Benedikt Buchner

Grundsätze und Rechtmäßigkeit der Datenverarbeitung unter der DS-GVO

Die neue europäische Datenschutz-Grundverordnung steht vor der Tür. Mit Beginn des Trilogs im Juni 2015 ging auf einmal alles ganz schnell. Parlament, Rat und Kommission hielten den ambitionierten Zeitplan ein, innerhalb eines halben Jahres ihr informelles Vermittlungsverfahren abzuschließen, und noch im ersten Quartal dieses Jahres soll die förmliche Annahme durch Parlament und Rat erfolgen. Zwei Jahre nach Inkrafttreten der Verordnung, also Anfang 2018, wird diese dann unmittelbar in jedem Mitgliedstaat gelten. Die folgenden Ausführungen sollen einen ersten Ausblick auf Grundsätze und Rechtmäßigkeit einer Datenverarbeitung unter der DS-GVO geben. Erörtert wird darüber hinaus auch, welche Harmonisierungskraft die Verordnung entfalten und wie sich dies auf das nationale Datenschutzrecht auswirken wird.

Vorbemerkung

Soweit im Folgenden Erwägungsgründe und Artikel zitiert werden, beziehen sich diese auf das Ratsdokument vom 15.12.2015, welches die Verhandlungsergebnisse der Trilogparteien in Form einer Arbeitsfassung wiedergibt.[1] Es handelt sich dabei um eine noch nicht konsolidierte Fassung der Verordnung; daher ist davon auszugehen, dass manche der hier zitierten Erwägungsgründe und Artikel hinsichtlich ihrer Nummerierung in der amtlichen Fassung noch Änderungen erfahren werden.

1 Anwendungsbereich der Verordnung

Im Ausgangspunkt verfolgt die Verordnung, ebenso wie schon die Richtlinie, einen einheitlichen Regelungsansatz und erfasst die Datenverarbeitung im öffentlichen Bereich ebenso wie im nicht-öffentlichen Bereich. Jedoch erfährt dieser einheitliche Regelungsansatz sogleich wieder eine Einschränkung dahingehend, dass die Mitgliedstaaten für die Datenverarbeitung im öffentlichen Bereich auch weiterhin nationale Regelungen erlassen können. Zwar findet sich diese Einschränkung in der endgültigen Fassung nicht mehr an so prominenter Stelle wie noch im Standpunkt des Rats. Letzterer sah bereits in Art. 1 die Einschränkung vor, dass die Mitgliedstaaten für den öffentlichen Bereich die Vorgaben der Verordnung durch spezifischere Regelungen ergänzen können.[2] Jedoch ist dieselbe Einschränkung nunmehr in Art. 6 Abs. 2a der Verordnung normiert. Die Mitgliedstaaten können danach für die Verarbeitung personenbezogener Daten zur Erfüllung einer rechtlichen Verpflichtung oder zur Wahrnehmung einer Aufgabe, die im öffentlichen Interesse liegt oder in Ausübung öffentlicher Gewalt erfolgt, spezifischere Bestimmungen vorsehen, sowohl hinsichtlich der Anforderungen an die Verarbeitung als auch hinsichtlich sonstiger Maßnahmen, die eine Verarbeitung nach Recht und Gesetz gewährleisten sollen.[3]

Die Eröffnung des sachlichen Anwendungsbereichs der Verordnung ist zunächst einmal durch Kriterien bestimmt, wie sie so oder so ähnlich schon aus dem bisherigen Datenschutzrecht bekannt sind, insbesondere die Anknüpfung an eine automatisierte Datenverarbeitung oder alternativ an eine nichtautomatisierte Datenverarbeitung in Dateiform sowie die Herausnahme einer Datenverarbeitung zu ausschließlich persönlichen oder familiären Zwecken durch natürliche Personen. Von zentraler Bedeutung für die Eröffnung des Anwendungsbereichs ist dann wie schon seit jeher, ob die verarbeiteten Daten einen Personenbezug aufweisen. Art. 4 Abs. 1 orientiert sich hierfür weitestgehend an der bisherigen Definition der Datenschutzrichtlinie.[4] Die Vorschrift führt lediglich einige zusätzliche Beispiele an, auf welche Weise ein Personenbezug hergestellt werden kann: mittels Zu-

1 Council of the European Union, Interinstitutional File: 2012/0011 (COD), No. 15039/15 v. 15.12.2015.

Prof. Dr. Benedikt Buchner, LL.M. (UCLA)

Institut für Informations-, Gesundheits- und Medizinrecht (IGMR)
Universität Bremen

E-Mail: bbuchner@uni-bremen.de

2 Vgl. BR-Drs. 290/15, S. 2.
3 Siehe dazu auch noch unten 3.3.
4 Vgl. auch *Karg*, DuD 2015, 520, 521.

ordnung zu einer Kennung wie einem Namen, zu Standortdaten oder auch zu einer Online-Kennung.[5]

Für den Dauerstreit, ob die Möglichkeit der Herstellung eines Personenbezugs nach absoluten (objektiven) oder relativen Maßstäben zu beurteilen ist, gibt die Definition des Art. 4 Abs. 1 zunächst einmal nichts her. Zur Auslegung sind jedoch des Weiteren auch die Erwägungsgründe heranzuziehen.[6] Nach diesen sollen für die Frage, ob eine Person bestimmbar ist, alle Mittel zu berücksichtigen sein, die von dem für die Verarbeitung Verantwortlichen *oder einer anderen Person* nach allgemeinem Ermessen aller Voraussicht nach genutzt werden, um die Person direkt oder indirekt zu bestimmen.[7] Dies spricht dafür, dass die Verordnung für die Frage der Bestimmbarkeit von einem absoluten Verständnis ausgeht. Für ein weites (und damit absolutes) Verständnis der Bestimmbarkeit einer Person spricht auch, dass sich in der endgültigen Fassung nicht mehr wie noch in den früheren Fassungen Einschränkungen dahingehend finden lassen, dass Kennnummern, Standortdaten, Online-Kennungen oder sonstige Elemente als solche „nicht zwangsläufig und unter allen Umständen" als personenbezogene Daten zu betrachten seien (Kommissionsentwurf) bzw. nur dann als personenbezogene Daten zu betrachten seien, wenn mit ihnen eine Person bestimmt oder bestimmbar gemacht wird (Ratsentwurf).[8]

