Legitimation von Datenverarbeitung via AGB?
Wider eine Verlagerung von datenschutzrechtlichen Abwägungen in das Vertragsrecht

Christian Aldenhoff

1. Einleitung

Die DS-GVO sieht verschiedene Instrumente zur Legitimation von Datenverarbeitungsvorgängen vor. Einerseits wird die Einwilligung als ein solches Instrument auch nach Geltungsbeginn der DS-GVO weiterhin von vielen Verantwortlichen als primäre Legitimationsgrundlage herangezogen. Andererseits wird schon seit längerem kritisiert, dass sie die ihr zugedachte Funktion unter den veränderten Bedingungen der digitalen Kommunikationsgesellschaft nicht mehr zufriedenstellend erfüllen kann. Die der Einwilligung zugrundeliegenden Datenschutzerklärungen sind regelmäßig entweder lang, umfassend und kompliziert – oder aber kurz, vereinfachend und ungenau. Daher sollen in diesem Beitrag zunächst die Defizite bei der praktischen Anwendung der Einwilligung anhand derjenigen Bestimmungen aufgezeigt werden, welche Anforderungen an die Wirksamkeit einer Einwilligung nach der DS-GVO stellen (vgl. Abschnitt 2.). Mitunter auch als Reaktion auf diese Problematik kann der Vorschlag von Malte Engeler verstanden werden, dass eine Legitimation der Datenverarbeitung in vielen Fällen besser über den Erlaubnistatbestand des Art. 6 Abs. 1 lit. b DS-GVO vorgenommen werden könne.[1] Danach ist die Verarbeitung rechtmäßig, wenn sie für die Erfüllung eines Vertrags, dessen Vertragspartei die betroffene Person ist, oder zur Durchführung vorvertraglicher Maßnahmen erforderlich ist, die auf Anfrage der betroffenen Person erfolgen. Engeler will das Merkmal der *Erforderlichkeit* dabei so auslegen, dass auf den konkreten Parteiwillen abzustellen ist. Im Ergebnis würde dies dazu führen, dass prinzipiell alles als erforderlich angesehen werden könnte, was der Verantwortliche als Leistungsbestimmung wirksam in seine Allgemeinen Geschäftsbedingungen (AGB) aufnimmt – ob die betroffene Person daran ein Interesse hat oder nicht. Es wird zu zeigen sein, dass eine solche Auslegung

1 Vgl. Engeler 2018: S. 58.

https://doi.org/10.14361/9783839446614-004 - am 13.02.2026, 16:22:37. https://www.inlibra.com/de/agb - Open Access -

wichtigen Wertungen des Datenschutzes, insbesondere dem Privatheitsschutz, zuwiderläuft und daher aus rechtspolitischer Sicht abzulehnen ist (vgl. Abschnitt 3.). Abschließend wird in Form eines Ausblicks der risikoorientierte Ansatz als alternative Möglichkeit zur Legitimation von Datenverarbeitung betrachtet (vgl. Abschnitt 4.).

2. Die Einwilligung als Legitimationsinstrument

2.1 Die Stellung der Einwilligung im Datenschutzrecht

Die Einwilligung als Instrument der Legitimation einer Verarbeitung von personenbezogenen Daten ist bereits im europäischen Primärrecht verankert. Eine Rechtfertigung der Datenverarbeitung wird in der deutschen Rechtstradition deswegen als notwendig angesehen, weil die Verarbeitung von personenbezogenen Daten einen Eingriff der verarbeitenden Stelle in das allgemeine Persönlichkeitsrecht in Form der informationellen Selbstbestimmung gemäß Art. 2 Abs. 1 GG in Verbindung mit Art. 1 Abs. 1 GG darstellt. Im europäischen Verfassungsrecht wird auf das Recht auf Privatleben gemäß Art. 7 GRCh sowie auf das Recht zum Schutz personenbezogener Daten gemäß Art. 8 GRCh verwiesen.[2] Ausdrücklich wird die Einwilligung in Art. 8 Abs. 2 S. 1 GRCh als ein Instrument der Legitimation von Datenverarbeitung normiert, wonach personenbezogene Daten nur nach Treu und Glauben für festgelegte Zwecke und mit Einwilligung der betroffenen Person oder auf einer sonstigen gesetzlich geregelten legitimen Grundlage verarbeitet werden dürfen. Somit gilt der Grundsatz des Verbots mit Erlaubnisvorbehalt, der besagt, dass personenbezogene Daten grundsätzlich nicht durch andere verarbeitet werden dürfen, wenn nicht eine Einwilligung oder ein anderer gesetzlicher Erlaubnistatbestand vorliegt. Die Einwilligung wird dabei häufig als besonderer Ausdruck der informationellen Selbstbestimmung angesehen, da die betroffene Person selbst entscheiden kann, ob der/die potenzielle Vertragspartner/in ihre personenbezogenen Daten verarbeiten darf.[3]

2 Ob es ein Rangverhältnis zwischen Art. 7 und 8 GRCh gibt, ist umstritten. Der Europäische Gerichtshof zitiert in seinen Entscheidungen zum europäischen Datenschutzrecht regelmäßig Art. 7 und 8 GRCh zusammen und lässt diese Frage offen (vgl. EuGH Urt. v. 08.04.2014 – C-293/12: Rn. 30-37; vgl. Urt. v. 21.12.2016 – C-203/15: Rn. 92f.). Naheliegend erscheint es, auf Art. 7 GRCh hinsichtlich der normativen Grundlage des Datenschutzes abzustellen, da Art. 8 GRCh vornehmlich Angaben dazu macht, *wie* Datenschutz zu bewerkstelligen ist.

3 Vgl. etwa Albrecht 2016: S. 91.

https://doi.org/10.14361/9783839446614-004 - am 13.02.2026, 16:22:37. https://www.inlibra.com/de/agb - Open Access -

In der DS-GVO ist in Art. 6 Abs. 1 lit. a geregelt, dass die Einwilligung ein Instrument der Datenverarbeitung darstellt.[4] Die Anforderungen an eine wirksame Einwilligung regelt Art. 4 Nr. 11 DS-GVO:

> ›Einwilligung‹ der betroffenen Person [bezeichnet] jede freiwillig für den bestimmten Fall, in informierter Weise und unmissverständlich abgegebene Willensbekundung in Form einer Erklärung oder einer sonstigen eindeutigen bestätigenden Handlung, mit der die betroffene Person zu verstehen gibt, dass sie mit der Verarbeitung der sie betreffenden personenbezogenen Daten einverstanden ist […].

Grundsätzlich kann durch die Einwilligung jede Verarbeitung von Daten legitimiert werden, sofern die Einwilligung rechtswirksam erteilt wurde.[5] Drei wesentliche Wirksamkeitsvoraussetzungen sind die Bestimmtheit, die Informiertheit und die Freiwilligkeit der Einwilligung. Dies liegt auf der Hand, da eine uninformierte oder unfreiwillige Entscheidung über einen unklaren Einwilligungstatbestand kein Ausdruck von Selbstbestimmung sein kann. Im Folgenden soll überblicksweise dargestellt werden, welche gesetzlichen Anforderungen jeweils erfüllt werden müssen und welche Probleme sich regelmäßig ergeben.

2.2 Die Einwilligung in der Praxis

Mittlerweile dürfte es einen weitgehenden Konsens darüber geben, dass die Einwilligung die ihr angedachte Funktion in der gegenwärtigen Datenschutzpraxis nicht zufriedenstellend erfüllt. Grundlage der Einwilligung ist in der Regel die Datenschutzerklärung der verarbeitenden Stelle. Diese häufig sehr langen und nicht selten kompliziert verfassten Dokumente werden jedoch regelmäßig nicht gelesen und noch seltener verstanden. Umstritten ist weiterhin, ob diese Schwierigkeiten eher an der Art und Weise liegen, wie die Einwilligung zurzeit eingeholt wird, oder ob ein grundlegenderes Problem vorliegt. So wird die Einwilligung von einigen Autor/en/innen teilweise weiterhin im Grundsatz als zeitgemäß bewertet und die Datenverarbeitung auf Grundlage einer Einwilligung als besonders legitim angesehen. Es bestehe nämlich ein Bedarf, die Möglichkeit der Selbstbestimmung in einer pluralen, heterogenen Gesellschaft sicherzustellen, zu erhalten und zu fördern. Die angesprochenen Probleme seien lediglich Vollzugsdefizite.[6]

4 Weitere gesetzliche Erlaubnistatbestände finden sich in Art. 6 Abs. 1 lit. b–f DS-GVO.

5 Eine Ausnahme sieht Art. 9 Abs. 2 lit. a DS-GVO vor, nach dem die Verarbeitung besonderer Kategorien personenbezogener Daten auch bei Vorliegen einer grundsätzlich wirksamen Einwilligung unzulässig bleibt, wenn dies das Unionsrecht oder das Recht der Mitgliedstaaten vorsieht.

6 Vgl. Paal/Pauly/Frenzel 2018: *DS-GVO*, Art. 7, Rn. 1.

https://doi.org/10.14361/9783839446614-004 - am 13.02.2026, 16:22:37. https://www.inlibra.com/de/agb - Open Access -

Es stellt sich jedoch die Frage, ob es sich aufgrund der zunehmenden Komplexität von Datenverarbeitungsvorgängen wirklich nur um Vollzugsdefizite handelt oder ob nicht doch prinzipielle Einwände bestehen.

2.2.1 Bestimmtheit

Die Einwilligung muss zunächst für bestimmte Zwecke der Datenverarbeitung erteilt werden. Dies ist Ausdruck des Zweckbindungsgrundsatzes gemäß Art. 5 Abs. 1 lit. b DS-GVO, wonach personenbezogene Daten für festgelegte, eindeutige und legitime Zwecke erhoben werden müssen und nicht in einer mit diesen Zwecken nicht zu vereinbarenden Weise weiterverarbeitet werden dürfen. Eine Zweckänderung ist nur nach den Regeln des Art. 6 Abs. 4 DS-GVO zulässig.

Die Bestimmtheit bezieht sich folglich auf den Verwendungszweck und muss auch die Mitteilung umfassen, ob und an wen eine Übermittlung geplant ist.[7] Das Maß der Bestimmtheit ist dabei im Einzelnen graduell festzulegen. Je tiefer der Eingriff in das Persönlichkeitsrecht, desto genauer muss der Zweck der Nutzung oder Weitergabe beschrieben werden, in die eingewilligt werden soll.[8]

Vor diesem Hintergrund ergeben sich insbesondere Probleme bei Big Data-Anwendungen[9]. Diese sind gerade dadurch gekennzeichnet, dass aus ihnen Verwendungszwecke gewonnen werden können, die zum Zeitpunkt der Datenerhebung noch nicht absehbar waren. Darüber hinaus ist vor allem bei komplexen Diensten absehbar, dass eine hinreichend bestimmt verfasste Einwilligung einen nicht unwesentlichen Umfang haben wird. Dies hat zur Folge, dass das Lesen und Verstehen einer Datenschutzerklärung einen erheblichen Aufwand für die betroffene Person nach sich ziehen würde.

