Maren Pollmann, Dennis-Kenji Kipker

Informierte Einwilligung in der Online-Welt

Die Einwilligung als Legitimationstatbestand für eine Datenverarbeitung ist seit jeher umstritten. Jedoch wird ihr auch unter der Datenschutz-Grundverordnung (DSGVO) eine zentrale Rolle als datenschutzrechtlicher Erlaubnistatbestand zukommen und ihre praktische Bedeutung angesichts einer immer komplexeren Verarbeitung personenbezogener Daten noch weiter zunehmen. Umso wichtiger ist es daher, dass die notwendigen Vorbedingungen für eine wirksame Einwilligung gewahrt werden. Insbesondere die Sicherstellung der Informiertheit stellt sich zunehmend als problematisch dar. Der folgende Beitrag stellt ein Konzept vor, wie dennoch eine informierte Einwilligung unter der DSGVO gewährleistet werden kann.

1 Rechtliche Anforderungen an die informierte Einwilligung

Das Erfordernis einer informierten Einwilligung soll sicherstellen, dass der Betroffene weiß, in was er einwilligt.[1] Entsprechend verlangt Art. 4 Abs. 11 DSGVO, wie auch schon die Datenschutzrichtlinie und das BDSG, dass der Betroffene seine Einwilligung in die Nutzung seiner personenbezogenen Daten „in informierter Weise", d.h. „in Kenntnis der Sachlage"[2] erteilt. Damit bleibt aber auch unter der DSGVO das gleiche – strukturelle – Problem bestehen wie schon bislang: Die Idee, die Einwilligungserteilung von der Informiertheit des Betroffenen abhängig zu machen, ist sicherlich überzeugend, die konkrete Umsetzung in der Praxis stellt sich jedoch mehr als schwierig dar. Verwiesen sei nur auf das viel zitierte Beispiel Facebook. Für eine „informierte" Einwilligung muss sich der Nutzer hier im Zuge der Registrierung mit Datenschutzbestimmungen auseinandersetzen, die vom Umfang her nahezu zehn DIN A4-Seiten umfassen. Innerhalb dieser Bestimmungen wird dann – unter Zuhilfenahme weiterer Verlinkungen – auf die Datenverwendungsrichtlinien integrierter Dienste verwiesen, wodurch der Umfang der Bestimmungen noch einmal deutlich zunimmt.[3] Auf diese Weise wachsen die Informationen derart an, dass sie anstelle einer allgemeinverständlichen Unterrichtung gem. § 13 Abs. 1 TMG, § 4a Abs. 1 Satz 2 BDSG eine Informationsüberflutung für den Einzelnen mit sich bringen.

Eine ausführliche Darstellung der Datenverwendung wie im Beispiel Facebook mag zwar auf den ersten Blick durchaus zu einer Informiertheit der Betroffenen beitragen. Jedoch wird der Durchschnittsnutzer in der Online-Welt nicht nur von Facebook, sondern auch von einer Vielzahl anderer Unternehmen dazu aufgefordert, sich mit den jeweiligen Datenschutzrichtlinien einverstanden zu erklären. Dabei muss die Einwilligung stets derart ausgestaltet sein, dass sie alle beabsichtigten Verarbeitungsvarianten personenbezogener Daten abdeckt. Um sich mit den teilweise äußerst umfangreichen Datenschutzbestimmungen auseinanderzusetzen, muss der Betroffene ein erhebliches Maß an Zeit und Anstrengungen aufwenden, um anhand der ihm unterbreiteten Informationen die Tragweite seiner Entscheidung abschätzen zu können.[4] Infolge der stetig zunehmenden Vernetzung und der damit einhergehend komplexeren Datenverarbeitung werden die Datenschutzbestimmungen zudem auch künftig weiter an Komplexität gewinnen, allein durch die Offenlegung sämtlicher Verarbeitungspraktiken wird damit dem Erfordernis der informier-

1 *Simitis*, in ders., BDSG, 8. Aufl., § 4a, Rn. 70 ff.
2 Siehe Erwägungsgrund 42 der DSGVO.

Maren Pollmann, LL.M.

