Niko Härting, RA

# Starke Behörden, schwaches Recht – der neue EU-Datenschutzentwurf

**Seit dem 25.1.2012 liegt der lang erwartete Vorschlag der EU-Kommission für eine umfassende Erneuerung des europäischen Datenschutzrechts vor. An die Stelle der Datenschutzrichtlinie 95/46 EG vom 24.10.1995 (DSRL) soll eine „Datenschutz-Grundverordnung" (DS-GVO) treten (KOM(2012) 11 endg.). Daneben soll es eine neue Richtlinie für die behördliche Datenverarbeitung zwecks Verhütung, Aufdeckung, Untersuchung oder Verfolgung von Straftaten oder der Strafvollstreckung (KOM(2012) 10 endg.) geben. Einige wesentliche Regelungskomplexe der DS-GVO werden nachfolgend einer ersten Analyse unterzogen, wobei die Bestimmungen zur Übermittlung von Daten in Drittländer (Art. 40 bis 45 DS-GVO) ausgeklammert bleiben.**

## I. Risiken und Chancen der Informationsgesellschaft

Die DS-GVO soll für alle Unternehmen verbindlich werden, die in einem der Mitgliedstaaten der EU niedergelassen sind. Darüber hinaus beansprucht die DS-GVO Geltung für außereuropäische Unternehmen, die sich (auch) an europäische Kunden wenden. All diese Unternehmen sollten den Diskussionsprozess, den der Entwurf in Gang setzt, sorgfältig verfolgen. Ob und inwieweit der Entwurf in seiner jetzigen Fassung Bestand haben wird, ist nicht absehbar. Ohne Zweifel wird der Entwurf jedoch früher oder später in einen neuen europäischen Rechtsrahmen münden, der die Rahmenbedingungen des Datenschutzes in ganz Europa über Jahre hinaus bestimmen wird.

Seit vielen Jahren sind sich Experten darüber einig, dass das geltende Datenschutzrecht den Anforderungen der Informationsgesellschaft des 21. Jahrhunderts nicht gerecht wird.[1] Die DSRL ist in den Vorstellungen und Instrumentarien der 70er-Jahre des vorigen Jahrhunderts verhaftet. Das geltende Datenschutzrecht stammt aus der Zeit der Großrechner und einer Ära der Straßenproteste, Großdemonstrationen, Bürgerinitiativen, Berufsverbote, Terroristenprozesse, „Gewissensprüfungen" und „Rosa Listen".[2] In der digitalisierten Informationsgesellschaft des Jahres 2012 prägen Prozesse der Datenverarbeitung das Alltagsleben. Daten sind der Rohstoff für zahlreiche Formen der Information und Kommunikation.[3] Eine unternehmerische Betätigung unter Verzicht auf die automatisierte Verarbeitung von Daten ist nicht mehr vorstellbar.

Die BVerfG-Entscheidungen zur Online-Durchsuchung[4] und zur Vorratsdatenspeicherung[5] liefern anschauliche Beispiele dafür, dass die Digitalisierung zwangsläufig zu einer unübersehbaren Menge von „Datenspuren" führt. Die Nutzung von Alltagsgeräten wie Laptops und Smartphones hinterlässt Datenbestände, deren Kenntnis einen „tiefen Einblick in die Persönlichkeit" ermöglicht. Ob nächtlicher Chat, diskreter Besuch auf gewissen Seiten oder der Austausch von SMS-Nachrichten mit geheimen Informationen: Die Spuren jedweder Kommunikation bedürfen des Schutzes gegen allzu neugierige Dritte. Dem Einblick durch staatliche Behörden müssen ebenso Grenzen gesetzt werden wie dem heimlichen Zugriff, den Unternehmen auf Datenbestände nehmen können. Die Regulierung darf dabei nicht als lästiges Hindernis für die vernetzte Information und Kommunikation verstanden werden. Nur wenn die Akteure darauf vertrauen können, dass es keinen ungezügelten, heimlichen Zugriff auf „Datenspuren" gibt, werden sie Computer, das Internet und Smartphones ungebremst nutzen. Das Vertrauen der Nutzer gehört zu den Grundbedingungen, die erfüllt sein müssen, damit sich die Informationsgesellschaft fortentwickeln kann. Um dieses Vertrauen zu sichern, bedarf es des Schutzes der Privatsphäre mit Instrumenten des Datenschutzes.[6]

Aber nicht nur die Privatsphäre ist schützenswert. Das Internet ist ein zentraler Bestandteil des öffentlichen Raums, in dem der Austausch von Informationen und die Kommunikation in einer offenen Gesellschaft stattfinden.[7] Und auch für den freien Wirtschaftsverkehr ist das Internet im 21. Jahrhundert unverzichtbar. Einseitigen Tendenzen, den Schutz der Privatsphäre zu überhöhen, muss das Recht entgegenwirken. „Meine Daten gehören mir."[8] Dies ist ein Satz, dem das BVerfG schon in seinem Volkszählungsurteil[9] deutlich durch den Hinweis widersprochen hat, dass es in einer offenen Gesellschaft keineswegs ein eigentumsähnliches Recht an Daten geben kann. Daten sind für die freie Kommunikation unverzichtbar. Sie sind stets (auch) ein „Abbild sozialer Realität":

„Der Einzelne hat nicht ein Recht im Sinne einer absoluten, uneinschränkbaren Herrschaft über ‚seine' Daten; er ist vielmehr eine sich innerhalb der sozialen Gemeinschaft entfaltende, auf Kommunikation angewiesene Persönlichkeit. Information, auch soweit sie personenbezogen ist, stellt ein Abbild sozialer Realität dar, das nicht ausschließlich dem Betroffenen allein zugeordnet werden kann."

Die vernetzte Informationsgesellschaft eröffnet Chancen, die noch vor zwei Jahrzehnten unvorstellbar waren: Das Internet gibt Menschen in aller Welt die Gelegenheit, sich frei und unzensiert zu informieren. Die Ereignisse im arabischen Raum haben jüngst deutlich gemacht, dass es Regierungen nicht mehr möglich ist, ihre Bürger von Informationen abzuschotten. Die Occupy-Bewegung und die Entwicklung der „Piraten" sind hierzulande Beispiele dafür, dass das Internet die Ausübung von Freiheitsrechten fördern kann und neue Organisationsformen ermöglicht.[10] Auch für die wirtschaftliche Ent-

1 Vgl. *Schneider/Härting*, ZD 2011, 63, 64 m. w. N.
2 Vgl. *Härting*, Internetrecht, 4. Aufl. 2010, Rn. 7 ff.
3 Vgl. *Härting/Schneider*, ZRP 2011, 233, 234.
4 BVerfG, 27.2.2008 – 1 BvR 370/07, 1 BvR 595/07, NJW 2008, 822 ff. – Online-Durchsuchung.
5 BVerfG, 2.3.2010 – 1 BvR 256/08, NJW 2010, 833 ff. – Vorratsdatenspeicherung.
6 Vgl. *Hoffmann-Riem*, JZ 2008, 1009, 1010 f.
7 Vgl. *Härting/Schneider*, ZRP 2011, 233 ff.
8 Vgl. *Künast*, ZRP 2008, 201 ff.
9 BVerfGE 65, 1, 41 f. – Volkszählung.
10 Vgl. *Härting/Schneider*, ZRP 2011, 233 ff.; *Schneider/Härting*, Leitlinien des Datenschutzes, abrufbar unter www.schneider-haerting.de/2011/09/leitlinien-des-datenschutzes (Abruf: 8.2.2012); Deutscher Anwaltverein, Stellungnahme zu dem Gesamtkonzept des Datenschutzes in der Europäischen Union, Stellungnahme 4/2011, abrufbar unter www.anwaltverein.de/downloads/Stellungnahmen-11/SN4-2011.pdf (Ab-

wicklung bietet das Netz neuen Freiraum: Indem Kunden in aller Welt direkt angesprochen werden, verkürzt sich der Weg neuer Unternehmen zum Markt. Das rasante Wachstum von jungen Unternehmen wie Google, eBay, Amazon und Facebook liefert hierfür faszinierendes Anschauungsmaterial.