2.2.2 Informiertheit

Hinsichtlich des Merkmals der Informiertheit im Sinne der DS-GVO wird vertreten, dass zumindest sichergestellt sein müsse, dass die Betroffenen die Möglichkeit haben, den Inhalt der von ihnen erwarteten Erklärung in zumutbarer Weise zur Kenntnis zu nehmen, was vor allem bei vorformulierten Einwilligungen und bei vorgefertigten Datenschutzhinweisen gelte.[10] Zu prüfen ist dann, was unter *in zumutbarer Weise* zu verstehen ist.

---

7 Vgl. Wolff/Brink/Schild 25. Ed.: *DS-GVO*, Art. 4, Rn. 129.

8 Vgl. Paal/Pauly/Frenzel 2018: *DS-GVO*, Art. 4, Rn. 78.

9 Vgl. Gola/Schulz 2018: *DS-GVO*, Art. 6, Rn. 254-259; ausführlich: Mayer-Schönberger/Cukier 2013.

10 Vgl. Paal/Pauly/Frenzel 2018: *DS-GVO*, Art. 4, Rn. 79.

https://doi.org/10.14361/9783839446614-004 - am 13.02.2026, 16:22:37. https://www.inlibra.com/de/agb - Open Access -

Unabhängig von einer entsprechenden Auslegung ist fraglich, ob ein solches rein formales Verständnis[11] überzeugend ist. Sofern die Einwilligung ein Ausdruck von Selbstbestimmung sein soll, müsste in der Praxis zumindest überwiegend zutreffen, dass die Einwilligung auch *tatsächlich* informiert erteilt wird. Ansonsten stellt sie eine Fiktion[12] dar. Dass aber Letzteres eher die Regel als die Ausnahme darstellt, ist keine neue Erkenntnis;[13] sie hat in den letzten Jahren immer mehr Anerkennung erfahren. Sowohl in der deutschen[14] als auch in der internationalen Literatur[15] wird herausgestellt, dass die typische Einwilligungssituation gegenwärtig nicht geeignet ist, um eine informierte, gut begründete Entscheidung zu treffen. Eine Studie aus dem Jahr 2008 kommt zu dem Ergebnis, dass eine betroffene Person in den USA im Jahr durchschnittlich circa 201 Stunden damit verbringen müsste, Datenschutzerklärungen zu lesen.[16] Vor diesem Hintergrund überrascht es nicht, dass sich viele Nutzer/innen für den einfacheren Weg entscheiden und in die Datenschutzbestimmungen einwilligen, selbst wenn ihnen manche erahnten Konsequenzen möglicherweise unangenehm sind.[17]

Selbst Gerichte nehmen diese Realität mittlerweile zur Kenntnis. Hatte der Bundesgerichtshof zum ›alten‹ nationalen Datenschutzrecht noch auf einen fiktiven durchschnittlich informierten und verständigen Verbraucher abgestellt und auf dieser Grundlage eine Einwilligung mittels Opt-out-Verfahrens für zulässig

11 Etwa in diesem Sinne: Die Nutzer/innen könnten theoretisch sämtliche Datenschutzbestimmungen lesen, wenn sie nur wollten, beziehungsweise sonst auf entsprechende Dienste verzichten.

12 Vgl. Kühling/Buchner/Buchner/Kühling 2018: *DS-GVO*, Art. 4 Nr. 11, Rn. 5.

13 Zur alten deutschen Rechtslage vgl. bereits Simitis/Simitis 2014: *BDSG*, § 4a BDSG, Rn. 3-6.

14 Vgl. Buchner/Kühling 2017: S. 545; Engeler 2018: S. 60; Pollmann/Kipker 2016: S. 379; Veil 2018: S. 688.

15 Vgl. Cate 2016: S. 4-12; Barocas/Nissenbaum 2014: S. 45; Solove 2013: S. 1880.

16 Vgl. McDonald/Cranor 2008: S. 565. Dabei wurde davon ausgegangen, dass jede relevante Datenschutzerklärung nur ein einziges Mal zu lesen ist. Es wurde also nicht eingerechnet, dass man Datenschutzerklärungen öfter lesen müsste, um sie auf Aktualisierungen zu prüfen. Der tatsächliche Zeitaufwand wird somit vermutlich noch höher liegen. An der durchschnittlichen Länge von Datenschutzerklärungen dürfte sich im Verhältnis zum heutigen Zeitpunkt kein so wesentlicher Unterschied ergeben, sodass von keinem signifikant geringeren Aufwand auszugehen ist (zu den Facebook-Datenschutzbestimmungen vgl. etwa Buchner 2015). Weitere empirische Befunde finden sich in Thorun u.a. 2018: S. 15f. und Rothmann/Buchner 2018: S. 344-346.

17 In diesem Zusammenhang wird immer wieder der Begriff des *privacy paradox* verwendet. Dieses bestehe darin, dass vor allem Jugendliche auf der einen Seite offenbar ihre Privatsphäre schätzen und diese auch schützen wollen würden, sie auf der anderen Seite aber bereitwillig persönliche Informationen auf Diensten wie Facebook teilen bzw. die mittlerweile bekannte Erhebung und Verarbeitung der entsprechenden Daten durch diese Dienste hinnehmen (vgl. Barnes 2006; Nissenbaum 2010: S. 104-108; Einspänner-Pflock 2017: S. 152-157).

https://doi.org/10.14361/9783839446614-004 - am 13.02.2026, 16:22:37. https://www.inlibra.com/de/agb - Open Access -

erklärt,[18] kommt das Landgericht Berlin – ebenfalls auf Grundlage des ›alten‹ nationalen Datenschutzrechts – zu einem anderen Ergebnis. In Bezug auf die Kenntnisnahme der Datenschutzbestimmungen von Facebook durch die betroffenen Personen stellt es darauf ab, dass »dies nach allgemeiner Lebenserfahrung im Zweifel nicht geschehen ist«[19]. Wenn somit davon ausgegangen werden kann, dass Einwilligungen in erheblicher Anzahl erteilt werden, obwohl die entsprechenden Datenschutzerklärungen nicht wirklich gelesen wurden, stellt sich die Frage, ob die Zumutbarkeit ein sinnvolles Kriterium darstellt.

Aus diesem Grund werden Ansätze diskutiert, die gewisse Anpassungen hinsichtlich der Darstellung der Einwilligung vornehmen wollen, damit tatsächlich eine informierte Einwilligung erteilt werden könne.[20] Eine Studie testete einen sogenannten One-Pager, also eine Datenschutzerklärung, in welcher wesentliche Informationen einer ursprünglich oftmals mehrere Seiten umfassenden Datenschutzerklärung auf einer Seite in einer standardisierten Form zusammengefasst werden. Es sollte überprüft werden, ob Nutzer/innen auf diese Weise einen Überblick über die wesentlichen Datenverarbeitungsprozesse eines Anbieters erhalten und sie gegebenenfalls mit anderen Anbietern vergleichen können.[21] Im Ergebnis konnte nicht gezeigt werden, dass diese Form der Datenschutzerklärung zu einem höheren Informationsniveau der Nutzer/innen führte. Es erhöhte sich lediglich die Wahrscheinlichkeit, dass eine solche Erklärung überhaupt gelesen wurde.[22] Einen anderen Ansatz stellt die Verwendung von Symbolen oder Piktogrammen dar.[23] Auch bei diesem Ansatz stellt sich jedoch die Frage, ob die hierdurch erreichte Vereinfachung noch ausreichende Informationen beinhaltet, um die tatsächliche Art und den Umfang der in Frage stehenden Datenverarbeitung ausreichend beurteilen zu können.

Derartige Vereinfachungen geraten in einen Konflikt mit der vorstehend genannten Voraussetzung der Bestimmtheit. Hier kann von einem Transparenz-Di-

18 Vgl. BGH Urt. v. 16.07.2008 – VIII ZR 348/06 – Payback; Urt. v. 11.11.2009 – VIII ZR 12/08 – Happy Digits.

19 LG Berlin Urt. v. 16.01.2018 – 16 O 341/15: Rn. 60; näher zum Urteil Rothmann/Buchner 2018: S. 342-344.

20 So etwa der One-Pager-Entwurf des Bundesministeriums der Justiz und für Verbraucherschutz (vgl. BMJV 2015); für die USA vgl. etwa Lipman 2016: S. 802-806.

21 Thorun u.a. 2018: S. 1; kritisch insbesondere für mobile Endgeräte ebenfalls Pollmann/Kipker 2016: S. 379.

22 Thorun u.a. 2018: S. 57f.; siehe aber auch die Studie von Rao u.a., die vorschlagen, eine Vereinfachung dadurch zu erreichen, dass in einer Zusammenfassung einer Datenschutzerklärung besondere Konstellationen hervorgehoben werden, welche typischerweise nicht den Vorstellungen von Nutzer/n/innen entsprechen (vgl. Rao u.a. 2016: S. 86-88).

23 Pollmann/Kipker halten diesen Ansatz für vielversprechend (vgl. Pollmann/Kipker 2016: S. 380).

https://doi.org/10.14361/9783839446614-004 - am 13.02.2026, 16:22:37. https://www.inlibra.com/de/agb - Open Access -

lemma[24] gesprochen werden. Je umfangreicher die Informationen bezüglich einer beabsichtigten Datenverarbeitung sind, desto höher wird die Wahrscheinlichkeit, dass sie überhaupt nicht gelesen werden. Umgekehrt führt eine Vereinfachung der Informationen dazu, dass nur noch pauschale Angaben gemacht werden können, welche einen hohen Spielraum im Detail zulassen.[25]

2.2.3 Freiwilligkeit

Neben dem bereits angesprochenen Aspekt der Informiertheit der Nutzer/innen stellt das Merkmal der Freiwilligkeit eine wesentliche Voraussetzung einer wirksamen Einwilligung dar. In diesem Kontext wurden und werden in der Literatur insbesondere sogenannte Kopplungsverbote thematisiert. Eine Kopplung liegt im Datenschutzrecht vor, wenn ein Vertragsabschluss oder die Erbringung einer Leistung davon abhängig gemacht wird, dass die Betroffenen in eine weitergehende Erhebung oder Verarbeitung ihrer personenbezogenen Daten einwilligen, welche nicht zur Abwicklung des Geschäfts erforderlich sind.[26] Mit Blick auf die DS-GVO findet diese Diskussion insbesondere im Rahmen der Auslegung von Art. 7 Abs. 4 DS-GVO statt. Diese Norm trifft Bestimmungen zum Auslegungsmaßstab für die Prüfung der Freiwilligkeit einer Einwilligung:

> Bei der Beurteilung, ob die Einwilligung freiwillig erteilt wurde, muss dem Umstand in größtmöglichem Umfang Rechnung getragen werden, ob unter anderem die Erfüllung eines Vertrags, einschließlich der Erbringung einer Dienstleistung, von der Einwilligung zu einer Verarbeitung von personenbezogenen Daten abhängig ist, die für die Erfüllung des Vertrags nicht erforderlich sind.

