Sachverständigenrat für Verbraucherfragen

Verbraucherdatenschutzrecht in der EU-Datenschutz-Grundverordnung

Philipp Schmechel

SVRV Working Paper Nr. 4

Veröffentlichungen des Sachverständigenrats für Verbraucherfragen

Dezember 2016

Berlin, Dezember 2016
ISSN 2365-919X

Herausgeber:

Sachverständigenrat für Verbraucherfragen
beim Bundesministerium der Justiz und für Verbraucherschutz
Mohrenstraße 37
10117 Berlin

Telefon: +49 (0) 30 18 580-0
Fax: +49 (0) 30 18 580-9525
E-Mail: info@svr-verbraucherfragen.de
Internet: www.svr-verbraucherfragen.de

Diese Veröffentlichung ist im Internet abrufbar.

Mitglieder des SVRV

Prof. Dr. Lucia Reisch (Vorsitzende)
Professorin für Interkulturelle Konsumforschung und europäische Verbraucherpolitik an der Copenhagen Business School

Dr. Daniela Büchel (stellv. Vorsitzende)
Mitglied der Geschäftsleitung REWE für die Bereiche Human Resources und Nachhaltigkeit

Prof. Dr. Gerd Gigerenzer
Direktor der Abteilung „Adaptives Verhalten und Kognition“ und des Harding-Zentrums für Risikokompetenz am Max-Planck-Institut für Bildungsforschung in Berlin

Helga Zander-Hayat
Leiterin des Bereichs Markt und Recht bei der Verbraucherzentrale Nordrhein-Westfalen

Prof. Dr. Gesche Joost
Professorin für das Fachgebiet Designforschung an der Universität der Künste und Internetbotschafterin der Bundesregierung im Gremium der „Digital Champions“ der EU

Prof. Dr. Hans-Wolfgang Micklitz
Professor für Wirtschaftsrecht am Europäischen Hochschulinstitut in Florenz

Prof. Dr. Andreas Oehler
Professor für Finanzwirtschaft an der Universität Bamberg und Direktor der Forschungsstelle Verbraucherfinanzen und Verbraucherbildung

Prof. Dr. Kirsten Schlegel-Matthies
Professorin für Haushaltswissenschaft an der Universität Paderborn

Prof. Dr. Gert G. Wagner
Professor für Empirische Wirtschaftsforschung und Wirtschaftspolitik an der Technischen Universität Berlin, Vorstandsmitglied des Deutschen Instituts für Wirtschaftsforschung und Max Planck Fellow am MPI für Bildungsforschung

Mitarbeitende des SVRV

Leiter der Geschäftsstelle: Thomas Fischer

Wissenschaftlicher Stab der Geschäftsstelle: Mathias Bug, Dr. Irina Domurath, Dr. Christian Groß

Disclaimer

Die Working Papers decken Arbeiten ab, die im Arbeitszusammenhang des SVRV entstanden sind. Für die Inhalte tragen die jeweiligen Autorinnen und Autoren alleinige Verantwortung, sie spiegeln nicht unbedingt die Meinung des Rates wider.

Verbraucherdatenschutzrecht in der EU-Datenschutz-Grundverordnung

Dipl.-Jur. Philipp Schmechel, Göttingen*

A. Einleitung

Die am 24. Mai 2016 in Kraft getretene Datenschutz-Grundverordnung[1] (DSGVO) schafft nicht nur ein neues, moderneres Datenschutzrecht für die gesamte Europäische Union, sie enthält auch zahlreiche Regelungen, die den Verbraucherschutz in der Union bedeutend stärken werden. Denn Datenschutz ist heutzutage zu großen Teilen auch immer Verbraucherschutz.[2] Die Verordnung wird gem. Art. 99 Abs. 2 DSGVO am 25. Mai 2018 in allen Mitgliedsstaaten der EU als Verordnung gem. Art. 288 Abs. 2 AUEV unmittelbar anwendbar sein (im Gegensatz zu einer Richtlinie, die erst in nationales Recht umgesetzt werden muss), sie wird mithin Vorrang vor dem nationalen Datenschutzrecht haben[3] sowie die EU-Datenschutzrichtlinie[4] (DS-Richtlinie) von 1995 gem. Art. 94 Abs. 1 DSGVO aufheben.

Für viele Verbraucher ist es zur Normalität geworden, ihre Kommunikation über soziale Online-Netzwerke oder mobile Applikationen auf ihrem Smartphone zu führen, Informationen werden fast ausschließlich über das Internet durch Suchmaschinen, Foren oder Bewertungsportale erlangt, zudem werden Bankgeschäfte online erledigt und sogar das „Smart Home“ mit seinen

---

* Dipl.-Jur. Philipp Schmechel ist wissenschaftlicher Mitarbeiter und Doktorand am Lehrstuhl von Prof. Dr. Gerald Spindler an der Georg-August-Universität Göttingen.

[1] Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung), Amtsblatt der Europäischen Union vom 4. Mai 2016, L 119/1-88.

[2] <http://www.vzbv.de/dokument/datenschutz-ist-verbraucherschutz> (zuletzt abgerufen am 20. Oktober 2016).

[3] Bzgl. des Anwendungsvorrangs des EU-Rechts siehe EuGH, CaseC-6/64, Costa v. E.N.E.L., EU:C:1964:66.

[4] Richtlinie 95/46/EG des Europäischen Parlaments und des Rates vom 24. Oktober 1995 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr, Amtsblatt der Europäischen Gemeinschaften vom 23. November 1995, L 281/31-50.

vielen intelligenten „Smart Devices“ des Internets der Dinge (Smart TV, Fitnessarmbänder, vernetzte Küchengeräte usw.) ist rund um die Uhr mit dem Internet verbunden. Dies hat selbstverständlich das Leben der Verbraucher deutlich erleichtert und Möglichkeiten der Kommunikation geschaffen, die vor einigen Jahren noch undenkbar waren. Allerdings darf bei aller Euphorie über diese neuen Möglichkeiten nicht in Vergessenheit geraten, dass viele Unternehmen mittlerweile riesige Mengen an personenbezogenen Daten gespeichert haben, welche etwa Dank intelligenter „Big Data“-Systeme und Cloud Computing zunehmend besser und schneller ausgewertet können. Hierdurch ist die Erstellung von genauen Persönlichkeitsprofilen der Verbraucher möglich geworden, die genau Aufschluss über verschiedenste Vorlieben und Verhaltensweisen der Verbraucher geben können. Dies kann für Verbraucher schwere Verletzungen ihrer Persönlichkeitsrechte bedeuten.[5]

In diesem Gutachten werden einige der für den Verbraucherdatenschutz relevanten Regelungen der DSGVO untersucht und mögliche Lücken für den Verbraucherschutz analysiert. Zunächst wird ein kurzer Überblick über die rechtliche Systematik des Verbraucherdatenschutzes in Deutschland gegeben. Anschließend wird ausführlich der Anwendungsbereich der DSGVO sowohl in territorialer als auch in materieller Hinsicht dargestellt, um danach die für Verbraucher sehr relevanten Regelungen zur Einwilligung sowie zur Zweckbindung zu untersuchen. Auch die Betroffenenrechte sowie Regelungen zum Scoring und zum Profiling haben für Verbraucher große Bedeutung und werden hier dargestellt und analysiert. Als möglicher „Königsweg“ für den Verbraucherdatenschutz werden schließlich die Prinzipien zum Privacy by Design und Privacy by Default vorgestellt. Weitere relevante Bereiche wie das Cloud Computing (insbes. die Auftragsdatenverarbeitung) oder die Durchsetzbarkeit[6] der Verbraucherdatenschutzrechte durch die staatliche Datenschutzaufsicht sowie durch den betrieblichen Datenschutzbeauftragten, ferner das im Vergleich zum BDSG deutlich verschärfte Sanktionsregime der DSGVO für Verstöße gegen das Datenschutzrechts werden hier ausgeklammert, um den Rahmen des Gutachtens nicht zu sprengen.

---

[5] Siehe zum Ganzen auch Spindler/Thorun/Wittmann, „Rechtsdurchsetzung im Verbraucherdatenschutz Bestandsaufnahme und Handlungsempfehlungen“ (2016), *Friedrich-Ebert-Stiftung*, S. 5, abrufbar unter: <http://library.fes.de/pdf-files/wiso/12536.pdf> (zuletzt abgerufen am 20. Oktober 2016).

[6] Zur Durchsetzbarkeit des Datenschutzrechts siehe Domurath/Kosyra, „Verbraucherdatenschutzrecht im Internet der Dinge“, SVRV Working Paper Nr. 5.

B. Systematik des Verbraucherdatenschutzrechts in Deutschland

Das europäische Datenschutzrecht findet seinen Ursprung in den ersten gesetzlichen Regelungen dieser Art in Deutschland,[7] insbesondere durch die Etablierung eines Grundrechts auf „informationelle Selbstbestimmung", abgeleitet aus Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG durch das BVerfG im sog. „Volkszählungsurteil".[8] Im europäischen (Verfassungs-) Recht finden sich noch ausgeprägtere datenschutzrechtliche Regelungen in Art. 8 EMRK, zudem in Art. 7 und Art. 8 der Charta der Grundrechte der Europäischen Union (EU-GRC) sowie in Art. 16 AEUV. Der EGMR sowie in letzter Zeit immer wieder der EuGH haben das europäische Datenschutzrecht mit ihren Entscheidungen maßgeblich vereinheitlicht.[9] Da die meisten deutschen Datenschutzgesetze heutzutage auf europäischen Richtlinien beruhen, sind die Entscheidungen des EuGH auch bei der Berücksichtigung der deutschen Umsetzungsgesetze vollumfänglich zu berücksichtigen.

Einfachgesetzlich finden sich die meisten für Verbraucher relevanten Regelungen des deutschen Datenschutzrechts im Bundesdatenschutzgesetz (BDSG) und im Telemediengesetz (TMG), es existieren allerdings unzählige weitere datenschutzrechtliche Spezialregelungen in einer Vielzahl anderer Gesetze.[10] Durch die unmittelbare Geltung der DSGVO werden die meisten Regelungen des deutschen Datenschutzrechts und insbesondere des BDSG ab Mai 2018 allerdings nicht mehr anwendbar sein. Nichtsdestotrotz finden sich in der DSGVO an vielen Stellen auch Öffnungsklauseln[11], deren Ausfüllung den nationalen Gesetzgebern in den Mitgliedsstaaten überlassen worden ist. Zu beachten ist allerdings, dass die Verordnung den Mitgliedsstaaten in

---

[7] Gola/Klug/Körffer, in: Gola/Schomerus (Hrsg.), BDSG Bundesdatenschutzgesetz – Kommentar, 12. Aufl. 2015, C.H.Beck, Rn. 1 zur Einleitung.

[8] BVerfGE 65, 1 – Volkszählung.

[9] Etwa EuGH, Case C‑362/14, Schrems v. Digital Rights Ireland, EU:C:2015:650; EuGH, CaseC‑131/12, Google Spain SL, Google Inc. v. Agencia Española de Protección de Datos (AEPD), Mario Costeja González, EU:C:2014:317.

[10] Vgl. Gola/Klug/Körffer (s.o. Fn. 7), Rn. 8 ff. zur Einleitung.

[11] Einen grafischen Überblick über die Systematik der Öffnungsklauseln findet sich unter: <https://www.flickr.com/photos/winfried-veil/29706462112/in/datetaken-public/> (zuletzt abgerufen am 07. Oktober 2016); siehe ausführlich zu den Möglichkeiten der nationalen Ausgestaltung der Öffnungsklauseln: Roßnagel (Hrsg.), *Europäische Datenschutz-Grundverordnung – Vorrang des Unionsrechts – Anwendbarkeit des nationalen Rechts* (NomosPraxis, 2016)

EG 8 DSGVO nur wenig Spielraum für etwaige nationale Ausgestaltungen gibt: „Wenn in dieser Verordnung Präzisierungen oder Einschränkungen ihrer Vorschriften durch das Recht der Mitgliedstaaten vorgesehen sind, können die Mitgliedstaaten Teile dieser Verordnung in ihr nationales Recht aufnehmen, soweit dies erforderlich ist, um die Kohärenz zu wahren und die nationalen Rechtsvorschriften für die Personen, für die sie gelten, verständlicher zu machen." Seit Anfang September kursiert ein erster Referentenentwurf des Bundesministeriums des Innern (BMI) für ein „Allgemeines Bundesdatenschutzgesetz" (ABDSG-E)[12], mithin für ein Gesetz zur Anpassung der Regelungen des nationalen Datenschutzrechts an die DSGVO, im Internet, schon die 62 Paragrafen des Entwurfs verdeutlichen, dass die DSGVO keine vollständige europaweite Harmonisierung des Datenschutzrechts erreichen wird und dass einige Bereiche weiterhin größtenteils national geregelt sein werden. Zukünftig wird für Verbraucher in datenschutzrechtlichen Fragen somit nicht alleine die DSGVO maßgeblich sein, es verbleiben vielmehr immer noch zahlreiche nationale Regelungen.

