DATENHOHEIT UND DATENSCHUTZ IM ZUSAMMENHANG MIT SMART SERVICES

Smart Service Welt

Prof. Dr. Dr. Jürgen Ensthaler
Dr. Martin S. Haase

Das folgende Positionspapier wurde von der Begleitforschung des vom Bundesministerium für Wirtschaft und Energie geförderten Technologieprogramms „Smart Service Welt I“ erstellt und gibt die Meinung der Rechtsexperten wieder. Prof. Dr. Dr. Jürgen Ensthaler ist Inhabers des Lehrstuhls für Wirtschafts-, Unternehmens- und Technikrecht an der Technischen Universität Berlin, an dem Dr. Martin S. Haase als Hochschuldozent tätig ist. Beide Autoren sind als Juristen für Unternehmens- und Technikrecht in der Begleitforschung des Technologieprogramms in der Arbeitsgruppe „Rechtliche Herausforderungen“ tätig.

Impressum

Herausgeber
Begleitforschung Smart Service Welt I
iit-Institut für Innovation und Technik in der
VDI / VDE Innovation + Technik GmbH
Dr. Steffen Wischmann
Steinplatz 1
10623 Berlin
Steffen.Wischmann@vdivde-it.de

Texte
Prof. Dr. Dr. Jürgen Ensthaler
Dr. Martin S. Haase

Gestaltung
Loesch*Hund*Liepold Kommunikation GmbH
Hauptstraße 28
10827 Berlin

Bilder
Begleitforschung Smart Service Welt I

Stand
November 2017

Gefördert durch:

Bundesministerium
für Wirtschaft
und Energie

aufgrund eines Beschlusses
des Deutschen Bundestages

TEIL I: DIE VERFÜGUNGSBEFUGNIS ÜBER DATEN (DATENHOHEIT)

Einführung – Relevanz des Umgangs mit Daten für Smart Services

Die Digitalisierung und die damit verbundenen Möglichkeiten, Mitteilungen über das Internet zu übertragen, haben dazu geführt, dass ständig Daten über die Art und Weise der Nutzung von Maschinen und anderen technischen Einrichtungen, Daten über die Abnutzung oder die Wartungsbedürftigkeit, über die Nutzergewohnheiten und die bei Anfragen übermittelten Informationen und vieles mehr an den Hersteller oder Dienstleister übermittelt werden. Diese Daten sind wertvoll. Sie geben Auskunft über die Nutzungsarten, die Konsumentenbedürfnisse, die Reparaturanfälligkeiten, die Wartungserfordernisse oder über Verbesserungspotentiale etc. Die Europäische Kommission ist in ihrer Strategie für einen digitalen Binnenmarkt der Auffassung, dass diese Daten zu einem Wirtschaftsgut geworden sind.[1] Damit sind dann auch die Fragen verbunden, wem die Daten gehören und wer die Nutzungsbefugnis hat. Diese Fragen sind bis heute unbeantwortet.

Die gegenständlichen Daten werden von den Kunden des Diensteanbieters oder des Herstellers – Endverbraucher oder Unternehmen – im Zusammenhang mit der Nutzung oder Bearbeitung generiert. Man könnte meinen, dass es dann auch ihre Daten sind. Der Hersteller oder auch Dienstleister hat aber regelmäßig die technischen Voraussetzungen für die Übermittlung der Daten und deren Speicherung in seiner Datenbank geschaffen: Er hat in die Übermittlung und Systematisierung der Daten investiert. Diese könnten daher auch seine Daten sein.

Für Smart Services ist die Frage nach der Datenhoheit, also nach der Berechtigung, von dritter Seite generierte bzw. übermittelte Daten nutzen zu dürfen, von herausragender Bedeutung. Daten sind in einem bedeutsamen Umfang die Grundlage von Geschäftsmodellen und der Entwicklung und Weiterentwicklung von technischen Einrichtungen. Das auf diese Daten angewiesene Unternehmen muss Rechtssicherheit hinsichtlich der erlaubten Verwendung seiner Arbeitsgrundlagen haben.

1 Commission Staff Working Document, A Digital Single Market Strategy for Europe – Analysis and Evidence, SWD (2015) 100 final, 59.

Der erste Teil der Publikation befasst sich nur am Rande mit personenbezogenen Daten.[2] Soweit aufgrund der übermittelten Daten natürliche Personen bestimmt oder bestimmbar sind, entscheidet über die Verwendung der Daten nach dem Bundesdatenschutzgesetz (BDSG) wie auch nach der europäischen Datenschutzgrundverordnung[3] bei Nichtgreifen einer gesetzlichen Erlaubnisnorm grundsätzlich die betroffene Person (vgl. §§ 4 I und 3 I BDSG). Der personenbezogene Datenschutz wird im zweiten Teil der Publikation behandelt.

Welche Daten sind gemeint? – Konkretisierung des Datenbegriffs

Unter „Daten" werden in diesem Teil der Publikation Informationen ohne Personenbezug bzw. anonymisierte Daten verstanden, die nicht oder nicht ausreichend derart bearbeitet wurden, dass sie den Schutzbereich von Immaterialgüterrechten, wie insbesondere das Patent- oder Urheberrecht, erreichen. Umgangssprachlich formuliert handelt es sich bei Daten um virtuelle Rohmaterialien, deren Zuordnung zu einer Person oder einem Unternehmen nicht durch ein besonderes Schutzrecht geregelt ist.

Im Folgenden sollen die Lösungsansätze für die Zuordnung der Daten vorgestellt werden, die in der Diskussion sind. Dies ist insbesondere für Jungunternehmen bzw. Start-ups von großer Bedeutung, weil diese Lösungsansätze nur unter Beachtung bestimmter Voraussetzungen tauglich sind und weil die Ansätze vielfach nur Scheinlösungen bieten.

Zuordnung über das Vertragsrecht

Die Frage nach der Nutzungsmöglichkeit und der dafür zu erbringenden Gegenleistung wird vielfach in Verträgen geregelt. Damit ist aber nicht die Frage beantwortet, wem die Daten ursprünglich zugeordnet sind, also wem sie gehören. Für die Vertragsgestaltung hat diese Frage zweifache Bedeutung: Es wird nur derjenige eine Gegenleistung erbringen, der etwas erhält, was ihm bislang nicht gehört. Bei den Vertragsregelungen wird es sich zudem regelmäßig

2 Zu den datenschutzrechtlichen Aspekten s. Reiter/Methner, InTeR 2015, 29 (32 ff.).

3 VO (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27.04.2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der RL 95/46/EG (Datenschutz-Grundverordnung), Inkrafttreten: 2018.

um allgemeine Geschäftsbedingungen handeln und für eine Inhaltskontrolle ist die ursprüngliche Zuordnung der Datenhoheit ein wichtiges Kriterium für die Wirksamkeit der vertraglichen Regelungen. Die im Vertrag festgelegten allgemeinen Geschäftsbedingungen werden dementsprechend zum Schutz beider Vertragsparteien einer gesetzlichen Kontrolle unterzogen. Sollte festgestellt werden, dass die Daten dem Nutzer gehören, so wird zumindest eine unentgeltliche Übernahme durch den Hersteller einer Inhaltskontrolle nach dem BGB nicht standhalten. Wenn das Nutzungsrecht an den Daten durch einen Vertrag begründet werden soll, so ist regelmäßig eine Gegenleistung zu vereinbaren. Die braucht nicht unbedingt in Geld zu bestehen. Die Partizipation an bestimmten Verwertungsergebnissen kann reichen.