Überwiegend wird in der Literatur mit Blick auf den Wortlaut darauf hingewiesen, dass es sich nicht um ein echtes Kopplungsverbot, sondern regelungstechnisch um eine Auslegungsregel zur Freiwilligkeit handele.[27] Sodann werden unterschiedliche Vorschläge gemacht, welche Umstände vorliegen müssen, um das Merkmal der Freiwilligkeit entfallen zu lassen, wobei überwiegend auf eine

24 Helen Nissenbaum bezeichnet diesen Umstand als »Transparency-Paradox« (Nissenbaum 2011a: S. 36). Allerdings scheint der Begriff *Dilemma* noch treffender zu sein, da hier beide Alternativen – mehr oder weniger Informationen – zu einem unerwünschten Ergebnis führen, was aber nicht zwangsläufig *widersprüchlich* ist.

25 Vgl. Solove 2013: S. 1882-1893.

26 Vgl. Dammann 2016: S. 311; Ehmann/Selmayr/Heckmann/Paschke: *DS-GVO*, Art. 7, Rn. 94.

27 Im Ergebnis aber von einem strengen Kopplungsverbot ausgehend Schantz 2016: S. 1845; abwartend Weidert/Klar 2017: S. 1860 und Dammann 2016: S. 311.

https://doi.org/10.14361/9783839446614-004 - am 13.02.2026, 16:22:37. https://www.inlibra.com/de/agb - Open Access -

umfassende Gesamtbewertung der Situation abgestellt wird.[28] Zu beachten sei, ob der Anbieter eine Monopolstellung innehabe[29], ob der Anbieter keine vergleichbare Bezahlvariante anbiete[30], wie sehr der/die Nutzer/in auf den Dienst angewiesen sei oder ob die Datenverarbeitung sich als völlig losgelöst vom Vertragsverhältnis erweise[31].

Freiwilligkeit wird dabei vornehmlich so verstanden, dass entscheidend ist, ob der/die Nutzer/in in der konkreten Situation der Entscheidung, ob er/sie in die Datennutzung einwilligt, eine echte Handlungsoption hat. Auch insoweit stellt sich jedoch die Frage, ob dieses eher formale Verständnis angemessen ist oder ob darüber hinaus auch die Bedingungen, unter denen die Wahl stattfindet, stärker berücksichtigt werden müssen. Zwar ist es sicher zutreffend, dass eine monopolartige Stellung oder die Abwesenheit einer Bezahlvariante in besonders hohem Maße die Freiwilligkeit beeinträchtigen. Im Umkehrschluss kann aber nicht angenommen werden, dass bei Abwesenheit dieser Faktoren kein erheblicher Einfluss auf den Entscheidungsprozess genommen wird. Empirische Studien legen nahe, dass gerade durch die Bereitstellung eines bestimmten Rahmens oder einer Entscheidungsarchitektur[32] ein erhebliches Beeinflussungspotenzial bestehen kann. Entscheidungssituationen sind häufig so gestaltet, dass die Entscheidung zugunsten der Einwilligung gelenkt werden soll[33], etwa in dem Fall, dass die weitere Nutzung des Dienstes von der Einwilligung abhängig gemacht wird oder die Auswahl einer datenschutzfreundlichen Einstellung deutlich komplizierter als eine entgegenstehende Einstellung konzipiert ist. Abhilfe könnte dadurch geleistet werden, dass die Einwilligungsentscheidung zum einen in einer möglichst neutralen[34] Entscheidungsstruktur und ohne unmittelbare Konsequenzen – ins-

28 Besonders differenzierend Kühling/Buchner/Buchner/Kühling 2018: *DS-GVO*. Art. 7, Rn. 41-54.

29 Vgl. Ehmann/Selmayr/Heckmann/Paschke 2018: *DS-GVO*, Art. 7, Rn. 98; Gola/Schulz 2018: *DS-GVO*. Art. 7, Rn. 27.

30 Vgl. Gierschmann 2016: S. 54; Sydow/Ingold 2018: *DS-GVO*, Art. 7, Rn. 33; Golland 2018: S. 134. Empirische Untersuchungen legen jedoch nahe, dass vermutlich überwiegend die ›günstigeren‹ oder die im Datenverbrauch intensiveren Produkte oder Dienste gewählt würden (vgl. etwa die Studie von Beresford u.a. 2012: S. 26f.). Ob das Problem der Freiwilligkeit auf diese Weise wirklich entschärft wird, bleibt fraglich, da weiterhin ein Anreiz zur Nutzung datenintensiver Dienste geschaffen wird, ohne dass die Datenverarbeitung selbst darauf hin überprüft wird, ob sie problematisch ist (hierzu vgl. unten Abschnitt 3.3).

31 Vgl. Gola/Schulz 2018: *DS-GVO*. Art. 7, Rn. 28; Schätzle 2017: S. 203.

32 Vgl. näher Sandfuchs 2015: S. 109-115.

33 Vgl. Acquisti u.a. 2015: S. 511f.; Hoofnagle u.a. 2012: S. 294f.

34 In Hinblick auf Art. 25 Abs. 2 DS-GVO sei bereits an dieser Stelle angemerkt, dass es auch insoweit auf die Auslegung des Merkmals der *Erforderlichkeit* (siehe dazu unten die Abschnitte 3.1 und 3.3.2) ankommt, ob und inwieweit datenschutzfreundliche Vorsteinstellungen vorgenommen werden müssen.

https://doi.org/10.14361/9783839446614-004 - am 13.02.2026, 16:22:37. https://www.inlibra.com/de/agb - Open Access -

besondere die Verweigerung des Dienstes – vorgenommen werden kann. Dies würde aber gleichzeitig bedeuten, dass das Geschäftsmodell *Dienst gegen Daten*[35] weitgehend seine Grundlage verlieren würde, da es in den meisten Fällen nur geringen Anreiz gäbe, die Einwilligung zu erteilen. Dies gilt vor allem für Programme wie Payback oder Angebote für Glückspiele, bei denen die Preisgabe der Daten für eine Gegenleistung im Vordergrund steht. Die häufig geäußerte Forderung nach einer entsprechenden Möglichkeit der Kapitalisierung von persönlichen Daten[36] macht eine solche Entwicklung jedoch aktuell unwahrscheinlich.

2.3 Zwischenfazit

Von einer Eignung der Einwilligung als wirksames Instrument der Legitimation von Datenverarbeitung kann zumindest unter den gegenwärtigen Bedingungen nicht gesprochen werden. Darüber hinaus bestehen insbesondere aufgrund des Transparenz-Dilemmas auch grundsätzliche Zweifel daran, dass sie als umfassend eingesetztes Instrument zur Legitimation komplexer Datenverarbeitung die beste Wahl darstellt.

3. Verlagerung datenschutzrechtlicher Wertungen in das Vertragsrecht?

Ein Ausweg aus diesem Dilemma könnte der Ansatz von Malte Engeler sein. Dessen Ausführungen haben zwar primär eine Auslegung des Art. 7 Abs. 4 DS-GVO zum Gegenstand. Im Rahmen derer kommt er jedoch zu dem Schluss, dass unter den Maßgaben der DS-GVO die Legitimation von Datenverarbeitung weitgehend über den gesetzlichen Erlaubnistatbestand des Art. 6 Abs. 1 lit. b DS-GVO stattfinden könne. Die Auslegung des Maßstabes der *Erforderlichkeit* führe zu dem Ergebnis, dass dieser durch das konkrete Vertragsverhältnis zu bestimmen sei.[37] Praktisch bedeutet dies, dass insbesondere die (wirksamen) AGB der Anbieter den Umfang der Erforderlichkeit bestimmen würden.

35 Ausführlich hierzu Metzger 2016.

36 Golland etwa spricht von einem »Monetarisierungsdilemma« (Golland 2018: S. 135); Krohm/Müller-Peltzer sprechen von »eine[r] veritable[n] Alternative zur kostenpflichtigen Nutzung von Online-Services« (Krohm/Müller-Peltzer 2017: S. 551).

37 Vgl. Engeler 2018: S. 57f.; in diese Richtung denken ebenfalls Krohm/Müller-Peltzer 2017: S. 554.

https://doi.org/10.14361/9783839446614-004 - am 13.02.2026, 16:22:37. https://www.inlibra.com/de/agb - Open Access -

3.1 Lösung über die Bestimmung des Maßstabs der Erforderlichkeit?

Entscheidend für diesen Ansatz ist, wie der Maßstab der *Erforderlichkeit* bestimmt werden sollte.[38] Engeler eröffnet diesbezüglich zwei Alternativen: einen abstrakt-wertenden oder einen konkret-objektiven Maßstab. Nach dem erstgenannten Ansatz würden unabhängig von der zwischen den Parteien vorgenommenen Absprache – also die im Vertrag vereinbarten Leistungsbestandteile – abstrakte Beurteilungskriterien aufgestellt, anhand derer die jeweils konkrete Datenverarbeitung zu bewerten wäre.[39] Danach würde etwa bei der Nutzung eines Social Media-Dienstes abstrakt bestimmt werden, welche Funktionen für die Nutzung eines solchen Dienstes notwendig sind, um diesen sinnvoll nutzen zu können. Konkret-objektiv wäre der Maßstab dagegen dann, wenn eben jene vertragliche Absprache selbst Ausgangspunkt für die Beurteilung sei.[40] Somit käme es darauf an, ob die regelmäßig in den AGB niedergelegten Leistungsbestimmungen wirksam vereinbart wurden. Sofern dies der Fall ist, wären diese Leistungen auch erforderlich im Sinne des Art. 6 Abs. 1 lit. b DS-GVO. Danach könnte der Anbieter etwa die Erbringung von personenbezogener Werbung in sein Leistungsangebot aufnehmen. Sämtliche Datenverarbeitungsvorgänge, die für diese Zwecke stattfinden, wären somit ohne Einwilligung bereits legitim, sofern eine solche Klausel der Inhaltskontrolle standhält.

Engeler argumentiert für den konkret-objektiven Maßstab.[41] Der abstrakt-wertende Maßstab werde dem Bestimmtheitsgebot nicht gerecht, da es an einem Kriterium fehle, wie man die abstrakt vorzunehmende Wertung prüfen könne. Der konkret-objektive Maßstab leide unter diesem Problem hingegen nicht. Denn das Kriterium der Erforderlichkeit werde hier durch die wirksam vereinbarten Vertragsinhalte definiert, welche mit Blick auf die Bestimmtheit wesentlich konkreter seien. Im Ergebnis würde »sich die Prüfung von Datenverarbeitungen im Kontext von Schuldverhältnissen teilweise auf die Ebene der zivilrechtlichen Wirksamkeitskontrolle«[42] verschieben. Zwar weist er darauf hin, dass sich durch diese Lösung eine gewisse Missbrauchsanfälligkeit ergebe, da der Verwender durch eine geschickte Vertragsgestaltung datenschutzrechtliche Zielsetzungen umgehen könne. Derartige Bedenken könnten aber kein anderes Ergebnis recht-

38 Dieser Maßstab ist darüber hinaus auch für die Frage relevant, wie das ›Kopplungsverbot‹ aus Art. 7 Abs. 4 DS-GVO auszulegen ist, da auch insoweit auf den Maßstab der Erforderlichkeit Bezug genommen wird.