## II. Defizite des geltenden Rechts

Das geltende europäische Datenschutzrecht leidet an zahlreichen Defiziten:[11]

- Die Terminologie und Instrumentarien des Datenschutzrechts sind nicht internettauglich. Dies führt zu erheblicher Rechtsunsicherheit.
- Das Datenschutzrecht baut auf dem Verbotsprinzip auf. Hierdurch werden die freie Kommunikation und die unternehmerische Betätigung übermäßig behindert.
- Das Datenschutzrecht behandelt grundsätzlich alle Daten gleich. Ob „harmlose" E-Mail-Adresse oder intime Informationen aus dem Sexualleben, das Datenschutzrecht kennt keine signifikanten Abstufungen.
- Es gibt ein erhebliches Vollzugsdefizit. Einem Dickicht aus Normen, das selbst für Experten oft schwer durchschaubar ist, stehen schwach ausgestattete Behörden gegenüber, die diese Normen durchsetzen sollen.
- In den einzelnen europäischen Staaten hat sich das Datenschutzrecht trotz der gemeinsamen Richtlinie unterschiedlich entwickelt. Nicht selten kommt es vor, dass ein und derselbe Datenverarbeitungsprozess in einem EU-Mitgliedstaat als rechtskonform und in anderen EU-Staaten als datenschutzwidrig angesehen wird.

## III. Der Entwurf einer DS-GVO: das zwiespältige Bild

Misst man den Entwurf einer DS-GVO an den vorstehenden Problemfeldern, so ergibt sich ein äußerst zwiespältiges Bild: Mit großer Akribie haben die Entwurfsverfasser ebenso innovativ wie kleinteilig Vorschriften entwickelt, die europaweit eine einheitliche Rechtsanwendung und Rechtspraxis gewährleisten und eine schlagfertige Behördenstruktur mit erheblicher Vollzugskraft schaffen sollen. Weit weniger innovativ sind die Vorschläge zum materiellen Datenschutzrecht. Bei näherer Betrachtung zeigt sich, dass sich die materiellen Bestimmungen der DS-GVO im Kern nicht wesentlich von den Bestimmungen der DSRL unterscheiden. Dies ist enttäuschend.

### 1. Rechtsdurchsetzung: die akribisch gebaute Kontrollpyramide

Der Entwurf umfasst 91 Artikel. Die Art. 46 bis 79 DS-GVO befassen sich ausschließlich mit der Rechtsdurchsetzung. Aber auch viele andere Artikel sind mehr oder weniger zentral um eine Rechtsdurchsetzung bemüht – bspw. Art. 29 DS-GVO, der die „Zusammenarbeit mit der Aufsichtsbehörde" zu einer der „allgemeinen Pflichten" eines jeden Datenverarbeiters erklärt.[12]

Jeglichen Vollzugsdefiziten wirkt der Entwurf entschlossen entgegen. Dabei setzt man ausschließlich auf den Vollzug durch staatliche Behörden. Mit großer Sorgfalt wird eine Pyramide von Gremien und Behörden errichtet, die den lückenlosen Vollzug des Datenschutzrechts und die flächendeckende Ahndung von Rechtsverstößen gewährleisten soll.

#### a) Die Spitze der Pyramide

An der Spitze der Pyramide steht die Europäische Kommission. In Art. 86 DS-GVO werden der Kommission umfangreiche Befugnisse eingeräumt, per delegiertem Rechtsakt datenschutzrechtliche Regelungen zu erlassen. An insgesamt 26 Stellen nehmen Vorschriften der DS-GVO auf Art. 86 Bezug und ermächtigen die Kommission, nähere Einzelheiten zu regeln.

Zu der Befugnisübertragung gem. Art. 86 DS-GVO treten zahlreiche Ermächtigungen der Kommission zum Erlass von Durchführungsrechtsakten gem. Art. 87 Abs. 2 und 3 DS-GVO hinzu. Durch diese Durchführungsrechtsakte soll die Kommission insbesondere in die Lage versetzt werden, technische Standards und Verfahren festzulegen.

Die weitreichende Delegierung von Regelungsbefugnissen an die Kommission führt dazu, dass es teilweise überhaupt erst einer Rechtssetzung durch die Kommission bedarf, um Grundsätze, die die DS-GVO aufstellt, in praktische Handlungsanforderungen umzusetzen. Dies ist bspw. bei dem Grundsatz der „Privacy by Design"[13] der Fall. Dieser Grundsatz, dem nach allen Verlautbarungen der Kommission[14] eine gewichtige Bedeutung bei der Modernisierung des Datenschutzrechts zukommen soll, ist in der DS-GVO nur in einem Programmsatz geregelt (Art. 23 Abs. 1 DS-GVO):

„Der für die Verarbeitung Verantwortliche führt unter Berücksichtigung des Stands der Technik und der Implementierungskosten sowohl zum Zeitpunkt der Festlegung der Verarbeitungsmittel als auch zum Zeitpunkt der Verarbeitung technische und organisatorische Maßnahmen und Verfahren durch, durch die sichergestellt wird, dass die Verarbeitung den Anforderungen dieser Verordnung genügt und die Rechte der betroffenen Person gewahrt werden."

Art. 23 Abs. 3 DS-GVO überlässt es der Kommission, diesen Programmsatz durch „weitere Kriterien und Anforderungen" in praktische Handlungsanforderungen „für ganze Sektoren und bestimmte Erzeugnisse und Dienstleistungen" umzusetzen. Art. 23 Abs. 4 DS-GVO ermächtigt die Kommission zudem, durch Durchführungsrechtsakte für „Privacy by Design" technische Standards festzulegen. Wenn es bei dem Entwurf der DS-GVO bleibt, ist es dem Belieben der Kommission überlassen, Vorstellungen zum „Privacy by Design" zu entwickeln und diese Vorstellungen europaweit durchzusetzen. Die Kommission würde auf diese Weise freie Hand bekommen, Standards zu schaffen und diese zugleich federführend durchzusetzen.

#### b) Der Europäische Datenschutzausschuss – eine zentrale Datenschutzbehörde für ganz Europa

Die zweite Ebene der Pyramide soll nach Art. 64 bis 72 DS-GVO der Europäische Datenschutzausschuss bilden, der an die Stelle der Datenschutzgruppe gem. Art. 29 DSRL treten und – anders als die Art. 29-Gruppe (vgl. Art. 29 Abs. 1 S. 2 DSRL) – nicht nur beratende Funktion haben soll.

Der Europäische Datenschutzausschuss soll aus dem Leiter einer Aufsichtsbehörde jedes EU-Mitgliedstaates und dem Europäischen Datenschutzbeauftragten bestehen (Art. 64 Abs. 2 DS-GVO). Gem. Art. 65

ruf: 8.2.2012); Stellungnahme der DGRI zur DS-GVO vom 21.12.2011, abrufbar unter www.dgri.de/index.php/fuseaction/download/lrn_file/stellungnahme-dgri-datenschutzvo.pdf (Abruf: 8.2.2012).

11 Vgl. *Schneider/Härting*, ZD 2011, 63 ff.

12 Art. 29 DS-GVO steht in engem Zusammenhang mit Art. 53 Abs. 2 DS-GVO und den dort geregelten Befugnissen der Aufsichtsbehörden zum Zugriff auf personenbezogene Daten sowie zum Zutritt zu Geschäftsräumen einschließlich Datenverarbeitungsanlagen. Art. 29 DS-GVO verpflichtet die Verantwortlichen zu einer „Zusammenarbeit" mit den Behörden, ohne dass ersichtlich ist, welche konkreten Pflichten sich hieraus neben Art. 53 Abs. 2 DS-GVO noch ergeben sollen.

13 Vgl. *Hornung*, ZD 2011, 51 ff.

14 Vgl. Mitteilung vom 4.11.2010, KOM(2010) 609 endg.

DS-GVO soll der Ausschuss unabhängig und weisungsfrei agieren. Zu seinen Kernaufgaben zählt die Beratung der Kommission in allen Fragen des Datenschutzes (Art. 66 Abs. 1 lit. a DS-GVO).

Gem. Art. 71 DS-GVO soll der Europäische Datenschutzausschuss durch Einrichtung eines Sekretariats gestärkt werden. Das Sekretariat, das für das Tagesgeschäft des Datenschutzausschusses zuständig sein soll (Art. 71 Abs. 3 lit. a DS-GVO), wird zur zentralen europäischen Datenschutzbehörde unter Regie des Europäischen Datenschutzbeauftragten (Art. 71 Abs. 1 S. 2 DS-GVO).

