GERRIT HORNUNG

Eine Datenschutz-Grundverordnung für Europa?

Licht und Schatten im Kommissionsentwurf vom 25.1.2012

Datenschutz in Europa
Reform der Datenschutzrichtlinie
Datenschutz-Grundverordnung
Moderne Datenschutzinstrumente
Rolle der EU-Kommission im Datenschutzrecht

■ Am 25.1.2012 hat die EU-Kommission den lange erwarteten Vorschlag für eine Reform des europäischen Datenschutzrechts vorgelegt, der aus einer „Datenschutz-Grundverordnung" (anstelle der bisherigen Datenschutzrichtlinie 95/46 EG) und einer Richtlinie zur Datenverarbeitung im Bereich von Strafverfolgung und Gefahrenabwehr (anstelle des Rahmenbeschlusses 2008/977/JHA) besteht. Der Beitrag stellt den Entwurf der Verordnung im Überblick vor und vertieft ausgewählte Neuerungen zu Anwendungsbereich, Betroffenenrechten, modernen Datenschutzinstrumenten und institutionellen Fragen. Der Entwurf der Richtlinie wird in einem Folgebeitrag in ZD 4/2012 besprochen. Im Ergebnis enthält der Vorschlag viele begrüßenswerte Regelungen, aber auch einige kritikwürdige Punkte.

■ On January 25, 2012, the EU Commission presented a suggestion which has long been awaited for a reform of European data protection law. This consists of a "General Data Protection Regulation" (in lieu of the hitherto Data Protection Directive 95/46/EC) and a Directive for Data Processing in the area of criminal prosecution and defense of a threat (in lieu of the Framework Resolution 2008/977/JHA). This article will introduce an overview of the draft of the Regulation and will discuss in detail certain innovations regarding area of application, rights of the data subject, modern data protection instruments and institutional issues. The draft of the Directive will be discussed in a subsequent article in ZD 4/2012. In sum, the draft contains many welcome regulations, but also several issues which deserve criticism.

I. Hintergrund

Die europäische Datenschutzrichtlinie (DSRL) ist – gemessen an den Innovationszyklen der Informationsgesellschaft – ein steinaltes Regelungsinstrument. Der erste Vorschlag der *Kommission* datiert vom 5.11.1990,[1] also einem Zeitpunkt, zu dem es kein WWW gab. Die am 24.10.1995 verabschiedete DSRL[2] enthält für die nationalen Datenschutzregeln verbindliche Vorgaben, die nach praktisch allgemeiner Meinung dringend modernisierungsbedürftig sind.[3] Die *Kommission* hat die Initiative ergriffen und zunächst Ende 2010 eine Mitteilung zu einem „Gesamtkonzept für den Datenschutz in der Europäischen Union" veröffentlicht.[4] Der nun vorgelegte Entwurf einer „Verordnung zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr (Datenschutz-Grundverordnung)"[5] (im Folgenden: DS-GVO-E; Artikelangaben ohne Bezeichnung beziehen sich auf diese) führt die Modernisierungsideen der Mitteilung fort. Erwägungsgrund (EG) 7 stellt zu Recht heraus, dass bei allem Überarbeitungsbedarf die grundsätzlichen Ziele der DSRL nach wie vor gültig sind: Gewährleistung eines einheitlichen Grundrechtsschutzes bei der Verarbeitung personenbezogener Daten in der Union sowie Gewährleistung des freien Verkehrs dieser Daten zwischen den Mitgliedstaaten. Technologischer Fortschritt und Globalisierung zwingen jedoch zu einer Neuordnung der entsprechenden Vorschriften (EG 5 ff.).

Das Vorhaben der *Kommission*, das sich nunmehr auf Art. 16 AEUV stützt,[6] bezieht sich nicht nur auf den Regelungsbereich der DSRL. Der parallele Vorschlag einer „Richtlinie zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die zuständigen Behörden zum Zwecke der Verhütung, Aufdeckung, Untersuchung oder Verfolgung von Straftaten oder der Strafvollstreckung sowie zum freien Datenverkehr"[7] soll diesen bisher durch den Rahmenbeschluss 2008/977/JHA[8] regulierten Bereich weiter harmonisieren. Die Gesamtstrategie wird in einer übergreifenden Mitteilung „Der Schutz der Privatsphäre in einer vernetzten Welt. Ein europäischer Datenschutzrahmen für das 21. Jahrhundert"[9] erläutert.