39 Vgl. Engeler 2018: S. 57; in diese Richtung etwa Golland 2018: S. 132; vgl. auch Ehmann/Selmayr/Klabunde 2018: *DS-GVO*, Art. 4, Rn. 51.

40 Vgl. Engeler 2018: S. 57f.

41 Vgl. Engeler 2018: S. 57f.

42 Engeler 2018: S. 57.

https://doi.org/10.14361/9783839446614-004 - am 13.02.2026, 16:22:37. https://www.inlibra.com/de/agb - Open Access -

fertigen. Stattdessen gelte, dass, solange vertragliche Bedingungen weder sittenwidrig sind, noch gegen Treu und Glauben verstoßen und auch einer AGB-Kontrolle standhalten, die datenschutzrechtliche Prüfung die wirksam vereinbarten konkreten Vertragsbestimmungen akzeptieren und konsequenterweise zu dem Ergebnis kommen müsse, dass die zur Erfüllung dieser Vereinbarungen erforderlichen Datenverarbeitungen durch Art. 6 Abs. 1 lit. b DS-GVO gerechtfertigt würden.[43] Auch im Datenschutzrecht sei anzuerkennen, dass die Vertragsfreiheit nach deutschem Recht keinen Anspruch auf angemessene Gegenleistung kenne, es vielmehr nur einen Schutz vor unverhältnismäßigen Austauschverhältnissen gebe. Innerhalb dieser äußeren Schranken richte sich das Verhältnis von Leistung und Gegenleistung grundsätzlich nach den Gesetzen von Angebot und Nachfrage.[44]

Grundsätzlich positiv an dem Ansatz ist zunächst der Versuch, die Legitimation von Datenverarbeitung nicht mehr schwerpunktmäßig über Einwilligungen zu lösen. Wie im Folgenden gezeigt werden soll, ist der Vorschlag mit Blick auf die zu schützenden Rechtsgüter dennoch nicht zufriedenstellend.[45] Dies liegt vor allem daran, dass dem Vertragsrecht – und in seiner speziellen Ausformung dem AGB-Recht – andere Wertungen zugrunde liegen. Die unterschiedlichen Schwerpunkte sollen daher in Form eines Überblicks dargestellt werden.

3.2 Vertragsrecht als Schutz der Vertragsabschlussfreiheit

AGB sind ein fester Bestandteil des wirtschaftlichen Handelns geworden. Durch die Verwendung von vorformulierten Vertragsbedingungen soll eine Rationalisierung des Vertragsabschlusses erreicht werden. Verwendet ein Unternehmen immer identische AGB, vereinfacht dies die Organisation des Unternehmens, erleichtert dessen Kalkulation und erspart diesem und den Kund/en/innen die Kosten und Mühen, die anderenfalls dadurch entstünden, dass der Inhalt der einzelnen Verträge ausgehandelt werden müsste. Zudem kann das Unternehmen auf diese Weise auch auf den Fall Einfluss nehmen, dass es bei der Vertragsabwicklung zu Streitigkeiten kommt.[46]

Die Verwendung von AGB ist aus Sicht des Unternehmens Ausdruck der Privatautonomie, welche nach deutschem Recht gemäß Art. 2 Abs. 1 GG und nach europäischem Recht durch die unternehmerische Freiheit gemäß Art. 16 GRCh geschützt wird. Allerdings kann die Privatautonomie eingeschränkt werden. Es

43 Vgl. Engeler 2018: S. 57.

44 Vgl. Engeler 2018: S. 58.

45 Insofern ist anzumerken, dass Engeler eine Interpretation der Normen der DS-GVO vornimmt und selbst keinen eigenen rechtspolitischen Entwurf vorstellt.

46 Vgl. Säcker/Rixecker/Oetker/Limperg/Basedow 2016: *BGB*, Vorbemerkung zu § 305, Rn. 2.

https://doi.org/10.14361/9783839446614-004 - am 13.02.2026, 16:22:37. https://www.inlibra.com/de/agb - Open Access -

gilt nämlich zu bedenken, dass die Privatautonomie beider potenzieller Vertragsparteien zu wahren ist. Wie das Bundesverfassungsgericht (BVerfG) ausführt, kann in dem Fall, dass die Schwäche einer Vertragspartei durch gesetzliche Regelungen bedingt ist, der verfassungsrechtliche Schutz der Privatautonomie zu einer Pflicht des Gesetzgebers führen, für eine rechtliche Ausgestaltung des Rechtsverhältnisses der davon betroffenen Vertragsparteien zu sorgen, die ihren Belangen hinreichend Rechnung trägt.[47] Im Rahmen von Vertragsabschlüssen unter Einbeziehung von AGB wird insoweit angenommen, dass die Klauselgegner/innen, also die Kund/en/innen, in einer strukturell unterlegenen Position sind. Der Grund für diese Unterlegenheit wird in dem Umstand gesehen, dass der Verwender die Bedingungen im Vorhinein ohne Zeitdruck und regelmäßig unter Inanspruchnahme rechtskundiger Beratung im eigenen Sinne ausformulieren kann, während der/die Klauselgegner/in typischerweise unter dem Druck einer konkreten Abschlusssituation überfordert ist, deren Angemessenheit zu beurteilen.[48] Ganz ähnlich wie bei der Erörterung der tatsächlichen Gegebenheiten im Rahmen der Erteilung der datenschutzrechtlichen Einwilligung ist davon auszugehen, dass AGB in der Regel nicht – oder zumindest nicht in vollem Umfang – gelesen werden. Dass solche Verträge dennoch ›ins Blaue‹ abgeschlossen werden, kann auf zwei Umstände zurückgeführt werden: Der erste Grund besteht darin, dass es sich für Kund/en/innen nicht lohnt, Zeit und Geld in diejenigen Bemühungen zu investieren, die aufzuwenden wären, um entweder im Verhandlungswege eine Änderung der AGB zu erreichen oder andere Anbieter ausfindig zu machen, deren AGB-Texte in diesem oder jenem Punkt eine für ihn/sie günstigere Regelung enthalten. Aufwand und Nutzen stehen hier in keinem angemessenen Verhältnis. Anders ausgedrückt:

> Es trifft also zwar zu, dass dort, wo AGB Vertragsinhalt werden, die Vertragsfreiheit nicht funktioniert und es daher zu einem ›Marktversagen‹ kommt, das gesetzlich korrigiert werden muss. Dieses ›Marktversagen‹ hat aber – ökonomisch gesprochen – seinen Grund nicht in der wirtschaftlichen oder sonstigen Übermacht der Verwender, sondern in den prohibitiv hohen ›Transaktionskosten‹, die dem Kunden durch die Führung von Vertragsverhandlungen entstehen.[49]

Die hohen Transaktionskosten entstehen also zum einen durch das beschriebene Informationsdefizit, zum anderen aber auch durch die Tatsache, dass es überhaupt eine Überwindung darstellt, in Vertragsverhandlungen einzutreten, über

47 Vgl. BVerfG, Beschl. v. 15.02.2006 – 1 BvR 1317/96: Rn. 57.

48 Vgl. Leuschner 2007: S. 495.

49 Säcker/Rixecker/Oetker/Limperg/Basedow 2016: *BGB*, Vorbemerkung zu § 305, Rn. 5.

https://doi.org/10.14361/9783839446614-004 - am 13.02.2026, 16:22:37. https://www.inlibra.com/de/agb - Open Access -

deren (juristischen) Inhalt man häufig keine Expertise verfügt.[50] Ferner ist zu bedenken, dass die AGB nicht von einem neutralen Akteur verfasst werden. Das Unternehmen hat nicht nur ein Interesse daran, seine Transaktionskosten zu senken. Es ist darüber hinaus davon auszugehen, dass es die AGB auch inhaltlich zu seinem Vorteil ausgestalten und auf diese Weise die eigene Rechtsposition stärken wird.[51]

Um diese asymmetrische, faktische Machtstellung auszugleichen, sieht das BGB die AGB-Kontrolle in den §§ 305ff. vor. Sofern einzelne Klauseln den Wirksamkeitsvoraussetzungen nicht entsprechen, werden sie nicht Bestandteil der vertraglichen Absprache. Die Verwendung dieses Rechtsinstruments, welches in Deutschland zumindest in vielen Bereichen als üblich wahrgenommen wird, kann als zweiter Grund gelten, dass AGB in der Praxis nicht auf erheblichen Widerstand stoßen. Dagegen würde die wiederholte Erfahrung, dass in AGB ganz überraschende Klauseln enthalten sein können, die darüber hinaus auch keiner inhaltlichen Kontrolle unterlägen, das Rechtsinstitut vermutlich nachhaltig in Frage stellen.[52]

Auf Rechtsfolgenseite ist zu betonen, dass etwaige negative Folgen von überraschenden AGB den Kund/en/innen spätestens bekannt werden, wenn das Unternehmen sich auf die entsprechende Klausel beruft und deren Rechtsfolge einfordert. In vielen Fällen wird es sich dabei um eine Position handeln, welche letztlich durch einen Geldwert ausgedrückt werden kann. Dies bedingt, dass eine Rückabwicklung in diesen Fällen häufig unproblematisch möglich ist. Selbstverständlich ist die Geltendmachung von Rechten sowohl mit allgemeinen Unannehmlichkeiten als auch häufig mit einem finanziellen Risiko verbunden; davon abgesehen können etwaige Schäden aber grundsätzlich im Vertragsverhältnis endgültig rückabgewickelt werden. Dies spricht dafür, dass die Inhaltskontrolle einen angemessenen Ausgleich zwischen den unternehmerischen Interessen an einer zweckmäßigen Vertragsgestaltung einerseits und den Schutzbedürfnissen der Vertragspartner/innen andererseits sicherstellt.

3.3 Privatheitsschutz als eine normative Grundlage des Datenschutzrechts

Betrachtet man nun die Ausgangslage in der praktischen Situation der datenschutzrechtlichen Einwilligung sowie bei der Einbeziehung von AGB, scheint es weitgehende Überschneidungen zu geben. Strukturell betrachtet gestaltet in beiden Fällen das Unternehmen die Bedingungen, ohne dass der/die Nutzer/in

50 Vgl. Leuschner 2007: S. 496-498.

51 Vgl. Leuschner 2007: S. 504.

52 Vgl. Leuschner 2007. S. 508f.

https://doi.org/10.14361/9783839446614-004 - am 13.02.2026, 16:22:37. https://www.inlibra.com/de/agb - Open Access -

Einfluss auf die konkreten Fassungen nehmen könnte. Für das Unternehmen hat die Einholung einer Einwilligung grundsätzlich Vor- und Nachteile. Der Vorteil besteht darin, dass die Einwilligung ein flexibles Instrument darstellt, das insbesondere im Hinblick auf den rasanten technischen Fortschritt und damit einhergehende innovative Dienstleistungsmodelle, die auf der Verarbeitung personenbezogener Daten basieren, eine effektive Möglichkeit für eine datenschutzrechtskonforme Datenverarbeitung bieten kann.[53] Der Nachteil besteht darin, dass wegen der gesteigerten Wirksamkeitsvoraussetzungen an die Einwilligung in der DS-GVO eine gewisse Unsicherheit dahingehend besteht, ob eine Einwilligung tatsächlich wirksam erteilt wurde.