C. Relevante Regelungen der DSGVO für Verbraucher

I. Anwendungsbereich der DSGVO

Einen elementar wichtigen Stellenwert für das Schutzniveau des Datenschutzrechts nimmt die Frage ein, wann der Anwendungsbereich des Datenschutzrechts eröffnet ist. Dies gliedert sich in einen territorialen und in einen materiellen Anwendungsbereich – und bei letztgenannten hauptsächlich in die Frage, ob ein Datum einen Personenbezug aufweist. Denn gem. Art. 2 Abs. 1 ist die DSGVO, wie auch schon das BDSG, nur bei der Verarbeitung personenbezogener Daten anwendbar; reine Sachdaten ohne Personenbezug oder anonyme Daten fallen nicht unter den Anwendungsbereich (siehe EG 26 S. 5).

[12] Entwurf eines Gesetzes zur Anpassung des Datenschutzrechts an die Datenschutz-Grundverordnung und zur Umsetzung der Richtlinie (EU) 2016/680 (DSAnpUG-EU), abrufbar unter: <https://www.datenschutz-grundverordnung.eu/wp-content/uploads/2016/09/Entwurf-ABDSG-E-08.2016.pdf> (zuletzt abgerufen am 7. Oktober 2016); siehe hierzu auch die ausführliche „Gemeinsame Stellungnahme der deutschen Landesdatenschutzbehörden zum ABDSG", abrufbar unter: <https://fragdenstaat.de/files/foi/57158/eckpunktepapier-datenschutz-anpassung1.pdf> (zuletzt abgerufen am 21. November 2016).

1. Weiter territorialer Anwendungsbereich – Marktortprinzip

Der territoriale Anwendungsbereich der DSGVO ist weit gefasst und wird dazu führen, dass auch viele US-Unternehmen sich künftig an das europäische Datenschutzrecht halten müssen, was für eine große Stärkung des Verbraucherdatenschutzes sorgen wird. Gem. Art. 3 Abs. 1 DSGVO findet die Verordnung Anwendung auf die Verarbeitung personenbezogener Daten, soweit diese im Rahmen der Tätigkeiten einer Niederlassung[13] eines Verantwortlichen oder eines Auftragsverarbeiters in der Union erfolgt, unabhängig davon, ob die Verarbeitung in der Union stattfindet. Die DSGVO setzt somit das „Sitzlandprinzip" aus Art. 4 Abs. 1 lit. a) der DSRL fort;[14] sobald ein Unternehmen nun allerdings eine Niederlassung in der EU betreibt, unabhängig davon, in welchem Mitgliedstaat sich diese Niederlassung befindet, und ferner auch, wenn die Datenverarbeitung nicht in der EU stattfindet, gilt die DSGVO.[15] Auch wenn ein Unternehmen *keine* Niederlassung in der EU hat, aber personenbezogene Daten von natürlichen Personen, die sich in einem Mitgliedsstaat befinden, verarbeitet, kann die Verordnung nach Art. 3 Abs. 2 lit. a) DSGVO anwendbar sein, wenn die Datenverarbeitung damit im Zusammenhang steht „betroffenen Personen in der Union Waren oder Dienstleistungen anzubieten, unabhängig davon, ob von diesen betroffenen Personen eine Zahlung zu leisten ist" – mithin fallen auch kostenlose oder werbefinanzierte Angebote unter den Anwendungsbereich der Norm. Der Verantwortliche oder Auftragsverarbeiter muss „offensichtlich" beabsichtigen, betroffenen Personen in einem oder mehreren Mitgliedstaaten der Union Dienstleistungen *anzubieten* (EG

---

[13] Eine Niederlassung setzt nach EG 22 S. 2 DSGVO die effektive und tatsächliche Ausübung einer Tätigkeit durch eine feste Einrichtung voraus. Befindet sich der Verantwortliche oder der Auftragsverarbeiter in einem Drittstaat, so bedarf es einer „untrennbaren Verbundenheit" zwischen der Niederlassung in der EU und dem Verantwortlichen oder dem Auftragsverarbeiter, siehe EuGH, Case C-131/12, Google Spain SL, Google Inc. v. Agencia Española de Protección de Datos (AEPD), Mario Costeja González, EU:C:2014:317, Rn. 56 ff.; siehe ausführlich zum Merkmal der „wirtschaftlichen Verbundenheit": Article 29 Data Protection Working Party, „Update of Opinion 8/2010 on applicable law in light of the CJEU judgement in Google Spain" vom 16. Dezember 2015, *WP 179 update*, S. 4 ff.

[14] Piltz, „Die Datenschutz-Grundverordnung – Teil 1: Anwendungsbereich, Definitionen und Grundlagen der Datenverarbeitung" (2016), *Kommunikation und Recht*, 557-567, S. 558; somit gilt auch in weiten Teilen die Rechtsprechung des EuGH zum territorialen Anwendungsbereich der DSRL für die DSGVO fort, siehe hierzu u.a Case C-131/12 (s.o. Fn. 13); Case C-230/14, Weltimmo s. r. o. v. Nemzeti Adatvédelmi és Információszabadság Hatóság, EU:C:2015:639; Case 191/15, Verein für Konsumenteninformation v. Amazon EU Sàrl, EU:C:2016:612.

[15] Härting, „Datenschutz-Grundverordnung – Anwendungsbereich, Verbotsprinzip, Einwilligung" (2015), *Der IT-Rechts-Berater*, 36-40, S. 38.

23 S. 2 DSGVO), was ähnlich der Regelungen des internationalen Verbraucherschutzes ist.[16] Nach S. 3 genügt hierfür nicht alleine die bloße Zugänglichkeit einer Website in der EU, einer E-Mail-Adresse oder die Verwendung einer Sprache, die in dem Drittland, in dem der Verantwortliche niedergelassen ist, allgemein gebräuchlich ist – gleichwohl soll auch die Verwendung einer Sprache oder Währung, die in einem oder mehreren Mitgliedstaaten gebräuchlich ist, in Verbindung mit der Möglichkeit, Waren und Dienstleistungen in dieser anderen Sprache zu bestellen, darauf hindeuten können, dass der Verantwortliche beabsichtigt, den Personen in der Union Waren oder Dienstleistungen anzubieten. Dies umfasst etwa US-amerikanische Social Media Plattformen, die ihre Angebote auch in deutscher Sprache betreiben.[17] Nach Art. 3 Abs. 2 lit. b) DSGVO findet die Verordnung ferner Anwendung, wenn die Verarbeitung personenbezogener Daten eines nicht in der Union niedergelassenen Verantwortlichen oder auch Auftragsverarbeiters im Zusammenhang mit der *Beobachtung* des Verhaltens einer betroffenen Person steht, soweit dieses Verhalten in der Union erfolgt. Dies soll nach EG 24 S. 2 DSGVO dann der Fall sein, wenn durch sog. Tracking Internetaktivitäten des Betroffenen nachvollzogen[18] und dadurch personenbezogene Daten verarbeitet werden. Dies bedeutet eine Stärkung der Verbraucherrechte; allerdings ist zu beachten, dass mittlerweile auf so gut wie jedem Besuch einer Website Trackingtechnologien verwendet werden, sodass demnach fast jede Website, die User aus der EU erreicht, der DSGVO unterfällt.[19] Auch die Möglichkeit einer nachfolgenden Verwendung der personenbezogener Daten durch Techniken zur Profilbildung (Profiling, siehe unten C.V.) als Grundlage für Entscheidungen, die die natürliche Person betreffen oder „anhand dessen ihre persönlichen Vorlieben, Verhaltensweisen oder Gepflogenheiten analysiert oder vorausgesagt werden sollen“, fällt unter den Begriff des „Beobachtens“. Umfasst hiervon sind insbesondere durch Targeting generierte

---

[16] Spindler, „Die neue EU-Datenschutz-Grundverordnung“ (2016), *Der Betrieb*, 937-947, S. 938, unter Verweis auf EuGH, Case C-585/08, Peter Pammer v. Reederei Karl Schlüter GmbH & Co. KG, EU:C:2010:740.

[17] Plath, in ders. (Hrsg.), Kommentar zum BDSG und zur DSGVO sowie den Datenschutzbestimmungen des TMG und TKG, 2. Aufl. 2016, Verlag Dr. Otto Schmidt KG, Rn. 19 zu Art. 3 DSGVO.

[18] Piltz (s.o. Fn. 14), S. 559; Schantz, „Die Datenschutz-Grundverordnung – Beginn einer neuen Zeitrechnung im Datenschutzrecht“ (2016), *Neue Juristische Wochenschrift*, 1841-1847, S. 1842; Spindler (s.o. Fn. 16), S. 938.

[19] Härting (s.o. Fn. 15), S. 39.

Produktempfehlungen der Online-Werbung oder das Suchverhalten von Suchmaschinennutzern.[20] Die Schaffung dieses sog. „Marktortprinzips“[21] in Art. 3 Abs. 2 DSGVO ist einer der großen Erfolge der Datenschutzreform.[22] Ferner müssen der Verantwortliche oder Auftragsverarbeiter in diesen Fällen gem. Art. 27 Abs. 1 DSGVO einen Vertreter in der Union als zentrale Anlaufstelle für die Betroffenen und die Aufsichtsbehörden bestellen. Die DSGVO hat somit das Potential, einen weltweit hohen datenschutzrechtlichen Standard zu etablieren, da es sich für viele Unternehmen außerhalb Europas nicht lohnen wird, ihre Produkte zusätzlich zu den hohen Anforderungen der DSGVO an verschiedene Datenschutzregelwerke anzupassen.[23] Allerdings ist zu beachten, dass sich der Anwendungsbereich des Abs. 2 nur auf die oben genannten Tätigkeiten bezieht, es somit immer noch Bereiche der Verarbeitung personenbezogener Daten geben wird, die nicht von der DSGVO umfasst sein werden, wenn sich etwa eine Website nicht an Personen in der Union richtet und auch keine Verhaltensbeobachtung vorliegt.[24]

Das Marktortprinzip ermöglicht mithin eine weite territoriale Anwendbarkeit der DSGVO und etabliert somit einen stärkeren Rechtsschutz für Verbraucher in der EU auch gegen Unternehmen, die keine Niederlassung in der Union haben. Dies geschieht insbesondere dadurch, dass sich die Verordnung auch auf kostenlose Onlinedienste erstreckt, sofern ein europäische Publikum Adressant ist, sowie dadurch, dass jede Form des Profilings oder Trackings von Nutzern, die sich in der Union aufhalten, den Anwendungsbereich der Verordnung eröffnet.

---

[20] Plath (s.o. Fn. 17), Rn. 23 zu Art. 3 DSGVO.

[21] Siehe hierzu etwa Albrecht, „Das neue EU-Datenschutzrecht – von der Richtlinie zur Verordnung – Überblick und Hintergründe zum finalen Text für die Datenschutz-Grundverordnung der EU nach der Einigung im Trilog“ (2016), *Computer und Recht* CR 2016, 88-98, S. 90.

[22] Dammann, „Erfolge und Defizite der EU-Datenschutzgrundverordnung: Erwarteter Fortschritt, Schwächen und überraschende Innovationen“ (2016), *Zeitschrift für Datenschutzrecht*, 307-314, S. 309; Plath (s.o. Fn. 17), Rn. 11 zu Art. 3 DSGVO.

[23] Schantz (s.o. Fn. 18), S. 1842.

[24] Plath (s.o. Fn. 17), Rn. 12 zu Art. 3 DSGVO.

2. Materieller Anwendungsbereich

Die DSGVO behält den Grundsatz der DS-Richtlinie und des BDSG bei, dass sie materiell nur anwendbar ist, wenn personenbezogene Daten verarbeitet werden. Die Verordnung ist gem. Art. 1 Abs. 1 ferner wie die DS-Richtlinie nur auf die Verarbeitung personenbezogener Daten von natürlichen Personen anwendbar, juristische Personen fallen somit nicht unter ihren Anwendungsbereich.

a) Definition des „Verbrauchers“

Anders als § 13 BGB beinhalten weder das BDSG noch die DSGVO Regelungen, die sich explizit an „Verbraucher“ richten. Es ist mithin für die Anwendbarkeit der Verordnung einzig entscheidend, ob personenbezogene Daten verarbeitet werden.[25]

b) Personenbezug von Daten

Wie schon in der DS-Richtlinie bleibt in der DSGVO ebenfalls die Frage weitgehend offen, auf wessen Fähigkeiten oder Wissen abzustellen ist, um eine natürliche Person zu identifizieren. Sind nur die Kenntnisse der datenverarbeitenden Stelle ohne unverhältnismäßigen Aufwand zu berücksichtigen (sog. relativer Personenbezug) oder ist ein objektiver Ansatz heranzuziehen, der theoretisch das ganze Weltwissen berücksichtigt (sog. absoluter Personenbezug)?[26] Ein weiter Anwendungsbereich des Personenbezugs bedeutet generell größeren Verbraucherschutz, denn hierdurch fallen mehr Datenverarbeitungen rechtfertigungsbedürftig unter das Datenschutzrecht. Art. 4 Nr. 1 DSGVO definiert „personenbezogene Daten“ als „alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person (…) beziehen“. Eine natürliche Person wird dann als identifizierbar angesehen, wenn sie „direkt oder indirekt, insbesondere mittels Zuordnung zu einer Kennung wie einem Namen, zu einer Kennnummer, zu Standortdaten, zu einer Online-Kennung oder zu einem oder mehreren besonderen Merkmalen, die Ausdruck der physischen, physiologischen, genetischen, psychischen, wirtschaftlichen, kulturellen oder sozialen Identität dieser natürlichen Person sind,

---

[25] Spindler, „Consumer Data Protection in Germany”, in Metz et al., (Hrsg.), *Consumer Data Protection in Brazil, China and Germany – A Comparative Study* (2016), S. 81.