### c) Zusammenarbeit und Kohärenz – das Zusammenwirken aller europäischen Behörden

Auf der dritten Stufe der Pyramide stehen – gemeinsam – die Europäische Kommission, der Europäische Datenschutzausschuss und die Datenschutzbehörden der einzelnen EU-Mitgliedstaaten, die in Art. 55 bis 63 DS-GVO zur Zusammenarbeit und zur kohärenten Anwendung des Datenschutzrechts verpflichtet werden. Die Zusammenarbeit der nationalen Aufsichtsbehörden erfolgt im Wege der Amtshilfe (Art. 55 DS-GVO) und durch gemeinsame Maßnahmen, die die Aufsichtsbehörden in Fällen ergreifen, in denen Personen in mehreren EU-Mitgliedstaaten von Verarbeitungsvorgängen betroffen sind (Art. 56 DS-GVO). Bei Maßnahmen mit grenzüberschreitender Wirkung verpflichtet Art. 58 Abs. 1 und 2 DS-GVO die nationalen Datenschutzbehörden, vorab ein Kohärenzverfahren durchzuführen. Kommt eine Datenschutzbehörde dieser Verpflichtung nicht nach, können alle anderen Aufsichtsbehörden und der Europäische Datenschutzausschuss die Durchführung eines solchen Verfahrens verlangen (Art. 58 Abs. 3 DS-GVO). Die Europäische Kommission soll nach Art. 58 Abs. 4 DS-GVO sogar uneingeschränkt berechtigt sein, zu verlangen, dass „eine Sache" in einem Kohärenzverfahren „behandelt" wird.

In Art. 58 Abs. 7 sowie den Art. 59 bis 61 DS-GVO finden sich ausgeklügelte Verfahrensvorschriften zu den Abstimmungen, die zwischen den nationalen Aufsichtsbehörden, dem Europäischen Datenschutzausschuss und der Kommission im Zuge eines Kohärenzverfahrens erfolgen müssen. Nach Art. 59 Abs. 1 DS-GVO ist die Kommission berechtigt, die ordnungsgemäße und einheitliche Anwendung der DS-GVO durch Abgabe einer Stellungnahme sicherzustellen. Die Aufsichtsbehörden sind allerdings nicht verpflichtet, einer solchen Stellungnahme zu folgen. Wenn eine Maßnahme allerdings von einer Stellungnahme der Kommission abweichen möchte, muss sie dies gem. Art. 59 Abs. 4 S. 1 DS-GVO der Kommission und dem Europäischen Datenschutzausschuss zunächst in begründeter Form mitteilen. Für den Zeitraum eines Monats nach der Mitteilung darf die geplante Maßnahme nicht ausgeführt werden (Art. 59 Abs. 4 S. 2 DS-GVO). Die Kommission kann auf diese Mitteilung mit einer Aufforderung an die Aufsichtsbehörde reagieren, die geplante Maßnahme für einen Zeitraum von zwölf Wochen nicht auszuführen (Art. 60 DS-GVO). In dringenden Fällen ist die Aufsichtsbehörde allerdings gem. Art. 61 Abs. 1 DS-GVO berechtigt, einstweilige Maßnahmen zu ergreifen und beim Europäischen Datenschutzausschuss ein Dringlichkeitsverfahren durchzuführen (Art. 61 Abs. 4 DS-GVO).

Abgerundet werden die Bestimmungen zum Kohärenzverfahren durch umfangreiche Befugnisse der Kommission zu Durchführungsrechtsakten gem. Art. 87 Abs. 2 und 3 DS-GVO (Art. 62 Abs. 1 und 2 DS-GVO) und durch eine Verpflichtung aller anderen betroffenen Mitgliedstaaten, eine „durchsetzbare Maßnahme" der Datenschutzbehörde eines EU-Mitgliedstaats Geltung zu verschaffen (Art. 63 Abs. 1 DS-GVO).

Die Kommission erhält in den Art. 57 bis 63 DS-GVO keine ausdrückliche Befugnis zur Letztentscheidung. Für den Europäischen Datenschutzausschuss sehen die Bestimmungen zum Kohärenzverfahren zudem lediglich Befugnisse zu Stellungnahmen, nicht jedoch Entscheidungskompetenzen vor. Somit bleibt trotz der äußerst komplexen Ausgestaltung der Verfahrensbestimmungen offen, welche Folgen es hat, wenn zwischen den Beteiligten keine Einigung erzielt wird. Die Bestimmungen zum Kohärenzverfahren bieten letztlich zwar Gewähr dafür, dass datenschutzrechtliche Anwendungsfragen zwischen den verschiedenen Behörden und Stellen intensiv diskutiert werden. Die Effizienz, Angemessenheit und Nachvollziehbarkeit der Ergebnisse sind jedoch in keiner Weise gesichert.

### d) Die nationalen Datenschutzbehörden

Die vierte Ebene der Pyramide bilden die Aufsichtsbehörden der einzelnen EU Mitgliedstaaten, deren Unabhängigkeit, Aufgaben und Befugnisse in Art. 46 bis 54 DS-GVO geregelt ist. Die Bestimmungen der Art. 46 bis 54 DS-GVO knüpfen an Art. 28 DSRL an. Dass in jedem Mitgliedstaat ein oder mehrere Datenschutzbehörden bestehen müssen, ergibt sich aus Art. 46 DS-GVO. Art. 47 DS-GVO sieht sodann weit reichende Maßnahmen zur Gewährleistung der Unabhängigkeit der Behörden vor. So wird den Mitgliedern der Aufsichtsbehörde vorgeschrieben, dass sie sich auch nach Ablauf ihrer Amtszeit im Hinblick auf die Annahme von Tätigkeiten und Vorteilen „ehrenhaft und zurückhaltend" zu verhalten haben (Art. 47 Abs. 4 DS-GVO). Die Mitgliedstaaten müssen die Aufsichtsbehörden mit angemessenen personellen, technischen und finanziellen Ressourcen, Räumlichkeiten und mit der erforderlichen Infrastruktur ausstatten, um alle Aufgaben und Befugnisse gem. der DS-GVO effektiv wahrnehmen zu können (Art. 47 Abs. 5 DS-GVO). Art. 47 Abs. 6 und 7 DS-GVO verpflichtet die Mitgliedstaaten – mit großer Detailfreude – zur Sicherstellung der Ernennung eigenen Personals durch die Aufsichtsbehörden und zur Gewährleistung eigener jährlicher Haushalte mit Haushaltsplänen, die veröffentlicht werden. Art. 48 DS-GVO stellt genaue Anforderungen an die Berufung und Auswahl von Mitgliedern der Aufsichtsbehörde auf und regelt sogar die Voraussetzungen, unter denen ein Mitglied einer Aufsichtsbehörde vom zuständigen nationalen Gericht seiner Ruhegehaltsansprüche für verlustig erklärt werden kann (Art. 48 Abs. 4 DS-GVO).

Art. 52 DS-GVO enthält einen umfangreichen Katalog von Aufgaben der Aufsichtsbehörden. Zu diesen Aufgaben zählt bspw. die „Verfolgung relevanter Entwicklungen, soweit sie sich auf den Schutz personenbezogener Daten auswirken" (Art. 52 Abs. 1 lit. d DS-GVO), sowie die Information der Öffentlichkeit über Risiken, Vorschriften, Garantien und Rechte im Zusammenhang mit der Verarbeitung personenbezogener Daten unter besonderer Beachtung spezifischer Maßnahmen für Kinder (Art. 52 Abs. 2 DS-GVO). Nur bei offensichtlich missbräuchlichen Anträgen dürfen die Aufsichtsbehörden für ihre Leistungen von den Betroffenen Gebühren verlangen oder davon absehen, die von dem Betroffenen beantragte Maßnahme zu treffen, wobei die Aufsichtsbehörde die Beweislast trägt für den offensichtlich missbräuchlichen Charakter eines Antrags (Art. 52 Abs. 6 DS-GVO).