Der/Die Nutzer/in hingegen steht – wie beim Akzeptieren von AGB – vor der Situation, dass die Transaktionskosten in einem Missverhältnis zu dem von ihm/ihr gewünschten Ziel stehen. Insoweit wurde bereits ausgeführt, dass das Lesen von Datenschutzbestimmungen verschiedener Angebote für den/die Nutzer/in keine praktisch sinnvolle Alternative zum einfachen ›Abnicken‹ der konkret erbetenen Einwilligung darstellt. Die Erteilung der Einwilligung führt unmittelbar zum zunächst gewollten Ergebnis, dass man den fraglichen Dienst nutzen kann.[54] Hier enden jedoch die Parallelen zum AGB-Recht. Dies hat zwei Gründe, die aufeinander aufbauen: Vertragsrecht und Datenschutz verfolgen unterschiedliche Schutzziele. Daher stellt der Ausgleichsmechanismus der AGB-rechtlichen Inhaltskontrolle kein adäquates Schutzinstrument für den Datenschutz dar.[55]

Konzeptionell scheinen zunächst sowohl das AGB-Recht als auch das Datenschutzrecht einen ähnlichen Ausgangspunkt zu haben. In beiden Fällen soll eine Form der Selbstbestimmung geschützt werden. Die konkrete Art der Selbstbestimmung ist jedoch nicht identisch.[56] Der Schutzzweck des allgemeinen Vertragsrechts liegt darin, allen Parteien einen möglichst fairen Geschäftsverkehr zu ermöglichen, also insbesondere die allgemeine *Handlungs*freiheit zu schützen. Konkreter verfolgt die Inhaltskontrolle im AGB-Recht den Zweck, ein systematisches Ungleichgewicht, das in den *Umständen* des konkreten Vertragsabschlusses begründet ist, auszugleichen. Die sich aus diesem Ungleichgewicht ergebenden Gefahren sind für die Klauselgegner/innen auf dieses Vertragsverhältnis beschränkt. Die Schutzrichtung des Datenschutzes geht jedoch über die Freiheit zum Abschluss beziehungsweise Ablehnen eines Vertrages hinaus. Dies hängt auch damit zusammen, dass die Folgen der Datenverarbeitung im Rahmen eines Vertragsverhältnisses nicht notwendig auf dieses konkrete Rechtsverhältnis begrenzt sind. Für moderne digitale Dienste ist es vielmehr charakteristisch, dass

53 Vgl. Pollmann/Kipker 2016: S. 379.

54 Lewinski spricht in diesem Zusammenhang von »rationaler Apathie« (Lewinski 2013: S. 13).

55 Zur Abgrenzung nach geltendem Recht vgl. Lewinski/Herrmann 2017: S. 172.

56 So auch Lewinski/Herrmann 2017: S. 169.

https://doi.org/10.14361/9783839446614-004 - am 13.02.2026, 16:22:37. https://www.inlibra.com/de/agb - Open Access -

sie nur deswegen ihre Funktion erfüllen können, weil sie auf Daten aus ganz verschiedenen Quellen zugreifen können. Es stellt sich somit die Frage, was das Datenschutzrecht im Kern leisten muss.[57]

Aus Sicht des deutschen Verfassungsrechts wird nach wie vor auf die damals wegweisende Rechtsprechung des BVerfG im Zuge des Volkszählungsurteils[58] Bezug genommen. In dem Urteil liegt bekanntlich der Fokus darauf, dass der/die Einzelne selbst entscheiden oder zumindest ungefähr absehen können müsse, wann innerhalb welcher Grenzen persönliche Lebenssachverhalte offenbart werden. Jede Person müsse daher mit hinreichender Sicherheit überschauen können, welche Informationen mögliche Kommunikationspartner/innen über sie haben. Ansonsten sei sie in ihrer Freiheit gehemmt, selbstbestimmt zu planen oder zu entscheiden. Der durch das BVerfG angesprochene Gedanke der informationellen Selbstbestimmung ist von der Forschungsliteratur zum Privatheitsbegriff aufgenommen und erweitert worden, indem der Einfluss von Wissensasymmetrien in der Kommunikation auf die Bedingungen der Möglichkeit von autonomem Handeln stärker hervorgehoben wurde.[59]

Beate Rössler stellt in diesem Zusammenhang auf den Begriff der *informationellen Privatheit* ab.[60] Privatheit wird von Rössler in einem ersten Schritt folgendermaßen definiert: »[A]ls privat gilt etwas dann, wenn man selbst den Zugang zu diesem ›etwas‹ kontrollieren kann.«[61] Damit folgt sie im Ausgangspunkt theoretischen Ansätzen – etwa von Alan F. Westin[62] –, welche den Kontrollaspekt in den Vordergrund rücken. Der Kontrollaspekt wird verdeutlicht durch den funktionalen Zusammenhang zwischen Privatheit und Freiheit, genauer Autonomie. Diesen Zusammenhang formuliert sie wie folgt:

> [W]ir halten Privatheit deshalb für wertvoll […], weil wir Autonomie für wertvoll halten und weil nur mit Hilfe der Bedingungen von Privatheit und mittels Rechten und Ansprüchen auf Privatheit Autonomie in all ihren Aspekten lebbar, in allen Hinsichten artikulierbar ist. Begreift man als das *telos* von Freiheit, ein autonomes Leben führen zu können, dann kann man, in der Ausbuchstabierung der Bedin-

57 Die Frage, was die normative Begründung für den Datenschutz darstellt, ist häufig gestellt worden, wird jedoch bis heute uneinheitlich beantwortet (vgl. etwa Steigmüller u.a. 1971; Albers 2017). Auch die folgenden Ausführungen erheben nicht den Anspruch, eine umfassende, systematische Begründung des Datenschutzrechts in normativer Hinsicht leisten zu können.

58 Vgl. BVerfG, Urt. v. 15.12.1983 – 1 BvR 209/83.

59 Im Folgenden soll dargestellt werden, wie der Gedanke der *informationellen Privatheit* als *eine* normative Begründung für Datenschutz herangezogen werden kann. Damit ist noch nicht gesagt, dass es keine weiteren Gesichtspunkte gibt, welche relevant sein können.

60 Vgl. Rössler 2001: S. 208-214.

61 Rössler 2001: S. 23.

62 Vgl. zu dessen Definition von Privatheit Westin 1967: S. 7.

https://doi.org/10.14361/9783839446614-004 - am 13.02.2026, 16:22:37. https://www.inlibra.com/de/agb - Open Access -

> gungen eines solchen autonomen Lebens, sehen, dass für den Schutz von Autonomie Freiheitsrechte nicht ausreichend sind, sondern dass Autonomie angewiesen ist auf die Substantialisierung dieser Freiheitsrechte in Rechte und Ansprüche auf den Schutz des Privaten.[63]

So verstanden ist Privatheit eine notwendige, aber keine hinreichende Vorbedingung dafür, dass wir nicht nur frei, sondern auch autonom sein können. Sie steht in einem funktionalen Verhältnis zur Autonomie.[64] Dabei muss Autonomie nicht als anthropologische Eigenschaft des Menschen verstanden werden. Notwendig, aber auch ausreichend, ist, Autonomie als normatives Ideal anzusehen, welches nie vollständig erreicht werden kann.[65] Akzeptiert man dieses Ideal als normative Grundlage für ein Recht auf Privatheit, besteht die Aufgabe einer positiven Rechtsordnung darin, möglichst solche Bedingungen zu befördern, von denen angenommen werden kann, dass sie einer Annäherung an dieses Ideal dienen.

Dies ist aber mehr als die bloße Handlungsfreiheit. Denn es geht nicht nur um die Frage, ob formal betrachtet Handlungsalternativen vorhanden sind, sondern vor allem darum, unter welchen Bedingungen von diesen Handlungsalternativen Gebrauch gemacht werden kann. Für die hier einschlägige Dimension der *informationellen Privatheit* kann dies am Beispiel des Falles einer gestörten Kommunikation verdeutlicht werden. Unter Kommunikation ist im vorliegenden Kontext insbesondere eine solche gemeint, in der eine Person mit einer unbestimmten Anzahl anderer, nicht bekannter Personen kommuniziert. Dies ist typischerweise bei der Nutzung des Internets der Fall, denn sobald eine Website aufgerufen wird, wird häufig nicht nur mit dem Betreiber der Seite kommuniziert, sondern auch mit anderen Entitäten, wobei den Nutzer/n/innen dies nicht notwendig bewusst sein muss. Ein Fall der gestörten Kommunikation liegt dann vor, wenn eine Person in einen Kommunikationsprozess eintritt, bei dem ihr nicht bewusst ist, dass ihren Kommunikationspartner/n/innen Informationen zur Verfügung stehen, die ihre Persönlichkeit betreffen. Dies betrifft beispielsweise den Fall, dass sie erwartet, dass die Kommunikation zwischen ihr und eine/r/m ihr bis dahin gänzlich unbekannten Kommunikationspartner/in auf keinen anderen Informationen beruht als solchen, die über sie öffentlich bekannt sind, diese Erwartung jedoch nicht zutrifft. Des Weiteren ist die Kommunikation gestört, wenn im Verlauf der Kommunikation Informationen über sie gesammelt und aggregiert werden und auf dieser Grundlage die Kommunikation mit ihr angepasst wird und sie davon keine Kenntnis hat. Eine so entstehende Wissensasymmetrie kann problematisch sein, wenn die sich daraus ergebende Überlegenheit dazu führt, dass die Kom-

63 Rössler 2001: S. 26.

64 Vgl. Rössler 2001: S. 132-136.

65 Vgl. Cohen 2013: S. 1910f.

https://doi.org/10.14361/9783839446614-004 - am 13.02.2026, 16:22:37. https://www.inlibra.com/de/agb - Open Access -

munikationsstruktur, welche im Machtbereich des/der überlegenen Kommunikationspartner/s/in liegt, derart moduliert wird, dass Einfluss auf bestimmte Verhaltensweisen der unterlegenen Person genommen werden soll.[66]

Wenn Datenschutz jedenfalls auch Schutz informationeller Privatheit leisten soll, bedeutet dies, dass nicht nur die Entscheidung geschützt werden muss, welche Daten die Betroffenen preisgeben. Darüber hinaus muss auch berücksichtigt werden, welche Form der Datenverarbeitung problematisch ist, unabhängig davon, wie die verarbeitende Stelle in den Besitz der Daten gekommen ist. Der Aspekt der Kontrolle muss daher normativ erweitert werden.[67] Privatheitsverletzungen können zum einen darin bestehen, dass Individuen die Kontrolle in Bereichen entzogen wird, die wir in der jeweiligen gesellschaftlichen Situation als privat betrachten. Hier dient der Schutz der Privatheit der individuellen Ausübung von Autonomie. Darüber hinaus kann es aber ebenfalls gesellschaftliche Strukturen geben, die der individuellen Gestaltung entzogen sind. Diese können aber nicht minder Einfluss darauf haben, wer Informationen über Individuen erhält und wie Kommunikation strukturiert wird. Die Gestaltung entsprechender Strukturen stellt somit die Vorbedingung dafür dar, überhaupt effektiv Kontrolle auszuüben. Privatheitsschutz ist auch in dieser Hinsicht relevant. Diesbezüglich steht dann aber nicht primär die Stärkung des Selbstschutzes des Individuums im Fokus, vielmehr müssen die gesellschaftlichen Strukturen als solche in den Blick genommen werden. Die Vermeidung problematischer Datenverarbeitung stellt dann einen positiven Schutzauftrag an den Staat oder die jeweils zuständige politische Gemeinschaft dar, welche die in Frage stehenden gesellschaftlichen Strukturen gestalten kann.[68]