Eine vorläufige Fassung der drei Texte wurde im November 2011 bekannt.[10] Offenbar gab es u.a. von Seiten der datenverarbeitenden Wirtschaft und i.R.d. Konsultationen mit den USA deutliche Vorbehalte gegen die Pläne der *Kommission*. In einer „informal note" kritisierte die *US-Administration* insbesondere die Einführung neuer Schutzinstrumente (data breach notification, Recht auf Vergessenwerden, Datenschutz bei Kindern), die Regeln zum Datentransfer in Drittstaaten sowie die Pflicht, bei Anordnungen zur Offenlegung von Daten durch Gerichte und Behörden von Drittstaaten die Genehmigung der eigenen Aufsichtsbehörde einzuholen (Art. 42 Abs. 2 des Entwurfs).[11] Die Wirkungen dieser Kritik sind von außen nicht zu beurteilen. Jedenfalls unterscheidet sich die letztlich verabschiedete Fassung an einigen wichtigen Stellen von der aus dem November 2011; das betrifft insbesondere die Absenkung der Einwilligungsfähigkeit von Kindern von 18 auf 13 Jahre (Art. 8 Abs. 1; dies ent-

1 ABl. Nr. C 277 v. 5.11.1990, S. 3.
2 RL 95/46/EG, ABl. EG Nr. L 281 v. 23.11.1995, S. 31.
3 S. statt vieler *Simitis*, in: Herzog/Neumann, FS für Winfried Hassemer, 2010, S. 1235.
4 Mitt. v. 4.11.2010, KOM(2010) 609 endg.
5 KOM (2012) 11 endg.
6 Zu den primärrechtlichen Änderungen im Bereich des Datenschutzrechts durch den Lissabon-Vertrag s. *Spiecker gen. Döhmann/Eisenbarth*, JZ 2011, 169.
7 KOM(2012) 10 endg.
8 ABl. EU Nr. L 350/60 v. 30.12.2008.
9 KOM(2012) 9 endg.
10 S. http://www.statewatch.org/eu-dp.htm.
11 S. die Dokumentation unter: http://www.edri.org/US-DPR. Das Genehmigungserfordernis hätte insb. den Bereich der sog. „E-Discovery" betroffen, dazu z.B. *Brisch/Laue*, RDV 2010, 1; *Özbek*, DuD 2010, 576; *District Court of Utah* MMR 2010, 275 m. Anm. *Spies/Schröder*.

spricht der US-amerikanischen Rechtslage) sowie die Streichung von Art. 42 des Entwurfs (s. in abgeschwächter Form nunmehr noch EG 90).

II. Der Wechsel zur Verordnung

Der vorgeschlagene Wechsel zum Instrument der Verordnung hat sowohl Symbolcharakter als auch weitreichende rechtliche Folgen. Symbolisch steht der Wechsel für die Auffassung der *Kommission*, die DSRL habe nicht zu einer hinreichenden Harmonisierung des Datenschutzrechts in der Union geführt (EG 7), sowie für die Hoffnung auf eine stärkere Rechtsvereinheitlichung und mehr Rechtssicherheit zur Stärkung der Betroffenenrechte und Förderung des gemeinsamen Markts (EG 11). Rechtlich bewirkt der Wechsel des Instruments, dass die neuen Regeln bei ihrer Annahme nach Art. 288 Abs. 2 AEUV in allen Teilen verbindlich und unmittelbar in jedem Mitgliedstaat gelten würden. Deutsche Gerichte und Behörden würden nicht mehr Bundes- und Landesdatenschutzgesetze, sondern direkt die Regeln der DS-GVO-E anwenden, für deren Auslegung der *EuGH* nach den Regeln des Vorabentscheidungsverfahrens (Art. 267 Abs. 1 lit. b AEUV) zuständig wäre.

Wegen dieser Folgen hat der für den Datenschutz zuständige Richter des BVerfG, *Johannes Masing*, das Vorhaben der *Kommission* sehr grundsätzlich kritisiert.[12] In der Tat würden – akzeptiert man den Vorrang des Europarechts – die Grundrechte des GG im Geltungsbereich der DS-GVO-E ihre Wirkung verlieren und die Entscheidungsbefugnis des *BVerfG* entsprechend beschränkt.[13] Das betrifft bei der Datenverarbeitung durch nichtöffentliche Stellen klassische Drittwirkungsfragen im Spannungsfeld zwischen Persönlichkeitsschutz und anderen Grundrechten. Da die DS-GVO-E mit Ausnahme von Gefahrenabwehr und Strafverfolgung auch die staatliche Verwaltung erfasst, wäre darüber hinaus aber auch ein weiter Bereich der hoheitlichen Datenverarbeitung nicht mehr durch das *BVerfG* kontrollierbar. Um es hart auszudrücken: Das betrifft auch den Fall der Volkszählung und hätte einer entsprechenden Verfassungsfortbildung des *BVerfG* in einer Entscheidung zu diesem Bereich entgegengestanden.[14]

Diese Verschiebung ist aus zwei Gründen bedeutsam: Zum einen existiert auf EU-Ebene kein der Verfassungsbeschwerde vergleichbarer Rechtsbehelf einzelner Grundrechtsträger, zum anderen ist der *EuGH* trotz des Ausbaus seiner Grundrechtsrechtsprechung nach wie vor weit davon entfernt, eine dem *BVerfG* vergleichbare Grundrechtsdogmatik zu entwickeln und anzuwenden.[15] Schon aus personellen Gründen wird sich hieran in Zukunft kaum etwas ändern. Eine spezifische Grundrechtskontrolle wäre auf europäischer Ebene wohl nur durch den Beitritt der Union zur EMRK zu erreichen, der sich allerdings weiter verzögert und überdies den *EGMR* ressourcenmäßig (weiter) überfordern könnte.