Ebenso ausführlich wie der Katalog der Aufgaben in Art. 52 DS-GVO ist der – sich mit Art. 52 erheblich überschneidende – Katalog der Befugnisse der Aufsichtsbehörden in Art. 53 DS-GVO. Zu diesen zählen unter anderem die Abgabe von Stellungnahmen und die Information der Öffentlichkeit zu allen Fragen des Datenschutzes (Art. 53 Abs. 1

lit. i und j DS-GVO). Zwangsrechte finden sich im Art. 53 Abs. 2 DS-GVO, nämlich der Zugriff beim Verarbeiter auf alle personenbezogenen Daten und – weitergehend – auf „Informationen, die zur Erfüllung der Aufgaben (der Behörden) notwendig sind" sowie der Zugang zu den Geschäftsräumen des Verarbeiters einschließlich aller Datenverarbeitungsanlagen und -geräte, sofern Grund zu der Annahme besteht, dass dort Tätigkeiten ausgeführt werden, die gegen die DS-GVO verstoßen.

Die Rechtsbehelfe sind in Art. 73 bis 76 DS-GVO geregelt. Art. 73 DS-GVO berechtigt Betroffene zur Beschwerde bei den Aufsichtsbehörden, wenn sie der Auffassung sind, dass Bestimmungen der DS-GVO oder – generell – „der Schutz personenbezogener Daten" (vgl. Art. 63 Abs. 3 DS-GVO) verletzt worden sind. Art. 74 DS-GVO regelt Rechtsbehelfe gegen eine Aufsichtsbehörde. Sieht sich eine natürliche oder juristische Person durch eine Entscheidung einer Aufsichtsbehörde in ihren Rechten verletzt, hat sie nach Art. 74 Abs. 1 DS-GVO das Recht auf einen gerichtlichen Rechtsbehelf. Wenn es sich um eine Entscheidung einer Aufsichtsbehörde mit Sitz in einem anderen Mitgliedstaat handelt, soll der Betroffene nach Art. 74 Abs. 4 DS-GVO berechtigt sein, die Aufsichtbehörde seines Heimatstaates zur Klageerhebung gegen die Behörde des anderen Mitgliedstaates zu ersuchen. Ein Berliner Unternehmer, der eine Untersagungsverfügung einer griechischen Aufsichtsbehörde erhält, soll demnach die Möglichkeit haben, den Datenschutzbeauftragten des Landes Berlin um Klageerhebung gegen seine griechischen Kollegen zu bitten. Dies ist eine absurde Regelung, da eine Behörde nicht einerseits zur Zusammenarbeit und Kohärenz mit anderen Behörden verpflichtet (Art. 55 bis 63 DS-GVO) und gleichzeitig Sachwalter der Interessen von Bürgern sein kann, deren Rechte durch Entscheidungen dieser Behörden verletzt worden sind.

Art. 75 DS-GVO behandelt Klagerechte der Betroffenen gegen Datenverarbeiter. In Art. 76 DS-GVO finden sich Verfahrensvorschriften, die insbesondere einen einheitlichen Schutz personenbezogener Daten innerhalb der EU sicherstellen sollen (vgl. Art. 76 Abs. 2 DS-GVO). Insgesamt ist es bezeichnend, dass sich auf zwei Seiten mit Regelungen zu Rechtsbehelfen – von der fragwürdigen Vorschrift des Art. 74 Abs. 4 DS-GVO abgesehen – ein einziger Satz zu den Rechten findet, die ein Datenverarbeiter hat, der von einer rechtswidrigen Maßnahme einer Aufsichtsbehörde betroffen ist.

Art. 79 DS-GVO berechtigt die Aufsichtsbehörden der Mitgliedstaaten zur Verhängung von Geldbußen bis zur Höhe von 2% des weltweiten Jahresumsatzes eines Unternehmens. Vergleicht man den umfangreichen Bußgeldkatalog des Art. 79 DS-GVO mit der Norm zum Schadensersatz (Art. 77 DS-GVO), die zwar eine Beweislastumkehr für das Verschulden vorsieht, sich ansonsten aber im Rahmen üblicher deliktischer Haftungsnormen bewegt, so wird deutlich, dass der Entwurf davon ausgeht, dass die Durchsetzung des Datenschutzrechts weitaus besser bei den staatlichen Datenschutzbehörden aufgehoben ist als bei den Betroffenen selbst. Recht unentschieden dazwischen steht Art. 78 DS-GVO, der den Mitgliedstaaten die Festlegung (weiterer) Sanktionen überlässt und dabei offensichtlich, wenn auch nicht zwingend, privatrechtliche Sanktionen wie etwa Ansprüche auf Schmerzensgeld im Auge hat.

### e) Der Fuß der Pyramide

#### aa) Die europäische Wirtschaft

Am Fuß der Pyramide finden sich die Datenverarbeiter und somit die Unternehmen, gegenüber denen das Datenschutzrecht durchzusetzen ist. Dieser Personenkreis wird in Art. 4 Nr. (5) DS-GVO mit dem Begriff der „für die Verarbeitung Verantwortlichen" definiert. Dem Datenschutzrecht unterworfen werden alle natürlichen oder juristischen Personen, Behörden, Einrichtungen oder jede andere Stelle, die allein oder gemeinsam mit anderen die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheidet. Hierzu zählen EU-weit alle Unternehmen, da es heutzutage kein Unternehmen mehr geben wird, in dem nicht in der einen oder anderen Weise Daten mit Personenbezug verarbeitet werden. All diese Unternehmen werden dem vereinheitlichten europäischen Datenschutzrecht und den Kontrollen, Maßnahmen und Sanktionen der Aufsichtsbehörden und der weiteren europäischen Datenschutzstellen unterworfen.

#### bb) Der globale Geltungsanspruch

Das europäische Datenschutzrecht soll nicht nur für Unternehmen gelten, die eine Niederlassung in der EU unterhalten (Art. 3 Abs. 1 DS-GVO). Art. 3 Abs. 2 DS-GVO erstreckt den Anwendungsbereich der Verordnung auf Anbieter außerhalb der EU, die Daten von EU-Bürgern verarbeiten. Dies soll zum einen gelten, wenn die Datenverarbeitung dazu dient, EU-Bürgern Waren oder Dienstleistungen anzubieten (lit. a). Zum anderen soll die DS-GVO anwendbar sein, wenn es um eine Datenverarbeitung geht, die der „Beobachtung" des „Verhaltens" von EU-Bürgern dient (lit. b).

Die Formulierungen des Art. 3 Abs. 2 DS-GVO sind ersichtlich auf das Internet zugeschnitten. Wenn sich außereuropäische Unternehmen über das Internet (auch) an europäisches Publikum wenden, soll europäisches Datenschutzrecht auf ihre Aktivitäten anwendbar sein. Dies ist der Abschied vom Territorialitätsprinzip (Art. 4 DSRL). Und noch mehr: Global Player sollen durch Art. 25 DS-GVO verpflichtet werden, einen Vertreter in der Union zu benennen, der dann in der uneingeschränkten Verantwortung steht für die Einhaltung der Bestimmungen der DS-GVO.

Der Geltungsanspruch des europäischen Datenschutzrechts geht bedenklich weit: Die Regelung in Art. 3 Abs. 2 lit. b DS-GVO läuft darauf hinaus, dass jeder Internetanbieter, der das „Surfverhalten" der Website-Besucher zwecks zielgerichteter Werbung („Targeted Advertising"[15]) auswertet, das EU-Datenschutzrecht zu beachten hat. Man stelle sich einmal vor, die Regierung der Volksrepublik China würde Verbotsvorschriften mit ähnlichem Geltungsanspruch erlassen und europäische Online-Anbieter, die die Filterung, Sperrung oder Unterdrückung bestimmter Inhalte verweigern, mit drakonischen Bußgeldern oder anderen Sanktionen drohen und zudem – wie in Art. 25 DS-GVO – die Bestellung eines in China niedergelassenen Vertreters verlangen, der dem chinesischen Recht unterworfen ist. Die Weltgeltung,[16] die das europäische Datenschutzrecht bei der Profilbildung beanspruchen soll, geht zu weit.