Urheberrechtlicher Datenbankschutz

Sehr häufig wird dahingehend argumentiert, dass die Daten wegen ihrer Einstellung in die Datenbank des Herstellers oder Diensteanbieters dann auch im Zusammenhang mit dem Datenbankrecht (§ 87a UrhG) geschützt werden.

Dieser Schutz bezieht sich aber nicht auf die noch zu erhebenden und entsprechend einzuordnenden Daten. Deren Schutz ist nicht in den Schutz der Datenbankstruktur einbezogen. Der EuGH[4] hat dies gerade auf der Grundlage eines Vorlagebeschlusses des BGH[5] bestätigt.

Die Europäische Datenbankrichtlinie (96/9) bestimmt auch ausdrücklich, dass der Schutz nicht auf die Inhalte, also gerade nicht auf die eingebrachten Daten, bezogen ist. Dies ist im Hinblick auf die Begründung des Schutzes selbstverständlich. Es soll durch dieses im Urheberrechtsgesetz aufgeführte Leistungsschutzrecht nicht erreicht werden, dass die in eine Sammlung aufgenommenen Daten/Informationen selbst einen Schutz erfahren, nur weil sie für die jeweils gegenständliche Sammlung tauglich waren.

Es verhält sich auch nicht so, dass die fremdbezogenen Daten durch die Struktur oder die Gliederung der Datenbank geschützt wären oder dass ein Eingriff in das Datenbankrecht vorliegen würde, wenn die dort eingeordneten Daten ganz oder doch in einem schon erheblichen Umfang entnommen werden würden. Das Datenbankrecht kann nur in dem Umfang schützen, wie der Datenbankersteller auch die Nutzungsrechte an den eingebrachten Daten hat; und genau deshalb hat der EuGH in der oben zitierten Entscheidung auch die noch zu erhebenden Daten vom Schutzbereich ausgenommen.

Das Datenbankrecht beantwortet nicht die Frage nach der Berechtigung an den einzelnen Daten; das gehört nicht zu seinem Normzweck.

Schutz der Daten als Betriebsgeheimnis

Die Daten sind auch nicht als Geschäftsgeheimnis für den Hersteller der Erfassungseinrichtungen geschützt. Der Geheimnisschutz nach § 17 UWG wie auch der Geheimnisschutz nach dem europäischen Richtlinienentwurf hat zur Voraussetzung, dass die entsprechenden Informationen dem Unternehmen zuzuordnen sind. Im Richtlinienentwurf steht, dass der „Inhaber des Geschäftsgeheimnisses" geschützt wird.[6] Solange die Frage nach der Berechtigung offen ist, greift der Geheimnisschutz ins Leere.

Kein Schutzrecht vorhanden – Folgerungen: Was wird kommen?

Leistungsschutzrechte, die Informationen als solche schützen, sind nicht vorhanden.

Wahrscheinlich wird die Europäische Kommission darauf hinwirken, dass ein besonderes Recht für die Datenhoheit geschaffen wird, ein Leistungsschutzrecht, wie es zahlreich für Bereiche geschaffen wurde, die dadurch gekennzeichnet sind, dass technische Neuerungen eine Übernahme von Leistungen ermöglichen, ohne dass der diese Technik einsetzende Unternehmer zumindest der alleinige Nutznießer sein soll.

4 EuGH, ECLI:EU:C:2015:735 = GRUR 2015, 1187 = EuZW 2015, 955 mit Anm. Czychowski, EuZW 2015, 957 – Verlag Esterbauer.

5 BGH, GRUR 2014, 1197 = NJW 2015, 816 Ls. – TK 50.

6 Art. 2 I Buchst. C des Richtlinienentwurfs; dazu unter Nennung weiterer entsprechend regelnder Quellen Zech, GRUR 2015, 1151 (1155).

Rechtliche Grundlagen für ein neues Leistungsschutzrecht für Daten

Eine Vorbildfunktion hat hier der § 950 BGB, der die Rechtsfolgen der Bearbeitung eines Rohstoffs bzw. die der Weiterbearbeitung eines Produkts regelt. Der Bearbeiter erwirbt das Eigentum, soweit nicht der Wert der Bearbeitung geringer als der des Stoffs ist. Die Norm bezieht sich nur auf Sachen; die der Norm zugrundeliegenden Wertungen können aber auch bei den Daten zur Anwendung kommen. Bei den hier gegenständlichen Informationen handelt es sich um „Rohmaterialien", um unbearbeitete Informationen, „Rohinformationen", mit denen etwas geschieht. Sie werden systematisiert, sie werden für bestimmte Zwecke geordnet.

Der Normzweck von § 950 BGB ist dann auch darauf gerichtet, dem Bearbeiter das Verfügungsrecht über die bearbeitete Sache zuzuweisen.

Das ist interessengerecht, soweit man nachvollziehen will – und wohl auch sollte –, dass eine ins Gewicht fallende, für eine Nutzung des Ausgangsstoffs bedeutsame Bearbeitung wohl dem am besten nützt, der entsprechend bearbeitet hat bzw. das Ergebnis der Bearbeitung entsprechend nutzen will. Den Eigentumsverlust durch Bearbeitung/Verarbeitung regeln auch alle europäischen Sachenrechtsordnungen.[7]

Die Frage, wer Bearbeiter und wer Lieferant der Daten ist, lässt sich leicht feststellen: Bearbeiter ist das Unternehmen, das die technischen Vorrichtungen zur Erfassung und Übermittlung der Daten geschaffen hat und die Daten systematisiert; der Nutzer, der die Daten generiert, liefert das Rohmaterial. Regelmäßig wird es sich so verhalten, dass die Datengenerierung ohne gesonderten Aufwand erfolgt, und weiterhin wird man regelmäßig dahingehend urteilen können, dass der Wert der Rohdaten erst durch die vorbereitende Bearbeitung wertvoll wird: Die vorbereitende Bearbeitung schafft erst die semantische Ebene.

7 Krimphove, Das europäische Sachenrecht, 2006, 450. Nach britischem Recht erwirbt der Verarbeiter das Eigentum, wenn die verarbeitete Sache nicht mehr mit der Ausgangssache identisch ist und auch nicht mehr zurückversetzt werden kann.

Neues Leistungsschutzrecht: Regelungsbereiche

Der rechtlichen Einordnung nach würde es sich bei einem dem Normzweck von § 950 BGB entsprechenden Recht um ein Leistungsschutzrecht handeln. Belohnt wird nicht die neue technische Idee oder eine geistige persönliche Schöpfung, sondern der für die Erhebung der Daten erforderliche Aufwand im gewerblichen Bereich. Geschaffen würde auch nicht ein Ausschließlichkeitsrecht an Daten der entsprechenden Art. Jedermann dürfte entsprechende Daten erheben und verwerten; verboten wäre die Entnahme der bzw. einzelner Daten aus der Sammlung.

Von einem bereits vorhandenen Leistungsschutzrecht, dem urheberrechtlichen Datenbankrecht, würde sich das neue Leistungsschutzrecht unterscheiden, weil es hier um den Schutz der Daten selbst geht, und nicht um den Schutz der Struktur, nach der die Daten geordnet sind. Begrenzt wäre dieses Recht durch die Voraussetzung, dass die Informationsgenerierung vom Hersteller der benutzten technischen Einrichtung vorbereitet wurde.