[26] Zum Streit, ob ein relativer oder absoluter Ansatz für die Herstellbarkeit des Personenbezugs zu wählen ist, siehe ausführlich nur Haase, *Datenschutzrechtliche Fragen des Personenbezugs*, (Univers. Diss., Tübingen 2015), S. 290 ff. m.w.Nachw.

identifiziert werden kann“. Folglich unterfallen gemäß dieser Definition alle Kennungen, und somit gerade auch dynamische IP-Adressen, dem Datenschutzrecht, was zunächst für einen absoluten Ansatz der DSGVO sprechen würde.[27] EG 26 S. 3 DSGVO stellt auf den Aufwand ab, der getätigt werden muss, um festzustellen, ob eine natürliche Person identifizierbar ist. Demnach sollen alle Mittel berücksichtigt werden, die von dem Verantwortlichen oder einer anderen Person *nach allgemeinem Ermessen wahrscheinlich* genutzt werden, um die natürliche Person direkt oder indirekt zu identifizieren, wie beispielsweise das Aussondern. Bei der Feststellung der Wahrscheinlichkeit der Mittel sollen alle objektiven Faktoren, wie die Kosten der Identifizierung und der dafür erforderliche Zeitaufwand, herangezogen werden, wobei die zum Zeitpunkt der Verarbeitung verfügbare Technologie und technologische Entwicklungen zu berücksichtigen sind. Dass nur Mittel berücksichtigen sind, die „nach allgemeinem Ermessen wahrscheinlich“ genutzt werden, um eine natürliche Person zu identifizieren, spricht für eine relative Auslegung des Personenbezugs, allerdings nennt EG 26 auch Mittel, die von einer *anderen Person* genutzt werden können, was wiederum für einen absoluten Ansatz sprechen könnte.[28] Jedoch müssen diese Mittel von dem Dritten wiederum nach allgemeinem Ermessen wahrscheinlich genutzt werden. Diese doch wieder relative Auslegung trifft auch der EuGH zur ähnlichen Formulierung in der DS-Richtlinie in einer kürzlich erschienen Entscheidung zur Frage des Personenbezugs von dynamischen IP-Adressen.[29] Gegen einen absoluten Ansatz spricht ferner auch EG 30 der DSGVO, wonach Online-Kennungen wie IP-Adressen, Cookie-Kennungen und Funkfrequenzkennzeichnungen (RFID-Tags) natürlichen Personen zugeordnet werden können und durch die Kombination mit eindeutigen Kennungen und anderen beim Server eingehenden Informationen Profile von natürlichen Personen erstellt und diese identifiziert werden können, d.h. eine Identifikation kann mit vorhandenem Zusatzwissen erfolgen, die Kennungen sind allerdings nicht per se personenbezogen (dies steht jedoch wiederum in einem

---

[27] Brink/Eckhardt, „Wann ist ein Datum ein personenbezogenes Datum? Anwendungsbereich des Datenschutzrechts“ (2015), *Zeitschrift für Datenschutzrecht*, 205-212, S. 208; Härting (s.o. Fn. 15), S. 36. Buchner, „Grundsätze und Rechtmäßigkeit der Datenverarbeitung unter der DS-GVO“ (2016), *Datenschutz und Datensicherheit*, 155-161, S. 156.

[28] Buchner, (s.o. Fn. 27).

[29] EuGH Case C‑582/14, Patrick Breyer v. Bundesrepublik Deutschland, EU:C:2016:779, Rn. 46: es dürfe kein „unverhältnismäßigen Aufwand an Zeit, Kosten und Arbeitskräften erfordern (…), so dass das Risiko einer Identifizierung de facto vernachlässigbar erschiene“.

Spannungsverhältnis zur Aussage des Art. 4 Nr. 1 DSGVO, s.o.).[30] Gerade im Bereich des Internets der Dinge (Internet of Things – IoT) wird somit allerdings auch deutlich, dass viele Technologien, die etwa RFID-Chips nutzen, personenbezogene Daten verarbeiten und somit der DSGVO unterfallen werden, was eine Stärkung des Datenschutzes für Verbraucher darstellt. Hier werden oftmals zwar Zustands- oder Sachdaten verarbeitet, die zunächst keinen Personenbezug aufweisen, die Kombination dieser Daten mit personenbezogenen Informationen führt dann jedoch in vielen Fällen dazu, dass natürliche Personen und deren Verhaltensweisen identifizierbar werden können.[31]

Hinsichtlich der Frage, wann eine natürliche Person identifizierbar ist, beinhaltet die Verordnung mithin sowohl relative als auch absolute Elemente, allerdings ist immer darauf abzustellen, ob eine Identifizierbarkeit nach allgemeinem Ermessen wahrscheinlich ist. Damit schafft die DSGVO, ähnlich wie die DS-Richtlinie, eine flexible Lösung, die einerseits den Interessen der Unternehmen dient, nicht bei allen Datenverarbeitungsvorgängen dem strengen Regime der DSGVO unterworfen zu sein, andererseits aber durch ihren weiten Anwendungsbereich auch für hinreichenden Verbraucherschutz sorgt, insbesondere hinsichtlich neuer Technologien.

c) Technische Schutzmaßnahmen: Anonymisierung, Pseudonymisierung und Verschlüsselung

Die DSGVO räumt der Anonymisierung von personenbezogenen Daten im Gegensatz zu § 3 Abs. 6 BDSG keinen großen Stellenwert mehr ein. Dies ist für Verbraucher bedauerlich, handelt es sich bei der Anonymisierung doch um eine geeignete Methode, um die Risiken für die Privatsphäre der Betroffenen zu verringern.[32] In der DSGVO wird die Anonymisierung nur in EG 26 S. 5 erwähnt, demnach soll die Verordnung nicht für Informationen gelten, die sich nicht auf eine identifizierte oder identifizierbare natürliche Person beziehen, oder für personenbezogene Daten, die in einer Weise anonymisiert worden sind, dass die betroffene Person nicht oder nicht

---

[30] Schantz (s.o. Fn. 18), S. 1843; a.A. Buchner (s.o. Fn. 27).

[31] Krings/Mammen, „Zertifizierungen und Verhaltensregeln - Bausteine eines modernen Datenschutzes für die Industrie 4.0“, *Recht der Datenverarbeitung*, (2015), 231-236, S. 231.

[32] Artikel-29-Datenschutzgruppe, „Stellungnahme 5/2014 zu Anonymisierungstechniken“, *WP 216*, S. 5, abrufbar unter: <http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp216_de.pdf> (zuletzt abgerufen am 18. Oktober 2016).

mehr identifiziert werden kann, also für anonyme Informationen. Die DSGVO Verordnung umfasst somit nicht die Verarbeitung solcher anonymer Daten, auch für statistische oder für Forschungszwecke. Allerdings ist auch zu beachten, dass in Zeiten von Big Data und mit Hilfe intelligenter Software eine Re-Anonymisierung in vielen Fällen möglich ist und so fast jedes Datum einen Personenbezug aufweisen kann.[33] Wurde ein Datenbestand erfolgreich anonymisiert und die Identifizierung von Einzelpersonen zuverlässig ausgeschlossen, fallen die betreffenden Daten allerdings zunächst nicht mehr in den Anwendungsbereich der europäischen Datenschutzvorschriften.

„Pseudonymisierung" wird von der DSGVO in Art. 4 Nr. 5 als „die Verarbeitung personenbezogener Daten in einer Weise, dass die personenbezogenen Daten ohne Hinzuziehung zusätzlicher Informationen nicht mehr einer spezifischen betroffenen Person zugeordnet werden können, sofern diese zusätzlichen Informationen gesondert aufbewahrt werden und technischen und organisatorischen Maßnahmen unterliegen, die gewährleisten, dass die personenbezogenen Daten nicht einer identifizierten oder identifizierbaren natürlichen Person zugewiesen werden", definiert. Nach EG 26 S. 2 DSGVO sollen allerdings einer Pseudonymisierung unterzogene personenbezogene Daten als Informationen über eine identifizierbare natürliche Person betrachtet werden und mithin nicht aus dem Anwendungsbereich der Verordnung fallen. Jedoch kommt es auch hier wieder auf die strittige Frage an, ob für die Beurteilung des Personenbezugs ein absoluter oder, vorzugswürdig, ein relativer Ansatz zu wählen ist.[34] Der Hauptanwendungsbereich der Pseudonymiserung liegt ferner gem. EG 28 DSGVO darin, die Risiken für die betroffenen Personen zu senken und die Verantwortlichen und die Auftragsverarbeiter bei der Einhaltung ihrer Datenschutzpflichten unterstützen, die Verwendung von Pseudonymen soll Datenschutzmaßnahmen jedoch nicht ausschließen.

---

[33] Härting, (s.o. Fn. 15), S. 37; Sarunski, „Big Data – Ende der Anonymität? Fragen aus Sicht der Datenschutzaufsichtsbehörde Mecklenburg-Vorpommern", *Datenschutz und Datensicherheit* (2016), 424-427, S. 425.

[34] Plath (s.o. Fn. 17), Rn. 20 zu Art. 4 DSGVO; Spindler/Schmechel, „Personal Data and Encryption in the European General Data Protection Regulation" (2016), *Journal of Intellectual Property, Information Technology and E-Commerce Law*, 163-177, S. 171, abrufbar unter: <https://www.jipitec.eu/issues/jipitec-7-2-2016/4440> (zuletzt abgerufen am 18. Oktober 2016).

Anders als der Parlamentsentwurf beinhaltet die DSGVO keine Definition von „verschlüsselten Daten“, jedoch taucht die Verschlüsselung als technische und organisatorische Maßnahme an verschiedenen Stellen der Verordnung auf.[35] Ungeklärt bleibt allerdings weiterhin der Streit, ob durch Verschlüsselung der Personenbezug von Daten aufgehoben werden kann, was insbesondere für das Cloud Computing von Relevanz ist.[36]

d) Haushaltsausnahme

Eine besondere Bedeutung für Verbraucher hat die sog. „Haushaltsausnahme“ in Art. 2 Abs. 1 lit. c) DSGVO (auch das BDSG beinhaltet in § 1 Abs. 2 Nr. 2 schon eine Haushaltsausnahme). Demnach findet die Verordnung keine Anwendung auf die Verarbeitung personenbezogener Daten durch natürliche Personen „zur Ausübung ausschließlich persönlicher oder familiärer Tätigkeiten“. Nach EG 18 S. 1 DSGVO darf die Datenverarbeitung keinerlei Bezug zu einer beruflichen oder wirtschaftlichen Tätigkeit aufweisen. Beispiele für persönliche oder familiäre Tätigkeiten sind nach EG 18 das Führen eines Schriftverkehrs oder von Anschriftenverzeichnissen oder die Nutzung sozialer Netze und Online-Tätigkeiten im Rahmen solcher Tätigkeiten. Allerdings besteht hierdurch gerade in sozialen Netzwerken die Gefahr, dass aus einem zunächst beschränkten Empfängerkreis ein potenziell unbeschränkter wird, wenn sich Empfänger von Nachrichten oder Bildern ebenfalls auf das Haushaltsprivileg berufen, um diese Daten wiederum anderen zugänglich zu machen.[37] Die Datenverarbeiter können sich mithin jeweils auf ihr Haushaltsprivileg berufen, sodass hieraus eine mögliche Schutzlücke für den Verbraucher entstehen kann. Nichtsdestotrotz ist die Haushaltsausnahme restriktiv auszulegen und „öffentlichkeitsfeindlich“, dies macht der Wortlaut schon mit der Eingrenzung auf

---

[35] Etwa gem. Art. 32 Abs. 1 lit. a DS-GVO bezüglich der Sicherheit der Verarbeitung, ferner auch bei einer späteren Zweckänderung gem. Art. 6 Abs. 4 lit. e DS-GVO oder bei der Benachrichtigungspflicht gem. Art. 34 Abs. 3 lit. a DS-GVO.

[36] Ausführlich hierzu Stiemerling/Hartung, „Datenschutz und Verschlüsselung – Wie belastbar ist Verschlüsselung gegenüber dem Anwendungsbereich des Datenschutzrechts?“, *Computer und Recht* (2012), 60-68, S. 60 ff.; Borges, in: ders./Meents (Hrsg.), Cloud Computing, 1. Auflage 2016, Verlag C.H. Beck, Rn. 34 ff. zu § 6; Spindler/Schmechel (s.o. Fn. 34), S. 171 ff.; von einem Personenbezug von verschlüsselten Daten ausgehend Wagner/Blaufuß, „Datenexport als juristische Herausforderung: Cloud Computing“, *Betriebs-Berater* (2012), 1751-1755, S. 1751.

[37] Gola/Lepperhoff, „Reichweite des Haushalts- und Private Datensammlung – Aufnahme und Umfang der Ausnahmeregelung in der DS-GVO“, *Zeitschrift für Datenschutzrecht* (2016), 9-12, S. 11; Härting (s.o. Fn. 15), S. 37.

