LEGAL REVOLUTIONary
Rechtsmagazin der digitalen Wirtschaft

Datengewerkschaften

Eine Lösung für das Einwilligungsdilemma?

Jörn Erbguth | Diplom-Jurist, Diplom-Informatiker, Datenschutzbeauftragter (udis zertifiziert), Berater zu Blockchain und Datenschutz |
Olga Stepanova | Rechtsanwältin, externe Datenschutzbeauftragte | WINHELLER Rechtsanwaltsgesellschaft mbH
Andreas Diehl | Informatiker, CEO | Bitquadrat GmbH | Datenschützer

18. Mai 2020

LR 2020, Seiten 145 bis 155 (insgesamt 11 Seiten)

Jeder von uns kennt das: Man besucht eine Webseite und wird mit einer Vielzahl von Informationen zum Datenschutz „überflutet". Früher waren es noch teils dezente Banner am unteren Rand einer Webseite, heute hat sich die Bannerbelästigung zugespitzt, woran nicht zuletzt die Planet49-Entscheidung des EuGH[1] schuld ist. Verunsicherte Webseitenbetreiber agieren nach dem Motto „viel hilft viel" und lassen daher keine Gelegenheit aus, etwas zum Datenschutz mitzuteilen. Der gut gemeinte Ansatz, den Verantwortlichen zu verpflichten, den Betroffenen über die Verarbeitung seiner personenbezogenen Daten zu informieren, ist in einer „Informationstortour" für den Verantwortlichen und zugleich einer Bannerbelästigung für den Betroffenen gemündet. Gegenwärtig investieren Webseitenbetreiber viel Geld in Einwilligungsmanagementsysteme, Einwilligungsbanner und juristische Beratung. Es ist zu befürchten, dass dies lediglich die ungewollte Belästigung der Nutzer vermehrt, aber dem Datenschutz nicht wirklich nutzt: Weder nahm die Verwendung von Third-Party-Cookies spürbar ab, noch gibt es einen Anreiz für Webseitenbetreiber, sich mit einem datenschutzfreundlichen Ansatz dem „Bannerzirkus" zu entziehen. Eine Verbesserung der Position der Betroffenen ist nicht erkennbar. 1

Dieser Aufsatz stellt zunächst die juristischen Vorgaben dar und zeigt dann praktische Alternativen zum zunehmend bedeutungsentleerten Einwilligungsmarathon auf, darunter die Idee einer Datengewerkschaft. 2

I. Einwilligung

Die Einwilligung steht im Zentrum der Diskussion, obwohl sie lediglich eine von sechs verschiedenen Rechtfertigungsgründen für die Verarbeitung von personenbezogenen 3

[1] EuGH, Urt. v. 01.10.2019, Rs. C-673/17, ECLI:EU:C:2019:801 – Planet 49.

Daten in Art. 6 DSGVO[2] ist. Sie steht für die informationelle Selbstbestimmung – im positiven, wie im negativen Sinne: Die Betroffenen können selbst über die Datenverarbeitung entscheiden. Auf Basis der Einwilligung ist damit jede Verarbeitung möglich, solange sie nur einem legitimen Zweck dient, in den eingewilligt wurde (Art. 5 Abs. 1 lit. b). Zur Vermeidung einer etwaigen Machtungleichheit stellt Art. 7 hohe Anforderungen an wirksame Einwilligungen, welche über die alte Richtlinie[3] sowie den auf ihrer Grundlage geschaffenen § 4 a BDSG a.F. hinausgehen. Erst kürzlich hat der Europäische Datenschutzausschuss (EDSA) eine neue Stellungnahme zur Einwilligung[4] publiziert, in der er diese hohen Anforderungen in gewohnt datenschutzfreundlicher Weise restriktiv interpretiert.