Was schließlich den räumlichen Anwendungsbereich angeht, erübrigen sich künftig viele Streitigkeiten, wie sie für die Frage des räumlichen Anwendungsbereichs nationaler Datenschutzgesetze wie etwa des BDSG kennzeichnend waren. Die leidige Auseinandersetzung mit Google, Facebook und Co, ob nun deutsches oder irisches Datenschutzrecht gilt,[9] bleibt Juristen künftig erspart, weil unter der Verordnung von vornherein keine Wahl mehr zwischen mehr oder weniger attraktiven einzelstaatlichen Rechtsordnungen besteht. Was die Anwendbarkeit der Verordnung als solcher angeht, eröffnet Art. 3 Abs. 1 den Anwendungsbereich zunächst einmal für den Fall, dass personenbezogene Daten im Rahmen der Tätigkeiten einer Niederlassung eines für die Verarbeitung Verantwortlichen oder eines Auftragsverarbeiters in der Union verarbeitet werden – und zwar unabhängig davon, ob auch die Datenverarbeitung selbst in der Union erfolgt.[10] Gemäß Art. 3 Abs. 2 gilt die Verordnung darüber hinaus auch für außerhalb der EU niedergelassene Datenverarbeiter, wenn diese Daten verarbeiten, um betroffenen Personen in der EU – entgeltlich oder unentgeltlich – Waren oder Dienstleistungen anzubieten oder um das Verhalten der betroffenen Personen zu beobachten, soweit sich dieses in der EU abspielt. Damit hat in die Verordnung das sog. Marktortprinzip Eingang gefunden: Wer innerhalb der EU Waren und Dienstleistungen anbietet, muss auch EU-Datenschutzrecht beachten – egal, ob der Anbieter seine Niederlassung innerhalb oder außerhalb der EU hat. Vor allem im Sinne der Rechtssicherheit ist diese klare Regelung zu begrüßen – unabhängig davon, dass der Sache nach auch schon unter Geltung der Richtlinie das Marktortprinzip mehr und mehr Geltungskraft erlangt hat.[11]

2 Grundsätze der Datenverarbeitung

2.1 Die Grundsätze im Allgemeinen

Die allgemeinen Grundsätze der Datenverarbeitung, die nach Art. 5 der Verordnung gelten, sind allesamt gut bekannt, egal ob es um den Grundsatz der Transparenz, der Zweckbindung, der Datensparsamkeit oder der Richtigkeit der Datenverarbeitung geht. Die Vorgabe der Datensparsamkeit – die Verordnung spricht von Datenminimierung – findet sich dann auch noch einmal in Art. 23 in der Gestalt eines technischen Datenschutzes normiert. Die für die Datenverarbeitung Verantwortlichen haben danach die Systeme technisch derart auszugestalten, dass die Risiken für die Rechte und Freiheiten der betroffenen Personen minimiert werden. Des Weiteren haben die Verantwortlichen durch technische Voreinstellungen sicherzustellen, dass tatsächlich nur diejenigen Daten verarbeitet werden, deren Verarbeitung zum Erreichen eines bestimmten Zwecks erforderlich ist. Art. 23 entspricht damit im Wesentlichen dem Konzept der Datenvermeidung und -sparsamkeit, wie es von § 3a BDSG bekannt ist.[12] Ein anderer zentraler Grundsatz des deutschen Datenschutzrechts, die Direkterhebung (§ 4 Abs. 2 BDSG), hat hingegen keinen Eingang in die Verordnung gefunden – zumindest nicht ausdrücklich.[13] Art. 14a sieht lediglich eine Reihe von Informationspflichten für den Fall vor, dass Daten nicht bei der betroffenen Person erhoben wurden.

2.2 Der Zweckbindungsgrundsatz im Besonderen

Dass althergebrachte Grundsätze wie Datensparsamkeit und Zweckbindung auch in die Verordnung übernommen worden sind, wird insbesondere die Anhänger von Big Data enttäuschen, die sich von der Verordnung ein sog. „modernes" (= möglichst großzügiges) Datenschutzrecht erhofft haben.[14] Big Data-Anwendungen beruhen auf dem Prinzip, dass Daten zweckfrei in möglichst großen Mengen zusammengetragen werden, um dann zur Gewinnung neuer Erkenntnisse frei ausgewertet zu werden.[15] Spannend zu beobachten wird es daher vor allem sein, ob und inwieweit sich der Zweckbindungsgrundsatz künftigen Auslegungsbegehrlichkeiten widersetzen können wird, die auf dessen Aufweichung im Dienste von Big Data abzielen.

5 Schon in der Richtlinie sind darüber hinaus die Beispiele der Zuordnung zu einer Kennnummer oder zu einem oder mehreren spezifischen Elementen, die Ausdruck ihrer physischen, physiologischen, psychischen, wirtschaftlichen, kulturellen oder sozialen Identität sind, aufgeführt.

6 Vgl. *Stolz*, in: *Riesenhuber*, Europäische Methodenlehre (2015), S. 498 f.

7 Erwägungsgrund 23.

8 Vgl. jeweils Erwägungsgrund 24 des Kommissions- bzw. Ratsentwurfs; zur Frage der Einordnung von IP-Adressen als personenbezogene Daten siehe auch das Vorabentscheidungsersuchen des BGH an den EuGH (DuD 2015, 199).

9 Siehe beispielhaft einerseits OVG Schleswig DuD 2013, 463 (Klarnamenpflicht bei Facebook; keine Anwendbarkeit des deutschen Datenschutzrechts) und andererseits KG Berlin DuD 2014, 417 (Facebook-Freundefinder; Anwendbarkeit des deutschen Datenschutzrechts); dazu auch *Caspar*, DuD 2015, 589, 590.

10 Ausführlich zu den verschiedensten Aspekten des räumlichen Anwendungsbereichs *Wieczorek*, DuD 2013, 644 ff.

11 Siehe etwa zu den Ansätzen eines Marktortprinzips in der Rechtsprechung des EuGH die Ausführungen von *Caspar*, DuD 2015, 589, 590, und *Kühling*, EuZW 2015, 527 ff. (zur Google Spain-Entscheidung) sowie *Karg*, ZD 2015, 584 (zur Weltimmo-Entscheidung).

12 *Roßnagel/Nebel/Richter*, ZD 2015, 455, 459.

13 Transparenz- und Verhältnismäßigkeitsprinzip können durchaus auch in dem Sinne verstanden werden, dass es grundsätzlich einer Direkterhebung beim Betroffenen bedarf.

14 Zum Widerspruch zwischen datenschutzrechtlichen Grundsätzen und Big Data-Ansatz *Richter*, DuD 2015, 735 ff. und *Ohrtmann/Schwiering*, NJW 2014, 2984 ff.