Das noch zu lösende Problem ist die Bestimmung des Wertausgleichs. Wie ist der generierende Kunde zu entlohnen? Nicht richtig wäre es, den Wert der Daten danach zu bestimmen, in welchem Umfang sie dem Hersteller/Diensteanbieter für seine Planungen von Wert sein könnten; ebenso falsch wäre es, den Wert danach zu bestimmen, welche Gegenleistung auf dem Markt – soweit er besteht – zu erlangen wäre. Solche Berechnungen sind für das Sacheigentum von Bedeutung, wegen der durch die Körperlichkeit gegebenen Exklusivität. Bei den Leistungsschutzrechten wird diese Exklusivität gerade nicht geschaffen. Daten könnten von jedermann erhoben werden, und jeder könnte sie entsprechend strukturiert erheben. Dies hat auch für den gegenständlichen Ausgleichsanspruch Bedeutung. Dieser Anspruch ist am Aufwand im Zusammenhang mit der Datenerhebung zu messen und dürfte gering ausfallen, weil die Daten regelmäßig „nebenbei", bei zweckentsprechender Nutzung der Maschine, erhoben werden. Eine sachgerechte Preisfindung wäre über einen Vergleich zu den Kosten für die Speicherung von Datenmengen bei Dritten angezeigt.

Es wird sich zudem in vielen Fällen so verhalten, dass dem die Daten generierenden Nutzer bzw. dem Datengeber

unmittelbar dadurch Vorteile zukommen und dies auch erkennbarer Gegenstand des Geschäftsmodells ist. Dann wäre die Frage nach der Gegenleistung dadurch beantwortet.

Von mehreren Unternehmen gemeinsam unterhaltene Datensammlungen – Rechtegemeinschaften

Ein Phänomen der Digitalisierung ist das verstärkte Zusammenwirken der Unternehmen gerade im Zusammenhang mit der Verwendung von Daten. Daten verschiedener Unternehmen werden zusammengeführt und für unterschiedliche Zwecke verwendet. Soll es eine Berechtigung an Daten geben, muss auch geklärt werden, wie in einer Rechtegemeinschaft die Nutzungsrechte geregelt sein sollen.

Leistungsschutzrechte orientieren sich, wo immer dies möglich ist, an den klassischen Schutzrechten, also am Patent- und Urheberrecht. Beiden Rechtsgebieten ist in diesem Zusammenhang gemein, dass die rechtliche Ausgangslage die Bruchteilsgemeinschaft ist. Eine Gesamthand entsteht nur, wenn das Werk in „gewollter schöpferischer Zusammenarbeit" geschaffen wurde.[8]

Daten des einen Unternehmens, die mit den Daten anderer Unternehmen verlinkt/vermengt werden, berechtigen jedes beteiligte Unternehmen zur Eigennutzung, insofern besteht bei der Bruchteilsgemeinschaft kein Zustimmungserfordernis.[9]

Die Eigennutzung bezieht sich dann auch auf die mit den jeweils eigenen Daten vermengten Daten der anderen Unternehmen. Wie der BGH zutreffend für das Patentrecht ausgeführt hat, wäre es andernfalls keinem Teilhaber möglich, ohne Zustimmung des anderen eine Nutzung vorzunehmen.

Empfehlungen

1. Solange es kein neues Leistungsschutzrecht gibt, sollte im Zusammenhang mit der Nutzung von dritter Seite generierter bzw. übermittelter Daten eine vertragliche Regelung vereinbart werden, die die Nutzung der Daten erlaubt und dabei auch eine Gegenleistung vorsieht, soweit die Daten nicht unmittelbar für den Übermittler allein oder in spürbarem Ausmaß für ihn von Vorteil sind. Die Gegenleistung braucht nicht in Geld zu bestehen.

2. Soweit mehrere Unternehmen gemeinsam Daten nutzen, sollte es zur Vermeidung von Streitfällen zumindest eine Vereinbarung darüber geben, was unter „Eigennutzung" zu verstehen ist (zu der jede Partei berechtigt ist). Es sollte festgelegt werden, wie jede Partei ohne weitere Zustimmung einer anderen Partei die Daten verwerten darf.

8 Vgl. Thum, in: Wandtke/Bullinger, UrhR, § 8 UrhG Rn. 16.
9 BGHZ 162, 342 = NJW-RR 2005, 1200 = GRUR 2005, 663 – Gummieelastische Masse II.

Wem gehören welche Daten?

Datenhoheit und personenbezogener Datenschutz bei Smart Services

Nutzung von Daten

ENTSTEHUNG
Generierung von Daten

VERARBEITUNG
Sammlung und Aufbereitung zu Smart Data

BEREITSTELLUNG
Smart Service wird über Plattform bereitgestellt

Rechtliche Fragestellungen

Datenhoheit

ZENTRALE FRAGESTELLUNG
Wer hat die Verfügungshoheit über welche Daten? Wie muss der Anbieter eines Smart Services diejenigen entschädigen, die ihre Daten zur Verfügung stellen, die einen Smart Service ermöglichen?

LÖSUNGSANSATZ
Anbieter von Smart Services sollten eine vertragliche Regelung aufsetzen, die die Nutzung benötigter Daten regelt. Die Regelung sollte eine entsprechende Gegenleistung vorsehen, die nicht finanziell sein muss. Nutzen mehrere Unternehmen gemeinsam Daten, sollte festgelegt werden, wie jede Partei ohne weitere Zustimmung einer anderen Partei Daten verwerten darf.

KLÄRUNGSBEDARF FÜR DEN GESETZGEBER
Ein neues Leistungsschutzrecht, das die Frage der Datenhoheit im Zusammenhang mit Smart Services verbindlich und einheitlich regelt.

Personenbezogener Datenschutz

ZENTRALE FRAGESTELLUNG
Wie können Smart Services erzeugt und angeboten werden, die auf der Einbindung personenbezogener Daten setzen, ohne dabei das Grundrecht auf informationelle Selbstbestimmung zu verletzen?

LÖSUNGSANSATZ
Es kann durch Mittel der Anonymisierung gewährleistet werden, dass die einzelne natürliche Person nicht identifiziert werden kann. Ist eine Anonymisierung nicht möglich, muss die Person ihre Einwilligung geben – es sei denn, es liegt ein höheres allgemeines Interesse vor (Erlaubnisnorm).

KLÄRUNGSBEDARF FÜR DEN GESETZGEBER
- Eine Konkretisierung des Datenschutzrechtes durch eine stärkere Eingrenzung des Merkmals „natürliche Person“.
- Eine Konkretisierung der Beurteilungskriterien, wann Instrumente zur Identifizierung einer natürlichen Person „nach allgemeinem Ermessen“ „wahrscheinlich“ genutzt werden.
- Konkretisierung der datenschutzrechtlichen Verantwortlichkeit für den immer häufigeren Fall, dass mehrere Akteure unternehmensübergreifend Daten verarbeiten.