„*ausschließlich*" persönliche oder familiäre Tätigkeiten deutlich.[38] Verglichen werden kann die Haushaltsausnahme mit sog. „PowerSellern" im E-Commerce-Recht, hierbei kann aus einem Verbraucher ein Unternehmer und dieser damit zum Adressaten von Verantwortlichkeiten werden;[39] sobald es sich bei der Datenverarbeitung folglich nicht mehr um rein persönliche oder familiäre Tätigkeiten handelt, ist die DSGVO mit all ihren Pflichten für den Verantwortlichen anwendbar. EG 18 S. 3 DSGVO stellt ferner klar, dass auch wenn die natürliche Person bei einer Verarbeitung personenbezogener Daten nicht die Vorschriften der DSGVO zu beachten hat, der jeweilige Verantwortliche oder Auftragsverarbeiterder, der die Instrumente für die Verarbeitung personenbezogener Daten bereitstellt, etwa ein Betreiber von sozialen Netzwerken[40], nicht aus dem Anwendungsbereich der Verordnung ausgenommen ist und somit verantwortlich bleibt.

3. Bewertung

Sowohl der weite räumliche als auch der weite materielle Anwendungsbereich der Verordnung sorgen für gebührenden Verbraucherschutz. Durch den erweiterten territorialen Einfluss werden sich auch Datenverarbeiter außerhalb der Union an das strenge europäische Datenschutzrechte halten müssen. Der weit gefasste materielle Anwendungsbereich sorgt dafür, dass viele Daten als personenbezogene Daten bestimmbar sind. Hier hat die DSGVO eine gute Balance zwischen dem Schutz der Verbraucher vor übermäßiger Datenverarbeitung durch Unternehmer und dem Schutz der Unternehmer, für die ein strikt absoluter Ansatz des Personenbezugs viele Geschäftsmodelle erheblich erschwert hätte, erreicht. Zu bedauern ist, dass die DSGVO wenig Anreize für Anonymisierung und Verschlüsselung setzt, obwohl gerade diese Technologien dazu geeignet sind, die informationelle Selbstbestimmung der Verbraucher zu schützen.

---

[38] Ernst, in: Paal/Pauly, Datenschutz-Grundverordnung, 1. Aufl. 2017, C.H.Beck, Rn. 21 zu Art. 2 DS-GVO; vgl. auch EuGH, Case C-101/01, Lindqvist, EU:C:2003:596, Rn. 47.

[39] Siehe hierzu Micklitz/Purnhagen, in: Münchener Kommentar zum BGB, 7. Aufl. 2015, C.H.Beck, Rn. 29 zu § 14 BGB; Krüger/Peintinger, in: Martinek/Semler/Flohr, Handbuch des Vertriebsrechts, 4. Aufl. 2016, C.H.Beck, Rn. 161 zu § 36.

[40] Piltz (s.o. Fn. 14), S. 558; Plath (s.o. Fn. 17), Rn. 15 zu Art. 2 DSGVO.

II. Verbotsprinzip und Einwilligung

Die DSGVO bleibt dem sog. „Verbotsprinzip“ treu, wie schon in der DS-Richtlinie gilt in der Verordnung ein generelles Verbot der Verarbeitung personenbezogener Daten mit Erlaubnisvorbehalt.[41] Eine Verarbeitung personenbezogener Daten ist gem. Art. 6 Abs. 1 S. 1 DSGVO nur zulässig, wenn der Verbraucher in die Datenverarbeitung eingewilligt hat oder wenn ein sonstiger Erlaubnistatbestand vorliegt, etwa wenn die Verarbeitung für die Erfüllung eines Vertrags oder zur Erfüllung einer rechtlichen Verpflichtung erforderlich oder wenn die Verarbeitung zur Wahrung der berechtigten Interessen des Verantwortlichen oder eines Dritten erforderlich ist, sofern nicht die Interessen oder Grundrechte und Grundfreiheiten der betroffenen Person, die den Schutz personenbezogener Daten erfordern, überwiegen.

1. Anforderungen der DSGVO an eine Einwilligung

Art. 4 Nr. 11 DSGVO definiert die Einwilligung als „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“. Der Vorschlag der Kommission und des Parlaments, wonach jede Einwilligung „ausdrücklich“ zu sein hatte, wurde nur für bestimmte sensible Daten übernommen (s.u. C.II.4.). Eine konkrete Form der Einwilligung wird von der DSGVO nicht verlangt, mithin sind auch konkludente Einwilligungen möglich, das Anklicken eines Kästchens im Online-Bereich als Einwilligung bleibt somit als wirksame Einwilligungsart bestehen.[42] Unklar ist, ob alleine die Voreinstellungen des Browsers bereits ausreichend sind, denn dies wurde vom Rat in EG 25 S. 5 vorgeschlagen, in die endgültige Version der DSGVO jedoch nicht aufgenommen.[43] Bloßes Schweigen oder ein Opt-out sind nicht ausreichend für

---

[41] Härting, *Datenschutz-Grundverordnung – Das neue Datenschutzrecht in der betrieblichen Praxis* (Verlag Dr. Otto Schmidt KG, 2016), Rn. 318; Plath (s.o. Fn. 17), Rn. 2 zu Art. 6 DSGVO.

[42] Härting (s.o. Fn. 15), S. 39; Krohm, „Abschied vom Schriftformgebot der Einwilligung – Lösungsvorschläge und künftige Anforderungen“, *Zeitschrift für Datenschutzrecht* (2016), 368-373, S. 370; Piltz (s.o. Fn. 14), S. 562; Spindler, (s.o. Fn. 16), S. 940.

[43] Spindler, (s.o. Fn. 16), S. 940; a.A. aber Härting (s.o. Fn. 15), S. 39, der sich darauf beruft, dass dies als „technische Einstellung“ gem. EG 32 S. 2 DSGVO möglich sei.

eine wirksame Einwilligung.[44] Nach EG 32 S. 5 DSGVO müssen Einwilligung im elektronischen Weg, also etwa auf Websites, zudem „in klarer und knapper Form und ohne unnötige Unterbrechung des Dienstes, für den die Einwilligung gegeben wird, erfolgen". Ferner trägt der Verantwortliche und nicht der Verbraucher gem. Art. 7 Abs. 1 DSGVO die Beweislast dafür, dass die betroffene Person wirklich in die Datenverarbeitung eingewilligt hat.

Soll eine Einwilligung Teil von AGB sein, ist sie schriftlich nach bisherigen Recht gem. § 4a Abs. 1 S. 4 BDSG besonders hervorzuheben. Die DSGVO normiert nun in Art. 7 Abs. 2 ein sog. „Trennungs- und Transparenzgebot".[45] Demnach müssen schriftliche[46] Einwilligungserklärungen, die Teil einer anderen Erklärung sind, nicht nur in „verständlicher und leicht zugänglicher Form in einer klaren und einfachen Sprache" verfasst und von anderen Erklärungen „klar zu unterscheiden" sein, vorformulierte Einwilligungserklärungen dürfen ferner keine missbräuchlichen Klauseln enthalten (EG 42 S. 3 DSGVO, unter Verweis auf die Richtlinie 93/13/EG vom 5.4.1993 über missbräuchlich Klauseln in Verbraucherverträgen). Rechtsfolge eines Verstoßes gegen das Trennungsgebot ist gem. Art. 7 Abs. 2 S. 2 DSGVO nur die Unwirksamkeit der Einwilligung – der übrige Teil des Vertrages bleibt davon unberührt.[47] Im Vergleich zu § 306 Abs. 3 BGB ist zu beklagen, dass eine Regelung, die eine Gesamtnichtigkeit des Vertrags bei einem Verstoß gegen eine derart elementare Regelung vorsieht, nicht in die DSGVO aufgenommen wurde.[48]

---

[44] Spindler, (s.o. Fn. 16), S. 940; differenzierend Krohm (s.o. Fn. 42), S. 372, der noch Möglichkeiten für eine wirksame Einwilligung durch ein Opt-out sieht; Piltz, (s.o. Fn. 14), S. 563.

[45] Plath, (s.o. Fn. 17), Rn. 5 zu Art. 7 DSGVO.

[46] Wozu, gerade für den Online-Bereich, auch Einwilligungen in Textform i.S.v. § 126a BGB zu zählen sind, siehe Plath, (s.o. Fn. 17), Rn. 7 zu Art. 7 DSGVO.

[47] Plath, (s.o. Fn. 17), Rn. 9 zu Art. 7 DSGVO.

[48] Der Wortlaut des Art. 7 Abs. 2 S. 2 DSGVO lautet: „Teile der Erklärung sind dann nicht verbindlich, wenn sie einen Verstoß gegen diese Verordnung darstellen." Fraglich ist allerdings, ob ein Vertrag für die Parteien dann noch Sinn ergibt, wenn die Einwilligung in die Datenverarbeitung nicht mehr Teil der Erklärung ist. Eine Rechtmäßigkeit der Datenverarbeitung müsste dann nach den sonstigen Erlaubnistatbeständen der DSGVO geprüft werden, etwa, ob „berechtigte Interessen" des Verantwortlichen vorliegen.

Anders als das BDSG[49] sieht die DSGVO in Art. 7 Abs. 3 nun ausdrücklich die verbraucherfreundliche Möglichkeit eines jederzeitigen Widerrufs einer Einwilligung ohne Notwendigkeit eines Grundes oder einer Begründung durch die betroffene Person vor. Demnach hat der Betroffene das Recht, die Einwilligung jederzeit mit *ex nunc*-Wirkung zu widerrufen, sodass eine weitere Datenverarbeitung, die nur auf dieser Einwilligung basiert, ohne rechtliche Grundläge wäre. Ein Widerruf der Einwilligung muss so einfach möglich sein, wie die Möglichkeit besteht, diese zu erteilen, zudem muss der Verantwortliche den Betroffenen über die Widerruflichkeit der Einwilligung vor deren Abgabe in Kenntnis setzen.

EG 171 DSGVO behandelt schließlich die Fortwirkung von Einwirkungen, die noch auf der DS-Richtlinie beruhen. Nach einem Beschluss des *Düsseldorfer Kreises* erfüllen bisher rechtswirksame Einwilligungen grundsätzlich die Voraussetzungen der DSGVO, allerdings müssen zusätzlich die Regelungen der Verordnung zur Freiwilligkeit (s.u. C.II.2.), insb. das Kopplungsverbot, gewahrt werden sowie die Altersgrenze von sechzehn Jahren für eine wirksame Einwilligung (s.u. C.II.3.). beachtet werden.[50]

2. Freiwilligkeit und Kopplungsverbot

Hinsichtlich der Freiwilligkeit der Einwilligung schafft die DSGVO insbesondere durch das Kopplungsverbot für Verbraucher wichtigen Rechtsschutz, um sich gegen Online-Dienste wie Facebook behaupten zu können. Eine Einwilligung ist nach Art. 4 Nr. 11 DSGVO nur wirksam, sofern sie ohne Zwang, mithin freiwillig abgeben wurde (siehe auch EG 42 S. 5 DSGVO, welcher eine echte Wahlfreiheit des Betroffenen verlangt). Art. 7 Abs. 4 DSGVO regelt hierzu, dass bei der Beurteilung, ob die Einwilligung freiwillig erteilt wurde, dem Umstand in größtmöglichem Umfang Rechnung getragen werden muss, ob unter anderem die Erfüllung eines Vertrags,

---

[49] Für das BDSG ist die Möglichkeit eines Widerrufs einer Einwilligung allgemein aufgrund des Schutzes der informationellen Selbstbestimmung des Betroffenen, neben einer punktuellen Regelung in § 28 Abs. 3a, anerkannt, vgl. nur Simitis in: ders. (Hrsg.), Bundesdatenschutzgesetz – Kommentar, 8. Auf. 2014, Nomos Verlag, Rn. 94 zu § 4a BDSG.

[50] Düsseldorfer Kreis, „Beschluss der Aufsichtsbehörden für den Datenschutz im nicht-öffentlichen Bereich vom 13./14. September 2016: Fortgeltung bisher erteilter Einwilligungen unter der Datenschutz-Grundverordnung“, abrufbar unter: <https://www.lda.bayern.de/media/dk_einwilligung.pdf> (zuletzt abgerufen am 20. Oktober 2016); a.A. Plath (s.o. Fn. 17), Rn. 2 zu Art. 7 DSGVO, der hinsichtlich der englischen Formulierung „in line with the conditions of this Regulation“ davon ausgeht, dass eine vollständige Einhaltung der Vorgaben der DSGVO gefordert wird.

einschließlich der Erbringung einer Dienstleistung, von der Einwilligung zu einer Verarbeitung von personenbezogenen Daten abhängig ist, die für die Erfüllung des Vertrags nicht erforderlich ist und schafft hiermit ein sog. Kopplungsverbot, unabhängig von der Marktmacht eines Unternehmens.[51] EG 43 S. 2 DSGVO präzisiert dies folgendermaßen:

> „Die Einwilligung gilt nicht als freiwillig erteilt, wenn zu verschiedenen Verarbeitungsvorgängen von personenbezogenen Daten nicht gesondert eine Einwilligung erteilt werden kann, obwohl dies im Einzelfall angebracht ist, oder wenn die Erfüllung eines Vertrags, einschließlich der Erbringung einer Dienstleistung, von der Einwilligung abhängig ist, obwohl diese Einwilligung für die Erfüllung nicht erforderlich ist."