15 Zu den verfassungsrechtlichen Rahmenbedingungen von Big Data s. *Roßnagel/Nebel*, DuD 2015, 455 ff.

Mögliches Einfallstor für eine solche Aufweichung ist zunächst einmal die Einschränkung in Art. 5 Abs. 1 lit. b, wonach eine Weiterverarbeitung von Daten für im öffentlichen Interesse liegende Archivzwecke oder für wissenschaftliche, historische oder statistische Zwecke nicht als unvereinbar mit den ursprünglichen Zwecken gilt. Jedoch ist diese Öffnung von vornherein eng zu verstehen, nicht nur weil sie der Sache nach eine – vom Gesetzgeber gewünschte – Ausnahme vom Zweckbindungsgrundsatz darstellt, sondern vor allem auch mit Blick auf die detaillierten Ausführungen in den Erwägungsgründen 125 ff., die deutlich machen, dass solcherlei Zwecksetzungen hohen Anforderungen genügen müssen. Keinesfalls reicht es aus, dass lediglich die Datenverarbeitung selbst eine irgendwie geartete wissenschaftliche, historische oder statistische Methode darstellt. Daher ist es auch von vornherein ausgeschlossen, dass etwa Profiling- und Scoring-Verfahren oder Big Data-Analysen als „Statistik" vom Zweckbindungsgrundsatz ausgenommen sind.[16]

Ein zweites mögliches Einfallstor für eine Aufweichung des Zweckbindungsgrundsatzes ist daneben die Regelung in Art. 6 Abs. 3a, wonach anhand von fünf Kriterien zu bestimmen ist, ob die Datenverarbeitung zu einem anderen Zweck als dem ursprünglich verfolgten gleichwohl noch mit dem ursprünglichen Erhebungszweck vereinbar ist. Berücksichtigt werden sollen hierfür: jede Verbindung („any link") zwischen ursprünglichem Erhebungszweck und weiteren Verarbeitungszwecken, der Kontext der Datenerhebung, die Art der Daten, mögliche Konsequenzen der beabsichtigten Datenverarbeitung für den Betroffenen sowie das Vorhandensein angemessener Schutzmaßnahmen wie etwa Verschlüsselung oder Pseudonymisierung. Aus Sicht der Konferenz der Datenschutzbeauftragten des Bundes und der Länder macht die Regelung Zweckänderungen in einem derart weiten Umfang zulässig, dass dies einer Preisgabe des in der Europäischen Grundrechtecharta enthaltenen Prinzips der Zweckbindung gleichkommt.[17] Ob eine solche Preisgabe tatsächlich zu befürchten ist, wird vor allem auch davon abhängen, wie streng oder großzügig die Anforderungen an die ursprüngliche Zwecksetzung nach Art. 5 Abs. 1 lit. b („festgelegt" und „eindeutig") ausgelegt werden. Je höher die Anforderungen an die Festlegung und Eindeutigkeit der ursprünglichen Zwecksetzung sind,[18] desto geringer ist dann auch das Risiko einer Aufweichung über Art. 6 Abs. 3a.[19]

3 Rechtmäßigkeit der Datenverarbeitung

Die Entscheidung, unter welchen Voraussetzungen eine Verarbeitung personenbezogener Daten rechtmäßig ist, ist eine der zentralen Stellschrauben in jedem datenschutzrechtlichen Regelungsregime. Dies gilt sowohl für die – im Gesetzgebungsverfahren heftig umstrittene – Frage, ob für die Verarbeitung personenbezogener Daten im Ausgangspunkt ein Verbot mit Erlaubnisvorbehalt gelten soll, als auch für die Ausgestaltung der Erlaubnistatbestände für eine Datenverarbeitung im Einzelnen.

3.1 Verbotsprinzip mit Erlaubnisvorbehalt

Schon die Richtlinie hat den Mitgliedstaaten aufgegeben, eine Datenverarbeitung nur dann zuzulassen, wenn eine der in Art. 7 der Richtlinie abschließend bestimmten Voraussetzungen erfüllt ist. Art. 6 der Verordnung nimmt dieses Grundprinzip auf und normiert entsprechend, dass eine Verarbeitung personenbezogener Daten nur dann rechtmäßig ist, wenn eine der in Art. 6 Abs. 1 abschließend aufgezählten Bedingungen erfüllt ist. Grundsätzlich ist und bleibt damit eine Verarbeitung personenbezogener Daten zunächst einmal unzulässig, es sei denn, der von der Datenverarbeitung Betroffene hat in diese wirksam eingewilligt oder die Datenverarbeitung lässt sich auf einen der sonstigen, gesetzlichen Erlaubnistatbestände stützen.

Die Kritik am Verbotsprinzip, die – wenig überraschend – auch in die Diskussion um die Datenschutz-Grundverordnung Eingang gefunden hat, ist nicht neu. Die Hauptvorwürfe lassen sich dahingehend zusammenfassen, dass ein Verbotsprinzip die Grundrechtspositionen der datenverarbeitenden Stelle verkenne („Kommunikationsverbot") und alle Datenverarbeiter über einen Kamm schere (auch den harmlosen „Bäcker um die Ecke").[20] Als moderne und innovative Alternative zum Verbotsprinzip wird von den Kritikern dann ein sog. risikobasierter Regelungsansatz propagiert, der nicht alle Vorgänge der Datenverarbeitung gleich behandelt, sondern diese je nach ihrem Risikopotential unterschiedlich streng reguliert.

Gegen einen solchen risikobasierten Ansatz ist zunächst einmal wenig einzuwenden. Nicht nachvollziehbar ist allerdings, warum dieser als mit dem Verbotsprinzip unvereinbar präsentiert wird. Das Datenschutzrecht reguliert seit jeher – auch unter Geltung des Verbotsprinzips – risikobasiert und auch die Grundverordnung behält dies so bei: Die Verordnung differenziert nach mehr oder weniger sensiblen Daten (Art. 9), sie berücksichtigt das Gefährdungspotential von Datenverarbeitungsprozessen im Rahmen der gesetzlichen Erlaubnistatbestände, etwa über die schutzwürdigen Interessen des Betroffenen (vgl. Art. 6 Abs. 1 lit. f), sie verpflichtet zur Durchführung einer Datenschutz-Folgeabschätzung (Art. 33) usw. Ebenso misst das Datenschutzrecht seit jeher auch den Grundrechtspositionen der datenverarbeitenden Stellen eine hohe Bedeutung bei – nicht nur in Form des Medienprivilegs, sondern auch im Rahmen der gesetzlichen Erlaubnistatbestände und last but not least durch die Möglichkeit, über den Weg des privatautonomen Interessenausgleichs (Einwilligung) die Erlaubnis zur Datenverarbeitung zu erlangen.[21]