## 2. Materielles Recht: Festhalten an der überkommenen Regelungsstruktur

Regelungen zum materiellen Datenschutzrecht finden sich in Art. 1 bis 39 DS-GVO. Diese Regelungen werden durch Bereichsausnahmen in den Art. 80 bis 85 DS-GVO ergänzt. Zu allen zentralen Fragen findet man Antworten, die sich von der DS-RL nur marginal unterschei-

15 Vgl. *Peiffer*, K&R 2011, 543 ff.; *Rammos*, K&R 2011, 692 ff.

16 Jeff Jarvis per Twitter am 25.1.2012: „While Merkel talks about turning the EU into a government for Europe, the EU's Reding tries to become a government for the net."

den. Der Fokus bleibt auf dem Schutz von Daten verhaftet und nicht auf dem Schutz der Persönlichkeit.[17]

### a) Personenbezogene Daten

Es soll bei dem Schwarz-Weiß-Prinzip[18] bleiben: Wenn Daten Personenbezug haben, gilt uneingeschränkt das Datenschutzrecht. Ohne einen Personenbezug sind Daten dem Datenschutzrecht komplett entzogen.

An der Definition des Begriffs personenbezogener Daten, die sich in Art. 4 Abs. 1 und 2 DS-GVO findet und für die ergänzend die Erwägungsgründe 23 und 24 gelten, hat man gegenüber Art. 2 lit. a DSRL nur minimale Modifikationen vorgenommen. Diese Modifikationen bleiben merkwürdig unentschieden zwischen einer absoluten[19] und einer relativen[20] Betrachtungsweise. Im Sinne einer absoluten Betrachtungsweise soll es nach Art. 4 Abs. 1 DS-GVO ausreichen, dass (irgendeine) Person „nach allgemeinem Ermessen aller Voraussicht nach" die Daten einer bestimmten Person zuordnen kann.

Was IP-Adressen, Cookies, Standortdaten und andere „Spuren im Netz" angeht, werden „Online-Kennungen" und Standortdaten als (potenziell) personenbezogene Daten in Art. 4 Abs. 1 DS-GVO ausdrücklich erwähnt. In Erwägungsgrund 24 heißt es jedoch – ohne klare Begründung, aber im Sinne einer relativen Betrachtungsweise –, dass derartige „Spuren" „nicht zwangsläufig und unter allen Umständen" als personenbezogene Daten zu betrachten seien. Damit bleibt die Kontroverse um die Voraussetzungen des Personenbezuges von IP-Adressen, Cookies und Standortdaten und um die Anwendbarkeit des Datenschutzrechts auf diese Daten[21] offen. Dies verbessert die Rechtssicherheit nicht.

### b) Verbotsprinzip

Das Verbotsprinzip wird derzeit in Art. 7 DSRL geregelt. Es soll nicht gelockert, sondern – durch Art. 6 DS-GVO – verschärft werden. Angesichts der exponentiellen Zunahme der datengestützten Kommunikation ist dies ein rückwärtsgewandter Ansatz, der den Erfordernissen der Informationsgesellschaft nicht gerecht wird. Ohne eine Modifikation, wenn nicht gar eine Abschaffung des Verbotsprinzips wird indes jedwede Modernisierung des Datenschutzrechts misslingen.[22]

### c) Einwilligung

Zwar enthalten die Art. 11 bis 14 DS-GVO Vorschriften zur Transparenz, deren Grundtendenz zu begrüßen ist.[23] Zugleich bleibt es indes dabei, dass von dem (aufgeklärten) Internetnutzer zur Legitimation der Datenverarbeitung vielfach zusätzlich eine Einwilligung verlangt wird.

In Art. 4 Abs. 8 DS-GVO werden die Anforderungen an eine wirksame Einwilligung verschärft, indem zum einen eine „ausdrückliche" Einwilligung verlangt und zum anderen eine Erklärung oder „sonstige eindeutige Handlung" gefordert wird. Nach Art. 6 Abs. 1 lit. a DS-GVO soll die Einwilligung des Betroffenen eine Datenverarbeitung zudem nur noch dann legitimieren, wenn die Einwilligung zugleich die Zwecke „genau festlegt", auf die sie sich bezieht.

Paternalistische Tendenzen werden in Art. 7 Abs. 4 DS-GVO besonders deutlich. Ein „erhebliches Ungleichgewicht" zwischen Datenverarbeiter und Betroffenen soll ausreichen, um jedweder Einwilligung die Legitimation als Rechtsgrundlage für eine Datenverarbeitung zu nehmen. Als Beispiel für ein solches „Ungleichgewicht" wird in Erwägungsgrund 34 lediglich das Arbeitsverhältnis genannt. Dies ist schon deshalb merkwürdig, weil Art. 82 DS-GVO den Mitgliedstaaten die genaue Ausgestaltung des Arbeitnehmerdatenschutzes gestattet. Dieser Spielraum wird durch Art. 7 Abs. 4 DS-GVO und Erwägungsgrund 34 nachhaltig eingeschränkt.

Wenn sich ein Verbraucher und ein Unternehmen gegenübertreten, wird man stets von einem „Ungleichgewicht" sprechen können. Ein solches „Ungleichgewicht" ist schließlich – bei typologisierender Betrachtungsweise – die Basis der Legitimation des gesamten Verbraucherschutzrechts. Art. 7 Abs. 4 DS-GVO läuft darauf hinaus, Einwilligungen der Verbraucher in die Datenverarbeitung jegliche Rechtsbedeutung zu nehmen.

Die Entwertung der Einwilligung als Rechtsgrundlage für eine Datenverarbeitung führt dazu, dass noch mehr als bisher Einzelfallabwägungen über die Rechtmäßigkeit der Datenverarbeitung entscheiden. Weitgehend unverändert (vgl. Art. 7 lit. f DSRL) heißt es in Art. 6 Abs. 1 lit. f DS-GVO, dass die Datenverarbeitung zur Wahrung der berechtigten Interessen des Datenverarbeiters erlaubt ist, sofern nicht die Interessen oder Grundrechte und Grundfreiheiten der Betroffenen überwiegen. Die Rechtmäßigkeitsprüfung noch viel deutlicher einer Einzelfallabwägung zu überlassen als bisher, schafft ein Mehr an Rechtsunsicherheit an einer Stelle, an der das Bedürfnis nach Rechtssicherheit evident ist.[24] Aus Sicht der Unternehmen bedeutet dies, dass sie bei jeder Verarbeitung von personenbezogenen Verbraucherdaten darauf angewiesen sind, eine gem. Art. 6 Abs. 1 lit. f DS-GVO „richtige" Abwägung der Interessen vorzunehmen, wobei sie stets befürchten müssen, dass staatliche Aufsichtsbehörden die Abwägung überprüfen und zu abweichenden Ergebnissen gelangen.

Dem tiefen Misstrauen der Entwurfsverfasser gegen autonome Entscheidungen des Betroffenen entspricht es, wenn der Betroffene in Art. 7 Abs. 3 DS-GVO ein jederzeitiges Widerrufsrecht erhalten soll. Dieses Widerrufsrecht soll an keinerlei Voraussetzungen gebunden sein und auch ohne Weiteres (d. h. sofort) wirksam werden.[25] Ein Online-Anbieter, der personenbezogene Daten der Nutzer aufgrund deren Einwilligung zur Gestaltung seines Angebots einsetzt, müsste damit rechnen, die Legitimation für die Datennutzung jederzeit mit sofortiger Wirkung verlieren zu können.

### d) Sensible Daten

Art. 9 DS-GVO enthält Regelungen zu besonders schutzwürdigen Daten und entspricht im Wesentlichen Art. 8 DSRL. Neu ist die Aufnahme genetischer Daten in den Katalog der Daten mit besonderem Schutzbedarf. Es entsteht ein bunter Potpourri: Dass die „Zugehörigkeit zu einer Gewerkschaft" auf derselben Sensibilitätsstufe steht wie Daten über das Sexualleben, mag den Vorstellungen der siebziger Jahre des vergangenen Jahrhunderts entsprochen haben. Heute wirkt dies befremdlich. Es fehlt zudem an einem übergreifenden Maßstab für die Verstärkung des Schutzes. Als Anknüpfungspunkte kommen bspw. die Intimsphäre (auf Basis der BGH-Rechtsprechung zum Persönlichkeitsrecht[26]) und der Kernbereich privater Lebensgestaltung

17 Kritisch zum geltenden Recht *Wieczorek*, DuD 2011, 476 ff.
18 *Schneider/Härting*, ZD 2011, 63, 64 f.
19 Vgl. *Weichert*, in: Däubler/Klebe/Wedde/Weichert, BDSG, 3. Aufl. 2010, § 3 Rn. 3.
20 Vgl. *Dammann*, in: Simitis, BDSG, 7. Aufl. 2011, § 3 Rn. 21.
21 Vgl. *Eckhardt*, CR 2011, 339 ff.; *Krüger/Maucher*, MMR 2011, 433 ff.; *Sachs*, CR 2010, 547 ff.; *Venzke*, ZD 2011, 114 ff.
22 Vgl. *Härting/Schneider*, ZRP 2011, 233, 234; *Peiffer*, K&R 2011, 543 ff.
23 Vgl. *Härting*, CR 2011, 169 ff.
24 Vgl. *Schneider/Härting*, ZD 2011, 63, 66.
25 Zur derzeitigen Rechtslage *Simitis*, in: Simitis, BDSG, 7. Aufl. 2011, § 4a, Rn. 94 f.
26 Vgl. zuletzt BGH, 25.10.2011 – VI 332/09.