Einen solchen Ansatz entwirft Helen Nissenbaum.[69] Stark vereinfacht ausgedrückt ist nach diesem von einer Privatheitsverletzung auszugehen, wenn die *kontextuelle Integrität* von persönlichen Informationen nicht gewahrt wird. Dies soll dann der Fall sein, wenn die begründeten Erwartungen der Betroffenen an die Verwendung von Informationen dadurch enttäuscht werden, dass diese in einem anderen Kontext verwendet werden. Dieser Ansatz bietet den Vorteil, dass durch den Fokus auf die Trennung der Verarbeitung von Informationen in bestimmten Kontexten besonders problematische Fälle von Wissensasymmetrien

66 Näher dazu Cohen 2013: S. 1912-1918. Ein solcher Fall ist etwa gegeben, wenn ein soziales Netzwerk bestimmte Inhalte auf der Grundlage des Vorverhaltens des/der Nutzer/in auswählt oder anordnet und wenn damit auf die politische Willensbildung Einfluss genommen werden soll, ohne dass dies kenntlich gemacht wird.

67 In diese Richtung denkt auch Albers 2013: S. 40.

68 Eine dogmatische Verankerung eines solchen positiven Schutzauftrags ließe sich im geltenden europäischen Verfassungsrecht vermutlich am besten über den Begriff des Privatlebens in Art. 7 GRCh erzielen.

69 Ausführlich zum Folgenden vgl. Nissenbaum 2010: S. 129-230.

https://doi.org/10.14361/9783839446614-004 - am 13.02.2026, 16:22:37. https://www.inlibra.com/de/agb - Open Access -

vermieden werden sollen.[70] Nach diesem Ansatz kann es zunächst nicht nur unproblematisch, sondern für den Behandlungserfolg notwendig sein, wenn sensible Gesundheitsdaten von einem/r Arzt/Ärztin zu einem/r andere/n übertragen werden. Auch die zuständige Krankenkasse ist unter Umständen auf diese Informationen angewiesen. Etwas anderes könnte sich aber dann ergeben, wenn auch Arbeitgeber/innen ohne Einschränkung Kenntnis solcher Informationen erhalten könnten. Die Weitergabe solcher Daten würde eine Verletzung der kontextuellen Integrität bedeuten.

3.4 Datenschutzrecht und Vertragsrecht

Was bedeutet dies nun für die Legitimation von Datenverarbeitung? Die oben aufgezeigten Schwierigkeiten im Hinblick auf die Einwilligung scheinen mit einem Verständnis von Privatheit in Konflikt zu geraten, welches auf die Kontrolle des/der Einzelnen abstellt. Dies ist jedoch nur dann der Fall, wenn ein solches Verständnis nicht wie oben vorgeschlagen um eine objektive Dimension des Privatheitsschutzes erweitert wird. Verstünde man Privatheitsschutz so, dass der/die Einzelne bei jedem Kommunikationsakt im Detail überblicken und darüber entscheiden können muss, welche seiner/ihrer personenbezogenen Daten auf welche Weise verarbeitet werden, wäre dies ein Anspruch, der aus den genannten Gründen wegen der hohen Transaktionskosten nicht erfüllt werden kann bzw. wird. Wie dargelegt stellt es aber eine unzulässige Verkürzung dar, den Anspruch auf Privatheitsschutz allein auf den Akt zu beziehen, in dem über eine Datenpreisgabe entschieden wird. Hier liegt ein wichtiger Unterschied zum Vertragsrecht. Die dort geschaffene Rechtsbeziehung ist wesentlich konkreter und in ihren Konsequenzen eher zu überschauen. Genau dies ist jedoch bei der Datenverarbeitung in der modernen Kommunikationsgesellschaft nicht notwendigerweise der Fall. Könnte zum Beispiel in AGB wirksam die Weitergabe von Daten an Dritte vereinbart werden, könnten diese Daten als Grundlage für ganz unterschiedliche Prozesse dienen, sei dies das Scoring eines Kreditinstituts oder als Bewertungsgrundlage für die Vorauswahl eines Arbeitgebers.

Vor diesem Hintergrund stellt die von Engeler vorgeschlagene Interpretation des Erfordernisses der Erforderlichkeit (jedenfalls rechtspolitisch) ein äußerst unbefriedigendes Ergebnis[71] dar. Sofern die Bestimmung der Erforderlichkeit durch die Vertragsparteien im Rahmen von AGB vorgenommen wird, können

70 Bei der konkreten Umsetzung ergeben sich jedoch Fragen, etwa danach, wie problematische Kontexte zu bestimmen sind (vgl. Nissenbaum 2010: S. 129-150) oder im Hinblick auf die von ihr favorisierte konservative Ausrichtung des Modells (vgl. Nissenbaum 2010: S. 159-165).

71 Im Ergebnis lehnen auch Wendehorst/Graf von Westphalen (2016: S. 3746f.) eine Verlagerung ins Vertragsrecht ab und schlagen hinsichtlich des Erfordernisses der Erforderlichkeit eine

https://doi.org/10.14361/9783839446614-004 - am 13.02.2026, 16:22:37. https://www.inlibra.com/de/agb - Open Access -

zunächst alle Einwände vorgebracht werden, die für AGB im Allgemeinen gelten. Insbesondere ist zu berücksichtigen, dass Datenschutzerklärungen von der verantwortlichen Stelle formuliert werden und diese eigene Interessen verfolgt.[72] Anders als im allgemeinen Vertragsrecht kann durch die Inhaltskontrolle aber kein angemessener Ausgleich hergestellt werden, da das Datenschutzrecht und die §§ 305ff. BGB keine identische Schutzrichtung verfolgen.[73] Der Schutz der Autonomie, den Datenschutz als Privatheitsschutz jedenfalls auch bezweckt, geht über den Schutz der autonomen Entscheidung in der Einwilligungssituation – als Pendant zum Vertragsschluss im AGB-Recht – hinaus. So sollte in die Bewertung, ob eine Datenverarbeitung legitim ist, ebenfalls *mit*einfließen, ob in ihrer Konsequenz Fälle von gestörter Kommunikation begünstigt werden, vor allem wenn diese als strukturell problematisch anzusehen sind, etwa weil eine Verletzung der kontextuellen Integrität zu befürchten ist.

Probleme werden auch bei Betrachtung der Rechtsfolgenseite deutlich. Nutzer/innen haben wenig Grund, sich nach dem Vertragsschluss noch einmal mit den Bestimmungen im Vertrag auseinanderzusetzen, welche die Datenverarbeitung betreffen. Sie werden aber vermutlich auch nicht mit für sie erkennbaren Folgen offen konfrontiert werden. Das Instrument der Klauselkontrolle wird jedenfalls von Nutzer/innen nicht angestrengt werden, weil sie keinen Grund haben, etwaige Klauseln infrage zu stellen. Dies verlegt die volle Kontrolle auf die Aufsichtsbehörden und zumindest bei Betroffenheit von Verbraucher/n/innen auch auf Verbraucherschutzverbände. Aktuell sind jedoch beide Institutionen personell und finanziell nicht ausreichend ausgestattet, um diese Aufgabe effektiv auszufüllen.[74]

Aber selbst wenn einmal der Fall eintreten würde, dass eine Klausel für unwirksam erklärt wird, hätte bis zu diesem Zeitpunkt eine unzulässige Datenverarbeitung stattgefunden. Der hierdurch erzielte Effekt kann vor dem Hintergrund der fast gleichzeitig eintretenden Wirkung von Datenverarbeitungsvorgängen nicht rückgängig gemacht werden. Ein effektiver Schadensausgleich, der im allgemeinen Zivilrecht als angemessenes Instrument des Schadensersatzes angesehen wird, kann im Datenschutzrecht nicht in vergleichbarer Weise erreicht werden.

(durch den Europäischen Gerichtshof vorzunehmende) teleologische Reduktion vor. Allerdings wird eine Lösung dann wieder in der Einwilligung gesucht.

72 Vgl. Lewinski 2013: S. 13f.

73 Darüber hinaus hätte dieser Vorschlag eine erneute Zersplitterung dieser zentralen Wertung in nationales Recht zur Folge (vgl. Golland 2018: S. 132). Die Richtlinie 93/13/EWG (Klausel-RL) nimmt nach Art. 8 und Erwägungsgrund 12 nur eine Mindestharmonisierung vor (vgl. dazu Lewinski/Herrmann 2017: S. 172).

74 Vgl. Schütz/Karaboga 2015: S. 20; kritisch auch Wolff 2017: S. 110f.; zur Problematik der Unabhängigkeit der Datenschutzbeauftragen vgl. Lewinski 2013: S. 16f.

https://doi.org/10.14361/9783839446614-004 - am 13.02.2026, 16:22:37. https://www.inlibra.com/de/agb - Open Access -

3.5 Zwischenfazit

Festzuhalten bleibt, dass die von Engeler vorgeschlagene Verlagerung von datenschutzrechtlichen Wertungen in das Vertragsrecht aus rechtspolitischen Gesichtspunkten[75] abzulehnen ist. Beide Rechtsinstitute müssen zum einen unterschiedliche Rechtspositionen berücksichtigen. Zum anderen zeigen sich auch auf Rechtsfolgenseite deutliche Unterschiede, die jeweils einer eigenen Regulierung bedürfen. Der Maßstab der *Erforderlichkeit* sollte daher eng gefasst werden und darauf reduziert werden, dass nur diejenigen Datenverarbeitungsvorgänge als erforderlich gelten sollten, an denen im synallagmatischen Verhältnis beide Parteien ein Interesse haben.[76] Sofern der Verantwortliche darüber hinaus an einer Datenverarbeitung interessiert ist, sollte diese über andere Instrumente legitimiert werden, welche die vorgenannten Rechtspositionen angemessen berücksichtigen können.