Unabhängig davon bleibt die Kritik am Verbotsprinzip auch noch zwei andere Antworten schuldig. Zum einen, wie sich eine Abkehr vom Verbotsprinzip mit Art. 8 GRCh vereinbaren lassen soll: Nach Art. 8 Abs. 2 GRCh bedarf jede Verarbeitung per-

16 Ausführlich dazu *Richter*, DuD 2015, 735, 737 f.; s.a. *Roßnagel/Nebel/Richter*, ZD 2015, 455, 457 f.

17 Positionspapier der DSK zur Datenschutz-Grundverordnung vom August 2015 (DuD 2015, 722). Ausführlich zur Frage, ob und inwieweit der Zweckbindungsgrundsatz grundrechtlich vorgegeben ist, *von Grafenstein*, DuD 2015, 789 ff.

18 Siehe die Beispiele bei *Roßnagel/Nebel/Richter*, a.a.O., für eine genaue und eindeutige Zweckbestimmung: „Reise nach Mallorca im Mai 2015" oder „Bearbeitung des Antrags auf Sondernutzungsgenehmigung v. 15.7.2015"; zum notwendigen „Präzisionsgrad" der Zweckangabe siehe auch *von Grafenstein*, DuD 2015, 789, 793 f.

19 *Richter*, DuD 2015, 735, 739.

20 Vgl. u.a. die Stellungnahme des DAV zum Verordnungsvorschlag (47/2012), S. 15; *Schneider/Härting*, ZD 2012, 199, 202; *Veil*, ZD 2015, 347; kritisch auch *Kramer*, DuD 2013, 380 f., in seiner Anmerkung zu *Weicherts* Plädoyer zugunsten des Verbotsprinzips in DuD 2013, 246 ff. Wie *Weichert* für eine Beibehaltung des Verbotsprinzips auch *Karg*, DuD 2013, 75 ff., sowie *Eckhardt/Kramer*, DuD 2013, 287, 289.

21 Für die Verordnung siehe Art. 80 (Verarbeitung personenbezogener Daten und Freiheit der Meinungsäußerung und Informationsfreiheit) sowie Art. 6 (Rechtmäßigkeit der Datenverarbeitung).

sonenbezogener Daten einer Einwilligung des Betroffenen oder einer gesetzlichen Legitimation. Ausgangspunkt des Art. 8 GRCh ist, „dass der Einzelne grundsätzlich selbst Herr seiner Daten sein soll".[22] Realistisch ist dies nur, wenn zumindest im Ausgangspunkt nicht das Prinzip der Verarbeitungsfreiheit, sondern das des Verarbeitungsverbots gilt.[23] Zum anderen bleibt auch unklar, weshalb das Verbotsprinzip als so „unmodern" und mit der heutigen Informationsökonomie unvereinbar eingeordnet wird. Das Gegenteil ist der Fall: Selbst bei einer rein effizienzorientierten, ökonomischen Herangehensweise an das Datenschutzrecht bedarf es im Ausgangspunkt eines Rechts des Einzelnen an „seinen" Daten, um eine effiziente Verteilung des Wirtschaftsguts Daten zu gewährleisten. Unter dem Modell einer ökonomischen Analyse des Rechts lässt sich zeigen, dass die Transaktionskosten im Falle anfänglicher Informationsfreiheit so prohibitiv hoch wären, dass dies eine Verschiebung von Daten an den Ort ihrer effizientesten Verwendung von vornherein unmöglich machen würde. Bei einem anfänglichen Recht an den eigenen Daten hingegen fällt die Höhe der Transaktionskosten ungleich niedriger aus, so dass eine effiziente Informationsverteilung erheblich wahrscheinlicher und leichter zu erreichen ist.[24]

3.2 Einwilligung

Dass die Einwilligung unter der Grundverordnung in der Bedeutungslosigkeit versinken wird, weil an ihre Wirksamkeit zu hohe Anforderungen gestellt werden,[25] steht kaum zu erwarten. Die Voraussetzungen, die nach der Verordnung für eine wirksame Einwilligung gelten, sind allesamt Selbstverständlichkeiten – jedenfalls dann, wenn man die Einwilligung auch tatsächlich als Ausdruck privatautonomer Selbstbestimmung ernst nehmen möchte. Wie auch schon bislang gilt, dass eine Einwilligung nur wirksam ist, wenn sie ohne Zwang, für den konkreten Fall und in Kenntnis der Sachlage erteilt wird. Neu, und uneingeschränkt zu begrüßen ist, dass die Verordnung mit dem Erfordernis einer eindeutigen Handlung (clear affirmative action) den bislang so beliebten Opt out-Varianten der Einholung einer Einwilligung eine klare Absage erteilt.[26] Erwägungsgrund 25 führt in diesem Zusammenhang explizit auch das (Negativ-)Beispiel der „pre-ticked boxes" an. Künftig wird es also nicht mehr dazu kommen, dass dem Betroffenen ein Einverständnis mit der Datenverarbeitung allein deshalb unterstellt wird, weil sich eine entsprechende Einwilligungsklausel bereits vorformuliert (und ggf. angekreuzt bzw. „angeklickt") im Vertragswerk befindet. Anders als bislang ist es künftig nicht mehr am einzelnen Betroffenen, durch Auskreuzen, Ausklicken, Durchstreichen o.Ä. die unterstellte Einwilligung im konkreten Fall wieder hinfällig zu machen. Vielmehr ist es am jeweiligen Unternehmen, dafür Sorge zu tragen, dass Kunden, Nutzer etc. eine Einwilligung – aktiv – erteilen, wenn das Unternehmen eine Verarbeitung personenbezogener Daten über das gesetzlich zulässige Maß hinaus anstrebt.[27]

Ausscheiden soll die Einwilligung als Erlaubnistatbestand für eine Datenverarbeitung, wenn zwischen Betroffenem und Datenverarbeiter ein „klares Ungleichgewicht" (clear imbalance) besteht. Beispielhaft führt Erwägungsgrund 34 die Konstellation an, dass Daten durch eine Behörde verarbeitet werden und die konkreten Umstände des Einzelfalls es als unwahrscheinlich ansehen lassen, dass die Einwilligung uneingeschränkt freiwillig erteilt worden ist. Sicherlich sind über dieses Beispiel hinaus auch Konstellationen denkbar, in denen im Verhältnis zu nicht-staatlichen Datenverarbeitern ein klares Ungleichgewicht besteht. Im Kommissionsentwurf wurde noch beispielhaft das Abhängigkeitsverhältnis zwischen Arbeitgeber und Arbeitnehmer angesprochen. Und auch zwischen Verbraucher und Unternehmen mag ein solches Ungleichgewicht in bestimmten Konstellationen anzunehmen sein, insbesondere dann, wenn ein Unternehmen eine Monopolstellung am Markt hat und der Einzelne auf die Dienstleistungen oder Produkte dieses Unternehmens angewiesen ist. Zu weit geht es aber sicherlich, ein klares Ungleichgewicht „praktisch immer"[28] im Verkehr zwischen Unternehmen und Verbrauchern anzunehmen und mit dieser Argumentation die Relevanz der Einwilligung als Legitimationsgrundlage für eine Datenverarbeitung insgesamt in Zweifel ziehen zu wollen.

