auf der ersten Ebene stehen sollen. Das non-invasive Banner entspricht dem nicht. Das Dokument der Art. 29 WP richtet sich jedoch an das klassische Hypertext System und will vermeiden, dass auf der ersten Ebene nur Marketing-Text steht, der leicht weggeklickt wird. Der hier vorgestellte Ansatz weicht davon so weit ab, dass es vertretbar sein kann, die von der Art. 29 WP gegebenen Empfehlungen hier nicht ohne weiteres zu verwenden. Das Banner hat wie oben beschrieben 3 interaktive Schalter. Einer davon ist mit «Mehr» gekennzeichnet und weist in das interaktive Dashboard, welches einen vollen Zugriff auf das eigene Profil erlaubt. Dies wird dem Nutzer während der Installation auch sehr genau erklärt. Passiert ein Fehler, kann dieser jederzeit über das Dashboard korrigiert werden.

Wenn also nicht nur Informationen gegeben werden, sondern im nächsten Layer sogar eine Interaktion mit dem System möglich ist, dann ist das ein Mehr gegenüber den Forderungen nach einer textlichen Information des Nutzers. Im hier verfolgten Ansatz wurde eine zusätzliche Sicherung eingebaut: Während der Installation des Datenschutzinterface werden schon bestimmte Informationen gegeben und der Nutzer muss dem innovativen non-invasiven Interface zustimmen. Damit stimmt der Nutzer einer erleichterten Zustimmung zu. Die erleichterte Zustimmung durch das Banner wiederum lässt sich rechtlich nur vertreten, weil es dahinter ein innovatives Dashboard und eine mögliche Interaktion mit dem System gibt. Art. 10 der vorgeschlagenen ePrivacy Regulierung in der Fassung des LIBE-Kommitees[22] hätte eine sehr viel einfachere Grundlage für den Ansatz geliefert, ist aber dem Grabenkrieg der Medien gegen Datenschutz und Parlament zum Opfer gefallen.

Weil das erst einmal sehr abstrakt klingt, werden im Folgenden einige Screenshots beschrieben. An dem Interface wird derzeit mit Hochdruck gearbeitet. Die Präsentation gliedert sich in eine Installationsphase, in eine Nutzungsphase und eine Kontrollphase.

[21] https://de.wikipedia.org/wiki/Dark_Pattern

[22] http://www.europarl.europa.eu/doceo/document/A-8-2017-0324_EN.html.



2.3.1. Die Installationsphase

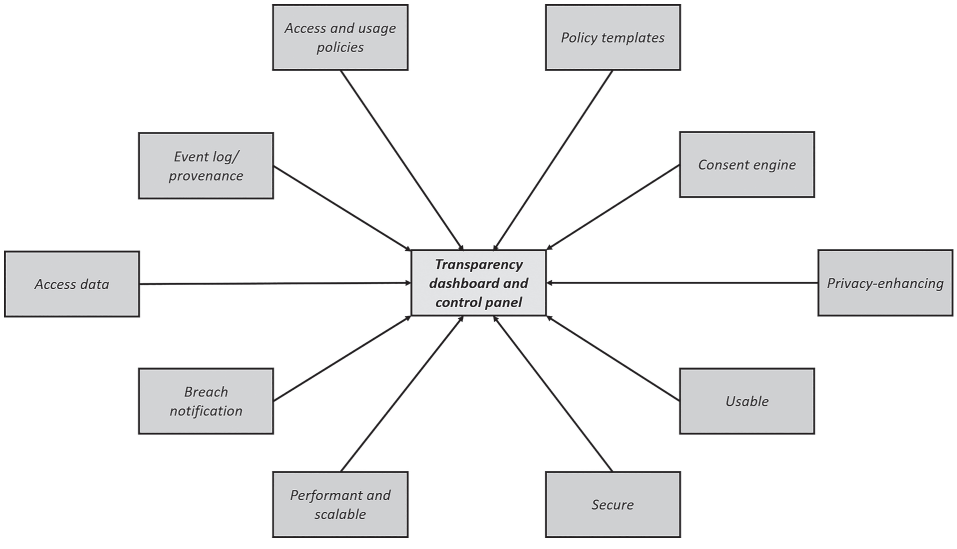
Die Installationsphase[23] wird genutzt, um grundsätzliche Informationen über das System zu geben. Es wird dann die Zustimmung zum Zustimmungssystem abgefragt. Damit der Nutzer sich an das Interface gewöhnen kann und nicht verwirrt wird, gibt es einen interaktiven Demo-Screen der den Nutzer in einer Sandbox ausprobieren lässt. Alle generischen, immer aktiven Daten nach Art. 13 werden ebenfalls erwähnt. Nur der variable Teil soll ja im Zustimmungssystem erfasst werden. Erstaunlich war dabei, dass fast alle mit der Erstellung des Systems befassten Forscher immer wieder in die angestammte Form der Datenschutzerklärung zurückgefallen sind und versucht haben, alles schon während der Installation zu erklären. In diesem Falle macht aber das Banner in der Nutzungsphase keinen Sinn mehr.