Eine Einwilligung eines Verbrauchers etwa in die Zusendung von Werbematerialien an seine Postadresse während des Registrierungsprozesses bei einem Online-Shop hätte demnach zur Folge, dass diese Einwilligung in die Werbung für die Erfüllung des Vertrags (also die Lieferung der Waren und die Zahlung des Kaufpreises) nicht erforderlich und somit unwirksam wäre.[52] Das Kopplungsverbot der DSGVO steht allerdings in einem Widerspruch zur Rechtsprechung des EuGH, so hat der Gerichtshof erst kürzlich Kopplungsangebote als grundsätzlich lautere Geschäftspraktiken qualifiziert[53], allerdings urteilte das EuG wiederum 2007 in einer AGB-rechtlichen Streitigkeit für ein strenges Kopplungsverbot[54]. Wie sich das datenschutzrechtliche Kopplungsverbot in die Systematik dieser Entscheidungen einfügen wird, bleibt abzuwarten.

An der Freiwilligkeit mangelt es zudem, wenn zwischen der betroffenen Person und dem Verantwortlichen „ein klares Ungleichgewicht" besteht (EG 43 S. 1 DSGVO). Sofern eine Leistung zu vergleichbaren Konditionen von einem anderen Anbieter bezogen werden kann, kann

---

[51] Vgl. Plath (s.o. Fn. 17), Rn. 14 zu Art. 7 DSGVO; Spindler, (s.o. Fn. 16), S. 940.

[52] Härting, „Kopplungsverbot – der Einwilligungskiller nach der DSGVO", *CR-online.de Blog* v. 11. Oktober 2016, abrufbar unter: <http://www.cr-online.de/blog/2016/10/11/kopplungsverbot-der-einwilligungskiller-nach-der-dsgvo/> (zuletzt abgerufen am 20. Oktober 2016), demzufolge deswegen die "berechtigten Interessen" des Art. 6 Abs. 1 S. 1 lit. f) DSGVO „als zweites Standbein einer datenschutzkonformen Strategie oder gar als Alternative zur einwilligungsbasierten Datenverarbeitung" in den Fokus rücken.

[53] EuGH, Case C‑310/15, Vincent Deroo-Blanquart v. Sony Europe Limited, EU:C:2016:633, Rn. 52.

[54] EuG, Case T‑201/04, Microsoft Corp. v. Kommission der Europäischen Gemeinschaften, EU:T:2007:289.

allerdings wohl noch nicht von einem „klaren“ Ungleichgewicht ausgegangen werden, selbst wenn es sich hierbei um einen großen Konzern handelt, eine Kopplung der Leistung an die Einwilligungserklärung kann mithin trotzdem möglich sein.[55] Nichtsdestotrotz wird es für Unternehmen zukünftig oftmals riskant werden, sich auf die Wirksamkeit der Einwilligung zu verlassen, da ein Ungleichgewicht im Massenverkehr von Unternehmern und Verbrauchern regelmäßig vorliegen wird, denn individuelle Verhandlungen zwischen Verbrauchern und Unternehmern sind in der Praxis zumeist nicht durchführbar.[56] Ob sich das „Ungleichgewicht“ auf faktische oder wirtschaftliche Faktoren bezieht, ist schließlich noch unklar.[57]

3. Minderjährigenschutz

Neu in der DSGVO ist, dass Kindern unter sechzehn Jahren nach Art. 8 DSGVO ein besonderer Schutz zukommen soll, da diese sich ihrer Rechte bei der Verarbeitung personenbezogener Daten möglicherweise weniger bewusst sind. Demnach hängt die Wirksamkeit in die Verarbeitung personenbezogener Daten von Kindern, die noch nicht das sechzehnte Lebensjahr vollendet haben, von der Einwilligung oder Zustimmung ihrer Eltern ab. Sofern eine solche Einwilligung oder Zustimmung fehlt, sind die Einwilligungserklärungen des Kindes unwirksam. Jugendliche über sechzehn Jahre können in Angebote von Diensten der Informationsgesellschaft, d.h. in Dienste aus dem elektronischen Fernabsatz einwilligen.[58] EG 38 S. 2 DSGVO macht deutlich, dass dies insbesondere für die Verwendung personenbezogener Daten von Kindern für Werbezwecke oder für die Erstellung von Persönlichkeits- oder Nutzerprofilen und die Erhebung von personenbezogenen Daten von Kindern bei der Nutzung von Diensten, die Kindern direkt angeboten werden, gelten soll. Erfasst werden demnach nur solche Dienste, die etwa in ihrer Werbung deutlich Kinder ansprechen.[59]

---

[55] So auch Plath (s.o. Fn. 17), Rn. 15 zu Art. 7 DSGVO; a.A. aber Albrecht (s.o. Fn. 21), S. 91.

[56] Härting (s.o. Fn. 15), S. 40, der dies für ein “Damoklesschwert, das einen rechtskonformen Datenverkehr mit Verbrauchern erheblich erschwert“ hält.

[57] Piltz (s.o. Fn. 14), S. 563.

[58] Plath (s.o. Fn. 17), Rn. 5 zu Art. 8 DSGVO.

[59] Spindler, (s.o. Fn. 16), S. 940.

Gem. Art. 8 Abs. 3 DSGVO bleibt das Vertragsrecht der Mitgliedstaaten allerdings ausdrücklich unberührt.[60] Dies betrifft auch die Normen über das Zustandekommen und die Gültigkeit von Verträgen in Bezug auf Minderjährige, sodass Art. 8 DSGVO keinen Einfluss auf die Geschäftsfähigkeit von Minderjährigen hat. Demnach können Minderjährigen zwar in die Verarbeitung ihrer personenbezogenen Daten durchaus einwilligen, aber keine wirksamen Verträge ohne Zustimmung der Eltern abschließen.[61] Einen Herausgabeanspruch bezüglich der Daten hätte der Minderjährige dann nur nach bereicherungsrechtlichen Vorschriften.[62]

Um herauszufinden, ob die Einwilligung tatsächlich durch den Träger der elterlichen Verantwortung erteilt wurde, müssen die Verantwortlichen gem. Art. 8 Abs. 2 DSGVO „unter Berücksichtigung der verfügbaren Technik angemessene Anstrengungen unternehmen“, um Lösungen zur Verifikation im Internet zu schaffen, um sich zu vergewissern, ob die Einwilligung tatsächlich von den Eltern des Kindes stammt.[63] Die DSGVO sieht zudem eine Öffnungsklausel für die Mitgliedstaaten vor, durch welche die Altersgrenze auf dreizehn Jahre gesenkt werden darf, dies wird jedoch wieder zu einem uneinheitlichen System des Minderjährigenschutzes zwischen den Mitgliedstaaten führen.

4. Einwilligung in die Verarbeitung besonderer Kategorien personenbezogener Daten

Wie auch in Art. 8 Abs. 1 DS-Richtlinie ist die Verarbeitung besonderer Kategorien personenbezogener Daten einer natürlichen Person nach Art. 9 Abs. 1 DSGVO grundsätzlich untersagt. Zu den besonderen Kategorien personenbezogener Daten zählen genetischen Daten, biometrische Daten zur eindeutigen Identifizierung einer natürlichen Person, Gesundheitsdaten oder Daten zum Sexualleben oder der sexuellen Orientierung einer natürlichen Person (jeweils

---

[60] Der Anwendungsbereich des Abs. 3 beschränkt sich somit auf das allgemeine Vertragsrecht der Mitgliedsstaaten. In Verbindung mit dem bzgl. der Einwilligung eines Kindes abschließenden Art. 8 Abs. 1 DSGVO wird deutlich, dass Abs. 3 somit gerade nicht Voraussetzungen der Einwilligung regeln soll, siehe Plath (s.o. Fn. 17), Rn. 15 zu Art. 8 DSGVO.

[61] Spindler, (s.o. Fn. 16), S. 940.

[62] Spindler, „Verträge über digitale Inhalte – Anwendungsbereich und Ansätze - Vorschlag der EU-Kommission zu einer Richtlinie über Verträge zur Bereitstellung digitaler Inhalte“ (2016), *Multimedia und Recht*, 147-153, S. 148.

[63] Piltz, (s.o. Fn. 14), S. 564.

definiert in Art. 4 Nr. 13 bis 15 DSGVO). Art. 9 Abs. 2 DSGVO listet abschließend die Ausnahmetatbestände auf, wann eine Verarbeitung besonderer Kategorien personenbezogener Daten nicht untersagt ist, etwa durch eine *ausdrückliche* Einwilligung der betroffenen Person (welche jedoch durch die Mitgliedstaaten als Erlaubnistatbestand wiederum ausgeschlossen werden kann, Art. 9 Abs. 2 lit. a)). In § 5 ABDSG-E des BMI wird ferner von der Öffnungsklausel des Art. 9 Abs. 2 lit. g) DSGVO Gebrauch gemacht. Die Verarbeitung besondere Kategorien personenbezogener Daten soll demnach auch aus Gründen eines „erheblichen öffentlichen Interesses" erlaubt sein, wozu etwa die Verarbeitung geometrischer Daten zu Zwecken der eindeutigen Identifikation einer Person (§ 5 Abs. 1 Nr. 1 ABDSG-E) zu zählen sei. Eine Neuerung der DSGVO stellt der Schutz von genetischen und biometrischen Daten dar. Dies kann nach EG 51 DSGVO dazu führen, dass der Abgleich eines Bildes mit einer Gesichtserkennungssoftware in sozialen Netzwerken oder auch Identifizierungsverfahren von Verbrauchern durch Fingerabdruckscanner zukünftig dem besonderen Schutz des Art. 9 DSGVO unterfallen.[64]

5. Daten als Entgelt für die Nutzung von Internetangeboten

Neben der DSGVO herrscht momentan eine rege Debatte über die Frage, ob Daten als Entgelt für die Nutzung von Internetangeboten angesehen werden können, da deren Nutzer häufig keine Vergütung in Geld zahlen, um die Leistung in Anspruch nehmen zu können, wobei sich die Anbieter solcher Dienste dann regelmäßig das Recht einräumen lassen, diese Daten z.B. zu Werbezwecken zu gebrauchen.[65] Hierbei kann einerseits die Eingabe der Daten erforderlich sein, um den Dienst überhaupt erbringen zu können. Andererseits wird die Erbringung der Leistung teilweise davon abhängig gemacht, dass der Verbraucher Daten übermittelt, die für die Erbringung der eigentlichen Leistung nicht von Relevanz sind, etwa wenn für den Abruf eines journalistischen Artikels verlangt wird, dass der Verbraucher vorher seine E-Mail-Adresse eingibt. Ferner lassen sich Unternehmer oftmals weitere Rechte an den Daten als für die

---

[64] Plath (s.o. Fn. 17), Rn. 8 zu Art. 9 DSGVO.

[65] Faust, „Digitale Wirtschaft – Analoges Recht: Braucht das BGB ein Update?", *Gutachten A zum 71. Deutschen Juristentag 2016*, S. 16; siehe auch Art. 3 Abs. 1 des Vorschlags für eine Richtlinie des Europäischen Parlaments und des Rates über bestimmte vertragliche Aspekte der Bereitstellung digitaler Inhalte, COM(2015) 634 final 2015/0287 (COD), abrufbar unter: <http://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=CELEX:52015PC0634&qid=1453386693189&from=DE> (zuletzt abgerufen am 20. Oktober 2016).

Leistungserbringung eigentlich erforderlich wären einräumen. Hierbei erbringt der Verbraucher durch die Rechteeinräumung eine Art Gegenleistung für die Dienstleistung.[66] Auf dem 71. DJT wurde beschlossen, dass von einem Entgelt nur auszugehen sei, wenn die Datennutzung aufgrund des Datenschutzrechts nur mit Einwilligung des Betroffenen zulässig ist, mithin, wenn personenbezogene Daten vorliegen.[67] Allerdings wäre ein Entgelt dann folglich nicht anzunehmen, wenn keine *personenbezogenen* Daten übermittelt würden, zudem können viele Datenverarbeitungen auch ohne Einwilligung in Zukunft nach Art. 6 Abs. 1 lit. f) und Abs. IV DSGVO gerechtfertigt werden, sodass nur wenige Verträge als entgeltlich einzustufen wären.[68] Ein ähnliches Ergebnis findet sich auch in Art. 3 Nr. 4 des Richtlinienvorschlags für digitale Inhalte, hiernach sind Daten, die aufgrund einer gesetzlicher Ermächtigungen verarbeitet werden dürfen, nicht als Gegenleistung zu qualifizieren.[69] Ist die Einwilligung in die Verarbeitung oder Nutzung der personenbezogenen Daten etwa aufgrund des datenschutzrechtlichen Kopplungsverbots (s.o. C.II.2.) unwirksam, etwa wenn die Anbieter die Daten über den eigentlichen Vertragszweck hinaus erheben und verarbeiten,[70] bleibt der Vertrag im Übrigen aber wirksam, es handelt sich dann um einen unentgeltlichen Vertrag.[71]

Ob Daten ein Entgelt darstellen, kann auch für die Anwendbarkeit der Verbraucherschutzvorschriften nach §§ 312 ff. BGB von Bedeutung sein, da hierfür nach deutschem Recht eine entgeltliche Leistung vorliegen muss.[72] So könnte etwa das

---

[66] Faust (s.o. Fn. 65), S. 17 f.