Schließlich scheidet eine Einwilligung als Erlaubnistatbestand für eine Datenverarbeitung künftig auch dann aus, wenn zu verschiedenen Datenverarbeitungsvorgängen nicht gesondert eine Einwilligung erteilt werden kann, obwohl dies im Einzelfall angebracht ist, oder wenn die Erfüllung eines Vertrags von der Einwilligung abhängig gemacht wird, obwohl dies für die Vertragserfüllung nicht erforderlich ist (Erwägungsgrund 34; letzteres Koppelungsverbot findet sich ausdrücklich auch in Art. 7 Abs. 4 normiert). Die bislang gängige „Take it or leave it"-Attitüde der großen Online-Anbieter wird sich in Anbetracht dieser Einschränkung so nicht einfach weiter fortsetzen lassen. Im Falle einer Suchmaschine etwa ist es angebracht, eine gesonderte Einwilligung für die langfristige Speicherung und Auswertung des Suchverhaltens einzuholen – und dies ist eben gerade nicht erforderlich, um die Suchdienstleistung als solche zu erbringen, und darf daher auch nicht zur Bedingung der Diensterbringung gemacht werden. Ebenso wie es bei einem sozialen Netzwerk angebracht ist, dass Nutzer in die Speicherung und Auswertung ihres Clickstreams, ihrer Kommunikation, ihrer Kontakte etc. jeweils separat (und zwar in Form eines Opt in – s.o.) einwilligen – und auch all diese Datenverarbeitungsprozesse sind keineswegs erforderlich, um die Grundfunktionen eines sozialen Netzwerks erbringen zu können, weshalb die Einwilligung auch nicht im Wege des „take it or leave it" eingeholt werden darf.

Verfrüht wäre es allerdings, diese Einschränkungen automatisch mit einem Ende der bisherigen Kostenloskultur im Netz gleichzusetzen. „Kostenlos" waren diese Angebote auch bislang nur dann, wenn man „Kosten" auf die Bezahlung in Form von Euro und Cent reduziert und ausblendet, dass gerade in der Online-Welt schon seit langem auch personenbezogene Daten eine Art von Währung sind. Und es ist auch keineswegs ausgeschlossen, dass Anbieter auch künftig auf Grundlage einer Einwilligung

22 *Frenz,* Handbuch Europarecht (2009), Bd. 4, Rn. 1380; ähnlich *Streinz/Michl*, EuZW 2011, 384, 385.

23 Zur Drittwirkung des Art. 8 GRCh als „selbstverständliche Reaktion" auf die globale Marktmacht von Unternehmen wie Google siehe *von Danwitz*, DuD 2015, 581, 585.

24 Näher dazu *Buchner*, Informationelle Selbstbestimmung im Privatrecht (2006), S. 175 ff.

25 So die Sorge von *Härting* in: Legal Tribune Online v. 16.12.2015 („Trilog erfolgreich, Einwilligung tot").

26 Siehe dazu schon *Caspar*, DuD 2013, 767, 770.

27 Ausführlich *Tinnefeld/Buchner/Petri*, Einführung in das Datenschutzrecht (2012), S. 353 ff.

28 So aber *Härting* a.a.O.

eine Dienstleistung im Tausch gegen personenbezogene Daten des Nutzers anbieten. „Angebracht" und „erforderlich" im Sinne der Verordnung ist die Einholung einer solchen Einwilligung vielmehr stets dann, wenn es sich bei dem Angebot dem Grunde nach um eben diesen Tausch Leistung gegen Daten handelt. Nur muss dann der eigentliche Kern dieses Angebots auch als solcher präsentiert und dem Nutzer transparent gemacht werden. Wenn daher Google, Facebook und Co ihr Geschäftsmodell auch unter der Verordnung weiter praktizieren wollen, können sie sich ihren Nutzern gegenüber nicht mehr als Anbieter von „kostenlosen" Suchdiensten, sozialen Netzwerken etc. präsentieren, sondern nur als das, was sie zuallererst einmal sind: als Datenhändler, die sich die Erlaubnis (= Einwilligung) zur wirtschaftlichen Verwertung unserer Daten mit bestimmten Dienstleistungen erkaufen. Und der Vertrag mit Google, Facebook und Co ist dann eben nicht mehr ein unentgeltlicher Dienstvertrag o.Ä., sondern ein entgeltlicher Kauf- bzw. Tauschvertrag über personenbezogene Daten und muss auch unmissverständlich als solcher transparent gemacht werden.[29] Das, was der Verbraucherzentrale Bundesverband (vzbv) aktuell in seiner Klage gegen Facebook beim LG Berlin zu Recht als irreführende Werbung einordnet, die Äußerung „Facebook ist und bleibt kostenlos",[30] ist künftig nicht nur wettbewerbsrechtlich, sondern auch datenschutzrechtlich unzulässig.

3.3 Gesetzliche Erlaubnistatbestände

Nach dem Vorbild der Richtlinie sieht auch die Verordnung zusätzlich zur Einwilligung eine Reihe von Erlaubnistatbeständen vor, auf deren Grundlage eine Verarbeitung personenbezogener Daten zulässig ist. Inhaltlich entsprechen diese gesetzlichen Erlaubnistatbestände ebenfalls weitestgehend denen der Richtlinie und zählen folgende Konstellationen auf, die (im Rahmen der Erforderlichkeit) eine Datenverarbeitung legitimieren können (Art. 6 Abs. 1 lit. b bis f):

- Datenverarbeitung zur Durchführung eines Schuldverhältnisses
- Datenverarbeitung zur Erfüllung einer gesetzlichen Verpflichtung
- Datenverarbeitung zum Schutz lebenswichtiger Interessen
- Datenverarbeitung zur Wahrnehmung einer Aufgabe, die im öffentlichen Interesse liegt oder in Ausübung öffentlicher Gewalt erfolgt
- Datenverarbeitung auf Grundlage einer Interessenabwägung.