Materiell-rechtlich wäre mit dem Übergang zur Verordnung nicht nur der Streit um die Voll- oder Mindestharmonisierung der DSRL obsolet.[16] Dem nationalen Gesetzgeber wäre es – insbesondere angesichts der weitreichenden Befugnisse der *Kommission* für delegierte Rechtsakte – auch weithin verwehrt, konkretisierende Bestimmungen zu erlassen: Eine Regelung spezifischer Normen für Videoüberwachung oder Chipkarten wie in §§ 6b, 6c BDSG wäre nicht möglich, statt der Grenze in § 4f Abs. 1 Satz 3 BDSG würde eine allgemeine Pflicht zur Bestellung betrieblicher Datenschutzbeauftragter gem. Art. 35 Abs. 1 lit. b erst ab 250 Mitarbeitern gelten, das grundsätzliche Schriftformerfordernis für die Einwilligung (§ 4a Abs. 1 Satz 2 BDSG) ließe sich wegen des Widerspruchs mit Art. 4 Abs. 8, Art. 6 Abs. 1 lit. a, Art. 7 nicht aufrechterhalten und die Erprobung neuer Regelungsinstrumente zum Schutz personenbezogener Daten würde unmöglich gemacht. Letzteres ist angesichts der Tatsache, dass der Entwurf mit den Regelungen für den Datenschutz durch Technik (Art. 23) und ein Überprüfungs- und Auditverfahren (Art. 22) Entwicklungen aufgreift, die i.R.d. Spielräume der DSRL durch die nationalen Rechtsordnungen entwickelt wurden, unter dem Gesichtspunkt der Ermöglichung innovativer Schutzinstrumente nur bedingt überzeugend.[17] Es wird hier sehr darauf ankommen, wie die *Kommission* die ihr zugedachte Rolle ausfüllt.[18]

Besteht also aus deutscher Sicht die Tendenz, die Regelungen der DS-GVO-E als Verlust zu deuten, sind die Motive der *Kommission* nachvollziehbar, wenn man den Stand des Datenschutzrechts in der Praxis in den Blick nimmt. Die DSRL hat zwar zu einer gewissen formalen Harmonisierung geführt. Die nationalen Regeln weisen jedoch immer noch eine erhebliche Bandbreite auf, und das tatsächliche Schutzniveau in den Mitgliedstaaten unterscheidet sich ebenfalls erheblich.[19] Hierzu trägt auch bei, dass die nationalen Aufsichtsbehörden ihre Rolle stark verschiedenartig interpretieren und über sehr unterschiedliche Ressourcen für ihre Tätigkeit verfügen.

Explizite Öffnungsklauseln enthält der Entwurf nur wenige. Die Mitgliedstaaten sollen die Befugnis erhalten, Abweichungen und Ausnahmen für die Verarbeitung personenbezogener Daten zu regeln, die allein zu journalistischen, künstlerischen oder literarischen Zwecken erfolgt (Art. 80). Besondere Regeln können auch für die „Verarbeitung personenbezogener Arbeitnehmerdaten im Beschäftigungskontext" erlassen werden (Art. 82); der Ball liegt hier also wieder beim deutschen Gesetzgeber, der seit der Anhörung im *Bundestags-Innenausschuss* am 23.5.2011 weitgehend untätig geblieben ist.[20] Daneben bestehen Öffnungsklauseln insbesondere hinsichtlich der Erlaubnistatbestände für die Datenverarbeitung (Art. 6 Abs. 3 lit. b), der Regeln zu besonderen Kategorien personenbezogener Daten (Art. 8 Abs. 2 lit. b, g), der Ausnahmen vom Recht auf Vergessenwerden und vom Verbot von auf Profiling basierenden Maßnahmen (Art. 17 Abs. 3 lit. d, Art. 20 Abs. 2 lit. b), der Beschränkungen der Rechte und Pflichten wegen verschiedener öffentlicher Interessen (Art. 21), der Bestimmung der Aufsichtsbehörde (Art. 46, 48), dem Verbandsklagerecht (Art. 73 Abs. 2), Gesundheitsdaten (Art. 81) und Geheimhaltungspflichten (Art. 84).