Wissenschaftliche Mitarbeiterin und Doktorandin am Institut für Informations-, Gesundheits- und Medizinrecht (IGMR), Universität Bremen

E-Mail: m.pollmann@uni-bremen.de

Dr. Dennis-Kenji Kipker

Wissenschaftlicher Mitarbeiter am Institut für Informations-, Gesundheits- und Medizinrecht (IGMR) der Universität Bremen, Lehrbeauftragter an der Hochschule Bremerhaven und Mitglied im Vorstand der Europäischen Akademie für Informationsfreiheit und Datenschutz (EAID) in Berlin
E-Mail: kipker@uni-bremen.de

3 *Buchner*, DuD 2015, 402 (404).
4 Zu dieser Zielsetzung der informierten Einwilligung siehe *Körffer*, in: Gola/Schomerus, BDSG, 12. Aufl., § 4a, Rn. 25.

ten Einwilligung zukünftig kaum noch entsprochen werden können. Die gesetzlichen Anforderungen an die Informiertheit stellen daher die Entscheidungsfreiheit des Einzelnen zunehmend nur noch dem Anschein nach sicher, dem Grundgedanken einer informationellen Selbstbestimmung können sie jedoch schon lange nicht mehr gerecht werden. Realistisch betrachtet ist eine vollständige Informiertheit unter den dargestellten Bedingungen nicht zu erreichen.

Es bedarf daher ergänzender Instrumente, um einen informed consent auch im Online-Bereich sicherzustellen, sodass die Einwilligung auch zukünftig als zentraler Erlaubnistatbestand genutzt werden kann. Die Einwilligung stellt im Gegensatz zu den gesetzlichen Erlaubnistatbeständen ein flexibles Instrument dar, mithilfe dessen sich der Datenverarbeiter datenschutzrechtlich absichern kann.[5] Insbesondere im Hinblick auf den rasanten technischen Fortschritt und damit einhergehende innovative Dienstleistungsmodelle, die auf der Verarbeitung personenbezogener Daten basieren, bildet die Einholung einer Einwilligung häufig die einzige Möglichkeit für eine datenschutzkonforme Datenverarbeitung. So hält auch die DSGVO an der Einwilligung und den ihr zugrundeliegenden Voraussetzungen fest. Somit bleibt auch in Zukunft das Problem der informierten Einwilligung bestehen.

Mit detaillierteren Vorgaben zur Formulierung der Einwilligung kann die Problematik nicht gelöst werden, da solche in der Regel nicht zur Verringerung des Umfangs der Informationen beitragen. Wenn das Lesen der Datenschutzbestimmungen für den Einzelnen im Vergleich zu der gesamten Dauer des Vertragsschlusses nicht angemessen erscheint, wird er davon absehen. Wenn ein Internetnutzer im Durchschnitt jährlich 76 Arbeitstage à 8 Stunden mit dem Lesen von Datenschutzbestimmungen verbringen müsste,[6] um eine informierte Entscheidung treffen zu können, bedarf es offensichtlich neuer Instrumente, welche unter den heutigen und zukünftigen Bedingungen der digitalen Vernetzung eine informierte Einwilligung sicherstellen können. Der Einzelne muss einschätzen können, welche Auswirkungen eine Einwilligungserteilung zur Folge hat – und zwar ohne sich im Detail mit umfangreichen Datenschutzbestimmungen auseinandersetzen zu müssen. Das theoretische Konzept der informierten Einwilligung muss auch praktisch realisierbar sein.

2 Lösungsvorschläge

2.1 „One-Pager"

Einen Schritt zu mehr Transparenz und damit einem höheren Grad an Informiertheit verspricht das kürzlich von der Plattform „Verbraucherschutz in der digitalen Welt" veröffentlichte Muster für Datenschutzhinweise „One-Pager".[7] Unternehmen können mithilfe einer Vorlage die wesentlichen Aussagen ihrer Datenverwendungsrichtlinien auf nur einer Seite präsentieren.