Vergleichbar ist die Verordnung mit der Richtlinie schließlich auch dahingehend, dass sie – eher im Stile einer Richtlinie als einer Verordnung – den Mitgliedstaaten für die Frage der Rechtmäßigkeit einer Datenverarbeitung in mancherlei Hinsicht einen Regelungsspielraum zugesteht. Sowohl hinsichtlich der Verarbeitung personenbezogener Daten zur Erfüllung einer rechtlichen Verpflichtung als auch hinsichtlich der Datenverarbeitung zur Wahrnehmung einer Aufgabe, die im öffentlichen Interesse liegt oder in Ausübung öffentlicher Gewalt erfolgt, können die Mitgliedstaaten im nationalen Recht spezifischere Anforderungen für die Datenverarbeitung normieren und auch sonstige Maßnahmen präziser bestimmen, um eine Verarbeitung nach Recht und Gesetz zu gewährleisten (siehe im Einzelnen Art. 6 Abs. 2a).[31]

Grundsätzlich stehen für eine Normierung gesetzlicher Erlaubnistatbestände zwei Regelungsmodelle zur Verfügung: Die Normierung kann entweder auf eine möglichst bereichsspezifische und detaillierte Regulierung abzielen, um den Rechte- und Interessenkonstellationen des jeweiligen Regelungsgegenstandes möglichst passgenau Rechnung zu tragen. Oder aber es erfolgt ein Rückgriff auf offen gehaltene Generalklauseln, die für eine Vielzahl auch ganz unterschiedlicher Rechte- und Interessenkonstellationen gelten. Die Verordnung hat augenscheinlich letzteren Weg gewählt, was mit Blick auf ihren umfassenden Geltungsanspruch auch nicht sonderlich überraschend ist. Jedoch geht mit jeder Unbestimmtheit datenschutzrechtlicher Erlaubnistatbestände stets auch eine entsprechende Rechtsunsicherheit einher. In besonderem Maße gilt dies für die Interessenabwägungsklausel des Art. 6 Abs. 1 lit. f. Die weitestgehend inhaltslosen und dehnbaren Kriterien eines berechtigten Verarbeitungs- und eines überwiegenden Betroffeneninteresses eröffnen eine so weitgehende Variationsbreite möglicher Norminterpretationen, dass praktisch jede Datenverarbeitung – je nach rechtspolitischer Positionierung – als zulässig oder unzulässig eingeordnet werden kann. Irgendeine Richtung, wie gegenläufige Interessen zu gewichten sind, gibt die Verordnung gerade nicht vor.[32]

Allerdings ist diese Herausforderung alles andere als neu, sie ist auch schon aus dem bisherigen Datenschutzrecht mit seinen allgemeinen Interessenabwägungsklauseln hinlänglich bekannt. Und so wird es denn auch weiterhin Aufgabe von Aufsichtsbehörden und Rechtsprechung sein, den gesetzlichen Allgemeinklauseln Konturen zu verleihen – und in letzter Instanz dann Sache des EuGH, die Auslegung einer unionsweiten Vereinheitlichung zuzuführen.[33] Der Ansatz, dass darüber hinaus auch die Kommission im Wege der delegierten Rechtssetzung für eine – von Anfang an einheitliche – Konkretisierung der Interessenabwägung je nach Bereich und Verarbeitungssituation sorgt, hat sich letztlich im Gesetzgebungsverfahren nicht durchsetzen können.[34]

4 Vereinheitlichung des europäischen Datenschutzrechts dank Verordnung?

Ganz grundsätzlich bleibt abzuwarten, wie viel mehr die neue Verordnung im Vergleich zur bisherigen Richtlinie an Harmonisierungskraft im europäischen Datenschutzrecht entfalten wird. Die Frage stellt sich vor allem mit Blick auf die weitreichenden Möglichkeiten, die die Verordnung den Mitgliedstaaten einräumt, Ausnahmen, Beschränkungen, Konkretisierungen u.Ä. im einzelstaatlichen Recht zu normieren.

29 Um beim Beispiel Facebook zu bleiben: Auf der Website steht dann künftig nicht mehr „Facebook ermöglicht es dir, mit den Menschen in deinem Leben in Verbindung zu treten und Inhalte mit diesen zu teilen", sondern vielmehr „Facebook möchte von dir eine Erlaubnis zur Verarbeitung, Auswertung und wirtschaftlichen Nutzung deiner personenbezogenen Daten und bietet dir dafür als Gegenleistung die Möglichkeit, mit den Menschen in deinem Leben in Verbindung zu treten und Inhalte mit diesen zu teilen."

30 Siehe Pressemitteilung des vzbv vom 16.10.2015 unter http://www.vzbv.de/pressemitteilung/vzbv-klagt-gegen-facebook.

31 Der Sache nach soll damit in erster Linie eine Befugnis zur Bewahrung und Fortentwicklung des mitgliedstaatlichen Datenschutzrechts im öffentlichen Bereich eingeräumt werden; vgl. BR-Drs. 290/15, S. 2; *Will*, ZD 2015, 345. Siehe dazu auch schon oben unter 1 (Anwendungsbereich).

32 Vgl. *Sydow/Kring*, ZD 2014, 271, 272.

33 Zur Sicherung einer einheitlichen Anwendung der DS-GVO durch den neu einzurichtenden Europäischen Datenschutzausschuss siehe Art. 66 der Verordnung; dessen Mittel hierzu sind jedoch hauptsächlich beratender Art (*Roßnagel/Nebel/Richter*, ZD 2015, 455).