[67] Beschlüsse des 71. Deutschen Juristentags 2016, S. 2, abrufbar unter: <http://www.djt.de/fileadmin/downloads/71/Beschluesse_gesamt.pdf> (zuletzt abgerufen am 20. Oktober 2016).

[68] Wendehorst, „Die Digitalisierung und das BGB“ (2016), *Neue juristische Wochenschrift*, 2609-2613, S. 2612.

[69] Spindler, „Digitale Wirtschaft – analoges Recht: Braucht das BGB ein Update?“, *Juristenzeitung* (2016), 805-816, S. 807.

[70] Vgl. Spindler (s.o. Fn. 69), S. 807.

[71] Faust (s.o. Fn. 65), S. 19.

[72] Diese Regelung in § 312 Abs. 1 BGB steht allerdings im Widerspruch zur Verbraucherrechte-RL, siehe: Faust (s.o. Fn. 65), S. 25.

Widerrufsrecht gemäß § 357 BGB dafür sorgen, dass der Unternehmer dem Verbraucher die sEinwilligung „zurückgewähren“ hat, diese mithin nicht mehr nutzen darf.[73]

6. Bewertung

Die Regelungen der DSGVO zur Einwilligung enthalten viele verbraucherfreundliche Neuerungen, seien es die hohen Transparenzanforderungen, das strenge Kopplungsverbot, der starke Minderjährigenschutz oder auch der erweiterte Schutz für besonders sensible Daten. Allerdings ist fraglich, ob durch die strengen Anforderungen an die Freiwilligkeit dem Verbraucherschutz wirklich gedient ist, wenn in der Folge viele Einwilligungen für unwirksam erklärt werden und sich Unternehmen deshalb verstärkt auf die Nutzung der weniger transparenten Regelung zur Verarbeitung personenbezogener Daten aufgrund „berechtigter Interessen“ stützen werden.

III. Zweckbindung und Zweckänderungen (Big Data)

Die Nutzung moderner Kommunikationsmittel sowie die immer weiterführende Vernetzung aller möglichen Konsumgeräte (IoT) sorgt unaufhörlich dafür, dass Unternehmen eine stetig wachsende Menge an personenbezogenen Daten über Verbraucher erheben, speichern und durch Big Data-Technologien auswerten können, wodurch ein bedrohlich anmutendes Überwachungspotential entsteht, welches das Grundrecht auf informationelle Selbstbestimmung immer weiter konterkariert.[74] Allerdings kodifiziert Art. 5 Abs. 1 lit. c) in der DSGVO das Prinzip der Datenminimierung, demzufolge personenbezogene Daten dem Zweck angemessen und erheblich sowie auf das für die Zwecke der Verarbeitung notwendige Maß beschränkt sein müssen, lit. e) normiert ferner eine Speicherbegrenzung. Zudem regelt Art. 5 Abs. 1 lit. b) Hs. 1 DSGVO eine Zweckbindung (welche auch schon im BDSG oder TMG geregelt ist) für die Erhebung personenbezogener Daten, welche für *festgelegte, eindeutige und legitime Zwecke erhoben* werden müssen und nicht in einer *mit diesen Zwecken nicht zu vereinbarenden*

[73] Faust (s.o. Fn. 65), S. 24.

[74] Siehe ausführlich zum Phänomen Big Data: Mayer-Schönberger, „Big Data: Die Revolution, die unser Leben verändern wird“, 2013, Redline Verlag.

Weise weiterverarbeitet werden dürfen.[75] Jedoch lockert die DSGVO in Art. 5 Abs. 1 lit. b) Hs. 2 die Zweckbindung für Weiterverarbeitungen für im öffentlichen Interesse liegende Archivzwecke, für wissenschaftliche oder historische Forschungszwecke oder für statistische Zwecke, die gemäß Art. 89 Abs. 1 DSGVO nicht als unvereinbar mit den ursprünglichen Zwecken gelten sollen. Greift diese Ausnahme nicht, muss die Vereinbarkeit mit dem Zweck der Datenerhebung im Einzelfall geprüft werden. Eine Weiterverarbeitung der Daten zu einem anderen Zweck als zu demjenigen, zu dem die personenbezogenen Daten erhoben wurden, kann zulässig sein, wenn dieser gem. Art. 6 Abs. 4 DSGVO mit dem ursprünglichen Zweck „vereinbar" ist.[76] Anhand eines „Kompatibilitätstests"[77] sind Faktoren wie die Verbindung zwischen den Zwecken, der Zusammenhang, in dem die personenbezogenen Daten erhoben wurden, die Art der personenbezogenen Daten, insbesondere ob besondere Kategorien personenbezogener Daten gemäß Artikel 9 EU-DSGVO verarbeitet werden, die möglichen Folgen für den Betroffenen sowie das Vorhandensein von geeigneten Garantien, wozu die DSGVO Verschlüsselung oder die Pseudonymisierung zählt, zu berücksichtigen. Wie weit der Zweckbindungsgrundsatz hierdurch aufgeweicht wird, wird u.a. daran zu messen sein, wie weit die Begriffe „festgelegt" und „eindeutig" aus Art. 5 Abs. 1 b EU-DSGVO ausgelegt werden.[78] In § 6 ABDSG-E regelt das BMI noch deutlich weitgehendere Möglichkeiten, personenbezogene Daten für einen anderen und auch mit dem Zweck der Erhebung unvereinbaren Zweck weiterzuverarbeiten, soweit kein Grund zu der Annahme besteht, dass das schutzwürdige

---

[75] Zur datenschutzrechtlichen Zweckbindung siehe Richter, „Datenschutz zwecklos? – Das Prinzip der Zweckbindung im Ratsentwurf der DSGVO", *Datenschutz und Datensicherheit* (2015), 735-740; von Grafenstein, „Das Zweckbindungsprinzip zwischen Innovationsoffenheit und Rechtssicherheit – Zur mangelnden Differenzierung der Rechtsgüterbetroffenheit in der Datenschutzgrund-VO, *Datenschutz und Datensicherheit* (2015), 789-795; Härting, „Zweckbindung und Zweckänderung im Datenschutzrecht" (2015), *Neue juristische Wochenschrift* (2015), 3284-3288; Monreal, „Weiterverarbeitung nach einer Zweckänderung in der DS-GVO – Chancen nicht nur für das europäische Verständnis des Zweckbindungsgrundsatzes", *Datenschutz und Datensicherheit* (2016), 507-512, S. 510 f.

[76] Gierschmann, „Was „bringt" deutschen Unternehmen die DS-GVO? Mehr Pflichten, aber die Rechtsunsicherheit bleibt, *Zeitschrift für Datenschutzrecht* (2016), 51-55, S. 54; Werkmeister/Brandt, „Datenschutzrechtliche Herausforderungen für Big Data", *Computer und Recht* (2016), 233-238, S. 237.

[77] Siehe Richter (s.o. Fn. 75), S. 739 f.; Buchner (s.o. Fn. 27), S. 157; Werkmeister/Brandt (s.o. Fn. 76), S. 237.

[78] Richter, (s.o. Fn. 75), S. 739; Buchner, (s.o. Fn. 27), S. 157; Schantz, (s.o. Fn. 18), S. 1843, der in der „eindeutigen" Festlegung des Zwecks einen Hinweis für ein enges Verständnis der Auslegung des ursprünglichen Zwecks erkennt.

Interesse der betroffenen Person an dem Ausschluss der Verarbeitung überwiegt. Hierdurch besteht die reelle Gefahr, dass der verfassungsrechtlich garantierte Grundsatz der Zweckbindung noch weiter ausgehöhlt wird.

IV. Betroffenenrechte und Informationspflichten

Von großer Bedeutung für die Durchsetzbarkeit des Verbraucherdatenschutzrechts sind die Betroffenenrechte.[79] Hierzu zählen u.a. das Auskunftsrecht nach Art. 15 DSGVO, das Recht auf Berichtigung gem. Art. 16 DSGVO, das Recht auf Löschung („Recht auf Vergessenwerden", Art. 17 DSGVO) sowie das Widerspruchsrecht gem. Art. 21 DSGVO.[80] Zudem normieren Art. 13 und 14 DSGVO strenge Informationspflichten der Verantwortlichen gegenüber den Betroffenen, welche zum Teil schon vor der Verarbeitung der Daten dem Betroffenen mitzuteilen sind. Dies ist auch notwendig, denn nach einer Studie der BayLDA erhalten Nutzer von IoT-Technologien in siebzig Prozent der Fälle entweder gar keine Informationen darüber, wie und wo ihre personenbezogenen Daten gespeichert werden noch wie die Daten wieder gelöscht werden können.[81] Das Auskunftsrecht aus Art. 15 DSGVO wird im Vergleich zur jetzigen Rechtslage u.a. um Auskunftspflichten über die geplante Speicherdauer der Daten oder über den Transfer von Daten in ein Drittland zusammen mit Angaben zu den geeigneten Garantien erweitert. Ferner hat der Verantwortliche dem Betroffenen gem. Abs. 3 auf Verlangen eine entgeltfreie Kopie aller verarbeiteten Daten zu überlassen. Zudem verlangt Art. 19 DSGVO, dass der Verantwortliche allen Empfängern, denen personenbezogenen Daten offengelegt wurden, jede Berichtigung oder Löschung der personenbezogenen Daten oder eine Einschränkung der Verarbeitung mitzuteilen hat (außer, wenn dies unmöglich oder mit einem unverhältnismäßigen Aufwand verbunden ist). Der Verantwortliche hat außerdem auf Verlangen der betroffenen Person diese über die Empfänger zu unterrichten. Nach Art. 17 Abs. 2 DSGVO muss ein Verantwortlicher, der personenbezogenen Daten öffentlich gemacht und zu deren Löschung er

---

[79] Spindler/Thorun/Wittmann (s.o. Fn. 5), S. 8.

[80] Siehe zu den Betroffenenrechten ausführlich Piltz, „Die Datenschutz-Grundverordnung – Teil 2: Rechte der Betroffenen und korrespondierende Pflichten des Verantwortlichen", *Kommunikation und Recht* (2016), 629-635.

[81] Bayerisches Landesamt für Datenschutzaufsicht, „Das Internet der Dinge: Internationale Prüfaktion deckt Mängel im Datenschutz auf", abrufbar unter: <https://www.lda.bayern.de/media/pm2016_06.pdf> (zuletzt abgerufen am 20. Oktober 2016).

verpflichtet ist, angemessene Maßnahmen treffen, um andere für die Datenverarbeitung Verantwortliche, die diese personenbezogenen Daten verarbeiten, darüber zu informieren, dass die Löschung aller Links oder von Kopien oder Replikationen hierzu verlangt wurde.

Einschränkungen für den Verbraucherschutz kann es allerdings zudem durch die Öffnungsklausel in Art. 23 DSGVO geben, wodurch die Betroffenenrechte noch an Kraft verlieren könnten. Das BMI hat von dieser Möglichkeit in seinen §§ 7 – 13 ABDSG-E schon Gebrauch gemacht. So regelt § 10 Abs. 2 ABDSG-E, dass das Recht auf Löschung nicht bestehen soll, wenn eine Löschung aufgrund der besonderen Art der Speicherung nicht oder nur mit unverhältnismäßigem Aufwand möglich ist. Hier besteht für Verbraucher die Gefahr, dass sich Unternehmen, gerade wenn sie große und komplizierte Datenmengen (Big Data) verarbeiten, regelmäßig auf den Einwand der Unverhältnismäßigkeit berufen werden. Ferner soll nach § 7 Abs. 2 ABDSG-E das Recht auf Information aus Art. 13 Abs. 3 DSGVO im Falle einer Weiterverarbeitung der personenbezogenen Daten zu einem anderen Zweck als den, für den diese Daten erhoben wurden, nicht bestehen, soweit die Erteilung der Information einen unverhältnismäßigen Aufwand erfordern würde. Auch dies würde eine Schwächung der Verbraucherrechte in Big Data-Szenarien bedeuten.