[23] Mock ups von Laurent Carcone, ERCIM.

2.3.2. Die Nutzungsphase

In der Nutzungsphase fragt das Interface den Nutzer im Falle der Erhebung neuer Daten. Es ist auch denkbar, dass Nutzer nach Zustimmung über die Zweitverwertung ihrer Daten befragt werden. Das Interface öffnet einen Schnelleinstieg ins Dashboard. Das Dashboard ist in der Lage, die für den Kontext relevanten Daten anzuzeigen. Gegebenenfalls wird es dem Nutzer erlaubt, die Daten zu korrigieren und zu löschen. Derzeit wird an weiteren Iterationen des Interface gearbeitet. Auch hier gibt es derzeit noch zu viel Text und zu viele Buttons.

2.3.3. Die Kontrollphase



Man kann nun multimodal vorgehen. Der Nutzer hat die Geo-Daten und Services auf der Reise eingesammelt und in sein Profil schreiben lassen. Dies erlaubt Empfehlungen von hoher Qualität, wird aber kaum für klassische invasive Werbung genutzt werden können. Ist der Nutzer mit der Interaktion nicht zufrieden oder will er Dinge aus dem Profil entfernen, kann er dies in Ruhe zu Hause vom Computer aus machen. Der Service kann durch das SPECIAL Metadatensystem dem Datenschutzbeauftragten, aber auch dem Nutzer jederzeit das volle Audit präsentieren.

3. Schlussfolgerungen

Die Elemente des oben beschriebenen Systems durften von Nutzergruppen in Studien erprobt werden. Hierbei ergaben sich noch anfängliche Gewöhnungsschwierigkeiten. Einige von den testenden Nutzern überforderte die Komplexität des neuen Ansatzes der dynamischen Einwilligung und das viele Möglichkeiten bereitstellende Dashboard.

In einer Nutzerstudie während eines Workshops auf der IFIP Summer School im August 2019 waren die Testergebnisse in Bezug auf das Verständnis des oben beschriebenen Ansatzes gemischt. Es gab Teilnehmer, die das Konzept der dynamischen Einwilligung nicht sofort verstanden. Doch diejenigen, welche die dahinterstehende Idee begriffen, sagten, dass sie die Klarheit und Übersichtlichkeit der Informationsbereitstellung sehr positiv bewerten. Diese Teilnehmer waren es dann auch, die im weiteren Verlauf präzise erfassten, dass es um ein System geht, welches eine nutzergesteuerte Profilbildung über längere Zeit ermöglicht und das jederzeit anpassbar ist. Sie schätzten die vergrößerten Möglichkeiten der Kontrolle nicht nur über die Datenerhebung, sondern auch über die Art und Weise der Benachrichtigungen und Information und dass sie jederzeit darüber im Bilde waren, was mit ihren personenbezogenen Daten geschieht. Diese Teilnehmer bewerteten die kontextbasierten Benachrichtigungen als einen positiv wahrgenommen Mehrwert gegenüber den klassischen Einwilligungsansätzen mit langer Datenschutzerklärung, die alle Varianten und Prozesse abbilden muss. Auch in den Studien zur Nutzung des Dashboards kam heraus, dass es einer gewissen Übung im Umgang damit braucht, um die durchaus komplexen Möglichkeiten verstehen und nutzen zu können.[24]