Als Grundsatz führt der EDSA aus[5], dass den Betroffenen **Kontrolle** sowie eine **echte Wahl** eingeräumt werden müssen. Angesichts von immer komplexeren Einwilligungsformularen stellt sich die Frage, ob dies tatsächlich erreicht wird. Dazu muss man vorab folgende Fragen klären: 4

- Erfolgen die Einwilligungen durch eine aktive Handlung des Einwilligenden (z.B. Ankreuzen eines Auswahlfeldes) (Erwägungsgrund 32)?
- Hebt sich der Einwilligungstext grafisch von anderen Texten ab (Größe, Schrift, Fettdruck[6])?
- Formulierung in angepasster Sprache[7] (z.B. bei Kindern)?
- Werden die konkreten Verarbeitungszwecke[8] benannt?
- Konnte in jeden Zweck separat[9] eingewilligt werden?
- Ist die Einholung der Einwilligung dokumentiert worden (Art. 7 Abs. 1)?
- Falls die verschiedenen Zwecke der Verarbeitung erst auf einer weiteren Seite angegeben werden, wurde diese Seite auch vom Betroffenen aufgerufen und kann dies nachgewiesen werden[10]?
- Liegt kein Verstoß gegen das Koppelungsverbot (Art. 7 Abs. 4) vor?
- Wurden alle Informationspflichten gegenüber den Betroffenen nach Art. 12–14 erfüllt?

[2] Im Folgenden sind Artikel und Erwägungsgründe ohne Gesetzesangabe Artikel und Erwägungsgründe der DSGVO.
[3] Richtlinie 95/46/EG des Europäischen Parlaments und des Rates vom 24. Oktober 1995 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr.
[4] EDSA, Guidelines 05/2020 on consent under Regulation 2016/679, Version 1.0, 04.05.2020, https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines_202005_consent_en.pdf (alle Links zuletzt aufgerufen am 13.05.2020).
[5] EDSA, aaO, Rn 3.
[6] Munz, in: v. Westphalen/Thüsing VertrR/AGB-Klauselwerke, 44. EL November 2019, Datenschutzklauseln Rn. 44. (noch zur alten Rechtslage); Stolz, in: Beck'sche Online-Formulare IT- und Datenrecht, 2. Edition 2020, Form. 2.1 Anmerkungen Rn. 4; Wolff, in: Schantz/Wolff, Das neue Datenschutzrecht, 1. Auflage 2017, D. Grundprinzipien und Zulässigkeit der Datenverarbeitung, Rn. 521.
[7] EDSA, aaO, Rn 126.
[8] EDSA, aaO, Rn 68.
[9] EDSA, aaO, Rn. 42-45, 60.
[10] EDSA, aaO, Fn. 40.

- Wurden die Betroffenen auf den jederzeit möglichen Widerruf ihrer Einwilligung mit Wirkung für die Zukunft hingewiesen (Art. 7 Abs. 3)?
- Wurden die Besonderheiten bei der Einwilligung von Minderjährigen in Bezug auf Dienste der Informationsgesellschaft beachtet (Art. 8)?

Erwägungsgrund 32 S. 6 gibt vor, dass die Aufforderung zur Einwilligung in klarer und knapper Form sowie ohne unnötige Unterbrechung des Dienstes erfolgen sollte. Doch in Anbetracht des immensen Katalogs an Anforderungen und bereitzustellenden Informationen, ist es kaum verwunderlich, dass Einwilligungserklärungen oftmals nicht knapp und klar, sondern lang, komplex und ausführlich sind. Deshalb darf man sich sehr wohl fragen, ob die gegenwärtig weit verbreitete Praxis des Informationsprofizits nicht kontraproduktiv wirkt und einer freiwilligen und informierten Einwilligung entgegensteht. 5

Dem EDSA ist dieses Dilemma durchaus bewusst. Er schlägt dazu zwei Lösungsansätze vor: 6

- Einen abgeschichteten Informationsansatz,[11] bei dem bestimmte Informationen erst durch weiteren Mausklick angezeigt werden.
- Eine Lösung via Browsersetting. Allerdings müsse auch bei diesem Lösungsansatz, welcher im Erwägungsgrund 32 S. 2 bereits angedeutet wird, die Granularität bzgl. der verschiedenen Zwecke erfüllt und die Verantwortlichen für die Datenverarbeitung benannt werden.[12]