(nach der BVerfG-Rechtsprechung[27]) in Betracht. Die Aufzählung der Art. 9 Abs. 1 DS-GVO wirkt demgegenüber beliebig und auch starr. Die Vorstellung darüber, welche Aspekte der Privatsphäre zur Intimsphäre und zum Kernbereich privater Lebensgestaltung zählen, unterliegt einem ständigen gesellschaftlichen Wandel, mit dem das Datenschutzrecht nur dann Schritt halten kann, wenn es keine starren Maßstäbe bildet.

### e) Kommunikationsfreiheit

Die Schaffung einer Balance zwischen Persönlichkeitsschutz und freier Kommunikation gehört zu den Kernaufgaben eines modernen Datenschutzrechts.[28] Daher ist es äußerst unbefriedigend, dass Art. 80 DS-GVO die Schaffung einer Balance den EU-Mitgliedstaaten überlässt. In dem ausführlichen Erwägungsgrund 121 wird die Bedeutung des Rechts auf freie Meinungsäußerung zwar nachdrücklich betont. Insgesamt bleibt es indes bei einer Regelung, die sich von dem – viel zu allgemein gefassten – „Medienprivileg" des Art. 9 DS-RL[29] nicht unterscheidet.

## 3. Materielles Recht: Neue Regelungen

### a) Schutz von Kindern

Art. 8 DS-GVO ist eine neue Spezialvorschrift für Onlinedienste. Für diese Onlinedienste schreibt Art. 8 DS-GVO die Einwilligung der Eltern für Kinder unter 13 Jahren vor, sofern es zu einer Verarbeitung personenbezogener Daten des Kindes kommt. Dies ist eine erfreuliche Klarstellung, da es nach geltendem Recht (in Deutschland) kein klares Mindestalter für die Einwilligungsfähigkeit von Minderjährigen gibt.[30] Allerdings ist kein Grund ersichtlich, weshalb es zur Einwilligungsfähigkeit Minderjähriger nicht auch außerhalb von Onlinediensten eine Regelung geben soll.

### b) Recht auf Vergessenwerden und auf Löschung

Nach Art. 12 lit. b DSRL besteht ein Löschungsrecht des Betroffenen bei unvollständigen oder unrichtigen Daten und bei Daten, deren Verarbeitung aus anderen Gründen rechtswidrig ist. Im Zeichen der Einführung eines „Right to be forgotten"[31] weitet Art. 17 DS-GVO die Löschungsrechte erheblich aus. Die Detailgenauigkeit der in Art. 17 DS-GVO enthaltenen Regelung zeigt, dass das „Recht auf Vergessenwerden" eine der (wenigen) zentralen Neuregelungen des materiellen Datenschutzrechts werden soll.

Art. 17 Abs. 1 DS-GVO unterscheidet zwischen vier Gründen für einen Löschungsanspruch. Während Art. 17 Abs. 1 lit. a DS-GVO noch an den Zweckbindungsgrundsatz anknüpft und somit im Kern Art. 12 lit. b DSRL entsprechen dürfte, führt Art. 17 Abs. 1 lit. b DS-GVO eine Löschungspflicht für den Fall ein, dass eine „Speicherfrist" abgelaufen ist oder dass der Betroffene eine Einwilligung widerruft. Da es in Art. 7 Abs. 3 DS-GVO an jedweder Einschränkung des Widerrufsrechts fehlt, muss der Datenverarbeiter in Zukunft damit rechnen, dass es weitgehend dem Belieben des Betroffenen überlassen ist, ob und wann eine (kraft Einwilligung) rechtmäßige Datenverarbeitung aufgrund eines Widerrufs rechtswidrig wird mit der Folge sofortiger Löschungspflichten.

Art. 17 Abs. 2 DS-GVO ist eine der wenigen Vorschriften, in denen einmal ausdrücklich auf eine Veröffentlichung Bezug genommen wird. Bei Veröffentlichungen stellen sich die Entwurfsverfasser vor, dass das „Recht auf Vergessenwerden" flankiert wird von erheblichen Handlungspflichten des Verarbeitenden: So soll ein Internetanbieter, der zu löschende Daten veröffentlicht hat, „alle vertretbaren Schritte, auch technischer Art" ergreifen, um Dritte von der Löschung zu informieren. Insbesondere soll er auf eine „Löschung aller Querverweise" und die Löschung von „Kopien oder Replikationen" hinwirken.

Wie angesichts der ständigen Vervielfältigungs- und Verknüpfungsvorgänge im Internet Art. 17 Abs. 2 DS-GVO umsetzbar sein soll, ist nicht ersichtlich. Aus Sicht desjenigen, der eine Veröffentlichung vornimmt, wird der Umgang mit personenbezogenen Daten zu einem unüberschaubaren Risiko. Denn der Anbieter muss jederzeit damit rechnen, dass der Betroffene sich auf ein Löschungsrecht gem. Art. 17 Abs. 1 DS-GVO beruft und – gestützt auf Art. 17 Abs. 2 DS-GVO – von dem Anbieter eine Einwirkung auf Dritte verlangt mit einem Aufwand, der für den Anbieter nicht abzuschätzen ist. Unter dem Blickwinkel des Schutzes der freien Kommunikation liefert Art. 17 Abs. 2 DS-GVO dem Internetakteur zu viel Motivation für die „Schere im Kopf".

Den Konflikt zur Kommunikationsfreiheit haben die Entwurfsverfasser nicht vollständig übersehen. Art. 17 Abs. 3 lit. a DS-GVO sieht eine Ausnahme von den Löschungspflichten vor für den Fall, dass die Datenspeicherung zur Ausübung des Rechts auf freie Meinungsäußerung gem. Art. 80 DS-GVO „erforderlich" ist. Schon das strenge Kriterium der „Erforderlichkeit" belegt allerdings, dass der Regelung die Vorstellung zu Grunde liegt, dass die freie Kommunikation die Ausnahme darstellt und die DS-GVO nicht von einem Gleichrang des Schutzes der Privatsphäre und des Schutzes der Kommunikationsfreiheit ausgeht.

Art. 17 Abs. 4 DS-GVO gestattet dem Verarbeiter, Daten lediglich zu sperren. Allerdings soll nach Art. 17 Abs. 4 lit. a DS-GVO eine Sperrpflicht bereits dann bestehen, wenn der Betroffene die Richtigkeit von Daten bestreitet. Das bloße (auch willkürliche) Bestreiten der Richtigkeit soll somit dem Verarbeiter bereits die Nutzung von Daten unmöglich machen.

Art. 17 Abs. 5 und 6 DS-GVO knüpft an das Recht (bzw. die Pflicht) zur Sperrung von Daten detaillierte Verfahrensregeln an. Eine Nutzung gesperrter Daten soll dem Verarbeiter nur in wenigen Ausnahmefällen gestattet sein (Art. 17 Abs. 5 DS-GVO). Die Aufhebung einer Sperre ist dem Betroffenen nach Art. 17 Abs. 6 DS-GVO „im Voraus" mitzuteilen.