III. Struktur und Inhalt im Überblick

Der Entwurf enthält elf Kapitel. Die Allgemeinen Bestimmungen (Kap. I) regeln Zielsetzungen, den sachlichen und räumlichen Anwendungsbereich und Begriffsbestimmungen. Einige Definitionen sind aus Art. 2 DSRL übernommen, andere stammen aus anderen EU-Richtlinien oder waren bislang im Datenschutzrecht nicht legaldefiniert (genetische und biometrische Daten, Gesundheitsdaten, Unternehmensgruppe, Hauptniederlassung

12 „Ein Abschied von den Grundrechten", Süddeutsche Zeitung (SZ) v. 9.1.2012.
13 Zum Problem z.B. *Matz-Lück*, in: ders./Hong, Grundrechte und Grundfreiheiten im Mehrebenensystem – Konkurrenzen und Interferenzen, 2012, S. 161.
14 Weitere denkbare Beispiele sind der Bereich der Finanzverwaltung (zum Abruf von Kontostammdaten s. BVerfGE 118, 168) oder der Auskunftsanspruch gegen Behörden (z.B. *BVerfG* MMR 2008, 450). Ich danke *Matthias Bäcker* für die Anregungen zu diesem Punkt.
15 Zur Rspr. zum Datenschutz s. *Streinz*, DuD 2011, 602.
16 Der *EuGH* sieht in der DSRL eine „grundsätzlich umfassende Harmonisierung", s. Rs. C-101/01, MMR 2004, 95 m. Anm. *Roßnagel*, Abs. 96 – Lindqvist; Rs. C-524/06, EuZW 2009, 183, Abs. 51 – Huber; Rs. C-468/10, ZD 2012, 33, Abs. 29 ff. – Crédito ASNEF; überdies unmittelbare Wirkung von Art. 7 lit. f.
17 S. näher *Hornung*, ZD 2011, 51, 55 f.
18 Dazu noch unten IV.4.
19 S. den Evaluationsbericht der *Kommission* als Anhang zu SEC(2012) 72 final.
20 S. die Entwürfe der *Bundesregierung* (BT-Drs. 17/4230), der *SPD* (BT-Drs. 17/69) und von *BÜNDNIS 90/DIE GRÜNEN* (BT-Drs. 17/4852).

etc.). Die Definitionen der personenbezogenen Daten und der betroffenen Person werden auseinandergezogen, zusammen ergeben sie aber weiterhin die bisherigen Kriterien der bestimmten oder bestimmbaren Person. EG 23 hält daran fest, dass für die Frage der Bestimmbarkeit „alle Mittel zu berücksichtigen [sind], die von dem für die Verarbeitung Verantwortlichen oder einer anderen Person nach allgemeinem Ermessen aller Voraussicht nach zur Identifizierung der Person genutzt werden".

Als Allgemeine Grundsätze (Kap. II) werden Prinzipien normiert, die teils mit Art. 6 DSRL korrespondieren, teils darüber hinausgehen (v.a. bei den Grundsätzen der Transparenz, Datensparsamkeit und umfassenden Verantwortlichkeit der für die Datenverarbeitung Verantwortlichen). Art. 6 korrespondiert mit Art. 7 DSRL, enthält aber Modifizierungen (insbesondere hinsichtlich der begrüßenswerten[21] Beibehaltung des Verbotsprinzips). Es folgen Anforderungen an die Einwilligung (Art. 7), die Verarbeitung personenbezogener Daten von Kindern (Art. 8) und von besonderen Kategorien personenbezogener Daten (Art. 9, nunmehr unter Erweiterung um genetische Daten und Informationen zu Straftaten und Ordnungswidrigkeiten, während biometrische Daten außen vorbleiben).

Die Rechte der Betroffenen (Kap. III) werden ausführlicher als bisher geregelt und inhaltlich erweitert. Neben übergreifenden Bestimmungen zur Transparenz (Art. 11 ff.) enthält der Entwurf Rechte auf Information, Auskunft, Berichtigung, Löschung und Widerspruch (Art. 14 ff.). Das Recht, keiner Maßnahme unterworfen zu werden, die auf Profiling basiert (Art. 20), baut Art. 15 Abs. 1 DSRL aus. Neu sind dagegen das Recht auf Vergessenwerden (Art. 17, dem allerdings das Recht auf Löschung zu Grunde liegt) und das Recht auf Datenübertragbarkeit (Art. 18). Art. 21 enthält Ausnahmebefugnisse für Union und Mitgliedstaaten, die sich an Art. 13 DSRL anlehnen.