34 Anders noch als im Entwurf der Kommission; siehe zu diesem Aspekt auch noch unten 4.2.

4.1 Regelungsspielräume für die Mitgliedstaaten

Die Kompetenz der Mitgliedstaaten, auch unter der Verordnung eigene datenschutzrechtliche Vorgaben zu normieren, beschränkt sich nicht auf die oben bereits erwähnte Befugnis, im öffentlichen Bereich spezifischere Anforderungen für die Datenverarbeitung festzulegen. Auch darüber hinaus räumt die Verordnung in vielerlei Hinsicht den Mitgliedstaaten die Möglichkeit ein, im einzelstaatlichen Recht datenschutzrechtliche Vorgaben zu normieren. Zu den wichtigsten Regelungsspielräumen, die den Mitgliedstaaten unter der Verordnung bleiben, zählen:

- die Befugnis, weitere Bedingungen, einschließlich möglicher Beschränkungen, für eine Verarbeitung besonderer Arten personenbezogener Daten (Art. 9) zu normieren, insbesondere im Fall von genetischen und biometrischen sowie Gesundheitsdaten (Art. 9 Abs. 5)
- die Möglichkeit, das Mindestalter für die Einwilligungsfähigkeit Minderjähriger abweichend von den in Art. 8 Abs. 1 vorgesehenen 16 Jahren auf bis zu 13 Jahre abzusenken
- die Normierung von Ausnahmen von der Informationspflicht nach Art. 14a (Informationspflicht, wenn die Daten nicht bei der betroffenen Person erhoben wurden), vom Recht auf Löschung nach Art. 17 sowie vom Verbot der automatisierten Einzelentscheidung nach Art. 20
- die generelle Befugnis nach Art. 21, zu den verschiedensten, im öffentlichen Interesse liegenden Zwecken die folgenden Rechte und Pflichten zu beschränken: die in Art. 12 bis 20 normierten Betroffenenrechte, die Benachrichtigungspflicht für den Fall einer Verletzung des Schutzes personenbezogener Daten sowie die allgemeinen Grundsätze des Art. 5, soweit sich diese auf die Betroffenenrechte nach Art. 12 bis 20 beziehen
- die Schaffung rechtlicher Grundlagen für eine Auftragsdatenverarbeitung (Art. 26 Abs. 2)
- die Entscheidung, ob eine Datenschutz-Folgeabschätzung nach Art. 33 auch bei einer Datenverarbeitung durchzuführen ist, die zur Erfüllung einer rechtlichen Verpflichtung oder zur Wahrnehmung einer Aufgabe im öffentlichen Interesse / in Ausübung öffentlicher Gewalt erfolgt (Art. 6 Abs. 1 Buchstabe c und e)
- die Normierung einer Genehmigungspflicht im Fall der Datenverarbeitung zur Erfüllung einer im öffentlichen Interesse liegenden Aufgabe (einschließlich der Datenverarbeitung zu Zwecken des sozialen Schutzes und der öffentlichen Gesundheit; Art. 34 Abs. 7a)
- die Normierung einer Pflicht zur Benennung eines Datenschutzbeauftragten auch über die in Art. 35 Abs. 1 normierten Konstellationen hinaus (Art. 35 Abs. 4)
- die Möglichkeit der Beschränkung von Datenübermittlungen an Drittländer oder internationale Organisationen aus wichtigen Gründen des öffentlichen Interesses (Art. 44 Abs. 5a)
- die Möglichkeit, die Aufsichtsbehörden mit zusätzlichen Befugnissen (über die in Art. 53 normierten) auszustatten (Art. 53 Abs. 4)
- die Entscheidung, ob Einrichtungen, Organisationen und Verbände i.S.v. Art. 76 Abs. 1 auch unabhängig von einem Auftrag der betroffenen Person deren Rechte nach Art. 73 bis 75 geltend machen können
- die Festlegung, ob und in welchem Umfang gegen öffentliche Behörden und Einrichtungen Geldbußen verhängt werden können (Art. 79 Abs. 3b)
- die Sanktionierung von Verstößen, die nicht unter Art. 79 fallen (Art. 79b)
- das gesetzliche Austarieren von Datenschutz und Meinungs- sowie Informationsfreiheit einschließlich der Normierung von Abweichungen und Ausnahmen von den Vorgaben der Verordnung im Falle der Datenverarbeitung zu journalistischen, wissenschaftlichen, künstlerischen und literarischen Zwecken (Art. 80)
- die Normierung spezifischer Bedingungen für eine Verarbeitung nationaler Kennziffern oder anderer Kennzeichen von allgemeiner Bedeutung (Art. 80b)
- die Normierung spezifischerer Vorschriften zur Gewährleistung des Beschäftigtendatenschutzes (Art. 82)
- die Normierung diverser Ausnahmen von den Betroffenenrechten im Fall einer Datenverarbeitung für Archivzwecke oder für wissenschaftliche, historische und statistische Zwecke (Art. 83)
- die Regelung bestimmter aufsichtsbehördlicher Befugnisse gegenüber (Berufs-)Geheimnisträgern (Art. 84).

4.2 Regelungskompetenzen der Kommission

Im Unterschied zu den großzügigen Regelungsspielräumen, die die Verordnung den Mitgliedstaaten zubilligt, ist von den zahlreichen Befugnissen der Kommission zu einer delegierten Rechtssetzung, die sich diese in ihrem Entwurf von 2012 selbst eingeräumt hatte, letztlich nur noch wenig übrig geblieben. Hatte der Kommissionsentwurf noch in 26 Fällen die Kompetenz der Kommission vorgesehen, unbestimmte Regelungen des Verordnungsentwurfs durch delegierte Rechtsakte nachträglich zu konkretisieren, so ist nunmehr die Befugnis der Kommission zum Erlass delegierter Rechtsakte auf nur noch zwei Punkte beschränkt: die Festlegung, auf welche Art und Weise standardisierte Icons als Informationsmittel eingesetzt werden können und welche Informationen diese präsentieren müssen (Art. 12 Abs. 4c), sowie die Festlegung von Anforderungen, die bei Zertifizierungsverfahren zu berücksichtigen sind (Art. 39a Abs. 7).

Mit Blick auf Gewaltenteilung sowie demokratische und transparente Rechtssetzung mag man die fast vollständige Streichung der Rechtssetzungsbefugnisse der Kommission zunächst einmal begrüßen.[35] Zu Recht wird andererseits aber auf das Problem verwiesen, dass sich damit im Rahmen der Verordnung die Gewichtung zwischen zentraler und dezentraler Rechtssetzung nochmals in Richtung Letzterer verschiebt.[36] Die Kombination von teils sehr allgemein gehaltenen Vorgaben der Verordnung, weiten Regelungsspielräumen der Mitgliedstaaten und fehlender Konkretisierungsbefugnis der Kommission lässt erwarten, dass die Auslegung der datenschutzrechtlichen Vorgaben der Verordnung zunächst einmal dezentral in den Mitgliedstaaten bestimmt wird und damit das Ziel einer Vereinheitlichung in weite Ferne rückt.[37]

35 *Roßnagel/Nebel/Richter*, ZD 2015, 455; *Pötters*, RDV 2015, 10, 15; das Instrument der delegierten Rechtssetzung hingegen grundsätzlich befürwortend *Sydow/Kring*, ZD 2014, 271 , 273 f.