Jedoch: Auch wenn sich durch den „One-Pager" der Umfang der Datenschutzbestimmungen optisch zunächst erheblich reduziert, stellt er de facto keine Kürzung der Bestimmungen dar. Denn die Nutzer erhalten weiterhin detaillierte Erläuterungen, nur eben nun auf mehrere Ebenen verteilt, welche sie mittels einer Mouseover-Funktion oder eines Links sichtbar machen können. Auch beim „One-Pager" stellt sich somit weiterhin das Problem der Informationsmassen. Sein wesentlicher Vorteil liegt vielmehr in einer zumindest auf den ersten Blick übersichtlichen und gegliederten Darstellung einiger wichtiger Datenverwendungsarten. Nichtsdestotrotz macht es der Grundsatz einer informierten Einwilligung auch hier nötig, dass der Nutzer neben den auf eine Seite gekürzten Datenschutzbestimmungen auch die umfassenden Zusatztexte liest, soll er vollständig informiert sein. Zudem erscheint selbst der Text einer DIN A4-Seite etwa auf einem Smartphone alles andere als übersichtlich, weshalb der „One-Pager" zumindest bei der Nutzung mobiler Endgeräte nur eingeschränkt in der Lage sein wird, die Praxistauglichkeit des informed consent zu erhöhen.

Unabhängig davon stellt sich die Frage, ob die Bereitstellung der vollständigen Information allein durch einen Link oder die Mouseover-Funktion in Einklang mit den Unterrichtungspflichten gemäß § 13 TMG, § 33 BDSG steht. Von der Rechtsprechung wurde der Mouseover-Effekt in Bezug auf Informationspflichten mehrfach als unzureichend eingestuft.[8] Denn es könne auf diese Weise nicht sichergestellt werden, dass jeder Nutzer die Information, die erst nach einem kurzen Verweilen mit dem Cursor auf einem bestimmten Wort erscheint, tatsächlich zur Kenntnis nimmt.[9] Zwar bezogen sich die bisherigen Entscheidungen nicht auf datenschutzrechtliche Informationspflichten, sondern unter anderem auf die Pflicht zur Urheberbenennung auf einer Webseite, zur Angabe von Preisen und Kosten beim Online-Versandhandel oder auf die Aufklärungspflicht über allgemeine Geschäftsbedingungen auf einer Internetseite. Dennoch sind die für diese Entscheidungen bestimmten Anforderungen auch für die datenschutzrechtliche Einwilligung relevant, da es auch hier um die Erfüllung von Informationspflichten – nicht selten in einem technischen Zusammenhang – geht, welche den Schutz des Einzelnen bezwecken und somit einem Transparenzgebot unterliegen.

2.2 Visualisierung

Visualisierungen sind in der Lage, ein informiertes und selbstbestimmtes Handeln des Einzelnen zu fördern. Man denke beispielsweise an Vorschläge aus der Lebensmittelindustrie[10] sowie an Forderungen im Bereich der Risikobewertung von Finanzprodukten[11].

Solche Konzepte lassen sich ebenso auch auf das Datenschutzrecht übertragen, um die Informiertheit bei der Ausübung des informationellen Selbstbestimmungsrechts zu fördern. So sah der Parlamentsentwurf zur DSGVO noch eine Verpflichtung für Unternehmen vor, maschinenlesbare „standardisierte Informationsmaßnahmen" zu verwenden, um den Nutzer auf einfache Weise über das Vorliegen besonders relevanter Verarbeitungsar-

5 *Kühling*, in: Wolff/Brink, Datenschutzrecht, § 4a, Rn. 8.

6 Siehe dazu den Beitrag von *Bolsinger* (in diesem Heft).

7 Pressemitteilung des Bundesministeriums für Justiz und Verbraucherschutz vom 19.11.2015, online abrufbar unter: http://www.bmjv.de/SharedDocs/Pressemitteilungen/DE/2015/11192915_Vorstellung_OnePager.html (Stand: 25.04.2016).