Die Hoffnung ist nun, dass ein solches System ständig verbessert und schließlich von Nutzern angenommen wird. Der Lohn wären persönlich angepasste Informationssysteme, die nicht gegen die Nutzer, sondern mit den Nutzern für bessere Dienstleistungen arbeiten. Bis dahin ist noch eine gewisse Wegstrecke zurück zu legen, denn die Lösung kollidiert mit dem derzeitigen Trend, möglichst viel Kontrolle und Buttons aus dem Interface zu entfernen. Die nackte Google Suchzeile als ultimatives Design-Ziel ist jedoch mit dem hier verfolgten Ansatz nur schwer zu verbinden.

4. Literatur

Artikel-29-Datenschutzgruppe, Guidelines on Consent under Regulation 2016/679, WP259rev.01 vom 28. November 2017, in der zuletzt überarbeiteten und angenommenen Fassung vom 10. April 2018. Verfügbar unter: http://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=623051.

Artikel-29-Datenschutzgruppe, Guidelines on transparency under Regulation 2016/679, WP260rev.01, vom 29. November 2017, in der zuletzt überarbeiteten und angenommenen Fassung vom 11. April 2018. Verfügbar unter: http://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=622227.

Hildebrandt, Primitives of legal protection in the era of data-driven Platforms, Georgetown Law Technology Review (2) Rev. 252 (2018). Kamp/Rost, Kritik an der Einwilligung – ein Zwischenruf zu einer fiktiven Rechtsgrundlage in asymmetrischen Machtverhältnissen. Datenschutz und Datensicherheit (DuD) 2/2013, 80–83.

[24] Milošević/Raschke/Drozd/Kirrane, D4.4 Usability testing report V2, SPECIAL public deliverable 29. März 2019. Verfügbar unter: https://www.specialprivacy.eu/images/documents/SPECIAL_D44_M27_V10.pdf.

Kaye, Jane/Whitley, Edgar A/Lund, David/Morrison, Michael/Teare, Harriet/Melham, Karen, Dynamic consent: a patient interface for twenty-first century research networks. European Journal of Human Genetics (2015) 23, 141–146.

Litman-Navarro, Kevin, We Read 150 Privacy Policies. They Were an Incomprehensible Disaster, New York Times Artikel vom 12.06.2019, basierend auf einer Studie des New York Times Privacy Project. Verfügbar unter: https://www.nytimes.com/interactive/2019/06/12/opinion/facebook-google-privacy-policies.html.

Luguri/Strahilevitz, Shining a Light on Dark Patterns (August 1, 2019). University of Chicago, Public Law Working Paper No. 719; University of Chicago Coase-Sandor Institute for Law & Economics Research Paper No. 879. Verfügbar unter SSRN: https://ssrn.com/abstract=3431205 or http://dx.doi.org/10.2139/ssrn.3431205.

McDonald/Cranor, The cost of reading privacy policies , A Journal of Law and Policy for the Information Society 4(3), 543–568, 2008.

Raschke/Drozd/Bos Philip Raschke, Olha Drozd, Bert Bos, The SPECIALD4.3 Transparency dashboard and control panel release V2. SPECIAL public deliverable 31. Januar 2019. DOI: https://doi.org/10.5281/zenodo.2554207.

Utz/Degling/Fahl/Schaub/Holz, (Un)informed Consent: Studying GDPR Consent Notices in the Field. In2019 ACM SIGSAC Conference on Computer and Communications Security (CCS '19), November 11–15, 2019, London, United Kingdom. New York, NY, USA, 18 pages. DOI link: https://doi.org/10.1145/3319535.3354212. Auch verfügbar unter: https://www.syssec.ruhr-uni-bochum.de/media/emma/veroeffentlichungen/2019/09/05/uninformed-consent_Yl7FPEh.pdf.

Wenning, Quo vadis Datenschutz. Artikel für die Berliner Datenschutzrunde vom 14.08.2014. Verfügbar unter: https://www.wenning.org/Articles/1408-Datenschutz-Berliner-Runde.html.