TEIL II: SCHUTZ PERSONENBEZOGENER DATEN

Die Frage nach dem rechtlichen Schutz personenbezogener Daten ist vom Bereich der Datenhoheit abzugrenzen. Die entsprechenden Regelungen des Datenschutzrechtes dienen nicht der Feststellung, wem Nutzungsrechte an Daten zustehen. Der Schutz personenbezogener Daten verfolgt vielmehr das Ziel, das Grundrecht auf informationelle Selbstbestimmung und die persönliche Freiheit des Einzelnen zu gewährleisten.[10] Zur Erreichung dieses Ziels schränkt das Datenschutzrecht die Verarbeitungsmöglichkeiten in Bezug auf personenbezogene Daten ein. Dadurch sollen u. a. ein Missbrauch von personenbezogenen Daten und die Diskriminierung Einzelner verhindert werden.[11]

Der Umgang mit Daten und Informationen im Rahmen von Smart Services ist sehr vielfältig und unterliegt einer ständigen Fortentwicklung. Durch die intensive Einbindung des Menschen als Nutzer und Akteur kommt es in diesem Kontext häufig zur Verarbeitung personenbezogener Daten, d. h. von Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person beziehen. Eingesetzt werden Smart Services u. a. im Bereich der Mobilität, in verschieden Alltagssituationen (z. B. „Smart Home") und in der intelligenten Produktion.[12] Dabei spielen teilweise Standorte, Eigenschaften, Gewohnheiten und individuelle Bedürfnisse einzelner Menschen eine bedeutende Rolle (z. B. Fahrroute des vernetzten Kraftfahrzeuges, Lebensmittelbedarf eines Kühlschrankinhabers oder Gesundheitszustand eines App-Nutzers).

Kommt es im Rahmen eines Smart Service zu einem Verstoß gegen das Datenschutzrecht, drohen dem Verantwortlichen Strafen, Bußgelder und die Geltendmachung von Ansprüchen durch Betroffene oder dritte Stellen. Um Haftungsrisiken einschätzen und minimieren zu können, sind für einen Smart-Service-Betreiber neben der Frage nach dem Ausmaß der Haftungsrisiken in der Regel drei Fragenkomplexe besonders relevant:

1. Auf welche Verarbeitungsprozesse im Rahmen von Smart Services ist das Datenschutzrecht anwendbar?
2. Wer ist für einen Verarbeitungsprozess datenschutzrechtlich verantwortlich?
3. Wie kann im Fall der Anwendbarkeit und Verantwortlichkeit eine rechtliche Zulässigkeit gewährleistet werden?

Konkret können sich daraus z. B. die beiden folgenden Einzelfragen ergeben:

1. Wann sind Informationen über ein Kraftfahrzeug gleichzeitig Informationen über eine natürliche Person, so dass das Datenschutzrecht sachlich anwendbar ist?
2. Inwieweit ist ein Smart-Service-Betreiber, der über Privatpersonen personenbezogene Daten Dritter erlangt, dafür verantwortlich, dass die personenbezogenen Daten rechtmäßig erhoben worden sind?

Vor dem beschriebenen Hintergrund sollen im Folgenden ausgewählte datenschutzrechtliche Aspekte kritisch hinterfragt und fortentwickelt werden. Dabei liegt der Schwerpunkt auf der Analyse der gesetzlichen Ausgestaltung des sachlichen Anwendungsbereiches und den gesetzlichen Kriterien zur Festlegung der datenschutzrechtlichen Verantwortlichkeit. Aus den Ausführungen werden – soweit ausfüllbare Lücken vorhanden sind – Vorschläge für den Gesetzgeber hergeleitet.

Die Datenschutz-Grundverordnung

Derzeit ist das allgemeine Datenschutzrecht in der Bundesrepublik Deutschland auf Bundesebene im Bundesdatenschutzgesetz (BDSG) und auf Länderebene in dem jeweiligen Landesdatenschutzgesetz (LDSG) geregelt. Ab dem 25. Mai 2018 gilt EU-weit die Datenschutz-Grundverordnung.[13] Als Verordnung gelten ihre Regelungen in den Mitgliedstaaten – u. a. der Bundesrepublik Deutschland – unmittelbar. Dies hat zur Folge, dass die bisher geltenden gesetzlichen Grundlagen des Datenschutzrechts weitgehend reformiert werden. Vor diesem Hintergrund soll sich die Darstellung auf die neue Rechtslage konzentrieren.

10 Vgl. van Lewinski, in: Auernhammer, DSGVO BDSG, 5. Auflage 2017, Einführung, Rn. 15 ff.

11 Vgl. Haase, Datenschutzrechtliche Fragen des Personenbezugs, 2015, S. 113 ff.; van Lewinski, in: Arndt u. a., Freiheit – Sicherheit – Öffentlichkeit, S. 196 ff. (199).

12 BMWi, Smart Service Welt, Innovationsbericht 2017, Eine Studie im Rahmen der Begleitforschung zum Technologieprogramm Smart Service Welt.

13 Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27.04.2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung).

Der Anwendungsbereich der Datenschutz-Grundverordnung

Aufgrund der relativ strengen datenschutzrechtlichen Vorschriften (z. B. Verbot mit Erlaubnisvorbehalt, vgl. Art. 6 DSGVO) ist die Frage nach der Anwendbarkeit der Datenschutz-Grundverordnung besonders praxisrelevant.[14] Von der Anwendbarkeit hängt ab, ob die datenschutzrechtlichen Grundsätze und Pflichten zu beachten sind.

Hinsichtlich der Anwendbarkeit der Datenschutz-Grundverordnung kann auch in Zukunft zwischen einem „persönlichen", einem „sachlichen" und einem „räumlichen" Anwendungsbereich unterschieden werden. Diese Unterscheidung findet sich teilweise ausdrücklich im Verordnungstext (Art. 2 und Art. 3 DSGVO) und ergibt sich darüber hinaus aus der Gesetzessystematik.

1. Persönlicher Anwendungsbereich

Die Datenschutz-Grundverordnung gilt sowohl für öffentliche als auch für nichtöffentliche Stellen. Dies lässt sich aus Art. 2 DSGVO ableiten. Eine große Anzahl von Smart Services wird von privatwirtschaftlichen Unternehmen betrieben. Diese sind in der Regel den nichtöffentlichen Stellen zuzuordnen. Aber auch unter den öffentlichen Stellen (z. B. ein Krankenhaus, das sich in der Trägerschaft eines Bundeslandes befindet) wächst die Zahl der Betreiber und Anbieter von Smart Services.

2. Sachlicher Anwendungsbereich

Bisher unzureichend gelöst ist die Festlegung des sachlichen Anwendungsbereichs. Durch den technischen Fortschritt wird diese Herausforderung zunehmend verschärft.[15]

Abgrenzungsschwierigkeiten im Rahmen von Smart Services ergeben sich insbesondere durch die Verknüpfung und „Veredelung" verschiedenster Daten aus unterschiedlichen Quellen sowie die Einbeziehung unterschiedlichster Akteure. Insbesondere hinsichtlich des Vorliegens personenbezogener Daten – bei dem es sich um eines der umstrittensten Merkmale des Datenschutzrechts handelt – ist auch zukünftig eine sorgfältige und vertiefte Analyse erforderlich.[16]

Nach Art. 2 Abs. 1 DSGVO gilt die Datenschutz-Grundverordnung für die ganz oder teilweise automatisierte Verarbeitung personenbezogener Daten. Für die nichtautomatisierte Verarbeitung personenbezogener Daten gilt die DSGVO nur, wenn die Daten in einem Dateisystem gespeichert sind oder gespeichert werden sollen.

a) Vorliegen personenbezogener Daten

Die Legaldefinition für das Merkmal „personenbezogene Daten" wurde im Rahmen der DSGVO im Vergleich zur Datenschutzrichtlinie 94/46/EG nur leicht abgewandelt. Nach Art. 4 Nr. 1 DSGVO bezeichnet der Ausdruck „personenbezogene Daten" im Sinne der Datenschutz-Grundverordnung alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person beziehen.[17]

aa) Informationen, die sich auf eine natürliche Person beziehen

Das Datenschutzrecht ist auf sämtliche Informationen anwendbar, „unabhängig von der jeweiligen Semantik, Sigmatik, Pragmatik, Darstellungsart, Darstellungsform und Herkunft."[18] Darunter fallen auch Prognosedaten und Wahrscheinlichkeitsberechnungen. In die datenschutzrechtliche Betrachtung von Prozessen, die im Zusammenhang mit Smart Services stehen, sind also zunächst alle Daten- und Informationsverarbeitungen einzubeziehen.