Insgesamt lassen sich in Art. 17 DS-GVO lediglich zwei innovative Elemente identifizieren, die über die herkömmlichen Rechte auf Löschung und Sperrung hinausgehen: Dies ist zum einen die Einführung einer „Speicherfrist" (Art. 17 Abs. 1 lit. b DS-GVO) und zum anderen die in Art. 17 Abs. 2 DS-GVO getroffene Regelung zur Verantwortlichkeit des Internetanbieters für „Querverweise" und „Kopien oder Replikationen". Art. 17 Abs. 2 DS-GVO wird den technischen Gegebenheiten des Internet nicht gerecht und macht Internetveröffentlichungen zu einem unübersehbaren Risiko. Auch „Speicherfristen" behindern die freie Kommunikation im Übermaß jedenfalls dann, wenn es – wie in der DS-GVO vorgesehen – keine Option für den Betroffenen gibt, einer zeitlich unbegrenzten Speicherung zuzustimmen oder sogar auf unbegrenzte Speicherung zu bestehen.

27 Vgl. zuletzt BVerfG, 7.12.2011 – 2 BvR 2500/09, 2 BvR 1857/10.
28 Vgl. *Härting/Schneider*, ZRP 2011, 233 ff.; *Härting*, ITRB 2010, 280, 281 f.
29 Vgl. *Härting*, Internetrecht, 4. Aufl. 2010, Rn. 219 ff.
30 Vgl. *Simitis*, in: Simitis, BDSG, 7. Aufl. 2011, § 4a, Rn. 20 ff.; *Jandt/Roßnagel*, MMR 2011, 637 ff.
31 Vgl. *Nolte*, ZRP 2011, 236 ff.

### c) Portabilität von Daten

Das Anliegen des Art. 18 DS-GVO ist es, Daten „portabel" („übertragbar") zu machen. Die Entwurfsverfasser haben dabei ersichtlich vor allem an Facebook und andere soziale Netzwerke gedacht. Dem Facebook-Nutzer soll es durch „Portabilität" erleichtert werden, zu einem anderen Anbieter von Netzwerken zu wechseln.

Die in Art. 18 DS-GVO getroffene Regelung dient nicht dem Schutz der Privatsphäre. Es geht vielmehr um Verbraucherschutz in einem tendenziell monopolistisch strukturierten Markt. Und es kann nicht richtig sein, den Schutz der Privatsphäre zum Vorwand zu nehmen, um mit den Mitteln der Regulierung das Marktgeschehen zulasten einzelner Anbieter zu beeinflussen. Der Einfluss, den Anbieter wie Facebook oder auch Google aufgrund ihrer monopolistischen oder jedenfalls monopolähnlichen Stellung haben, mag das europäische Kartellrecht auf den Plan rufen. Es wäre eine problematische Entwicklung, wenn etwa der Europäische Datenschutzausschuss, zu dessen Aufgaben die Durchsetzung des Art. 18 DS-GVO zählen würden, zu einer umfassenden europäischen Regulierungsstelle ausgebaut würde, die über den Datenschutz hinaus in den (nicht nur) europäischen Datenverkehr eingreifen könnte, um Ungleichgewichten entgegenzuwirken.

### d) „Privacy by Default"

Art. 23 DS-GVO greift – neben „Privacy by Design" – das Konzept der „Privacy by Default"[32] auf. Außer in der Überschrift des Artikels werden allerdings „datenschutzrechtliche Voreinstellungen" nur in Art. 23 Abs. 3 DS-GVO erwähnt. Dort geht es um die Ermächtigung der Kommission zu delegierten Rechtsakten. Somit läuft Art. 23 DS-GVO darauf hinaus, dass es vollständig der Kommission überlassen wird, zu definieren, was sie unter „Privacy by Default" versteht und welche konkreten Anforderungen sich aus dem Grundsatz ergeben sollen.

### e) Abschaffung der Meldepflicht

Die Meldepflicht gem. Art. 18 und 19 DSRL wird abgeschafft. An die Stelle der Meldepflicht tritt eine detaillierte Verpflichtung zur Dokumentation (Art. 28 DS-GVO). Der Katalog der Informationen, die die Dokumentation mindestens enthalten muss (Art. 28 Abs. 2 DS-GVO), ist im Vergleich zu Art. 19 Abs. 1 DSRL erheblich erweitert und umfasst unter anderem Löschungsfristen für verschiedene Datenkategorien (Art. 28 Abs. 2 lit. g DS-GVO).

Unternehmen und Organisationen mit weniger als 250 Beschäftigten werden durch Art. 28 Abs. 4 lit. b DS-GVO von den Dokumentationspflichten befreit, sofern die Datenverarbeitung nur eine „Nebentätigkeit" darstellt. Dies stellt eine erfreuliche Entlastung kleiner Unternehmen dar.

### f) Pflichten bei Datenschutzverstößen

Art. 31 DS-GVO führt eine Verpflichtung des Datenverarbeiters ein, die Aufsichtsbehörde unverzüglich zu verständigen, wenn eine Verletzung datenschutzrechtlicher Bestimmungen festgestellt wird. Anders als in § 42a BDSG soll dies uneingeschränkt für alle Arten von Daten und für alle Arten von Rechtsverstößen gelten. Es gibt keine Bagatellgrenze und keine Differenzierung je nach Schwere des Verstoßes.

Statt differenzierte und abgestufte Voraussetzungen für eine Meldepflicht zu regeln, finden sich in Art. 31 DS-GVO detaillierte Verfahrensvorschriften. Im Falle einer verzögerten Meldung ist der Aufsichtsbehörde gegenüber zu begründen, weshalb eine Meldung nicht innerhalb von 24 Stunden erfolgt ist (Art. 31 Abs. 1 S. 1 DS-GVO). In der Meldung, für die eine Frist von 24 Stunden gilt, sind nach Art. 31 Abs. 3 DS-GVO zahlreiche Informationen aufzunehmen, beispielsweise (bereits) Empfehlungen für Maßnahmen zur Eindämmung negativer Auswirkungen (Art. 31 Abs. 3 lit. c DS-GVO). Art. 31 Abs. 4 DS-GVO verpflichtet den Verantwortlichen zur Erstellung einer Dokumentation, die der Aufsichtsbehörde eine Überprüfung ermöglicht. Dabei ist nach Art. 31 Abs. 4 S. 3 DS-GVO fein-säuberlich darauf zu achten, dass die Dokumentation lediglich Informationen enthält, die von dem Überprüfungszweck gedeckt sind. Art. 31 Abs. 5 und 6 DS-GVO runden das Bild ab, in dem die Kommission zur näheren Ausgestaltung durch delegierte Rechtsakte die Vorgabe von Standardformaten für Meldungen an die Aufsichtsbehörde nebst Verfahrensvorschriften und vom Bestimmungen ermächtigt wird, wobei die Ermächtigung auch Regelungen zu Löschungsfristen für die durch Art. 31 Abs. 4 DS-GVO vorgeschriebene Dokumentation umfasst (Art. 31 Abs. 6 DS-GVO).

Gegenüber den Betroffenen sollen nach Art. 32 DS-GVO nur eingeschränkte Meldepflichten bestehen. Eine Meldepflicht besteht nach Art. 32 Abs. 1 DS-GVO nur bei erheblichen Datenschutzverstößen („adversely affect"; die deutsche Übersetzung ist ungenau und stark redundant). Und es ist bezeichnend, dass die Entwurfsverfasser eine Reihenfolge festlegen für die Meldungen: Erst nach Verständigung der Aufsichtsbehörde (Art. 31 DS-GVO) besteht eine Benachrichtigungspflicht gegenüber den Betroffenen.

Nach Art. 32 Abs. 3 DS-GVO kann die „Zufriedenheit der Aufsichtsbehörde" eine Meldung an die Betroffenen gänzlich entbehrlich machen, wenn der Behörde nachgewiesen wird, dass geeignete technische Sicherheitsvorkehrungen getroffen worden sind, wobei es unstimmig erscheint, wenn in diesem Zusammenhang technische Sicherheitsvorkehrungen ohne Rücksicht auf die Umstände des Einzelfalls dahingehend konkretisiert werden, dass eine Verschlüsselungspflicht statuiert wird (Art. 32 Abs. 3 S. 2 DS-GVO).

Die Aufsichtsbehörde wird zum Dreh- und Angelpunkt der Benachrichtigungspflichten bei Datenpannen. In Art. 32 Abs. 4 DS-GVO wird es sogar für regelungsbedürftig geachtet, dass die Aufsichtsbehörden den Verantwortlichen jederzeit zur Benachrichtigung von Betroffenen auffordern können, und zwar „unbeschadet" einer eigenständigen Verpflichtung des Verpflichteten gem. Art. 32 Abs. 1 DS-GVO.