8 OLG Frankfurt, K&R 2011, 414; LG München I, MMR 2015, 467; LG Hamburg MMR 2014, 612; LG Bochum, K&R 2013, 754.

9 LG München I, MMR 2015, 467 (469).

10 Anschaulich dazu: http://www.vzbv.de/sites/default/files/mediapics/was_ist_die_ampel.pdf (Stand: 25.04.2016).

11 So z.B. von der Präsidentin der BaFin Elke König, online abrufbar unter http://www.zeit.de/wirtschaft/geldanlage/2014-02/prokon-bafin-anlegerschutz-finanzprodukte (Stand: 25.04.2016).

ten zu informieren.[12] Dadurch sollte der Betroffene beispielsweise Kenntnis darüber erlangen, ob das Unternehmen mehr Daten erhebt, als für die Erfüllung des spezifischen Verarbeitungszwecks erforderlich ist oder ob eine Übermittlung der Daten an Dritte erfolgt.

Für die Einholung einer Einwilligung sah der Parlamentsentwurf vor, dass das jeweilige Unternehmen die Informationen über seine Datenverwendungspraktiken dem Betroffenen mithilfe von Piktogrammen visuell darlegt. Dabei sollten die Informationen in Form einer dreispaltigen Tabelle veranschaulicht werden. In der ersten Spalte sollten verschiedene Verwendungsarten mithilfe von Bildsymbolen illustriert werden. Diese betrafen sowohl den Umfang als auch die Art und Weise der Datennutzung, zum Beispiel eine verschlüsselte Aufbewahrung personenbezogener Daten. Darüber hinaus war vorgesehen, Beschreibungen zu den Verwendungsarten in einer zweiten Spalte neben dem Symbol zu platzieren. Eine dritte Spalte sollte schließlich Auskunft darüber geben, ob das Unternehmen von der jeweiligen Verwendungsart Gebrauch macht. Hierfür waren wiederum Symbole vorgesehen – ein grünes Hakensymbol zur Bestätigung sowie ein rotes Kreuzsymbol, um das Vorhandensein der Verwendungsart zu verneinen.

Der Vorschlag, Datenschutzbestimmungen visuell darzustellen, bietet großes Potenzial, um dem strukturellen Problem der informierten Einwilligung zu begegnen. Ein solches System kann – bezogen auf die dargestellten Verwendungsarten – in einfacher Weise Aufschluss über die Datenverwendung geben und insoweit die Informiertheit der Einwilligung durch eine transparente und leicht zugängliche Darstellung sicherstellen.[13] Auch wenn der Einsatz von Bildsymbolen in der Endfassung der DSGVO nur noch als freiwillige Option vorgesehen ist (Art. 12 Abs. 7 DSGVO), so stellt er dennoch ein praktikables Instrument zur Umsetzung des informed consent dar. Die DSGVO räumt weiterhin der Kommission die Befugnis ein, delegierte Rechtsakte zur Bestimmung der Informationen, die durch Bildsymbole darzustellen sind, und der Verfahren für die Bereitstellung standardisierter Bildsymbole zu erlassen, Art. 12 Abs. 8 DSGVO. So kann die vorgesehene Visualisierung um weitere Elemente ergänzt und konkretisiert werden, die eine informierte Einwilligung und damit einen effektiven Schutz personenbezogener Daten realisieren.[14]

2.3 Verknüpfung mit Bewertungselementen

Eine reine Aufschlüsselung der Information nach einzelnen Attributen – wie im Parlamentsentwurf vorgesehen – ist zwar sinnvoll, aber noch nicht ausreichend, um der Problematik des steigenden Informationsbedarfs aufgrund der stärkeren digitalen Vernetzung praxisnah zu begegnen. Sie gibt lediglich Auskunft über das Vorhandensein bestimmter Verarbeitungsarten. Wie stark hiermit jedoch das Recht auf informationelle Selbstbestimmung des Betroffenen berührt wird, vermag dieser aufgrund des reinen Darstellungscharakters der Symbolik nicht abzuschätzen. Der Einzelne wird zudem nur über die aufgeführten Verwendungsarten informiert, eine datenschutzrechtliche Risikoabschätzung des infrage stehenden Dienstes findet jedoch nicht statt. Eine Ausweitung der Kategorien auf eine Vielzahl an Datenverarbeitungsarten birgt erneut die Gefahr, in eine Unübersichtlichkeit zu münden, die der Informiertheit des Einzelnen eher abträglich wäre. Aus diesem Grund sollte die Kommission mittels eines delegierten Rechtsaktes die rein bildliche Darstellung um eine Bewertung der einzelnen Kategorien ergänzen, um auch eine datenschutzrechtliche Gesamtwertung des in Rede stehenden Dienstes zu ermöglichen. Hierdurch wird dem Betroffenen die individuelle Folgenabschätzung seines Verhaltens im Internet deutlich erleichtert.