Durch die DSGVO werden nach wie vor ausschließlich natürliche Personen geschützt.[19] Gerade die Auslegung der Voraussetzung „natürliche Person" wurde bisher nicht ausreichend zur Abgrenzung des sachlichen Schutzbereiches herangezogen.[20] Diese Voraussetzung bringt zum Ausdruck, dass die Schutzbedürftigkeit in erster Linie aus dem Bezug zum einzelnen individuellen Menschen resultiert.[21] Es darf nicht verkannt werden, dass über das Merkmal der „natürlichen Person" gerade im Zusammenhang mit der

14 Vgl. Krügel, ZD 2017, 455, 455.
15 Vgl. Haase, Datenschutzrechtliche Fragen des Personenbezugs, 2015, S. 59 ff.
16 Haase, Datenschutzrechtliche Fragen des Personenbezugs, 2015; Krügel, ZD 2017, 455.
17 Art. 2 lit. a) DSRL lautet: „alle Informationen über eine bestimmte oder bestimmbare natürliche Person.".
18 Haase, Datenschutzrechtliche Fragen des Personenbezugs, 2015, S. 453; siehe hierzu auch Klar/Kühling, in: Kühling/Buchner, DSGVO, 2017, Art. 4 Nr. 1, Rn. 8 ff.
19 Klar/Kühling, in: Kühling/Buchner, DSGVO, 2017, Art. 4 Nr. 1, Rn. 3; Schreiber, in: Plath, BDSG/DSGVO, 2016, Art. 4, Rn. 5.
20 Vgl. Haase, Datenschutzrechtliche Fragen des Personenbezugs, 2015, S. 187 ff.
21 Als Definition wird vorgeschlagen: „Eine natürliche Person ist jeder lebende Mensch in allen seinen Handlungen und Wesenszügen, die dessen Individualität zum Ausdruck bringen und ihm somit das Bewusstsein geben, trotz räumlicher und zeitlicher Veränderungen ein- und derselbe zu sein.", Haase, Datenschutzrechtliche Fragen des Personenbezugs, 2015, S. 453.

zunehmenden Digitalisierung, Virtualisierung und Vernetzung eine Ausuferung des Anwendungsbereiches verhindert werden kann.

Denn schließlich muss sich die Information auf die natürliche Person beziehen. Hier dürfte weiterhin die von der Artikel-29-Datenschutzgruppe entwickelte Differenzierung nach „Inhaltselement", „Zweckelement" und „Ergebniselement" eine Rolle spielen,[22] wobei diese Kriterien auch in Zukunft (zumindest teilweise) kritisch zu hinterfragen sind.[23] Schließlich sind auch Informationen, die sich in erster Linie auf einen Gegenstand beziehen, zusätzlich jedoch Aussagen über eine identifizierbare natürliche Person enthalten, als personenbezogen anzusehen.[24] Dies wird u. a. relevant, wenn Standortdaten über einen Personenkraftwagen oder ein Mobiltelefon verarbeitet werden.

Zur Verdeutlichung der Voraussetzung „Informationen, die sich auf eine natürliche Person beziehen" dient folgender Beispielfall: Die Information über eine besonders gute Luftqualität in Berlin bezieht sich zunächst auf einen geographischen Ort. Darüber hinaus besteht jedoch auch ein Bezug zu jeder natürlichen Person, die sich regelmäßig in Berlin aufhält (u. a. Einwohnerinnen und Einwohner). Von diesen Personen ist ein Großteil identifizierbar. Personenbezug ist dennoch abzulehnen, da gerade ein ausreichender Bezug zum einzelnen individuellen Menschen fehlt.

ab) Identifizierbarkeit

Die natürliche Person muss – wie bereits erwähnt – identifiziert oder identifizierbar sein. Als identifizierbar wird gemäß Art. 4 Nr. 1 DSGVO eine natürliche Person angesehen, die 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, identifiziert werden kann.

In den verschiedenen Bereichen von Smart Services ist eine stark zunehmende Vernetzung mehrerer Unternehmen und Personen zu beobachten. Hier stellt sich insbesondere die Frage, welche Mittel und welches Zusatzwissen den einzelnen Stellen hinsichtlich der Festlegung ihrer Identifizierungsmöglichkeiten zugerechnet werden. Nach dem sogenannten relativen Ansatz richtet sich die Identifizierbarkeit in erster Linie nach den individuellen Möglichkeiten des jeweils Verantwortlichen. Nach dem sogenannten objektiven Ansatz sind neben den Möglichkeiten des Verantwortlichen auch die Mittel und das Wissen Dritter in die Beurteilung einzubeziehen.[25] Diese Unterscheidung ist für Smart-Service-Betreiber häufig von zentraler Bedeutung, denn vielfach sind die Informationen (gerade bei KMU) so verteilt, dass keine Stelle den Personenbezug allein herstellen kann.

Trotz kleiner Änderungen und Erweiterungen im Hinblick auf die Voraussetzung der Identifizierbarkeit im Verordnungstext sowie in den Erwägungsgründen wurde durch die DSGVO der Streit zwischen dem sogenannten objektiven Ansatz (auch „absoluter Ansatz" genannt) und dem sogenannten relativen Ansatz nicht ausreichend beigelegt.[26]

Für den objektiven Ansatz spricht bei Heranziehung der DSGVO die Definition pseudonymer Daten in Erwägungsgrund 26 S. 2 DSGVO sowie Erwägungsgrund 26 S. 3 f. DSGVO.[27] Nach Erwägungsgrund 26 S. 2 DSGVO sollten einer Pseudonymisierung unterzogene personenbezogene Daten, die durch Heranziehung zusätzlicher Informationen einer natürlichen Person zugeordnet werden könnten, als Informationen über eine identifizierbare natürliche Person betrachtet werden. Hierdurch wird deutlich, dass nicht nur unmittelbar vorliegende Möglichkeiten der Identifizierung einzubeziehen sind.

Erwägungsgrund 26 S. 3 und S. 4 DSGVO beziehen sich direkt auf die Mittel der Identifizierbarkeit. Um festzustellen, ob eine natürliche Person identifizierbar ist, sollten alle Mittel berücksichtigt werden, die von dem Verantwortlichen oder einer anderen Person nach allgemeinem Ermessen wahrscheinlich genutzt werden, um die natür-

22 Artikel-29-Datenschutzgruppe, Stellungnahme 4/2007 zum Begriff „personenbezogene Daten", WP 136, S. 582.

23 Haase, Datenschutzrechtliche Fragen des Personenbezugs, 2015, 255 f.; weitere Einzelheiten hierzu siehe bei Klar/Kühling, in: Kühling/Buchner, DSGVO, 2017, Art. 4 Nr. 1, Rn. 11.

24 Haase, Datenschutzrechtliche Fragen des Personenbezugs, 2015, S. 144 f., 174 f.

25 Vgl. Gerlach, CR 2013, S. 478 ff. (479); Pahlen-Brandt, DuD 2008, 34 ff. (38 f.); weitere Einzelheiten hierzu siehe bei Klar/Kühling, in: Kühling/Buchner, DS-GVO, 2017, Art. 4 Nr. 1, Rn. 20 ff.