Art. 20 DSGVO schafft ferner ein neues Recht für Verbraucher, das „Recht auf Datenübertragbarkeit“. Die betroffene Person hat hiernach das Recht, die sie betreffenden personenbezogenen Daten, die sie einem Verantwortlichen bereitgestellt hat, in einem strukturierten, gängigen und maschinenlesbaren Format zu erhalten. Diese Daten darf sie einem anderen Verantwortlichen ohne Behinderung durch den Verantwortlichen, dem die personenbezogenen Daten bereitgestellt wurden, übermitteln, sofern die Verarbeitung auf einer Einwilligung oder auf einem Vertrag basiert und die Verarbeitung mithilfe automatisierter Verfahren erfolgt. Durch das Recht auf Datenübertragbarkeit sollen Verbraucher die Möglichkeit erhalten, mit dem Online-Profil eines sozialen Netzwerks mit einem einzigen Klick zu einem anderen Netzwerk umziehen zu können, wobei hier viele Fragen noch offen sind, etwa wie ähnlich sich die Portale sehen müssen.[82] Zudem muss auch das Ausschlusskriterium der „technischen Machbarkeit“ erst noch konkretisiert werden, ansonsten kann es Unternehmen,

[82] Jülicher/Röttgen/v. Schönfeld, „Das Recht auf Datenübertragbarkeit – Ein datenschutzrechtliches Novum“, *Zeitschrift für Datenschutzrecht* (2016), 358-362, S. 360.

die in Zeiten von Big Data große Datenmengen verarbeiten, zu leicht gemacht werden, sich auf den Einwand wirtschaftlicher Unverhältnismäßigkeit nach Abs. 2 zu berufen.[83] Abs. 4 schließt ferner das Recht auf eine direkte Datenübermittlung zwischen den Verantwortlichen aus, soweit Rechte und Freiheiten Dritter beeinträchtigt werden. Das Recht auf Datenübertragbarkeit ist mithin eine zu begrüßende Innovation der DSGVO, die dem Verbraucher davon befreien kann, all seine Daten manuell von einer Online-Plattform zur nächsten zu transferieren und die zudem für mehr Wettbewerb zwischen den verschiedenen Portalen und Netzwerken sorgen kann, was zumeist auch mehr Verbraucherschutz bedeutet. Fraglich sind allerdings noch viele Aspekte der technischen Machbarkeit der Datenportabilität, zudem muss im Sinne der Verbraucher dafür gesorgt werden, dass die verschiedenen Ausnahmen des Art. 20 DSGVO dieses Recht nicht zu sehr wieder einschränken.

V. Automatisierte Einzelentscheidung – Profiling

Der Begriff des Profilings wird in Art. 4 Nr. 4 DSGVO als jede Art der automatisierten Verarbeitung personenbezogener Daten, die darin besteht, dass personenbezogenen Daten verwendet werden, um bestimmte persönliche Aspekte zu bewerten, weit definiert. Dies umfasst insbesondere Analysen, Prognosen oder Vorhersagen bezüglich Arbeitsleistung, der wirtschaftlichen Lage, Gesundheit, persönlichen Vorlieben, Interessen, Zuverlässigkeit, Verhalten, Aufenthaltsort oder Ortswechsel der Betroffenen. Unter diese Definition fallen mithin auch das Scoring sowie das Screening.[84] Sofern ein solches Profiling rechtliche Wirkung für den Betroffenen entfaltet oder es ihn in ähnlicher Weise erheblich beeinträchtigt, ist dies nur unter den Voraussetzungen des Art. 22 DSGVO zulässig, was insgesamt dem Verbot automatisierter Einzelentscheidungen aus § 6a BDSG ähnelt. Gründe für eine Zulässigkeit sind etwa, dass die automatisierte Entscheidung für die Erfüllung eines Vertrags erforderlich ist oder wenn die betroffene Person hierzu ausdrücklich eingewilligt hat. EG 71 S. 1 DSGVO nennt als Beispiel für eine erhebliche Beeinträchtigung die automatische Ablehnung eines Online-Kreditantrags oder Online-Einstellungsverfahrens ohne jegliches menschliche Eingreifen, also den für Verbraucher sehr relevanten Bereich des Scorings. Die Nutzung besonderer Kategorien

[83] Jülicher/Röttgen/v. Schönfeld (s.o. Fn. 83), S. 360.

[84] Härting (s.o. Fn. 41), Rn. 607.

personenbezogener Daten (s.o. C.II.4.), etwa von Gesundheitsdaten, ist grundsätzlich untersagt, außer wenn eine ausdrückliche Einwilligung gegeben ist. Ferner dürfen keine personenbezogenen Daten von Minderjährigen für Profiling genutzt werden (EG 71 S. 5 DSGVO). Die Möglichkeit des Art. 22 Abs. 2 lit. c) DSGVO zur Einwilligung ist, verglichen mit der Datenschutz-RL und § 6a BDSG, allerdings eine Neuerung, durch welche, der informationellen *Selbstbestimmung* folgend, der Verbraucher grundsätzlich selbst entscheiden soll, wer seine Daten für automatisierte Zwecke nutzen darf.[85]

Nach EG 71 S. 6 DSGVO muss der für die Verarbeitung Verantwortliche der betroffenen Person gegenüber eine faire und transparente Verarbeitung gewährleisten und hierfür geeignete mathematische oder statistische Verfahren verwenden, die verhindern, dass es zu diskriminierenden Wirkungen oder Maßnahmen durch das Profiling kommt.[86] Art. 13 Abs. 2 lit. f) DSGVO schreibt zudem vor, dass Unternehmen den Verbrauchern zum Zeitpunkt der Datenerhebung aussagekräftige Informationen über die involvierte Logik sowie die Tragweite und die angestrebten Auswirkungen einer derartigen Verarbeitung für die betroffene Person zur Verfügung zu stellen haben. Zudem besteht für den Verbraucher nach Art. 15 Abs. 1 lit. h) DSGVO ein Auskunftsrecht bezüglich aussagekräftiger Informationen über die involvierte Logik einer automatisierten Entscheidungsfindung. Allerdings wird eine Offenlegung des der Entscheidung zugrundeliegenden Algorithmus in den meisten Fällen nicht erforderlich sein, da es sich hierbei häufig um Geschäftsgeheimnisse des Unternehmens handelt.[87] Diese

---

[85] Martini, in: Paal/Pauly (s.o. Fn. 38), Rn. 14 zu Art. 22 DS-GVO.

[86] EG 71 S. 6 DSGVO: „Um unter Berücksichtigung der besonderen Umstände und Rahmenbedingungen, unter denen die personenbezogenen Daten verarbeitet werden, der betroffenen Person gegenüber eine faire und transparente Verarbeitung zu gewährleisten, sollte der für die Verarbeitung Verantwortliche geeignete mathematische oder statistische Verfahren für das Profiling verwenden, technische und organisatorische Maßnahmen treffen, mit denen in geeigneter Weise insbesondere sichergestellt wird, dass Faktoren, die zu unrichtigen personenbezogenen Daten führen, korrigiert werden und das Risiko von Fehlern minimiert wird, und personenbezogene Daten in einer Weise sichern, dass den potenziellen Bedrohungen für die Interessen und Rechte der betroffenen Person Rechnung getragen wird und mit denen verhindert wird, dass es gegenüber natürlichen Personen aufgrund von Rasse, ethnischer Herkunft, politischer Meinung, Religion oder Weltanschauung, Gewerkschaftszugehörigkeit, genetischer Anlagen oder Gesundheitszustand sowie sexueller Orientierung zu diskriminierenden Wirkungen oder zu Maßnahmen kommt, die eine solche Wirkung haben."

[87] Vgl. BGH, Urteil vom 28. Januar 2014 – VI ZR 156/13 – SCHUFA; hiergegen wurde von der Klägerin Verfassungsbeschwerde eingereicht, BVerfG – 1 BvR 756/14 (anhängig); Kühling/Martini et al., „Die Datenschutz-Grundverordnung und das nationale Recht", 2016, Verlagshaus Monsenstein und Vannerdat

Relativierung entspricht auch EG 63 DSGVO, wonach die Auskunftsrechte „die Rechte und Freiheiten anderer Personen, etwa Geschäftsgeheimnisse oder Rechte des geistigen Eigentums und insbesondere das Urheberrecht an Software, nicht beeinträchtigen“ sollen. Diese Einschränkung darf jedoch nicht dazu führen, dass der betroffenen Person jegliche Auskunft verweigert wird. Es müssen mithin zumindest die Grundannahmen der Algorithmus-Logik mitgeteilt werden.[88] Dennoch besteht die Gefahr, dass den Verbrauchern zum größten Teil die Möglichkeit verwehrt bleiben wird, eine sachlich falsche Berechnung eines Scorewerts aufzudecken und zu korrigieren.[89] Auch wenn den Unternehmen ein Investitionsschutz für die Entwicklung der Scoring-Algorithmen grundrechtlich zuzustehen ist, bedarf der immer größer werdende Einfluss dieser Algorithmen über die Entfaltungschancen und auf das tägliche Leben der Verbraucher in der heutigen digitalen Welt im Hinblick auf deren informationelle Selbstbestimmung und die dafür eingesetzten Prognoseverfahren einer effektiven Kontrolle.[90] Eine Lösungsmöglichkeit wäre die Schaffung einer behördlichen Kontrolle der Algorithmen.[91]

Art. 22 Abs. 2 lit. b) DSGVO beinhaltet ferner eine Öffnungsklausel, hierdurch wird der deutsche Gesetzgeber allerdings nur ermächtigt, Entscheidungen nach Abs. 1 zu konkretisieren, nicht jedoch, Regelungen zur Art und Weise des Profilings zu schaffen, hierzu sollen nach EG 72 DSGVO die allgemeinen Grundsätze des Datenschutzrechts herangezogen werden, etwa die

---

OHG Münster, S. 66, abrufbar unter: <http://www.foev-speyer.de/files/de/downloads/Kuehling_Martini_et_al_Die_DSGVO_und_das_nationale_Recht_2016.pdf > (zuletzt abgerufen am 21. November 2016).

[88] Paal, in: ders./Pauly (s.o. Fn. 38), Rn. 31 zu Art. 13 DS-GVO.

[89] Vgl. Bräutigam/Schmidt-Wudy, „Das geplante Auskunfts- und Herausgaberecht des Betroffenen nach Art. 15 der EU-Datenschutzgrundverordnung – Ein Diskussionsbeitrag zum anstehenden Trilog der EU-Gesetzgebungsorgane“, *Computer und Recht* (2016), 56-63, S. 62; Schmidt-Wudy, in: Wolff/Brink, Beck'scher Online-Kommentar Datenschutzrecht, 17. Ed., Stand: 01. August 2016, C.H.Beck, Rn. 78.3 zu Art. 15 DSGVO, der sich für eine analoge Anwendung von Art. 15 Abs. 4 DSGVO ausspricht und somit nach einer Grundrechtsabwägung die strikte Geheimhaltung der Scoreformel nach der BGH-Rspr. in Einzelfällen als nicht mehr aufrechtzuerhalten ansieht, wenn die Kenntnis der Formel für die betroffene Person notwendig sei, um fehlerhafte Berechnungen festzustellen und korrigieren zu lassen.

[90] Vgl. Martini, „Big Data als Herausforderung für das Datenschutzrecht und den Persönlichkeitsschutz“, 2015, S. 28, abrufbar unter: <http://www.uni-speyer.de/files/de/Lehrst%C3%BChle/Martini/PDF%20Dokumente/Typoskripte/2015_Tagungsband_BigDataalsHerausforderungf%C3%BCrdasDatenschutzrecht.pdf> (zuletzt abgerufen am 25. Oktober 2016).

[91] Martini (s.o. Fn. 90), S. 29, der dies zumindest in den Fällen für geboten sieht, die sensible Auswirkungen in persönlichkeitssensitiven Bereichen zeigten.

„berechtigten Interessen“ nach Art. 6 Abs. 1 lit. f) DSGVO.[92] EG 47 a.E. DSGVO regelt hierzu, dass die Verarbeitung personenbezogener Daten zum Zwecke der Direktwerbung als eine einem berechtigten Interesse dienende Verarbeitung betrachtet werden. Im Entwurf des BMI für ein ABDSG werden die Befugnisse für Unternehmen im Bereich des Scorings im Vergleich zur DSGVO erweitert, so soll nach § 39 Abs. 3 ABDSG-E die Verarbeitung personenbezogener Daten als Mittel für die Erfüllung eigener Geschäftszwecke zulässig sein, wenn es für die Begründung, Durchführung oder Beendigung eines Schuldverhältnisses mit der betroffenen Person erforderlich ist, dies entspricht der Regelung des bisherigen § 28b BDSG. Zudem enthält § 39 Abs. 3 S. 2 ABDSG-E eine Zweckänderungsbefugnis beim Scoring für Big Data-Zwecke, die über die Vorgaben der DSGVO hinausgeht und ein massives Einfallstor für die Verarbeitung von personenbezogenen Daten zu Zwecken, die mit den ursprünglichen Zwecken nicht kompatibel wären, ermögliche könnte. Allerdings sprechen gewichtige Argumente dafür, dass dem nationalen Gesetzgeber mit der DSGVO gerade kein Spielraum mehr für eine Beibehaltung oder Neufassung des § 28b BDSG bleiben wird.[93]

VI. Zertifizierungen

Zertifikate können einen Marktanreiz für Unternehmen bieten, sich datenschutzfreundlich zu verhalten, in dem sie Transparenz und Vertrauen für die Datenverarbeitung bei Verbrauchern und gleichzeitig Wettbewerbsvorteile für die zertifizierten Dienste des Unternehmens schaffen.[94] Durch funktionierende Zertifizierungsmechanismen wird ferner eine effiziente Datenschutzprüfung von Anwendungen i.S. einer bewussten und geförderten Selbstregulierung der Datenverarbeiter gewährleistet.[95] EG 100 DSGVO betont die verbraucherschützende Wirkung von Zertifizierungsmaßnahmen: „Um die Transparenz zu erhöhen und die Einhaltung dieser Verordnung zu verbessern, sollte angeregt werden, dass Zertifizierungsverfahren sowie Datenschutzsiegel und -Prüfzeichen eingeführt werden, die den betroffenen Personen einen raschen Überblick über das Datenschutzniveau einschlägiger Produkte und Dienstleistungen

[92] Kamlah, in; Plath, (s.o. Fn. 17), Rn. 9 zu Art. 22 DSGVO.