II. Koppelungsverbot

Die Frage nach der Reichweite des Koppelungsverbotes bleibt auch nach der Stellungnahme des EDSA ungeklärt. Reicht es, wenn es auf dem Markt andere Angebote gibt, die keiner Einwilligung bedürfen? Der EDSA will die Wirksamkeit einer Einwilligung nicht vom Verhalten anderer Marktteilnehmer abhängig machen und akzeptiert dieses Argument nicht.[13] Wie ist es, wenn alternativ zur Einwilligung in die Datenverarbeitung eine inhaltlich gleichwertige, aber nicht kostenfreie Variante angeboten wird? Golland sieht dies als zulässig an.[14] Der EDSA hält es dagegen für unzulässig, wenn der Widerruf einer Einwilligung zur Verweigerung eines Service oder zu Kosten führt.[15] Lässt sich daraus schließen, dass Alternativen ohne Einwilligung auch preislich identisch gestaltet sein müssen? Dies würde bedeuten, dass ein finanzieller Anreiz für personalisierte Werbung unzulässig wäre. Ganz so weit geht der EDSA jedoch nicht, da nur wesentliche Extrakosten als unzulässig erachtet werden.[16] Aber was sind **wesentliche Extrakosten**? 2009 hatte die Artikel 29-Gruppe in WP 163 personalisierte Werbung noch als prinzipiell 7

[11] EDSA, aaO, Rn. 69.
[12] EDSA, aaO, Rn. 89.
[13] EDSA, aaO, Rn. 38.
[14] Golland, MMR 2018, 130 ff.
[15] EDSA, aaO, Rn. 46.
[16] EDSA, aaO, Rn. 24.

zulässig erwähnt.[17] Allerdings hat die DSGVO seitdem die Anforderungen an die Einwilligung erhöht. Dennoch hat die österreichische Datenschutzbehörde Ende 2018 ein entsprechendes Angebot der Zeitung „Der Standard" geprüft, aber nicht beanstandet.[18] Es verbleibt daher bei der hier dargestellten Rechtsunsicherheit. Zudem erscheint es fraglich, ob das Verbot des Versprechens eines nicht in direkter Verbindung stehenden Vorteils für eine bestehende Einwilligung einer grundrechtlichen Prüfung standhalten würde. Eine zumindest teilweise Klärung könnte sich bald aus der Verkündung des Urteils des Bundesgerichtshofs (BGH) zu I ZR 7/16 am 28.05.2020 ergeben, daher wird auf weitere Ausführungen dazu an dieser Stelle verzichtet.

Aufgrund der aus Art. 5 Abs. 2 folgenden Rechenschaftspflicht ist der Verantwortliche stets gezwungen, die Einhaltung der DSGVO und insbesondere die Wirksamkeit der erhobenen Einwilligungen nachzuweisen. Dabei wurde zeitgleich die Bußgeldhöhe, insbesondere auch für Verstöße gegen die Bedingungen für Einwilligungen, drastisch erhöht. Verstöße werden nunmehr mit einer Geldbuße von bis zu 20 Millionen Euro bzw. 4 Prozent des gesamten weltweit erzielten Jahresumsatzes sanktioniert, je nachdem welcher Betrag höher ist (vgl. Art. 83 Abs. 5 lit. a). Dies führte seit Geltung der DSGVO dazu, dass viele verantwortliche Stellen im Zweifel Einwilligungen eingeholt haben, um sich vor dem Vorwurf einer rechtswidrigen Datenverarbeitung zu schützen. 8

Doch genau diese Unsicherheit stellt den Verfasser einer Einwilligungserklärung vor hohe Hürden, da es noch keine höchstrichterliche Rechtsprechung, sondern nur die recht weitgehende Meinung der Aufsichtsbehörden zu den Anforderungen an eine wirksame Einwilligung gibt. 9

Im Ergebnis sind daher Zweifel angebracht, ob das Machtungleichgewicht hier wirksam bekämpft wird. Immer höhere Kosten für aufwändig gestaltetes Einwilligungsmanagement stärken große Anbieter, die diese Kosten auf Grund der Skaleneffekte besser tragen können. Gleichzeitig wird die Handhabung der Einwilligungen durch die Nutzer komplizierter und die Usability immer schlechter. Die Regeln zur Einwilligung geben zudem nur wenig Anreize, Angebote datenschutzfreundlich zu gestalten. Oftmals entscheiden sich Webseitenanbieter daher für mehr statt weniger Tracking. Müssen sie ohnehin schon eine Einwilligung einholen und schalten dazu eine Landingpage mit Consent-Management-Tool vor, so versuchen sie möglichst viele Verhaltensweisen zu tracken, um so zumindest den größtmöglichen Nutzen zu erzielen. Dass sich diese erzwungene Informationspolitik kontraproduktiv auf den Datenschutz auswirkt und eine Intervention dringend erforderlich ist, dürfte nicht ernsthaft in Frage gestellt werden. 10

[17] Artikel-29-Datenschutzgruppe, Stellungnahme 5/2009 zur Nutzung sozialer Online-Netzwerke, WP 163, 12.06.2009, S. 11.
[18] Der Standard: In eigener Sache, Datenschutzbehörde: STANDARD-Angebot entspricht DSGVO, 03.12.2018, https://www.derstandard.at/story/2000093057312/datenschutzbehoerde-standard-angebot-entspricht-dsgvo.