26 Ähnlich Klar/Kühling, in: Kühling/Buchner, DSGVO, 2017, Art. 4 Nr. 1, Rn. 26; Schreiber, in: Plath, BDSG/DSGVO, 2016, Art. 4, Rn. 9.

27 So auch Schreiber, in: Plath, BDSG/DSGVO, 2016, Art. 4, Rn. 9.

liche Person direkt oder indirekt zu identifizieren, wie beispielsweise das Aussondern (Erwägungsgrund 26 S. 3 DSGVO). Bei der Feststellung, ob Mittel nach allgemeinem Ermessen wahrscheinlich zur Identifizierung der natürlichen Person genutzt werden, sollten 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 (Erwägungsgrund 26 S. 4 DSGVO).

In der Literatur wird bezweifelt, dass die Frage nach dem zurechenbaren Zusatzwissen dadurch einfacher zu beantworten ist.[28] Unklar sei beispielsweise das „Verhältnis von verfügbarer Technologie und technologischer Entwicklung".[29] Dabei wird die Befürchtung geäußert, dass in Zukunft die Gefahr einer Überforderung des Verantwortlichen beim Umgang mit dieser Festlegung entstehe.[30] Dieser Ansicht ist zuzustimmen.

Für den relativen Ansatz spräche, dass Datenverarbeitungen, „die kein Gefahrenpotenzial für den Schutz des informationellen Selbstbestimmungsrechts eines konkreten Grundrechtsträgers aufweisen", nicht in den Regulierungsbereich der DSGVO fallen sollten.[31] Außerdem ist für den Verantwortlichen kaum abschätzbar, welche Möglichkeiten der Identifizierung bei Dritten vorhanden sind.

Sowohl der relative als auch der objektive Ansatz wird wohl kaum noch in seiner strengsten Form vertreten.[32] In der Rechtsprechung ist mittlerweile eine Tendenz zu einer vermittelnden Ansicht festzustellen.[33] Vermutlich werden auch in Zukunft unter Anwendung der DSGVO sowohl die Literatur als auch die Rechtsprechung verstärkt zu einer vermittelnden Ansicht tendieren. Letztlich sollten dritte Stellen in die Beurteilung miteinbezogen werden (objektives Element), wobei diese Einbeziehung über die Kriterien „nach allgemeinem Ermessen" und „wahrscheinlich" (relatives Element) einzuschränken ist.[34]

28 Krügel, ZD 2017, 455, 456.
29 Krügel, ZD 2017, 455, 456.
30 Krügel, ZD 2017, 455, 456.
31 Schreiber, in: Plath, BDSG/DSGVO, 2016, Art. 4, Rn. 10.
32 Haase, Datenschutzrechtliche Fragen des Personenbezugs, 2015, S. 290 ff.
33 Zuletzt: EuGH, Urteil vom 19.10.2016 In der Rechtssache C 582/14; BGH, Urteil vom 16.05.2017, Az.: VI ZR 135/13.
34 In diese Richtung gehend bereits Haase, Datenschutzrechtliche Fragen des Personenbezugs, 2015, S. 320.

ac) Anonyme oder anonymisierte Daten

Der Begriff der „Anonymisierung" ist in der DSGVO nicht definiert. Nach Erwägungsgrund 26 S. 5 DSGVO sollten die Grundsätze des Datenschutzes nicht für anonyme Informationen gelten. Hierunter fallen nach Erwägungsgrund 26 S. 5 DSGVO Informationen, die sich nicht auf eine identifizierte oder identifizierbare natürliche Person beziehen, oder personenbezogene Daten, die in einer Weise anonymisiert worden sind, dass die betroffene Person nicht oder nicht mehr identifiziert werden kann. Der Begriff der „Anonymisierung" bleibt damit der Gegenbegriff zum „Personenbezug".

b) Verarbeitung

Die Voraussetzung „Verarbeitung" ist vom Verordnungsgeber weit gefasst worden und erstreckt sich auf fast alles, was mit Daten „gemacht" werden kann.[35] Nach Art. 4 Nr. 2 DSGVO bezeichnet der Ausdruck „Verarbeitung" im Sinn der Datenschutz-Grundverordnung jeden mit oder ohne Hilfe automatisierter Verfahren ausgeführten Vorgang oder jede solche Vorgangsreihe im Zusammenhang mit personenbezogenen Daten wie das Erheben, das Erfassen, die Organisation, das Ordnen, die Speicherung, die Anpassung oder Veränderung, das Auslesen, das Abfragen, die Verwendung, die Offenlegung durch Übermittlung, Verbreitung oder eine andere Form der Bereitstellung, den Abgleich oder die Verknüpfung, die Einschränkung, das Löschen oder die Vernichtung.

c) Automatisierte Verarbeitung sowie Speicherung in einem Dateisystem

Für die nichtautomatisierte Verarbeitung personenbezogener Daten gilt die DSGVO nur, wenn die Daten in einem Dateisystem gespeichert sind oder gespeichert werden sollen (Art. 2 Abs. 1 DSGVO). Der Ausdruck „Dateisystem" wird in Art. 4 Nr. 6 DSGVO definiert.[36]

d) Keine Anwendung

In Art. 2 Abs. 2 DSGVO wird schließlich festgelegt, in welchen Fallkonstellationen die Verordnung nicht anwendbar

35 So auch Schreiber, in: Plath, BDSG/DSGVO, Art. 4, Rn. 12.
36 Nach Art. 4 Nr. 6 DSGVO „bezeichnet der Ausdruck ‚Dateisystem' im Sinne der Datenschutz-Grundverordnung jede strukturierte Sammlung personenbezogener Daten, die nach bestimmten Kriterien zugänglich sind, unabhängig davon, ob diese Sammlung zentral, dezentral oder nach funktionalen oder geografischen Gesichtspunkten geordnet geführt wird.".

sein soll, selbst wenn die oben genannten Voraussetzungen vorliegen.[37]

Im Zusammenhang mit Smart Services kann insbesondere Art. 2 Abs. 2 c) DSGVO relevant werden, wenn Daten verarbeitet werden, die von Privatleuten erhoben worden sind.

3. Räumlicher Anwendungsbereich

Art. 3 DSGVO regelt den räumlichen Anwendungsbereich der Datenschutz-Grundverordnung.

4. Fazit zum sachlichen Anwendungsbereich des Datenschutzrechts

Sowohl der deutsche als auch der europäische Gesetzgeber hat den Anwendungsbereich des Datenschutzrechts in den vergangenen Jahren sinnvoll fortentwickelt. Im Hinblick auf den sachlichen Anwendungsbereich besteht weiterhin Gesetzgebungsbedarf. Die Identifizierbarkeit einer natürlichen Person sollte stärker durch den Gesetzestext konkretisiert werden.

Ein Teil der Rechtsprechung[38] und ein Teil der Literatur (streng objektiver Ansatz) haben den sachlichen Anwendungsbereich des Datenschutzrechts in der Vergangenheit zu weit ausgelegt. Die hierdurch entstandenen Unsicherheiten – insbesondere für kleine und mittelständische Unternehmen – sollten in Zukunft behoben werden. Auf gesetzgeberischer Ebene könnte der sachliche Anwendungsbereich des Datenschutzrechts dadurch konkretisiert und fortentwickelt werden, dass die datenschutzrechtliche Betroffenheit über das Merkmal „natürliche Person" stärker eingegrenzt wird.[39] Dies könnte mit einer noch stärkeren Konkretisierung des Schutzgegenstandes verknüpft werden.