36 *Roßnagel/Nebel/Richter*, a.a.O.

37 Zum Beispiel der Auslegung der Interessenabwägungsklauseln s. schon oben 3.3. Zur divergierenden Auslegung und Durchsetzung des neuen europäischen Datenschutzrechts durch die Aufsichtsbehörden s. *Ashkar*, DuD 2015, 796, 800.

4.3 Die Grundverordnung und das nationale Datenschutzrecht

Mit der Vielzahl an Regelungsgegenständen, die letztlich auf die Mitgliedstaaten übertragen worden sind, geht einher, dass es auch zur bis dato immer wieder prognostizierten Bedeutungslosigkeit des nationalen Datenschutzrechts nicht kommen wird bzw. zumindest nicht kommen muss – je nachdem, wie viel Notwendigkeit und Interesse der nationale Gesetzgeber verspürt, die ihm eröffneten Spielräume zu nutzen.

Betrachtet man die Regelungsspielräume im Einzelnen, fällt auf, dass diese gerade auch solche Fragestellungen betreffen, die hierzulande seit langem einer klaren und konsistenten Regelung harren, egal ob es um große Würfe wie den Gesundheits- oder Beschäftigtendatenschutz geht[38] oder auch nur um Einzelfragen wie die der Einwilligungsfähigkeit von Minderjährigen.[39] Bei anderen Fragestellungen wiederum hat sich das deutsche Datenschutzrecht bereits eindeutig positioniert, etwa bei der Pflicht zur Bestellung eines Datenschutzbeauftragten[40] oder auch – erst jüngst – beim Verbandsklagerecht im Fall von Datenschutzverstößen.[41] Schließlich finden sich auch Regelungsgegenstände, die im deutschen Recht bereits eine Normierung erfahren haben, bei denen die Verordnung aber Anlass dazu bietet, diese Normierung nochmals auf den Prüfstand zu stellen und zu überarbeiten. Verwiesen sei insoweit etwa auf § 41 BDSG, der mit seiner pauschalen Freistellung der Presse von den datenschutzrechtlichen Vorgaben bereits den Anforderungen von Art. 9 DS-RL nicht hinreichend Rechnung trägt[42] und künftig erst recht nicht den Vorgaben von Art. 80 Abs. 2 DS-GVO.

Mit Blick auf die Vielgestaltigkeit der Regelungsmöglichkeiten und -notwendigkeiten lässt sich bislang auch noch kaum prognostizieren, in welcher Form der deutsche Gesetzgeber diese umsetzen wird: neue bereichsspezifische Regelungen, punktuelle Beibehaltung bestehender Regelungen, ein neues „Begleitgesetz"? Unklar ist daher insbesondere auch die Zukunft des BDSG; denkbar ist durchaus, dass es – umfassend überarbeitet und ausgedünnt – auch unter Geltung der DS-GVO fortbesteht. Der Abschied von den §§ 11 ff. TMG zum Online-Datenschutz dürfte hingegen feststehen. Zum einen würde eine bereichsspezifische Regulierung des Onlinebereichs dem Anspruch der DS-GVO widersprechen, Datenschutz „technologieneutral" zu gewährleisten.[43] Zum anderen fehlt es an einschlägigen Öffnungsklauseln in der Verordnung, auf die sich eine sektorspezifische Regelung des Onlinebereichs stützen ließe.[44] Anders sieht es wiederum bei den Regelungen der §§ 91 ff. TKG zum Telekommunikationsdatenschutz aus: Im Widerspruch zum gerade erwähnten „technologieneutralen" Ansatz sieht Art. 89 DS-GVO vor, dass den Anbietern öffentlich zugänglicher elektronischer Kommunikationsdienste durch die Verordnung „keine zusätzlichen Pflichten" auferlegt werden sollen, soweit diese Anbieter besonderen Pflichten aus der Datenschutzrichtlinie für die elektronische Kommunikation (ePrivacy-Richtlinie; EK-DS-RL)[45] unterliegen, die dasselbe Ziel verfolgen. Soweit die §§ 91 ff. TKG daher auf der EK-DS-RL beruhen, gelten sie auch unter der Datenschutz-Grundverordnung weiter. Jedoch hat die EU-Kommission bereits eine Revision der ePrivacy-Richtlinie mit Mindestvorgaben für den Datenschutz in der Telekommunikation angekündigt.[46]

5 Fazit

Obige Ausführungen betreffen nur einige wenige Aspekte des neuen europäischen Datenschutzrechts – in Zahlen ausgedrückt: die Art. 1 bis 9 der Verordnung und damit gerade einmal rund ein Zehntel aller Bestimmungen der Verordnung. Und auch innerhalb dieses engen Rahmens haben sich die Ausführungen darauf beschränkt, einige wenige Problempunkte anzuschneiden und Lösungsoptionen anzudeuten. Jedoch zeigt bereits dieser kleine Ausschnitt, welche Chancen, aber auch welche Risiken die Verordnung für den künftigen europäischen Datenschutz birgt – je nachdem, wie die Mitgliedstaaten ihre Regelungsspielräume nutzen und welche Auslegung all die mehr oder weniger unbestimmten Regelungen erfahren werden.

38 Ausführlich zur Reformbedürftigkeit des Gesundheitsdatenschutzrechts *Kingreen/Kühling* (Hrsg.), Gesundheitsdatenschutzrecht (2015); speziell für den Bereich E-Health s. *Kühling/Klar* DuD 2013, 791 ff. Zum Beschäftigtendatenschutz im einzelstaatlichem Recht unter der Grundverordnung siehe schon *Schüßler/Zöll*, DuD 2013, 639 ff.

39 Dazu *Gola/Schulz*, ZD 2013, 475 ff.

40 § 4f BDSG.

41 Das Gesetz zur Verbesserung der zivilrechtlichen Durchsetzung von verbraucherschützenden Vorschriften des Datenschutzrechts wurde am 17.12.2015 vom Bundestag beschlossen; s. dazu auch DuD 2015, 487.

42 Siehe dazu BeckOK DatenSR/*Buchner*, BDSG § 41, Rn. 2 und *Simitis/Dix*, BDSG (2014), § 41, Rn. 6.

43 Erwägungsgrund 13.

44 Vgl. *Keppeler*, MMR 2015, 779, 780 f.

45 Richtlinie 2002/58/EG vom 12. Juli 2002 über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre in der elektronischen Kommunikation.

46 *Maas*, DuD 2015, 579 f.