4. Ausblick

Wie könnten nun solche Instrumente aussehen? Oder muss der Anspruch auf *informationelle Privatheit* zugunsten der gesellschaftlich-technologischen Entwicklung aufgegeben oder zumindest stark eingeschränkt werden? Da dem Schutz von *informationeller Privatheit* nach dem hier vertretenen Verständnis grundrechtliche Relevanz zukommt, kann dies schon prinzipiell nicht der Fall sein, da ein normativer Anspruch nicht ohne weiteres durch Veränderungen im Tatsächlichen unbegründet wird.[77] Etwaige Schutzinstrumente haben jedoch der gesellschaftlich-technologischen Entwicklung Rechnung zu tragen. Damit Datenschutz als Privatheitsschutz effektiv sein kann, sollte er einerseits als Vorfeldschutz[78] konzipiert werden, andererseits nicht primär als Aufgabe des/der Einzelnen verstanden werden. Das Instrument der Einwilligung sollte dabei auf Fälle beschränkt werden, in denen die entsprechenden Daten von gesteigerter Relevanz sind und der Verarbeitungskontext für die betroffene Person überschaubar ist.[79]

75 Das hier vertretene Verständnis von Privatheit als eine normative Stütze des Datenschutzrechts findet sich auf diese Weise nicht explizit in der Rechtsprechung des Europäischen Gerichtshofs wieder, weshalb die aus dieser Auffassung folgenden Gesichtspunkte als *rechtspolitisch* bezeichnet werden.

76 Vgl. Golland 2018: S. 132.

77 Instruktiv zum Verhältnis von Technik und Regulierung vgl. Nissenbaum 2011b.

78 Vgl. Lewinski 2014: S. 81-85.

79 Eine Subsidiarität der Einwilligung schlägt auch Radlanski vor (vgl. Radlanski 2016: S. 204-210).

https://doi.org/10.14361/9783839446614-004 - am 13.02.2026, 16:22:37. https://www.inlibra.com/de/agb - Open Access -

Eine Alternative zum Prinzip der Einwilligung stellt der risikoorientierte Ansatz[80] dar. Diesem Ansatz liegt die Annahme zugrunde, dass personenbezogene Daten nicht um ihrer selbst willen schützenswert seien, vielmehr sei entscheidend, ob durch ihre Verarbeitung in die Rechte des/der Einzelnen eingegriffen werden kann. Datenschutzrechtliche Pflichten sollten umso strenger sein, desto wahrscheinlicher ein Eingriff in die Rechte des/der Einzelnen und desto schwerer der drohende Schaden sei.[81] Hier liegt der Fokus nicht so sehr darauf, welche Daten erhoben werden. Stattdessen solle geprüft werden, welche Datenverarbeitung im jeweiligen Verwendungskontext problematisch sei.[82] So kann etwa die Manipulationsgefahr einer auf Profilbildung basierten, personalisierten Werbung in verschiedenen Kontexten unterschiedlich zu bewerten sein, etwa in Bezug auf die anvisierte Zielgruppe[83] oder die jeweilige mediale Umgebung der Werbung[84].

Die DS-GVO geht diesen Weg überwiegend nicht.[85] Es bleibt beim Verbot mit Erlaubnisvorbehalt und somit dem sogenannten ›*one-size-fits-all*‹-Ansatz. Erste Merkmale des risikoorientierten Ansatzes finden sich allerdings in den Vorschriften zum *privacy by design*, insbesondere zur Datenschutz-Folgenabschätzung (DSFA) gemäß Art. 35, 36 DS-GVO.[86] Die DSFA soll dafür sorgen, dass bereits bei der Entwicklung vor allem von neuen Technologien, bei denen voraussichtlich ein hohes Risiko für die Rechte und Freiheiten natürlicher Personen besteht, die Gesichtspunkte des Datenschutzes berücksichtigt werden. Hier sind Ansätze der Risikoabwägung bereits enthalten. Sofern es zutreffend ist, dass Gegenstand der DSFA die Rechtmäßigkeit des gesamten geplanten Verarbeitungsverfahrens ist, dass also letztlich zu überprüfen ist, ob die risikoreichen Verarbeitungen mit

80 Veil 2015: S. 348-351; in diese Richtung ist vermutlich auch Nissenbaums Ansatz der *contextual integrity* einzuordnen (vgl. Nissenbaum 2010).

81 Vgl. Veil 2015: S. 353.

82 Vgl. ausführlich zu verschiedenen Ansätzen zur Kategorisierung von Datenverarbeitung Radlanski 2016: S. 194-201.

83 Für Kinder gelten nach Art. 8 DS-GVO bereits strengere Vorschriften. Allerdings sind auch andere Zielgruppen denkbar, die jedenfalls in bestimmten Kontexten für Manipulation in besonderer Weise anfällig sein könnten (vgl. etwa das Beispiel von gezielter Werbung von US-amerikanischen *for-profit*-Universitäten an schwangere bzw. alleinerziehende Frauen bei O`Neil 2016: S. 68-83).

84 Hier können als Beispiele neue Werbeformen wie das *Influencer-Marketing* oder das *Native Advertising* genannt werden. Dabei ergibt sich in wettbewerbsrechtlicher Hinsicht insbesondere die Frage der richtigen Kennzeichnung (vgl. dazu Gerecke 2018). Darüber hinaus kann aber auch die Frage gestellt werden, ob in bestimmten Fällen (zum Beispiel gegenüber Kindern und Jugendlichen) eine Profilbildung zu solchen Werbezwecken gänzlich unzulässig sein sollte.

85 Forderungen für einen risikobasierten Ansatz gab es im Vorfeld der Verhandlungen um die DS-GVO durchaus (vgl. etwa Thoma 2013: S. 580f.; Veil 2015: S. 348-353).

86 Vgl. Phan 2016: S. 243; Schmitz/Dall'Armi 2017: S. 57; zum Ablauf einer DSFA vgl. Friedewald u.a. 2017: S. 18-37.

https://doi.org/10.14361/9783839446614-004 - am 13.02.2026, 16:22:37. https://www.inlibra.com/de/agb - Open Access -

den Anforderungen der DS-GVO in Einklang zu bringen sind, ist im Rahmen der DSFA insbesondere[87] sicherzustellen, ob eine Verarbeitungsgrundlage nach Art. 6 Abs. 1 DS-GVO besteht.[88] Durch die DSFA würde somit die eigentliche Frage, welche Grundform der Legitimation von Daten vorzugswürdig ist, nicht berührt, da das Risiko durch die vorgelagerte Auslegung der genannten Vorschriften der DS-GVO determiniert wird.

Es soll nicht unterschlagen werden, dass auch der risikobasierte Ansatz in der Umsetzung Probleme aufwirft, die bisher noch nicht ausreichend geklärt wurden. Zunächst stellt sich die Frage, wie auch in diesem Modell bewirkt werden kann, dass die Betroffenen einen zumindest ausreichenden Überblick darüber erhalten, wie ihre persönlichen Daten verarbeitet werden. Ferner sollte der Fokus auf die zu überprüfenden Risiken bei der jeweiligen Datenverarbeitung nicht dazu führen, jedwede Datenerhebung per se als zulässig zu betrachten. Auch insoweit sollten Risiken und Chancen in Abwägung gebracht werden. Darüber hinaus ist in praktischer Hinsicht unklar, ob einem risikobasierten System die Gefahr inhärent ist, dass Privatheitsinteressen über kurz oder lang in den Hintergrund treten. Wenn konkrete Risiken in einem stetigen Prozess ausgehandelt werden müssen, stehen die eher abstrakten Forderungen nach Privatheitsschutz (und möglichen anderen Begründungen für Datenschutz) den üblichen Forderungen entgegen, dass derartige Reglementierungen nicht Innovationen blockieren dürften. Diese Bedenken sind ernst zu nehmen, sollten aber nicht davon abhalten, allen Möglichkeiten nachzugehen, um auch unter veränderten technologisch-sozialen Bedingungen effektiven Privatheitsschutz gewährleisten zu können.

Literatur

Acquisti, Alessandro u.a. 2015: *Privacy and human behavior in the age of information*. In: *Science*. 347., 2015, S. 509-514.

Albers, Marion 2017: *Informationelle Selbstbestimmung als vielschichtiges Bündel von Rechtsbindungen und Rechtspositionen*. In: Friedewald, Michael u.a. (Hg.): *Informationelle Selbstbestimmung im digitalen Wandel*. Wiesbaden, S. 11-35.

Albers, Marion 2013: *Privatheitsschutz als Grundrechtsproblem*. In: Halft, Stefan/Krah, Hans (Hg.): *Privatheit. Strategien und Transformationen*. Passau, S. 15-44.

Albrecht, Jan Philipp 2016: *Das neue EU-Datenschutzrecht – von der Richtlinie zur Verordnung*. In: *Computer und Recht (CR)*. 2016, S. 88-89.

87 Darüber hinaus sind allerdings auch die weiteren Vorgaben etwa der Art. 24, 25 und 32 DS-GVO zu beachten.

88 So Paal/Pauly/Martini 2018: *DS-GVO*, Art. 35, Rn. 22.

https://doi.org/10.14361/9783839446614-004 - am 13.02.2026, 16:22:37. https://www.inlibra.com/de/agb - Open Access -

Barnes, Susan B. 2006: *A privacy paradox: Social networking in the United States*. In: *first Monday – peer reviewed journal on the internet*. 11.9., 2006. URL: https://firstmonday.org/article/view/1394/1312_2 (zuletzt abgerufen am: 16.03.2019).

Barocas, Solon/Nissenbaum, Helen 2014: *Big data's end run around anonymity and consent*. In: Lane, Julia u.a. (Hg.): *Privacy, Big Data, and the Public Good: Frameworks for Engagement*. New York, S. 44-75.

Beresford, Alastair R. u.a. 2012: *Unwillingness to pay for privacy: A field experiment*. In: *Economics Letters*. 117., 2012, S. 25-27. URL: http://preibusch.de/publications/Beresford-Kuebler-Preibusch__Unwillingness-to-pay-for-privacy.pdf (zuletzt abgerufen am: 16.03.2019).

Buchner, Benedikt 2015: *Message to Facebook*. In: *Datenschutz und Datensicherheit (DuD)*. 2015, S. 402-405.

Buchner, Benedikt/Kühling, Jürgen 2017: *Die Einwilligung in der Datenschutzordnung 2018*. In: *Datenschutz und Datensicherheit (DuD)*. 2017, S. 544-548.

BMJV 2015: *Datenschutz auf einen Blick: »One-Pager« als Muster für transparente Datenschutzhinweise vorgestellt*. URL: https://www.bmjv.de/SharedDocs/Pressemitteilungen/DE/2015/11192915_Vorstellung_OnePager.html;jsessionid=F17D37421EBF3F686F076C5CEDCCCB83.2_cid297 (zuletzt abgerufen am: 16.03.2019).

Cate, Fred H. 2016: *Big Data, Consent, and the Future of Data Protection*. In: Sugimoto, Cassidy R. u.a. (Hg.): *Big Data Is Not a Monolith*. Cambridge, S. 3-19.

Cohen, Julie E. 2013: *What privacy is for.* In: *Harvard Law Review*. 126., 2013, S. 1904-1933.

Dammann, Ulrich 2016: *Erfolge und Defizite der EU-Datenschutzgrundverordnung – Erwarteter Fortschritt, Schwächen und überraschende Innovationen*. In: *Zeitschrift für Datenschutz (ZD)*. 2016, S. 307-314.

Ehmann, Eugen/Selmayr, Martin 2018: *Datenschutz-Grundverordnung. Kurz-Kommentar.* München 2. Aufl.