Ein solcher Ansatz könnte als datenschutzrechtliche Vorbewertung in Form eines farblichen Leitsystems ausgestaltet sein, welches die Intensität der Datenverarbeitung im Hinblick auf das informationelle Selbstbestimmungsrecht des Betroffenen beurteilt (rot – hohe Intensität, gelb – mittlere Intensität, grün – geringe Intensität)[15], sobald es zur Einholung einer Einwilligung kommt. Dabei ist es durchaus denkbar, weitere graduelle Abstufungen in dem Farbsystem vorzunehmen, um ein differenzierteres Bewertungsergebnis zu ermöglichen.

2.4 Bewertungskriterien

Die Kriterien einer datenschutzrechtlichen Vorbewertung müssen in ihrer Gesamtheit in der Lage sein, ein aussagekräftiges Bild über den mit der Nutzung eines bestimmten Dienstes verbundenen Umfang der Verarbeitung personenbezogener Daten zu liefern. Eine Orientierung anhand der allgemeinen datenschutzrechtlichen Prinzipien, wie sie das BDSG und künftig die DSGVO[16] aufstellen, ist deshalb sinnvoll. So stellen Informationen über die Menge und die Art der verwendeten Daten sowie den Zweck der Verwendung wesentliche Angaben dar. Werden sensible Daten durch das Unternehmen erhoben, muss sich dies negativ in der Bewertung widerspiegeln. Hinsichtlich des Verarbeitungszwecks sollte zudem das Profiling als Negativmaßstab dienen: Je mehr die anzugebenden Informationen die Bildung eines Gesamtbildes der Persönlichkeit des Einzelnen ermöglichen, desto schwerwiegender ist die Beeinträchtigung zu bewerten. Eine Datenverarbeitung ist ferner nur erlaubt, soweit sie der Erreichung ihres Verarbeitungszweckes dient.[17] Deshalb ist zusätzlich zu berücksichtigen, inwieweit die erhobenen personenbezogenen Daten für die Diensteerbringung des jeweils Verantwortlichen erwartungsgemäß notwendig oder aber ob Änderungen des Verarbeitungszweckes vorgesehen sind. Insofern kann auch auf die Verwendungsarten des EU-Parlamentsentwurfs zur DSGVO zurückgegriffen werden. Auf diese Weise ist es möglich, eine Datenerhebung, welche über die Erfordernisse des konkreten Dienstes hinausgehende Informationen erfasst, negativ in die Bewertung einfließen zu lassen. Dies entspricht auch dem Prinzip der Datensparsamkeit, welches in der Privacy-by-design-Verpflichtung des Art. 25 DSGVO besonders zum Ausdruck gebracht wird. In die Gesamtbewertung einfließen müssen ebenso Angaben über eine Weitergabe von Informationen an Dritte sowie über die Dauer der Speicherung von Daten.

12 Siehe Art. 13a sowie Anhang zu Art. 13a der legislativen Entschließung des Europäischen Parlaments vom 12. März 2014 zu dem Vorschlag für eine Verordnung des Europäischen Parlaments und des Rates zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr
(allgemeine
Datenschutzverordnung) (COM(2012)0011 – C7-0025/2012 – 2012/0011(COD)).

13 Vgl. Erwägungsgrund 48 DSGVO.

14 Siehe Erwägungsgrund 166 DSGVO.

15 In diesem Sinne z.B. auch *Forgó* im Interview mit *Beer*, c't 04/2014, S. 27.

16 Siehe Art. 5 sowie Erwägungsgrund 39 DSGVO.

17 *Wolff*, in Wolff/Brink, Beck'scher Online-Kommentar Datenschutzrecht, 14. Ed., Prinzipien, Rn. 13.