III. Datengewerkschaft

Im Arbeitsverhältnis ist der klassische Ansatz zur Behebung von Machtungleichgewichten der Zusammenschluss von Arbeitnehmern zu einer Gewerkschaft, die gebündelt ihre Interessen vertritt. Nach dem Motto „zusammen sind wir stark" wird das Machtungleichgewicht zumindest deutlich reduziert. Im Gegensatz zu immer höheren gesetzlichen Anforderungen ist die Mitgliedschaft in einer Datengewerkschaft freiwillig. Es kann zudem mehrere Datengewerkschaften geben. Ein Paternalismus ist damit ausgeschlossen. Eine Datengewerkschaft kann in folgenden Bereichen für mehr informationelle Selbstbestimmung sorgen: 11

- Einwilligung – durch Bündelung der Ressourcen kann eine Datengewerkschaft intensiver prüfen und die Interessen der Betroffenen wirksamer wahrnehmen. Zudem kann durch abgestimmtes Verhalten der Nutzer effektiver Druck auf Anbieter aufgebaut werden, Dienste datenschutzfreundlich auszugestalten.
- Recht auf Auskunft – de facto ist es noch immer schwer, eine vollständige Auskunft über die verarbeiteten Daten zu erhalten. Ein starker Partner und der Einsatz von Legal Tech können an dieser Stelle helfen.
- Verwertung – eine Gewerkschaft verhandelt Löhne und Arbeitsbedingungen. Eine Datengewerkschaft kann hier Tarife und Bedingungen verhandeln und auch kontrollieren; sie handelt im Auftrag der Betroffenen und verfolgt keine eigenen Interessen.

Im Folgenden beschränkt sich die Betrachtung auf den Bereich der Einwilligung. Welche technischen und organisatorischen Mittel kann eine Datengewerkschaft bereitstellen, um dabei die Usability und die effektive Selbstbestimmung der Nutzer zu erhöhen? 12
Zu denken wäre an folgende Dienste:

1. Ein Ampelsystem für Online-Angebote

Die Datengewerkschaft kann ein Bewertungsportal betreiben, in dem entweder die Community oder/und ausgewählte Datenschutzexperten zu bekannten Internetseiten, Apps und Diensten eine Bewertung zu den verschiedenen, dort wahrnehmbaren Online-Angeboten abgeben. 13

Hier kann aus verschiedenen Teilbewertungen (etwa Weitergabe von personenbezogenen Daten, Datensparsamkeit etc.) eine Gesamtbewertung errechnet werden. Auch subjektive Bewertungen, Datenpannen und Presseberichte können Berücksichtigung finden. 14

Ebenso denkbar sind Empfehlungen für die Rechtevergabe. Beispielsweise könnte der Zugriff auf Ortungsdienste empfohlen werden: „Standortdaten werden nicht gespeichert, die Nutzung von Ortungsdiensten ist bei diesem Anbieter unbedenklich". Dies würde analog zur Lebensmittelampel geschehen, welche dem Verbraucher 15

aufzeigt, ob ein Lebensmittel gesund oder ungesund ist, wobei bei Lebensmitteln allerdings die Behörden die Beurteilungskriterien festlegen.[19]

2. Realisierung als Browser-Plugin

Im Webbrowser kann ein Benutzer ein Plug-In installieren, in welchem er seine Datenschutzpräferenzen einstellt. Beim Besuch einer Website wird die Bewertung der 16