Ebenfalls ausführlicher als bisher werden Regeln über die für die Verarbeitung Verantwortlichen und Auftragsdatenverarbeiter gefasst (Kap. IV). Diese sind – einige Punkte der Diskussion um den Grundsatz der Rechenschaftspflicht aufgreifend[22] – in Art. 22 im Überblick normiert und werden im Anschluss hinsichtlich einzelner Pflichten spezifiziert; das schließt die Pflicht zur Zusammenarbeit mit der Aufsichtsbehörde (Art. 29) und Vorgaben zur Datensicherheit (Art. 30) ein. Die allgemeine Meldepflicht nach Art. 18 Abs. 1, 19 DSRL wird zu Gunsten einer Pflicht der Verantwortlichen und Auftragsdatenverarbeiter aufgehoben, die Verarbeitungsvorgänge zu dokumentieren (sehr detailliert in Art. 28 geregelt). Neu sind die Pflichten in Bezug auf den Grundsatz des Datenschutzes durch Technik und das Gebot datenschutzfreundlicher Voreinstellungen (Art. 23), die Regelung zur gemeinsamen Verantwortung mehrerer Verantwortlicher (Art. 24), die Meldepflicht bei Verstößen gegen den Datenschutz (Art. 31 f.), die Pflicht, in bestimmten Fällen eine Datenschutz-Folgenabschätzung durchzuführen (Art. 33), und die Möglichkeit der Einführung von Zertifizierungsverfahren sowie von Datenschutzsiegeln und -prüfzeichen (Art. 39). Auftragsdatenverarbeiter werden viel ausführlicher als bisher in Art. 26 f. geregelt. Anstelle des nach Art. 18 Abs. 2 DSRL fakultativen internen Datenschutzbeauftragten führt Art. 35 diesen nunmehr verpflichtend ein, allerdings nur bei Verarbeitung durch eine öffentliche Stelle und bei Unternehmen, die entweder mindestens 250 Mitarbeiter beschäftigen oder deren Kerntätigkeit in Verarbeitungsvorgängen besteht, die eine „regelmäßige und systematische Beobachtung von betroffenen Personen erforderlich machen".[23] Die *Kommission* erhält schließlich die Befugnis, Verhaltensregeln mit allgemeiner Gültigkeit auszustatten (Art. 38).

Die Regeln zur Übermittlung in Drittländer oder an internationale Organisationen (Kap. V) enthalten mehrere Erlaubnistatbestände. Die Übermittlung kann danach zulässig sein auf Grund eines Angemessenheitsbeschlusses der *Kommission* (Art. 41), ausreichender Garantien (insbesondere in Form von Standard-Datenschutzklauseln, verbindlichen unternehmensinternen Vorschriften und Vertragsklauseln, Art. 42 f.; dabei können Standard-Datenschutzklauseln von der *Kommission* für allgemein gültig erklärt werden) sowie in weiteren Einzelfällen (u.a. nach informierter Einwilligung, aus „wichtigen Gründen des öffentlichen Interesses" und zur Verwirklichung eines berechtigten Interesses, wenn dieses „nicht als häufig oder massiv bezeichnet werden kann", Art. 44).

Deutlich ausführlicher als bisher fallen auch die Regelungen zu den Aufsichtsbehörden aus (Kap. VI). Neben der Pflicht zur Einrichtung (Art. 46) werden ihre Unabhängigkeit präzisiert (Art. 47) und Aufgaben und Befugnisse einheitlich festgeschrieben (Art. 51 ff., insbesondere die Befugnis zur Verhängung verwaltungsrechtlicher Sanktionen), die bislang in den Mitgliedstaaten sehr unterschiedlich normiert sind und noch unterschiedlicher gehandhabt werden. Völlig neu ist die Regelung einer (einzigen) federführenden Aufsichtsbehörde am Ort der Hauptniederlassung (sog. „Prinzip einer zentralen Anlaufstelle für den Datenschutz") in Art. 51. Im Anschluss werden Vorgaben zu Zusammenarbeit und Kohärenz getroffen (Kap. VII). Die Aufsichtsbehörden sind zur gegenseitigen Amtshilfe verpflichtet (Art. 55). Das Kohärenzverfahren findet insbesondere bei Verarbeitungsvorgängen Anwendung, die Personen in mehreren Mitgliedstaaten betreffen können, aber auch bei der Festlegung von Standard-Datenschutzklauseln und der Genehmigung von Vertragsklauseln und unternehmensinternen Vorschriften. In diesen Fällen können der *Europäische Datenschutzausschuss* (die Nachfolgeorganisation der *Art. 29-Datenschutzgruppe*; Einrichtung und Befugnisse werden in Art. 64 ff. normiert) und die *Kommission* eine Stellungnahme abgeben. Die *Kommission* erhält überdies die Befugnis, geplante Maßnahmen auszusetzen, soweit dies für die korrekte Anwendung der DS-GVO-E erforderlich ist (Art. 60) sowie zum Erlass von Durchführungsakten für das Kohärenzverfahren (Art. 62). Beides bedeutet eine erhebliche Machtverschiebung im institutionellen Gefüge des Datenschutzes.[24]