Darüber hinaus sollte die Voraussetzung der Identifizierbarkeit gesetzlich näher bestimmt werden, um Haftungsrisiken für verantwortliche Stellen kalkulierbarer zu machen. Im Rahmen der DSGVO könnten in einem ersten Schritt die Festlegungen zur Identifizierbarkeit aus Erwägungsgrund 26 in Artikel 4 DSGVO übertragen werden. Außerdem wären weitere gesetzliche Beurteilungskriterien für die Feststellung wünschenswert, wann Mittel zur Identifizierbarkeit von einem Verantwortlichen oder einer anderen Person „nach allgemeinem Ermessen" „wahrscheinlich" genutzt werden, um die natürliche Person direkt oder indirekt zu identifizieren. Schließlich sollte die Auseinandersetzung mit dem Merkmal der „Aussonderung"[40] fortgesetzt werden.

Datenschutzrechtliche Verantwortlichkeit

Ein weiterer Schwerpunkt soll auf die Bewertung der gesetzlichen Kriterien zur Festlegung der datenschutzrechtlichen Verantwortlichkeit gelegt werden. Im Rahmen von Smart Services liegen die Erhebung und die Verarbeitung von personenbezogenen Daten häufig nicht in einer Hand. In Fallkonstellationen, in denen mehrere Akteure bei der Verarbeitung personenbezogener Daten zusammenwirken, ist eine Festlegung und Abgrenzung der datenschutzrechtlichen Verantwortungsbereiche erforderlich. Eine intransparente Überschneidung ist zu vermeiden.[41]

Nach Art. 4 Nr. 7 DSGVO bezeichnet der Ausdruck „Verantwortlicher" im Sinne der DSGVO (wie bereits nach der Richtlinie[42]) die natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die allein oder gemeinsam mit anderen über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheidet.[43] Die Nennung der verschiedenen Adressaten macht deutlich, „dass es auf

37 Nach Art. 2 Abs. 2 DSGVO findet die Datenschutz-Grundverordnung keine Anwendung auf die Verarbeitung personenbezogener Daten
a) im Rahmen einer Tätigkeit, die nicht in den Anwendungsbereich des Unionsrechts fällt,
b) durch die Mitgliedstaaten im Rahmen von Tätigkeiten, die in den Anwendungsbereich von Titel V Kapitel 2 EUV fallen,
c) durch natürliche Personen zur Ausübung ausschließlich persönlicher oder familiärer Tätigkeiten,
d) durch die zuständigen Behörden zum Zwecke der Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten oder der Strafvollstreckung einschließlich des Schutzes vor und der Abwehr von Gefahren für die öffentliche Sicherheit; Art. 2 (3) DSGVO lautet: „Für die Verarbeitung personenbezogener Daten durch die Organe, Einrichtungen, Ämter und Agenturen der Union gilt die Verordnung (EG) Nr. 45/2001. Die Verordnung (EG) Nr. 45/2001 und sonstige Rechtsakte der Union, die diese Verarbeitung personenbezogener Daten regeln, werden im Einklang mit Artikel 98 an die Grundsätze und Vorschriften der vorliegenden Verordnung angepasst."; Art. 2 (4) DSGVO lautet: „Die vorliegende Verordnung lässt die Anwendung der Richtlinie 2000/31/EG und speziell die Vorschriften der Artikel 12 bis 15 dieser Richtlinie zur Verantwortlichkeit der Vermittler unberührt.".

38 Noch vor EuGH, Urteil vom 19.10.2016 in der Rechtssache C 582/14; BGH, Urteil vom 16.05.2017, Az.: VI ZR 135/13; siehe hierzu auch Klar/Kühling, in: Kühling/Buchner, DSGVO, 2017, Art. 4 Nr. 1, Rn. 25 ff.

39 Haase, Datenschutzrechtliche Fragen des Personenbezugs, S. 187 ff.

40 Vgl. Erwägungsgrund 26 DSGVO; Haase, Datenschutzrechtliche Fragen des Personenbezugs, 2015, S. 267 f., 335 ff.

41 Ausführlich zur bisherigen Rechtslage Ensthaler/Haase, in: Heinrich C. Mayr, Martin Pinzger (Hrsg.): INFORMATIK 2016.

42 Schreiber, in: Plath, BDSG/DSGVO, Art. 4, Rn. 25.

43 Im Einzelnen hierzu Artikel-29-Datenschutzgruppe, Stellungnahme 1/2010 zu den Begriffen „für die Verarbeitung Verantwortlicher" und „Auftragsdatenverarbeiter", WP 169.

die Organisationsform nicht ankommt".[44] Sind die Zwecke und Mittel dieser Verarbeitung durch das Unionsrecht oder das Recht der Mitgliedstaaten vorgegeben, so kann der Verantwortliche beziehungsweise können die bestimmten Kriterien seiner Benennung nach dem Unionsrecht oder dem Recht der Mitgliedstaaten vorgesehen werden (Art. 4 Nr. 7 a. E. DSGVO).

1. Bisherige Abgrenzung

In § 3 Abs. 7 BDSG war bisher nur eine einzelne verantwortliche Stelle definiert. Für die Begründung einer datenschutzrechtlichen Verantwortung im Sinne des. BDSG wurde als ausreichend angesehen, „dass die Verarbeitungstätigkeit im eigenen Tätigkeits- und Haftungsbereich stattfindet und die Möglichkeit besteht, in tatsächlicher Hinsicht auf den Verarbeitungsvorgang einzuwirken.".[45] Können „Verfügungs- und Entscheidungsgewalt" eindeutig festgestellt werden, handelt es sich bei diesen Kriterien um „geeignete Anknüpfungspunkte für die Festlegung der verantwortlichen Stelle, denn sie sind unmittelbar ausschlaggebend für die Missbrauchsgefahr und das Gefährdungspotenzial im Hinblick auf das informationelle Selbstbestimmungsrecht.".[46]

2. Fortentwicklung

In Anlehnung an die Datenschutzrichtlinie 95/46/EG wird in der DSGVO explizit eine gemeinsame datenschutzrechtliche Verantwortlichkeit mehrerer Stellen anerkannt (vgl. Art. 4 Nr. 7, Art. 36 DSGVO). Dies entspricht der Realität hinsichtlich Smart Services.

Im Rahmen der Feststellung der Verantwortlichkeit wird zu beachten sein, dass ein Teil der bisher herangezogenen Umstände, bei denen man häufig auf körperliche und physische Grenzen zurückgreifen konnte, auf digitalen Märkten zunehmend wegfallen wird. Das gesamte Wirtschaftsleben unterliegt einem starken Wandel in Richtung Virtualität. Digitale Marktplätze bewegen sich teilweise in einem ausschließlich digitalen Umfeld. Physische oder körperliche Abgrenzungen – wie beim Sacheigentum – können hier keine Rolle mehr spielen.[47]

Unter der Prämisse, dass die involvierten Parteien keine Vereinbarung zur Verantwortlichkeit treffen, d. h. insbesondere keine Auftragsdatenverarbeitung stattfindet, ist zu überlegen, ob die Verantwortlichkeit in einem virtuellen Umfeld in Zukunft in erster Linie anhand der Zugriffs- und Identifizierungsmöglichkeiten festgestellt werden sollte. Zugriff und Identifizierbarkeit sind der Entscheidung über Zwecke und Mittel vorgelagert. Um Abgrenzungen zu schaffen, könnte bei der Bewertung verstärkt auf Verschlüsselungstechnologien zurückgegriffen werden.