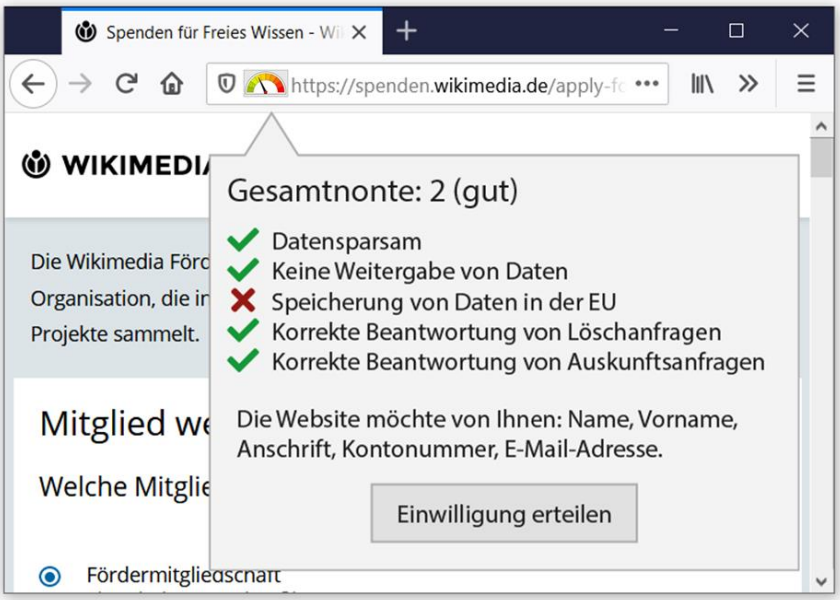

Abbildung 1: Kompakte Darstellung der Bewertung einer Website

Datengewerkschaft abgefragt und mit den persönlichen Datenschutzpräferenzen abgeglichen. Je nach Ergebnis erfolgt der Besuch der Webseite ohne Unterbrechung durch Datenschutzbanner, mit Datenschutzbannern oder aber der Zugriff wird gänzlich blockiert. Das Ergebnis des Abgleichs wird in der Statusleiste durch ein Symbol dargestellt, wobei die Details per Mausklick angezeigt werden können (vgl. Abbildung 1).

Diese Idee ist nicht neu. Bereits seit 2011 hat das World Wide Web Consortium W3C eine Tracking Preference Expression (DNT)[20] standardisiert. **DNT** steht dabei für „Do not Track". Zunächst als binäres Flag eingeführt, sollte es sogar in einer Erweiterung die differenzierten Tracking-Präferenzen an den Webserver übergeben, damit dieser ohne explizite Frage darauf reagieren kann. 17

[19] Verbraucherzentrale, Entscheidung für den Nutri-Score: Nährwertkennzeichnung kommt 2020, 28.04.2020, https://www.verbraucherzentrale.de/wissen/lebensmittel/kennzeichnung-und-inhaltsstoffe/entscheidung-fuer-den-nutriscore-naehrwertkennzeichnung-kommt-2020-36561.
[20] Tracking Preference Expression (DNT), letzte Version: W3C Working Group Note 17 2019, 17.01.2019, https://www.w3.org/TR/tracking-dnt/.

Hier können auch automatisiert verschiedene Funktionen (wie z.B. Ortungsdienste) basierend auf Empfehlungen blockiert werden oder Zugriffsrechte aufgrund des gewünschten Mindeststandards des Benutzers automatisch erteilt werden. 18

Ähnlich wie bei einem Passwort- oder Formular-Manager können zudem auch bereits gespeicherte Informationen automatisch in Formulare eingefüllt werden. 19

Das Browser-Plug-In kann eine Liste von erteilten Einwilligungen und übermittelten Informationen vorhalten. Es stellt den Benutzern eine Übersicht bereit, welchen Verantwortlichen eine Einwilligung für welche konkrete Datenverarbeitung erteilt wurde. 20

Als weitere Funktion ist denkbar, dass das Browser-Plug-In auch automatisiert Auskünfte erfragt, verschiedene Einwilligungen widerruft bzw. die Löschung der Daten anstößt. Daneben wäre es ebenso denkbar voreinzustellen, dass bei einer Absenkung des Datenschutzniveaus die Einwilligung automatisch widerrufen wird. 21

3. Realisierung als dezentrales Peer-to-Peer System

Die zuvor erteilten Einwilligungen können durch automatisierte Screenshots der ausgefüllten Formulare dokumentiert werden. Diese können zusammen mit einer digital signierten Bestätigung der Datenschutzerklärung sowie der empfangenen Daten zur Beweissicherung dienen. Dazu kann ein Hash-Wert gebildet werden, der auf einer Blockchain gespeichert als Beweis des Umfangs von Datenschutzerklärung und Einwilligung dienen kann.[21] Die eigentlichen Daten sollten jedoch nicht auf einer Blockchain, sondern verschlüsselt in der Cloud der Wahl der Nutzer gespeichert werden. Mozilla Firefox etwa speichert[22] bereits sensible Informationen wie Zugangsdaten verschlüsselt in seiner Cloud und könnte diese Funktionalität noch um die Informationen der Verarbeiter sowie die Dokumentation der Einwilligungen erweitern. 22