### g) Benennung eines Datenschutzbeauftragten

Nach Art. 35 Abs. 1 DS-GVO besteht eine Verpflichtung zur Benennung eines Datenschutzbeauftragten für Behörden und öffentliche Einrichtungen sowie für Unternehmen mit mindestens 250 Mitarbeitern bzw. für Unternehmen, bei denen die Datenverarbeitung als „Kerntätigkeit" zu sehen ist. Anders als nach § 4f Abs. 1 S. 3 BDSG würde dies für die meisten kleineren Unternehmen die Bestellung eines Datenschutzbeauftragten entbehrlich machen.

32 Vgl. *Hornung*, ZD 2011, 51, 52.

## IV. Fazit

Das Fazit einer ersten Analyse fällt überwiegend negativ aus. Das Verbotsprinzip und andere tragende Säulen des materiellen Datenschutzrechts (Begriff der personenbezogenen Daten; grundsätzliche Gleichbehandlung von banalen und sensiblen Daten; komplizierte Einwilligungserfordernisse; stiefmütterliche Behandlung der Kommunikationsfreiheit) bleiben unverändert. Punktuelle Neuregelungen des materiellen Rechts können nur teilweise überzeugen (Schutz von Kindern; Abschaffung der Meldepflicht; Erleichterungen für kleine Unternehmen). Mit großer Akribie haben die Entwurfsverfasser detaillierte Vorschriften zur Durchsetzung des Datenschutzrechts erarbeitet, die eine „Superbehörde" (den Europäischen Datenschutzausschuss) schaffen und die Befugnisse der Europäischen Kommission zur Setzung von Recht und dessen Vollzug bedenklich weit fassen möchten. Wenn jedoch starke europäische Datenschutzbehörden mit Instrumentarien des 21. Jahrhunderts Vorschriften durchsetzen sollen, die aus dem Zeitalter der Großrechner stammen, ist nichts Gutes zu erwarten.

// Autor

**Niko Härting**, RA und Partner von HÄRTING Rechtsanwälte, Berlin

Dr. Tim Oliver Brandi, LL.M. (Columbia), RA, und Dr. Karsten Müller-Eising, RA/Notar

# Neuauflage des Finanzmarktstabilisierungsgesetzes

**Der Bundestag hat am 26.1.2012 das Zweite Finanzmarktstabilisierungsgesetz beschlossen; am 10.2.2012 wurde es vom Bundesrat gebilligt. Das Gesetz dient der Umsetzung einer Entscheidung des Europäischen Rates vom 26.10.2011, nach der Kreditinstitute zum 30.6.2012 temporär höhere Eigenmittelanforderungen erfüllen müssen und die Mitgliedstaaten zur Unterstützung bereitstehen sollen, wenn die Institute den Kapitalbedarf nicht vollständig am Kapitalmarkt decken können. Zu diesem Zweck erfolgt eine Neuauflage der Finanzmarktstabilisierungsgesetze aus den Jahren 2008 bis 2010 und eine Reaktivierung des Finanzmarktstabilisierungsfonds (FMS). Dieser Beitrag stellt die wesentlichen Regelungen des Zweiten Finanzmarktstabilisierungsgesetzes vor.**

## I. Überblick

Der Gesetzestext entspricht im Wesentlichen dem Regierungsentwurf vom 14.12.2011[1] unter Berücksichtigung einiger Empfehlungen des Haushaltsausschusses des Bundestages.[2] Das reaktivierte Finanzmarktstabilisierungsgesetz soll neben die weiterhin fortgeltenden Regelungen des Bankenrestrukturierungsgesetzes treten.[3] Während das Bankenrestrukturierungsgesetz Eingriffe im Fall einer konkreten Gefahr eines einzelnen Instituts erlaubt (z. B. durch Übertragung der systemrelevanten Teile einer Bank auf eine andere private Bank oder eine „Brückenbank" im Wege der Übertragungsanordnung gem. §§ 48a ff. KWG), soll das Zweite Finanzmarktstabilisierungsgesetz vorbeugende Maßnahmen zur Sicherung der Stabilität des Finanzsystems insgesamt ermöglichen.[4]

Das Zweite Finanzmarktstabilisierungsgesetz sieht zu diesem Zweck eine Neuauflage derjenigen Stabilisierungsmaßnahmen des FMS vor, die auch bereits bis Ende 2010 zur Verfügung standen. Gesetzestechnisch wird dies dadurch erreicht, dass die an sich zum 31.12.2010 ausgelaufene Frist für die Gewährung von Stabilisierungsmaßnahmen nach dem Finanzmarktstabilisierungsfondsgesetzes nunmehr bis zum 31.12.2012 verlängert wird (vgl. § 13 Abs. 1 FMStFG n. F.).[5]

Auf der Basis der in der Finanzmarktkrise von 2008 bis 2010 gewonnenen Erfahrungen werden einige Regelungen des FMStFG zu Zulässigkeit und Umfang von Stabilisierungsmaßnahmen leicht erweitert und modifiziert (s. hierzu unten II.). In einem neu eingefügten § 3c FMStFG wird die Rechtsstellung der Mitglieder des Leitungsausschusses der Bundesanstalt für Finanzmarktstabilisierung (FMSA) im Sinne eines öffentlich-rechtlichen Amtsverhältnisses zur Bundesrepublik Deutschland neu geregelt.[6]

Ferner sind wichtige Ergänzungen im Kreditwesengesetz (KWG) vorgesehen. So wird der Bundesanstalt für Finanzdienstleistungsaufsicht (BaFin) nunmehr gem. § 10 Abs. 1b S. 2 KWG n. F. bis zum 31.12.2012 die Befugnis eingeräumt, eigenständig oder auf der Basis eines koordi-

1 Der Regierungsentwurf vom 14.12.2011 wurde als Gesetzesentwurf der Fraktionen der CDU/CSU und FDP in das Gesetzgebungsverfahren eingebracht (BT-Drucks. 17/8343, 5 ff.).

2 Beschlussempfehlung und Bericht des Haushaltsausschusses vom 25.1.2012, BT-Drucks. 17/8483. Das Zweite Finanzmarktstabilisierungsgesetz tritt am Tag nach seiner Verkündung im Bundesgesetzblatt in Kraft.

3 Das Gesetz zur Restrukturierung und geordneten Abwicklung von Kreditinstituten, zur Errichtung eines Restrukturierungsfonds für Kreditinstitute und zur Verlängerung der Verjährungsfrist der aktienrechtlichen Organhaftung (sog. Bankenrestrukturierungsgesetz) vom 9.12.2010, BGBl. I, 1900, war in allen Teilen spätestens zum 1.1.2011 in Kraft getreten. S. hierzu *Müller-Eising/Brandi/Sinhart/Lorenz/Löw*, BB 2011, 66, sowie umfassend *Brogl (Hrsg.)*, Handbuch Banken-Restrukturierung, Bankenabgabe – Prävention – Stabilisierung – Haftung, 2012.

4 Regierungsentwurf, Zweites Finanzmarktstabilisierungsgesetz, BT-Drucks. 17/8343, 2. Dabei soll die Nutzung der Instrumente des Finanzmarktstabilisierungsfonds nach Ansicht der Fraktionen der CDU/CSU und FDP die Ausnahme bleiben und im Regelfall das Restrukturierungsgesetz zur Anwendung gelangen (Beschlussempfehlung und Bericht des Haushaltsausschusses, BT-Drucks. 17/8483, 10).

5 Nach Einschätzung der Fraktionen der CDU/CSU und FDP ist eine Verlängerung dieser Frist denkbar, falls sich im Verlaufe des Jahres 2012 herausstellen sollte, dass Stabilisierungsmaßnahmen über den 31.12.2012 hinaus zur Sicherung der Funktionsfähigkeit der Finanzmärkte erforderlich seien (Beschlussempfehlung und Bericht des Haushaltsausschusses, BT-Drucks. 17/8483, 13).

6 Regierungsentwurf, Zweites Finanzmarktstabilisierungsgesetz, BT-Drucks. 17/8343, 12 f.