3. Übertragung der Verantwortlichkeit

Durch die Festlegungen in Art. 7 DSGVO wird deutlich, dass es auch in Zukunft keinen „Konzerndatenschutz" geben wird, bei dem der Konzern ein „Verantwortlicher" ist.[48] Darüber hinaus ist die datenschutzrechtliche Verantwortung „nur beschränkt delegierbar und wird auch nicht durch die Bestellung eines behördlichen oder betrieblichen Datenschutzbeauftragten abbedungen.".[49]

4. Pflichten des Verantwortlichen

Die Pflichten des Verantwortlichen sind in Art. 24 ff. DSGVO festgelegt. In Zukunft wird der Begriff insoweit ausgeweitet, dass auch der Auftragsdatenverarbeiter „Verantwortlicher" im Sinne des Datenschutzrechts sein wird.[50] Auch können mehrere gemeinsam Verantwortliche sein, wenn sie gemeinsam die Zwecke und die Mittel zur Verarbeitung festlegen (Art. 26 Abs. 1 S. 1 DSGVO),[51] was im Ansatz zu begrüßen ist, weil es einem Teil der Praxis in der Realität gerecht wird.

Art. 26 DSGVO macht deutlich, „dass alle Verantwortlichen gemeinsam festzulegen haben, wer von ihnen welche Verpflichtung gemäß der DSGVO erfüllt, insbesondere was die Wahrnehmung der Rechte der betroffenen Person angeht

44 Hartung, in: Kühling/Buchner, DSGVO, 2017, Art. 4 Nr. 7, Rn. 9.
45 Buchner, in: Taeger/Gabel, BDSG, 2013, § 3 Rdnr. 52.
46 Ensthaler/Haase, in: Heinrich C. Mayr, Martin Pinzger (Hrsg.): INFORMATIK 2016.
47 So bereits Ensthaler/Haase, in: Heinrich C. Mayr, Martin Pinzger (Hrsg.): INFORMATIK 2016.
48 Schild, in: Wolff/Brink, BeckOK Datenschutzrecht, 21. Edition, Stand: 01.08.2017, Art. 4, Rn. 88.
49 Schild, in: Wolff/Brink, BeckOK Datenschutzrecht, 21. Edition, Stand: 01.08.2017, Art. 4, Rn. 89.
50 Schild, in: Wolff/Brink, BeckOK Datenschutzrecht, 21. Edition, Stand: 01.08.2017, Art. 4, Rn. 90.
51 Schild, in: Wolff/Brink, BeckOK Datenschutzrecht, 21. Edition, Stand: 01.08.2017, Art. 4, Rn. 90 f.; dies war bereits in der Datenschutzrichtlinie 95/46/EG geregelt, wurde jedoch nicht ins BDSG umgesetzt; Schild, in: Wolff/Brink, BeckOK Datenschutzrecht, 21. Edition, Stand: 01.08.2017, Art. 4, Rn. 91.
Art. 26 Abs. 3 DSGVO lautet: „Ungeachtet der Einzelheiten der Vereinbarung gemäß Absatz 1 kann die betroffene Person ihre Rechte im Rahmen dieser Verordnung bei und gegenüber jedem einzelnen der Verantwortlichen geltend machen.".

und wer welchen Informationspflichten gemäß den Art. 13 und 14 nachkommt.".[52]

Daneben fehlt es in der DSGVO jedoch an einer ausreichenden Regelung zu einer mehrfachen „eigenständigen" Verantwortlichkeit verschiedener Stellen. Diese kann im Zusammenhang mit Smart Services z. B. dann entstehen, wenn zwei unabhängige Stellen zufällig Datensätze verarbeiten, durch deren Zusammenfügen Personenbezug hergestellt werden kann. Wenn man in dieser Konstellation den Personenbezug bei jeder Stelle bejaht, sollte auch bei jeder Stelle eine volle eigenständige datenschutzrechtliche Verantwortlichkeit entstehen. Die tatsächlichen Umstände müssten hier ausschlaggebend sein und nicht erst eine gemeinsame Entscheidung über Zwecke und Mittel der Verarbeitung.

Jeder Verantwortliche hat schließlich sicherzustellen, dass die Verarbeitung gemäß der DSGVO erfolgt. Art. 24 Abs. 1 DSGVO lautet: „Der Verantwortliche setzt unter Berücksichtigung der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere der Risiken für die Rechte und Freiheiten natürlicher Personen geeignete technische und organisatorische Maßnahmen um, um sicherzustellen und den Nachweis dafür erbringen zu können, dass die Verarbeitung gemäß dieser Verordnung erfolgt. Diese Maßnahmen werden erforderlichenfalls überprüft und aktualisiert."

5. Fazit in Bezug auf die datenschutzrechtliche Verantwortlichkeit

Konkretisierungsbedarf besteht auch im Hinblick auf die gesetzliche Bestimmung der datenschutzrechtlichen Verantwortlichkeit. Die gesetzlichen Kriterien für die datenschutzrechtliche Verantwortung sollten an die zunehmende Vernetzung mehrerer Akteure sowie unternehmensübergreifende Datenverarbeitungen angepasst werden. Dabei muss das Gesetz insbesondere Festlegungen für den Fall schaffen, dass die Parteien keine vertragliche Vereinbarung zu der datenschutzrechtlichen Verantwortung getroffen haben. Bevor in Bezug auf die datenschutzrechtliche Verantwortung weitere Gesetzgebungsprozesse konkret angeschoben werden, sollte zunächst die Auslegung der neuen Vorschriften der DSGVO zur Verantwortlichkeit durch Rechtsprechung und Literatur abgewartet werden.

Grundsätze der Datenschutz-Grundverordnung

Hinsichtlich der Datenverarbeitungsprozesse, durch die der persönliche, sachliche und räumliche Anwendungsbereich der Datenschutz-Grundverordnung eröffnet wird, sind die Vorschriften der Datenschutz-Grundverordnung zu beachten. In Kapitel II sind die Grundsätze der Datenschutz-Grundverordnung festgelegt, aus denen sich die Zulässigkeit der Verarbeitung personenbezogener Daten ergibt. Diese sind sehr umfangreich. Eine Auseinandersetzung mit den einzelnen Regulierungen der DSGVO würde an dieser Stelle den Rahmen sprengen. Sie ist jedoch die Konsequenz, die ein Smart-Service-Betreiber aus dem Vorliegen der Voraussetzungen für die Anwendbarkeit der DSGVO und der datenschutzrechtlichen Verantwortlichkeit stets ziehen sollte.

Ausblick

Der Gesetzgebungsprozess zur Datenschutz-Grundverordnung hat mehrere Jahre gedauert. Während dieser Zeit wurden die verschiedensten Änderungsvorschläge intensiv diskutiert. Mit einer erneuten umfassenden Reform des Datenschutzrechts ist mittelfristig nicht zu rechnen.

Die DSGVO enthält einerseits zahlreiche Öffnungsklauseln. In diesem Kontext entstehen für den nationalen Gesetzgeber neue Spielräume für die Fortentwicklung des Datenschutzrechts in der Bundesrepublik Deutschland. Außerdem sollten die einzelnen Regelungen der DSGVO weiterhin kritisch hinterfragt und ggf. zeitnah überarbeitet werden.

52 Schild, in: Wolff/Brink, BeckOK Datenschutzrecht, 21. Edition, Stand: 01.08.2017, Art. 4, Rn. 91.