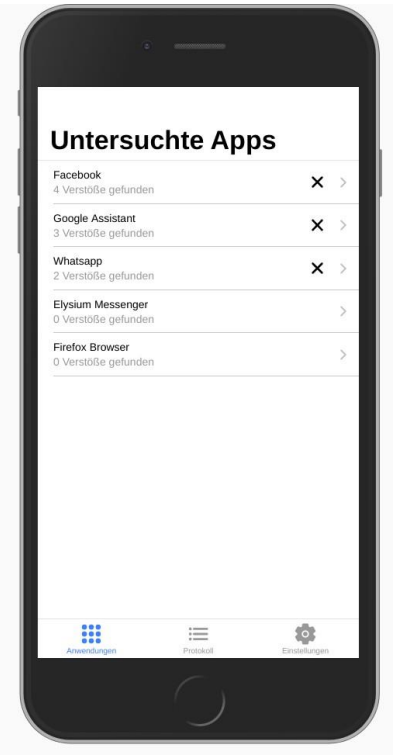

Abbildung 2: App zur Datenschutzkontrolle

[21] Erbguth, Datenschutzkonforme Verwendung von Hashwerten auf Blockchains, MMR 2019, 654-660 (658).
[22] mozilla Support, Wie Firefox Passwörter sicher speichert, https://support.mozilla.org/de/kb/wie-firefox-passworter-sicher-speichert.

4. Realisierung als Datenschutz-App

Eine Datenschutz-App kann, ähnlich einer Virenscanner-App, auf einem Mobilgerät installiert werden und bei der Installation von unsicheren Apps (bzw. Apps, die nicht den gewünschten Datenschutzpräferenzen des Benutzers entsprechen) eine Warnung anzeigen (vgl. Abbildung 2). 23

Hier kann auch eine Liste der Anwendungen gepflegt werden, damit der Benutzer den Überblick behält, welche Einwilligungen er auf seinem Mobilgerät bereits erteilt hat. 24

Zu den installierten Anwendungen können die Empfehlungen zu datenschutzkonformen Einstellungen sowie die Bewertungen der Datengewerkschaft angezeigt werden. Auch hier ist es wichtig, dass die Daten nicht zentral auf einem Server, sondern unter Kontrolle der Betroffenen verbleiben. 25

5. Durchsetzung von Ansprüchen via Legal Tech

Bei Verstößen, etwa der Verarbeitung trotz fehlender oder widerrufener Einwilligung, kann die Datengewerkschaft ihre Mitglieder anwaltlich vertreten und direkt Schadenersatzansprüche geltend machen. Hierbei kann Legal Tech zum Einsatz kommen, um per Mausklick Verfahren effizient auch bei geringem Streitwert durchführen zu können. Datengewerkschaften könnten zudem Musterfeststellungsklagen erheben. 26

Hinzu kommen die Bereiche, die in diesem Beitrag ausgeklammert wurden, wie die Auskunftserteilung sowie die aktive Verhandlung von Datenschutz- und Datenverwertungsbedingungen. Sobald Datenschutzrechte durch eine Datengewerkschaft wahrgenommen würden, würden die Verantwortlichen ihre Praxis ändern und mehr Betroffene selbstbestimmter mit ihren Daten umgehen. So hat z.B. auch die Plattform frag-den-staat[23] die Praxis der Behörden bei der Einhaltung des Informationsfreiheitsgesetzes (IFG) verbessert, nicht zuletzt, weil das Thema einer breiteren Öffentlichkeit bekannt wurde. 27

IV. Rechtliche Bewertung

Eine Datengewerkschaft wäre ein guter Ansatz zur Lösung des Einwilligungsdilemmas. Allerdings stellt sich auch die Frage der rechtlichen Umsetzbarkeit. 28

[23] Tagesspiegel, Wie Transparenz-Aktivisten deutsche Behörden löchern, 25.01.2020, https://www.tagesspiegel.de/themen/reportage/die-erstaunlichen-erfolge-von-frag-den-staat-wie-transparenz-aktivisten-deutsche-behoerden-loechern/25457788.html.