Einspänner-Pflock, Jessica 2017: *Privatheit im Netz – Konstruktions- und Gestaltungsstrategien von Online-Privatheit bei Jugendlichen*. Wiesbaden.

Engeler, Malte 2018: *Das überschätzte Kopplungsverbot – Die Bedeutung des Art. 7 Abs. 4 DS-GVO in Vertragsverhältnissen*. In: *Zeitschrift für Datenschutz (ZD)*. 2018, S. 55-61.

Friedewald, Michael u.a. 2017: *White Paper Datenschutz-Folgenabschätzung – Ein Werkzeug für einen besseren Datenschutz*. 3. Aufl. URL: www.forum-privatheit.de/forum-privatheit-de/publikationen-und-downloads/veroeffentlichungen-des-forums/themenpapiere-white-paper/Forum-Privatheit-WP-DSFA-3-Auflage-2017-11-29.pdf (zuletzt abgerufen am: 16.03.2019).

Gerecke, Martin 2018: *Kennzeichnung von werblichen Beiträgen im Online-Marketing*. In: *Gewerblicher Rechtsschutz und Urheberrecht (GRUR)*. 2018, S. 153-159.

https://doi.org/10.14361/9783839446614-004 - am 13.02.2026, 16:22:37. https://www.inlibra.com/de/agb - Open Access -

Gierschmann, Sibylle 2016: *Was ›bringt‹ deutschen Unternehmen die DS-GVO? – Mehr Pflichten, aber die Rechtsunsicherheit bleibt*. In: *Zeitschrift für Datenschutz (ZD)*. 2016, S. 51-55.

Gola, Peter 2018: *DS-GVO. Datenschutz-Grundverordnung. VO (EU) 2016/679. Kommentar*. München 2. Aufl.

Golland, Alexander 2018: *Das Kopplungsverbot in der Datenschutz-Grundverordnung – Anwendungsbereich, ökonomische Auswirkungen auf Web 2.0-Dienste und Lösungsvorschlag*. In: *Multimedia und Recht (MMR)*. 2018, S. 130-135.

Hoofnagle, Chris Jay u.a. 2012: *Behavioral Advertising: The Offer You Cannot Refuse*. In: *Harvard Law & Policy Review*. 6., 2012, S. 273-296.

Krohm, Niclas/Müller-Peltzer, Philipp 2017: *Auswirkungen des Kopplungsverbots auf die Praxistauglichkeit der Einwilligung – Das Aus für das Modell »Service gegen Daten«*. In: *Zeitschrift für Datenschutz (ZD)*. 2017, S. 551-556.

Kühling, Jürgen/Buchner, Benedikt 2018: *DS-GVO, BDSG. Datenschutz-Grundverordnung. Bundesdatenschutzgesetz. Kommentar*. München 2. Aufl.

Leuschner, Lars 2007: *Gebotenheit und Grenzen der AGB-Kontrolle – Weshalb M&A-Verträge nicht der Inhaltskontrolle der §§ 305ff. AGB unterliegen*. In: *Archiv für die civilistische Praxis (AcP)*. 2007, S. 491-529.

Lewinski, Kai von 2014: *Die Matrix des Datenschutzrechts*. Tübingen.

Lewinski, Kai von 2013: *Zwischen rationaler Apathie und rationaler Hysterie – Die Durchsetzung des Datenschutzes*. In: *Privacy in Germany (PinG)*. 2013, S. 12-17.

Lewinski, Kai von/Herrmann, Christoph 2017: *Vorrang des europäischen Datenschutzrechts gegenüber Verbraucherschutz- und AGB-Recht – Teil 1: Materielles Recht*. In: *Privacy in Germany (PinG)*. 2017, S. 165-172.

Lipman, Rebecca 2016: *Online Privacy and the Invisible Market for Our Data*. In: *Penn St. Law Review*. 2016, S. 777-806.

Mayer-Schönberger, Viktor/Cukier, Kenneth 2013: *Big Data – A Revolution That Will Transform How We Live, Work, and Think*. London.

McDonald, Aleecia M./Cranor, Lorrie Faith 2008: *The Cost of Reading Privacy Policies*. In: *A Journal of Law and Policy for the Information Society*. 2008, S. 543-568.

Metzger, Axel 2016: *Dienst gegen Daten – Ein synallagmatischer Vertrag*. In: *Archiv für die civilistische Praxis (AcP)*. 2016, S. 817-865.

Nissenbaum, Helen 2011a: *A Contextual Approach to Privacy Online*. In: *Dædalus*. 140.4., 2011, S. 32-48.

Nissenbaum, Helen 2011b: *From Preemption to Circumvention: If Technology Regulates, Why Do We Need Regulation (and Vice Versa)?* In: *Berkeley Technology Law Journal*. 26., 2011, S. 1367-1386.

Nissenbaum, Helen 2010: *Privacy in Context – Technology, Policy, and the Integrity of Social Life*. Stanford.

O`Neil, Cathy 2016: *Weapons of Math Destruction – How Big Data Increases Inequality and Threatens our Democracy*. New York.

https://doi.org/10.14361/9783839446614-004 - am 13.02.2026, 16:22:37. https://www.inlibra.com/de/agb - Open Access -

Paal, Boris P./Pauly, Daniel A. 2018: *Datenschutz-Grundverordnung. Bundesdatenschutzgesetz. Kompakt-Kommentar.* München 2. Aufl.

Phan, Iris 2016: *Die Datenschutz-Folgenabschätzung nach der Datenschutz-Grundverordnung*. In: *Privacy in Germany (PinG)*. 2016, S. 243-247.

Pollmann, Maren/Kipker, Dennis-Kenji 2016: *Informierte Einwilligung in der Online-Welt*. In: *Datenschutz und Datensicherheit (DuD)*. 2016, S. 378-381.

Radlanski, Philip 2016: *Das Konzept der Einwilligung in der datenschutzrechtlichen Realität*. Tübingen.

Rao, Ashwini u.a. 2016: *Expecting the Unexpected: Understanding – Mismatched Privacy Expectations Online*. URL: https://www.usenix.org/system/files/conference/soups2016/soups2016-paper-rao.pdf (zuletzt abgerufen am: 16.03.2019).

Rössler, Beate 2001: *Der Wert des Privaten*. Frankfurt a.M.

Rothmann, Robert/Buchner, Benedikt 2018: *Der typische Facebook-Nutzer zwischen Recht und Realität – Zugleich eine Anmerkung zu LG Berlin v. 16.01.2018*. In: *Datenschutz und Datensicherheit (DuD)*. 2018, S. 342-346.

Sandfuchs, Barbara 2015: *Privatheit wider Willen?* Tübingen.

Säcker, Franz Jürgen u.a. 2016: *Münchner Kommentar zum BGB – Band 2 Schuldrecht – Allgemeiner Teil*. München. 7. Aufl.

Schantz, Peter 2016: *Die Datenschutz-Grundverordnung – Beginn einer neuen Zeitrechnung im Datenschutzrecht*. In: *Neue Juristische Wochenschrift (NJW)*. 2016, S. 1841-1847.

Schätzle, Daniel 2017: *Zum Kopplungsverbot der Datenschutz-Grundverordnung – Warum auch die DSGVO kein absolutes Kopplungsverbot kennt*. In: *Privacy in Germany (PinG)*. 2017, S. 203-208.

Schmitz, Barbara/Dall'Armi, Jonas von 2017: *Datenschutz-Folgenabschätzung – verstehen und anwenden*. In: *Zeitschrift für Datenschutz (ZD)*. 2017, S. 57-64.

Schütz, Philip/Karaboga, Murat 2015: *Arbeitspapier Akteure, Interessenlagen und Regulierungspraxis im Datenschutz – Eine politikwissenschaftliche Perspektive*. URL: https://www.forum-privatheit.de/forum-privatheit-de/publikationen-und-downloads/veroeffentlichungen-des-forums/Schuetz-und-Karaboga-Akteure-Interessenlagen-und-Regulierungspraxis-im-Datenschutz-2015.pdf (zuletzt abgerufen am: 16.03.2019).

Simitis, Spiros 2014: *Bundesdatenschutzgesetz. Kommentar.* Baden-Baden 8. Aufl.

Solove, Daniel J. 2013: *Privacy Self-Management and the Consent Dilemma*. In: *Harvard Law Review*. 2013, S. 1880-1903.

Steigmüller, Wilhelm u.a. 1971: *Grundfragen des Datenschutzes – Gutachten im Auftrag des Bundesministeriums des Innern*. BT-Drs. VI/3826, Anlage 1, S. 5-161.

Sydow, Gernot 2018: *Europäische Datenschutzgrundverordnung. Handkommentar.* Baden-Baden 2. Aufl.

https://doi.org/10.14361/9783839446614-004 - am 13.02.2026, 16:22:37. https://www.inlibra.com/de/agb - Open Access -

Thoma, Florian 2013: *Risiko im Datenschutz – Stellenwert eines systematischen Risikomanagements in BDSG und DS-GVO-E*. In: *Zeitschrift für Datenschutz (ZD)*. 2013, S. 578-581.

Thorun, Christian u.a. 2018: *Wege zur besseren Informiertheit – Verhaltenswissenschaftliche Ergebnisse zur Wirksamkeit des One-Pager-Ansatzes und weiterer Lösungsansätze im Datenschutz*. URL: https://www.conpolicy.de/data/user_upload/Studien/Bericht_ConPolicy_2018_02_Wege_zur_besseren_Informiertheit.pdf (zuletzt abgerufen am: 16.03.2019).

Veil, Winfried 2018: *Die Datenschutz-Grundverordnung: des Kaisers neue Kleider – Der gefährliche Irrweg des alten wie des neuen Datenschutzrechts*. In: *Neue Zeitschrift für Verwaltungsrecht (NVwZ)*. 2018, S. 686-696.

Veil, Winfried 2015: *DS-GVO: Risikobasierter Ansatz statt rigides Verbotsprinzip – Eine erste Bestandsaufnahme*. In: *Zeitschrift für Datenschutz (ZD)*. 2015, S. 347-353.

Weidert, Stefan/Klar, Manuel 2017: *Datenschutz und Werbung – gegenwärtige Rechtslage und Änderungen durch die Datenschutz-Grundverordnung*. In: *Betriebsberater (BB)*. 2017, S. 1858-1864.

Wendehorst, Christiane/Graf von Westphalen, Friedrich 2016: *Das Verhältnis zwischen Datenschutz-Grundverordnung und AGB-Recht*. In: *Neue Juristische Wochenschrift (NJW)*. 2016, S. 3745-3750.

Westin, Alan F. 1967: *Privacy and Freedom*. New York.

Wolff, Heinrich Amadeus 2017: *Die überforderte Aufsichtsbehörde*. In: *Privacy in Germany (PinG)*. 2017, S. 109-111.

Wolff, Heinrich Amadeus/Brink, Stefan 25. Edition: *Online-Kommentar. Datenschutzrecht*. München.

https://doi.org/10.14361/9783839446614-004 - am 13.02.2026, 16:22:37. https://www.inlibra.com/de/agb - Open Access -