Rechtsbehelfe, Haftung und Sanktionen werden in Kap. VIII geregelt. Neben dem Recht auf Beschwerde bei der Aufsichtsbehörde (Art. 73; hier wird zusätzlich ein Verbandsklagerecht normiert) wird auch ein neuer gerichtlicher Rechtsbehelf vorgesehen, um das Tätigwerden derselben zu erzwingen (Art. 74, bei ausländischen Aufsichtsbehörden tritt das Recht hinzu, die eigene Aufsichtsbehörde um Klage gegen die ausländische Behörde zu ersuchen). Betroffene haben das Recht, gegen die Verantwortlichen oder Auftragsdatenverarbeiter entweder im eigenen Mitgliedstaat oder in demjenigen zu klagen, in dem der Beklagte niedergelassen ist (Art. 75). Art. 77 bestimmt das Recht auf Schadensersatz und erweitert es explizit auf Schäden, die der Auftragsdatenverarbeiter verursacht hat. Schließlich verpflichtet Art. 78 die Mitgliedstaaten zur Einführung von Sanktionsvorschriften, während Art. 79 die Aufsichtsbehörden ermächtigt, bei bestimmten Vergehen Geldbußen zu verhängen, die bis zu € 1 Mio. oder 2% (im Entwurf von 2011 noch 5%) des weltweiten Jahresumsatzes reichen können.

Vorschriften für besondere Datenverarbeitungssituationen sind schließlich in Kap. IX enthalten. Das betrifft die schon erwähnten Ausnahmen für journalistische, künstlerische und literari-

21 A.A. *Schneider*, AnwBl. 2011, 233; *ders./Härting*, ZD 2011, 63, 64.
22 Dazu z.B. *Art. 29-Datenschutzgruppe*, WP 173: Stellungnahme 3/2010 zum Grundsatz der Rechenschaftspflicht v. 13.7.2010.
23 Dazu noch unten IV.4.
24 Dazu noch unten IV.4.

sche Zwecke, Beschäftigtendaten sowie historische, statistische und wissenschaftliche Zwecke (Art. 80, 82, 83), Regelungen zur Verarbeitung von Gesundheitsdaten (Art. 81), Geheimhaltungspflichten (Art. 84) und Ausnahmen für Kirchen und andere Religionsgemeinschaften (Art. 85).

Kap. X regelt die Einzelheiten zu den vielfach enthaltenen Befugnissen zum Erlass delegierter Rechtsakte, die teils auf unbestimmte Zeit, teils auf Widerruf übertragen werden; hinzu kommen Normen zu Durchführungsrechtsakten. Die Schlussbestimmungen in Kap. XI heben die DSRL auf, regeln das Verhältnis zur Datenschutzrichtlinie für die elektronische Kommunikation und bestimmen eine Berichtspflicht der *Kommission* zur Bewertung und Überprüfung der DS-GVO-E.

IV. Ausgewählte Regelungsbereiche

Aus den vielen Regelungsproblemen, die der Entwurf der *Kommission* aufwirft, werden im Folgenden vier herausgegriffen, die als besonders diskussionswürdig erscheinen.

1. Anwendungsbereich und Drittstaaten

Der sachliche Anwendungsbereich entspricht im Wesentlichen dem der DSRL. Das Konzept der personenbezogenen und -beziehbaren Daten bleibt nach EG 23 erhalten. In den Beratungen wurde allerdings EG 24 in sein Gegenteil verkehrt: Hieß es dort im Entwurf, die DS-GVO-E erfasse Online-Kennungen wie IP-Adressen und Cookies wegen der durch sie hinterlassenen Spuren und Profilbildungsmöglichkeiten, lautet die Formulierung nunmehr (inhaltlich zutreffend, aber wenig logisch), hieraus folge, dass ein Personenbezug nicht zwangsläufig und unter allen Umständen gegeben sei.[25] Die Ausnahme für persönliche und familiäre Zwecke wurde aus Art. 3 Abs. 2 DSRL übernommen und klarstellend hinzugefügt, dass keine Gewinnerzielungsabsicht vorliegen darf. Der Entwurf hatte noch hinzugesetzt, dass die DS-GVO-E dennoch anwendbar sei, wenn personenbezogene Daten einer unbestimmten Zahl von Individuen zugänglich gemacht würden. Diese Übernahme des Lindqvist-Urteils[26] wurde offenbar in allerletzter Sekunde gestrichen; die Entscheidung dürfte aber auch die Neuregelung erfassen.