Besonders relevant ist in diesem Zusammenhang die Frage, inwieweit der Browser automatisch einwilligen kann, wenn der Verantwortliche im Protokoll sieht, dass der Browser und gerade nicht der Betroffene in Person diese Einwilligung abgegeben hat. 29

Wie man dem Wortlaut des Erwägungsgrundes 32 entnehmen kann, ist eine solche vorgelagerte Einwilligungserklärung nicht von vornherein ausgeschlossen. Danach **soll** die Einwilligung durch eine eindeutige bestätigende Handlung erfolgen, wobei auch eine **elektronische** Erklärung als zulässig erachtet wird. 30

Es ist gerade nicht zwingend, dass eine menschliche Handlung im Zeitpunkt der Abgabe der Einwilligung vorliegt, auch lässt sich aus dem Gesetzestext kein striktes Koinzidenzerfordernis herleiten, wie dies beispielsweise im Strafrecht[24] der Fall ist. Ausschlaggebend ist lediglich, dass die Einwilligung faktisch vor der Datenerhebung eingeholt wurde.[25] Bedenkt man, dass eine Vorverlagerung dem Recht nicht vollkommen fremd ist, würde es zu einem Wertungswiderspruch kommen, wenn man dem über seine eigene informationelle Selbstbestimmung disponierenden Betroffenen eine antizipierende Disposition versagen würde. Der Großteil der aktuellen juristischen Literatur geht davon aus, dass eine Stellvertretung bei Abgabe einer datenschutzrechtlichen Einwilligung auch über den gesetzlichen Vertretungsfall des Art. 8 Abs. 1 Satz 2 hinaus möglich ist.[26] Die gegenteilige Ansicht, wonach es sich bei der Einwilligung um ein höchstpersönliches Geschäft handelt, wurde zuletzt nur in der Kommentierung zum längst außer Kraft getretenen § 4a BDSG a.F. vertreten.[27] Es erscheint daher zweckmäßig, von dieser Ansicht abzukehren und die Stellvertretung zuzulassen. 31

Doch liegt hier der Fall einer Vertretung vor? Die Datengewerkschaft würde hier als eine Art „Dolmetscherin im Datenschutz“ fungieren. Sie würde die oftmals in wenig verständlicher juristischer Sprache verfassten Datenschutzerklärungen (s.o.) und vielleicht auch von diesen abweichenden Seitenquelltexte prüfen, um dem Betroffenen das Ergebnis dann auch tatsächlich in präziser, transparenter und insbesondere auch verständlicher Form zu präsentieren. Ausgehend von dieser Übersetzung in eine Kategorie, nehmen die Betroffenen eine vorverlagerte Entscheidung vor. Auch diese Konstellation ist dem Recht nicht fremd, da aufschiebend bedingte Willenserklärungen gang und gäbe sind (§ 158 Abs. 1 BGB). Wenn sogar für eine datenschutzrechtliche Einwilligung eine Stellvertretung zulässig ist, so sollte erst recht diese teilweise Verlagerung des Entscheidungsprozesses auf die Datengewerkschaft durch aufschiebende Bedingung möglich sein. 32

[24] Schmidt/Werner, in: Creifelds, Rechtswörterbuch, 23. Edition 2019, Vorsatz.
[25] Art-29-Datenschutzgruppe, Stellungnahme 15/2011 zur Definition von Einwilligung, WP187, S. 11.
[26] Taeger, in: Gabel/Taeger, DS-GVO, 3. Aufl. 2019, Art. 7 Rn. 9; Ingold, in: Sydow, EU-Datenschutzgrundverordnung, 2. Aufl. 2018, Art. 7 Rn. 19; Gola/Schomerus, BDSG, Aufl. 2015, § 4a Rn. 25; Hoffmann, NZS 2017, 807-812 (808); Kühling/Buchner, in: Buchner/Kühling, 2. Aufl. 2018, DS-GVO BDSG, Art. 7 Rn. 31.
[27] Spindler/Nick, in: Spindler/Schuster, BDSG, 2. Auflage 2011, § 4a Rn. 5; Simitis, in: Simitis, BDSG, 7. Auflage 2011, § 4a Rn. 30.