[93] Siehe nur Kühling/Martini et al. (s.o. Fn. 87), S. 476 ff.

[94] Krings/Mammen, „Zertifizierungen und Verhaltensregeln - Bausteine eines modernen Datenschutzes für die Industrie 4.0“, *Recht der Datenverarbeitung* (2015), 231-236, S. 232.

[95] Krings/Mammen (s.o. Fn. 94), S. 232.

ermöglichen.“ Gem. Art. 42 Abs. 1 S. 1 DSGVO können Zertifizierungen dazu dienen, nachzuweisen, dass die Verordnung bei Verarbeitungsvorgängen von Verantwortlichen oder Auftragsverarbeitern eingehalten wird. Allerdings folgt wiederum aus Abs. 4, dass eine Zertifizierung nicht die Verantwortung des Verantwortlichen oder des Auftragsverarbeiters für die Einhaltung dieser Verordnung mindert. Zumindest bei der Genehmigung einer Zertifizierung wird allerdings wohl eine Selbstbindung der Verwaltung vorliegen.[96] Verstoßen der Verantwortliche oder der Auftragsverarbeiter gegen Pflichten aus Art. 42 DSGVO, können gegen diese nach Art. 83 Abs. 4 lit. a) DSGVO Geldbußen von bis zu 10.000.000 Euro oder bei Unternehmen von bis zu 2 % des gesamten weltweit erzielten Jahresumsatzes des vorangegangenen Geschäftsjahrs, abhängig davon, welcher der Beträge höher ist, verhängt werden. Dies betrifft gem. Art. 83 Abs. 4 lit. b) DSGVO auch die Zertifizierungsstelle.

VII. Datenschutzfreundliche Technikgestaltung als Königsweg für den Verbraucherschutz? Privacy by Design und Privacy by Default

Das Internet der Dinge mit seinen immer smarteren Geräten ist nur einer der Gründe, warum Datenschutz durch Technikgestaltung für Verbraucher einen immer höheren Stellenwert einnimmt. So verarbeiten etwa viele medizinische Geräte sensible Gesundheitsdaten (die nach Art. 9 DSGVO besonders geschützt sind) unverschlüsselt und schützen die informationelle Selbstbestimmung des Verbrauchers meist nur unzureichend, obwohl gerade hier der Schutz durch technische Maßnahmen besonders wichtig ist.[97] Art. 25 DSGVO regelt nun explizit den Datenschutz durch Technikgestaltung (Privacy by Design, Abs. 1) sowie durch datenschutzfreundliche Voreinstellungen (Privacy by Default, Abs. 2).

Nach Abs. 1 hat der Verantwortliche unter Berücksichtigung des Stands der Technik, der Implementierungskosten und der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere der mit der

---

[96] Spindler, „Selbstregulierung und Zertifizierungsverfahren nach der DS-GVO – Reichweite und Rechtsfolgen der genehmigten Verhaltensregeln“, *Zeitschrift für Datenschutzrecht* (2016), 407-414, S. 409, 412.

[97] Bayerisches Landesamt für Datenschutzaufsicht, „Das Internet der Dinge: Internationale Prüfaktion deckt Mängel im Datenschutz auf“, abrufbar unter: <https://www.lda.bayern.de/media/pm2016_06.pdf> (zuletzt abgerufen am 20. Oktober 2016).

Verarbeitung verbundenen Risiken für die Rechte und Freiheiten natürlicher Personen sowohl zum Zeitpunkt der Festlegung der Mittel für die Verarbeitung als auch zum Zeitpunkt der eigentlichen Verarbeitung geeignete technische und organisatorische Maßnahmen (siehe Art. 32 DSGVO), wozu etwa die Pseudonymisierung, Verschlüsselung oder Zugangs- und Zutrittskontrollen zu (Cloud-)Servern zu zählen sind, zu treffen, um die Datenschutzgrundsätze wie die Datenminimierung wirksam umzusetzen.[98] Art. 25 DSGVO nennt als Adressaten nur den Verantwortlichen der Datenverarbeitung, nach EG 78 DSGVO sollen jedoch gerade auch die Hersteller ermutigt werden, das Datenschutzrecht bei der Entwicklung und Gestaltung der Produkte, Dienste und Anwendungen zu berücksichtigen und unter Berücksichtigung des Stands der Technik sicherstellen, dass die Verantwortlichen und die Verarbeiter in der Lage sind, ihren Datenschutzpflichten nachzukommen. Diese Ermutigung ist zwar keine Verpflichtung für die Hersteller, allerdings kann sie dafür sorgen, dass der Markt so viel Druck erzeugt, dass Datenverarbeiter nur noch solche Produkte nachfragen werden, mit denen sie auch ihre Verpflichtungen aus Art. 25 DSGVO erfüllen können.[99]

Abs. 2 stellt schließlich Regelungen zu Privacy by Default auf. Der Verantwortliche hat demnach geeignete technische und organisatorische Maßnahmen zu treffen, die sicherstellen, dass durch Voreinstellung grundsätzlich nur personenbezogene Daten, deren Verarbeitung für den jeweiligen bestimmten Verarbeitungs*zweck erforderlich* ist, verarbeitet werden. Grundsätzlich soll der Verbraucher hiernach keine zusätzlichen Veränderungen an den Einstellungen vornehmen müssen, um den maximalen Datenschutz für die jeweilige Verarbeitung erreichen zu können.[100] EG 78 S. 3 DSGVO nennt als Maßnahmen für Privacy by Default etwa die Minimierung der Verarbeitung personenbezogener Daten, die schnellstmögliche Pseudonymisierung personenbezogener Daten, Herstellung von Transparenz in Bezug auf die Funktionen und die Verarbeitung personenbezogener Daten oder Möglichkeiten der Überwachung der Verarbeitung personenbezogener Daten durch die betroffenen Person. Die Wichtigkeit des Datenschutzes durch Voreinstellungen zur Ermöglichung der Datensparsamkeit der Verbraucher wird durch eine Studie verdeutlicht, wonach sich Verbraucher stark an Voreinstellungen orientieren und

[98] Plath (s.o. Fn. 17), Rn. 4 zu Art. 25 DSGVO.

[99] Plath (s.o. Fn. 17), Rn. 7 zu Art. 25 DSGVO.

[100] Plath (s.o. Fn. 17), Rn. 9 zu Art. 25 DSGVO.

viele diese bei einem Onlinedienst noch nie verändert haben.[101] Um die Durchsetzbarkeit dieser Regelungen zu ermöglichen und den Druck auf die Unternehmen zu erhöhen, diese verbraucherfreundlichen Grundsätze zu beachten, sind hohe Sanktionen bei Verstößen gegen die Grundsätze des Art. 25 DSGVO gem. Art. 83 Abs. 4 DSGVO möglich, zudem auch bei Verstößen gegen Art. 25 Abs. 3 DSGVO, sofern man diesem eine Dokumentationspflicht entnimmt. Privacy by Design und Privacy by Default können mit ihren Verpflichtungen für die Verantwortlichen sowie der unmissverständlichen Aufforderung an die Industrie, datenschutzfreundliche Technologien zu entwickeln, mithin gerade im Zeitalter des Internets der Dinge durchaus als Königsweg für den Verbraucherdatenschutz angesehen werden.

D. Abschließende Bewertung

Abschließend ist festzustellen, dass die DSGVO sinnvolle und teilweise auch innovative Regelungen bereithält, um den Datenschutz für Verbraucher weiter zu stärken. Mit Vorsicht zu genießen sind die vielen Öffnungsklauseln der Verordnung, durch welche die nationalen Gesetzgeber das Schutzniveau teilweise erheblich wieder einschränken können. Zudem ist fraglich, ob das Kopplungsverbot der Einwilligung, welches auf dem ersten Blick als großer Gewinn für Verbraucher erscheint, wirklich dem Verbraucherschutz dient oder nicht doch aufgrund der Rechtsunsicherheit für Unternehmen für ein „Sterben“ der Einwilligungen sorgen wird. Der weite Anwendungsbereich der Verordnung sorgt sowohl materiell als auch territorial, insbesondere durch das Marktortprinzip, dafür, dass viele Datenverarbeitungen, sogar von Unternehmen außerhalb der EU, die aber personenbezogene Daten von Verbrauchern in der Union verarbeiten, zukünftig vom Schutz der DSGVO umfasst sein werden.

Ferner ist es für den Verbraucherdatenschutz von elementarer Bedeutung, dass die Betroffenenrechte der Verbraucher auch in der Praxis durchsetzbar sind. Die DSGVO hat hier, auch in Verbindung mit den hohen Sanktionsdrohungen, eine Reihe neuer Regelungen geschaffen, die dem Verbraucher eine Vielzahl an neuen Rechten gibt, die er Unternehmen bei der Verarbeitung seiner personenbezogenen Daten entgegensetzen kann. Die Regelungen des ABDSG-E hierzu schaffen allerdings sehr viele Ausnahmen für Datenverarbeiter, sodass die

[101] Zit. nach Spindler/Thorun/Wittmann (s.o. Fn. 5), S. 23.

Gefahr besteht, dass die Errungenschaften der DSGVO wiederum durch die Hintertür deutlich beschränkt werden. Auch sind die umfassenden Informationspflichten der DSGVO auf dem ersten Blick ein Erfolg für den Verbraucherschutz, doch die praktische Umsetzbarkeit dieser Verpflichtungen ist in vielen Bereichen noch unklar. So sorgen immer längere zur Verfügung gestellte Informationen dafür, dass diese häufig nicht mehr gelesen werden, vor allem, wenn sie gleichzeitig mit AGB oder verbraucherschützenden Informationsvorschriften des E-Commerce bereitzustellen sind.[102] Verstöße gegen die Informationspflichten können für Unternehmen zukünftig allerdings erhebliche Geldbußen nach Art. 83 Abs. 5 DSGVO bedeuten, sodass nicht damit gerechnet werden kann, dass diese freiwillig auf den erheblichen Umfang der Erklärungen verzichten werden. Einen Ausweg könnte Art. 12 DSGVO bieten, demzufolge die Informationen in präziser, transparenter, verständlicher und leicht zugänglicher Form in einer klaren und einfachen Sprache zu übermitteln sind, insbesondere, wenn sie sich speziell an Kinder richten. Nach Abs. 7 können diese Informationen in Kombination mit standardisierten Bildsymbolen bereitgestellt werden, um leicht wahrnehmbar einen aussagekräftigen Überblick über die beabsichtigte Verarbeitung zu vermitteln. Hierdurch könnte das Problem der Informationsüberlastung für Verbraucher eingedämmt werden und eine Möglichkeit geschaffen werden, dass der Verbraucher die Informationen auch tatsächlich aufnimmt.[103]

Positiv ist, dass die DSGVO Verbrauchern ein Auskunftsrecht hinsichtlich der Logik von Algorithmen gibt. Dies sollte im Sinne des Verbraucherschutzes möglichst weit interpretiert werden. Die einer Auskunft entgegenstehenden Geschäftsgeheimnisse der diese Algorithmen nutzenden Unternehmen dürfen im Sinne des Verbraucherschutzes nicht dermaßen stark geschützt werden, dass das Auskunftsrecht schließlich doch leerläuft. Auch sind die Reformideen bezüglich einer Kommerzialisierung von personenbezogenen Daten und die damit einhergehenden neuen Rechte für Verbraucher als Erfolg zu sehen, da diese Daten in der Realität schon lange einen wirtschaftlichen Wert für Unternehmen darstellen.

---

[102] Jaspers, „Die EU-Datenschutz-Grundverordnung – Auswirkungen der EU-Datenschutz-Grundverordnung auf die Datenschutzorganisation des Unternehmens“, *Datenschutz und Datensicherheit* (2012), 571-575, S. 572.

[103] Paal, in: ders./Pauly (s.o. Fn. 38), Rn. 77 zu Art. 12 DS-GVO.

Wichtig ist schließlich auch, dass konsequent das Privacy by Design und Privacy by Default gefördert wird und gerade auch für die Hersteller neuartiger Technologien Anreize geschaffen werden, dies in ihre Produkte zu integrieren, etwa durch wirksame Verschlüsselungstechnologien. Auch die Selbstregulierung durch Zertifizierungen ist ein wichtiger Schritt, um mehr Rechtssicherheit für Verbraucher zu schaffen.

Sachverständigenrat für Verbraucherfragen

Der Sachverständigenrat für Verbraucherfragen ist ein Beratungsgremium des Bundesministeriums der Justiz und für Verbraucherschutz (BMJV). Er wurde im November 2014 vom Bundesminister der Justiz und für Verbraucherschutz, Heiko Maas, eingerichtet. Der Sachverständigenrat für Verbraucherfragen soll auf der Basis wissenschaftlicher Erkenntnisse und unter Berücksichtigung der Erfahrungen aus der Praxis das Bundesministerium der Justiz und für Verbraucherschutz bei der Gestaltung der Verbraucherpolitik unterstützen.

Der Sachverständigenrat ist unabhängig und hat seinen Sitz in Berlin.

Vorsitzende des Sachverständigenrats ist Prof. Dr. Lucia Reisch.

SVRV Sachverständigenrat für Verbraucherfragen