Der Entwurf enthält in Art. 3 Neuerungen zum räumlichen Anwendungsbereich, die sich ebenfalls im Verfahren verändert haben. Neben der Anwendung auf Verantwortliche in der Union (auch dann, wenn die Verarbeitung außerhalb derselben stattfindet, EG 19) findet die DS-GVO-E nunmehr auch auf Verantwortliche in Drittstaaten Anwendung, wenn es um personenbezogene Daten von in der Union ansässigen Personen geht und die Datenverarbeitung entweder dem Angebot von Waren oder Dienstleistungen „in der Union" oder der „Beobachtung des Verhaltens" der Betroffenen dient.[27] Die zweite Alternative wird in EG 21 damit beschrieben, dass Internetaktivitäten mit Hilfe von Datenverarbeitungstechniken nachvollzogen würden, durch die einer Person ein Profil zugeordnet werde, das die Grundlage für sie betreffende Entscheidungen bilde oder anhand dessen ihre persönlichen Vorlieben, Verhaltensweisen oder Gepflogenheiten analysiert oder vorausgesagt werden sollten. Das dürfte zumindest auf diejenigen sozialen Netzwerke zutreffen, die wie *Facebook* über in andere Webseiten eingebettete Elemente (Like-Button[28] und andere) Daten über ihre Kunden sammeln. Die erste Alternative wird demgegenüber nicht näher erläutert. Das Beauftragen einer Dienstleistung für eine Reise im Ausland wird etwa nicht erfasst, während dies bei einer Warenbestellung nebst Lieferung der Fall ist. Probleme könnten sich dagegen bei der Frage ergeben, wann eine Online-Dienstleistung „in" der Union angeboten wird.

Für die verwandte Frage der Übermittlung in Drittstaaten enthält Art. 40 den Vorbehalt der Einhaltung von Kap. V und der übrigen Bestimmungen der DS-GVO-E; dies gilt auch für Weiterübermittlungen. Wie bisher nach Art. 25 Abs. 4, 6 DSRL sind gem. Art. 41 Datenübermittlungen auf Grundlage eines Angemessenheitsbeschlusses zulässig, der sich jedoch nunmehr nicht nur auf das Drittland, sondern explizit auch auf ein(en) „Gebiet oder Verarbeitungssektor" dieses Landes oder eine internationale Organisation beziehen kann. Die Kriterien für die Entscheidung werden in Art. 41 Abs. 2 erheblich spezifiziert. Stellt die *Kommission* das Fehlen eines angemessenen Schutzes fest, untersagt Art. 41 Abs. 6 die Übermittlung.

Nur wenn die *Kommission* noch keinen Beschluss nach Art. 41 erlassen hat, kann die Datenübermittlung auf der Grundlage „geeigneter Garantien" (Art. 42) erfolgen. Diese können insbesondere in Form von verbindlichen unternehmensinternen Vorschriften (binding corporate rules) und in Standardschutz- oder Vertragsklauseln bestehen, die von der *Kommission* oder einer Aufsichtsbehörde genehmigt wurden. Das Instrument der verbindlichen unternehmensinternen Vorschriften wird im Entwurf deutlich aufgewertet und in Art. 43 näher geregelt. Es findet auch auf Unternehmensgruppen Anwendung und muss eine Reihe inhaltlicher Kriterien erfüllen, die unter anderem die Rechtsverbindlichkeit der internen Vorschriften, Datenschutzgrundsätze, Betroffenenrechte, Haftungsfragen, die Einrichtung eines Datenschutzbeauftragten, die Zusammenarbeit mit der Aufsichtsbehörde und Compliance-Vorschriften umfassen. In der jetzt vorliegenden Fassung hat Art. 43 einen potenziell sehr weiten Anwendungsbereich und würde z.B. auch Cloud-Anwendungen in Konzernverbünden erfassen. Die Bedeutung verbindlicher unternehmensinterner Vorschriften könnte in der Praxis folglich deutlich zunehmen und wird mutmaßlich wichtiger werden als die relativ vielen Einzelausnahmen nach Art. 44.

Insgesamt ist die Zulässigkeit der Übermittlung in Drittländer erheblich genauer normiert worden als nach der DSRL. Das Problem des staatlichen Zugriffs auf Daten, die an im Ausland ansässige Unternehmen übermittelt wurden, bleibt freilich ungelöst. Der schließlich gestrichene Art. 42 des Entwurfs hätte zwar möglicherweise Unternehmen in die missliche Lage versetzt, entweder gegen ausländische (insbesondere US-amerikanische) Offenbarungspflichten oder gegen europäische Datenschutzvorgaben zu verstoßen.[29] Er hätte aber zumindest den Willen zum Ausdruck gebracht, europäische Schutzstandards nicht den Sicherheitsinteressen anderer Staaten unterzuordnen. Zumindest eine Informationspflicht der Verantwortlichen im Fall der Offenbarungsanordnung im Drittland hätte deshalb normiert werden sollen.