Allerdings sind bei der vorherigen Hinterlegung weder die Verantwortlichen noch der Zweck der Verarbeitung bekannt. Der EDSA fordert dagegen, dass die Granularität der hinterlegten Einwilligung nach Verarbeitungszwecken differenziert und die Verantwortlichen dort benannt werden müssen.[28] Im Browser vorab alle Verantwortlichen zu hinterlegen und nach allen Verarbeitungszwecken zu differenzieren, würde das jedoch – wenn nicht unmöglich – dann doch zumindest so komplex gestalten, dass ein Vereinfachungseffekt nicht mehr vorhanden wäre. 33

Zu fragen wäre jedoch, wie es sich mit den Informationspflichten verhält, welche nach Art. 13 Abs. 1 Satz 1 zum Zeitpunkt der Datenerhebung bereitgestellt werden müssen. Einen Verzicht auf Informationen kennt die DSGVO nicht und lässt nur eine Ausnahme zu, wenn die Information dem Betroffenen bereits vorliegt (Art. 13 Abs. 5). Allerdings erscheint es an dieser Stelle geboten, dem Betroffenen die verfassungsrechtlich garantierte Freiheit einzuräumen, frei über die Möglichkeit eines Verzichts zu entscheiden. Andernfalls würde die Pflicht des Verantwortlichen zur Bereitstellung der Informationen in eine Pflicht des Betroffenen zur Annahme uminterpretiert werden, was den Sinn und Zweck der Informationspflicht ad absurdum führen würde. Die Ausübung negativer Freiheitsrechte ist der EU-GRCh keinesfalls fremd. Wie aus der negativen Religionsfreiheit nach Art. 10 Abs. 1 EU-GRCh hervorgeht, steht es dem Grundrechtsträger frei, auf seine Religionsfreiheit zu verzichten.[29] Entsprechendes muss auch hier gelten, wonach die negative informationelle Selbstbestimmung es dem Betroffenen ermöglichen muss, sich der Informationsflut zu entziehen. Die Vielzahl der Datenschutzerklärungen, die wir lesen sollen, führt bereits auch dann zu einem „Information Overload“[30], wenn die einzelne Erklärung vorher noch nicht bekannt war. Selbst wenn bislang der Begriff des Information Overload nur dann verwendet wurde, wenn vorab eine informierte Einwilligung eingeholt wurde und sodann nochmals nach Art. 12 ff. informiert werden sollte. 34

V. Fazit

Auch fachkundigen Menschen ist es heutzutage kaum mehr möglich, den Überblick über Einwilligungen in Datenverarbeitungen zu behalten. An jeder Einwilligung hängen lange Datenschutzerklärungen, die zudem ständigen Änderungen unterliegen. Eine individuelle Prüfung der täglich aufs Neue eingeforderten Einwilligungen ist daher praktisch nicht möglich. So können wir nicht wirksam zwischen akzeptablen oder überbordenden Datenverarbeitungen differenzieren. Unternehmen haben in der Folge keinen Anreiz, ihre Verarbeitungen datenschutzfreundlich zu gestalten. 35

Eine striktere Interpretation der DSGVO, wie sie der EDSA vorgibt, scheint hier keine Lösung zu bieten. Wir schlagen deshalb einen technisch-organisatorischen 36

[28] EDSA, aaO, Rn. 89.
[29] Jarass, Charta der Grundrechte der Europäischen Union, 3. Aufl. 2016, Art. 10 Rn. 10.
[30] Ingold, in: Sydow, Europäische Datenschutzgrundverordnung, 2. Auflage 2018, Art. 13 Rn. 10.

Lösungsansatz vor, der nicht nur die informationelle Selbstbestimmung stärkt, sondern auch datenschutzfreundliches Verhalten von Unternehmen fördert. Statt Investitionen in Consent-Management-Systeme und immer ausgefeiltere Datenschutzbestimmungen zu tätigen, wäre es lohnender, an der eigenen Datenschutzperformance zu arbeiten. Von einer verbesserten User-Experience profitieren beide – Anbieter wie Nutzer. Dieser Lösungsansatz ist angelehnt an Plattformen wie frag-den-staat, die OpenData-Ansätze oder auch Legal-Tech-Ansätze zur Durchsetzung von Fluggastrechten. Der vorliegende Aufsatz hat nicht nur gezeigt, dass dieser Ansatz prinzipiell funktioniert, sondern, dass er auch de lege lata realisierbar ist. Wir hoffen, dass die Idee einer solchen Datengewerkschaft Zuspruch findet – gerade auch bei den Aufsichtsbehörden.