Eine besondere Gewichtung innerhalb der datenschutzrechtlichen Vorbewertung muss ferner den Betroffenenrechten zukommen, denn sie unterstreichen die Gestaltungs- und Entscheidungsfreiheit, die dem Einzelnen in Bezug auf seine personenbezogenen Daten zukommt, in besonderem Maße. So werden dem Betroffenen in Kapitel III DSGVO zwar bereits eine Vielzahl an Rechten eingeräumt. Es sollte darüber hinaus aber positiv bewertet werden, wenn die verantwortliche Stelle erleichterte Bedingungen für die Wahrnehmung dieser Rechte schafft. Diese könnten unter anderem in der Festlegung einer Maximaldauer für die Bearbeitung von Betroffenenansprüchen liegen oder auch in der Einrichtung eines gesonderten, verkürzten Verfahrens für den Fall, dass Betroffenenrechte in Bezug auf besonders sensible Daten geltend gemacht werden.

Nicht zuletzt bedingen Datenschutz und IT-Sicherheit einander. Deswegen sind neben den Betroffenenrechten auch technische und organisatorische Vorkehrungen notwendig, die den Schutz personenbezogener Daten vor einem unberechtigten Zugriff gewährleisten. Je umfassender Aspekte der IT-Sicherheit bei einem Diensteanbieter berücksichtigt werden, umso höher ist folglich auch sein Datenschutzstandard im Rahmen der Vorbewertung zu beurteilen.

2.5 Konkretisierung durch die Kommission

Artikel 12 Abs. 8 DSGVO überträgt der Kommission die Befugnis, mittels eines delegierten Rechtsaktes diejenigen Informationen festzulegen, welche durch standardisierte Bildsymbole dargestellt werden können, sowie ein Verfahren zur Bereitstellung standardisierter Symbole zu bestimmen. Delegierte Rechtsakte sollen eine Überladung des europäischen Sekundärrechts mit technischen Details dadurch verhindern, dass die Kommission Vorschriften eines Gesetzgebungsaktes, die nicht von wesentlicher Bedeutung für den jeweiligen Bereich sind, durch verbindliche Vorschriften ändern oder ergänzen kann.[18] Diese Ermächtigung muss in dem zugrundeliegenden Gesetzgebungsakt ausdrücklich als solche festgeschrieben sein und unterliegt der Kontrolle durch das Europäische Parlament und den Rat, Art. 290 AEUV und Art. 92 DSGVO.

Während der Kommissionsentwurf zur DSGVO noch weitgehende Kompetenzen für die Kommission vorsah, einzelne Vorschriften mithilfe delegierter Rechtsakte zu konkretisieren,[19] wurde im Zuge der Trilog-Verhandlungen diese Kompetenzübertragung auf nur noch zwei Fälle reduziert: auf nähere Bestimmungen zu den standardisierten Bildsymbolen sowie auf die Festlegung der Anforderungen an datenschutzspezifische Zertifizierungsverfahren, Art. 43 Abs. 8 DSGVO.

Da es der Kommission als Adressatin der Delegation nicht erlaubt ist, ihre Rechtssetzungsbefugnis an andere EU-Akteure weiterzureichen,[20] ist sie die zuständige Stelle, um die Kriterien für das datenschutzrechtliche Bewertungssystem festzulegen. Unterstützung erhält sie durch den Europäischen Datenschutzausschuss (Art. 68 ff. DSGVO), welcher mit Inkrafttreten der DSGVO die Art. 29-Datenschutzgruppe ablösen wird. Er bildet im Gegensatz zu seiner Vorgängerinstitution ein rechtlich selbstständiges Gremium, das neben seinen beratenden Aufgaben auch verbindliche Entscheidungen treffen kann. Hinsichtlich der standardisierten Bildsymbole beschränkt sich seine Kompetenz auf die Abgabe einer Stellungnahme für die Kommission gemäß Art. 70 Abs. 1 lit. r DSGVO.

Neben der Festlegung der Bewertungskriterien ist ein weiterer Bestandteil des delegierten Rechtsaktes die Bestimmung des Verfahrens für die Bereitstellung der standardisierten Bildsymbole, Art. 12 Abs. 8 DSGVO. Während die Bereitstellung der den einzelnen Kriterien zugeordneten Symbole durch die Kommission selbst vollzogen werden muss, kann die Zuweisung einer Farbe im Sinne des farblichen Leitsystems durch das jeweilige Unternehmen durchgeführt werden.[21] Die nationalen Datenschutzbehörden können sodann stichprobenartige Überprüfungen der Farbzuweisung durchführen. Mangels ausreichender finanzieller und personeller Ressourcen können die Behörden bei einer realistischen Betrachtungsweise keine umfassendere Kontrolle leisten.[22] Dennoch ließe sich die Überprüfung durch ein System dezentraler Beschwerdestellen effektivieren, an welche sich Betroffene wenden können, falls ein Unternehmen die Bewertung seines Dienstes möglicherweise nicht ordnungsgemäß durchgeführt hat. Liegen mehrere Beschwerden zu einem bestimmten Unternehmen vor, kann die Behörde überprüfend tätig werden.

3 Fazit

Die Informiertheit der Einwilligung stellt das Datenschutzrecht insbesondere bei Online-Diensten vor große Herausforderungen. Den Betroffenen ausreichend über die potenzielle Datenverarbeitung in Kenntnis zu setzen, ist häufig nicht mit den begrenzten zeitlichen Möglichkeiten des Nutzers sowie seinem Bedürfnis nach einer schnellen, transparenten und unkomplizierten Nutzung von Internetangeboten in Einklang zu bringen. Mit dem rasant wachsenden Funktionsumfang und Leistungsangebot von Online-Diensten und damit einhergehend immer umfangreicheren Anforderungen an eine Datenverwendung wächst zugleich das Interesse der Betroffenen an einer übersichtlichen und verständlichen Darstellung der Informationen über die Verwendung ihrer personenbezogenen Daten. Visualisierungen, idealerweise ergänzt um bewertende Elemente, können diesem Interesse nachkommen, indem sie dem Einzelnen auf einfache Weise veranschaulichen, in welchem Maße sein Recht auf informationelle Selbstbestimmung durch den jeweiligen Dienst tangiert wird. Durch den Erlass eines delegierten Rechtsaktes lässt sich ein solches System in die bestehenden Regelungen integrieren. Zwar ist die Verwendung der Symbole für die Unternehmen nicht verpflichtend, ein System aus Visualisierung und Bewertung stellt jedoch derzeit die beste Alternative dar, um dem Erfordernis einer informierten Einwilligung zu genügen.

18 *Gellermann*, in: Streinz, EUV/AEUV, 2. Aufl., § 290 AEUV Rn. 2 ff.

19 Diese weitreichenden Befugnisse für die Kommission wurden von der Literatur zumeist kritisch gesehen; s. etwa *Kahler*, RDV 2013, 69 ff., *Traung*, CRi 2012, 33 (34).

20 *Ruffert*, in: Calliess/Ruffert, EUV/AEUV, 4. Aufl., § 290 AEUV Rn. 8.

21 Dies entspricht auch der Aufgabenverteilung im Parlaments-Entwurf, wonach die verantwortliche Stelle die Bildsymbole aufzuführen hatte.

22 Zur Überlastung der Datenschutzbehörden siehe *Deutsches Institut für Menschenrechte*, „Zugang zu Datenschutz-Rechtsbehelfen in EU-Mitgliedstaaten" – eine Studie der EU-Grundrechteagentur, Hintergrundinformation zur Forschung in Deutschland, 27.01.2014, online abrufbar unter http://www.institut-fuer-menschenrechte.de/fileadmin/user_upload/PDF-Dateien/Factsheets/Zugang_zu_Datenschutz_Rechtsbehelfen_in_EU_Mitgliedstaaten_eine_Studie_der_EU_Grundrechteagentur_Hintergrundinformationen_zur_Forschung_in_Deutschland.pdf (Stand: 25.04.2016).