2. Rechte der Betroffenen

Der Entwurf verändert und erweitert die Rechte der betroffenen Personen; überdies werden in Art. 12 Verfahrenspflichten vorgegeben. Informations- und Auskunftsrechte sollen deutlich präzisiert werden. Die datenschutzrechtliche Einwilligung muss nunmehr „explizit" erfolgen (Art. 4 Abs. 8) und zum Ausdruck bringen, dass die betroffene Person mit der Verarbeitung „einverstanden" ist (bisher: „akzeptiert"; EG 33 betont die „echte Wahlfreiheit"). Art. 7 Abs. 3 regelt die Widerruflichkeit. Ein allgemeines Schriftformerfordernis besteht nicht, allerdings trägt

25 Der *EuGH* hat unlängst ohne nähere Begründung IP-Adressen als personenbezogene Daten bezeichnet, dabei aber weder nach Fallgruppen differenziert noch sich mit der Diskussion in der Literatur auseinandergesetzt, s. *EuGH*, Rs. C-79/10, ZD 2012, 29 m. Anm. *Meyerdierks*, Abs. 51.

26 *EuGH*, Rs. C-101/01, MMR 2004, 95 m. Anm. *Roßnagel*, Abs. 47 – Lindqvist; Rs. C-73/07, MMR 2009, 175, Abs. 44 – Satamedia.

27 Nach dem ursprünglichen Text sollte dagegen entscheidend sein, ob sich die Datenverarbeitungsaktivitäten an betroffene Personen in der Union „richten".

28 Dazu z.B. *Piltz*, CR 2011, 657; *Voigt/Alich*, NJW 2011, 3541.

29 S.o. I.

der Verantwortliche gem. Art. 7 Abs. 1 die Beweislast für das Vorliegen der Einwilligung, sodass in der Praxis die nachprüfbare schriftliche oder elektronische Dokumentation erforderlich sein wird. Art. 7 Abs. 4 schließt die Einwilligung aus, wenn „zwischen der Position der betroffenen Person und des für die Verarbeitung Verantwortlichen ein erhebliches Ungleichgewicht besteht". Der Entwurf hatte dies noch dahingehend präzisiert, dass eine Einwilligung gegenüber öffentlichen Stellen und im Beschäftigungsverhältnis ausgeschlossen war; dies wurde nunmehr in EG 34 verschoben. Dort wird davon ausgegangen, dass eine Einwilligung in behördlichen Subordinations- sowie in Abhängigkeitsverhältnissen – insbesondere im Beschäftigungsverhältnis – nicht rechtfertigend wirkt. Diese in der deutschen Diskussion kontroverse Frage[30] wäre damit verbindlich entschieden.

Art. 17 regelt das Recht auf Löschung, das präzisiert und um ein „Recht auf Vergessenwerden" ergänzt wird. Der durch die starke Bezeichnung zum Ausdruck kommende Anspruch dieses Rechts ist allerdings meilenweit von seinem normativen Inhalt entfernt: Neben den schon bekannten Löschungsanspruch tritt nach Art. 17 Abs. 2 im Fall der Veröffentlichung der Daten die Pflicht des Verantwortlichen, „alle vertretbaren Schritte, auch technischer Art [zu unternehmen], um Dritte, die die Daten verarbeiten, darüber zu informieren, dass eine betroffene Person von ihnen die Löschung aller Querverweise auf diese personenbezogenen Daten oder von Kopien oder Replikationen dieser Daten verlangt." Diese Formulierung ist realitätsnäher als die des Entwurfs,[31] enthält der Sache nach aber eine bloße Informationspflicht und kein „Recht". Eine Anpassung von Art. 17 Abs. 9 lit. b wurde offenbar vergessen; danach soll die *Kommission* Bedingungen für die Löschung gem. Abs. 2 festlegen, die dort nicht (mehr) als Pflicht enthalten ist.

Ebenfalls neu ist das Recht auf Datenübertragbarkeit in Art. 18. Soweit personenbezogene Daten in „strukturierten gängigen elektronischen Formaten" verarbeitet werden, haben die betroffenen Personen das Recht, hiervon eine elektronische Kopie zu erhalten. Die Vorschrift dürfte in Teilen durch die Diskussion um soziale Netzwerke beeinflusst sein, geht aber weit darüber hinaus. Der Anspruch ist von großer Bedeutung, da mit der Zunahme großer Datensammlungen über Einzelne in Internetprofilen und anderen Datenbanken ein Anbieterwechsel unter manueller Übertragung der gespeicherten Daten zunehmend unrealistisch wird. Dies birgt die Gefahr, dass Anbieter diese Position zum Nachteil der Kunden ausnutzen. Art. 18 trägt dazu bei, derartige Lock-In-Effekte zu vermeiden.

Anders als die DSRL enthält der Entwurf schließlich detaillierte Regelungen zum Datenschutz bei Kindern.[32] Dies sind nach Art. 4 Abs. 18 alle Personen unter 18 Jahren, die wichtigste Rechtsfolge greift allerdings gerade nicht bis zu dieser Grenze: Gem. Art. 8 Abs. 1 ist die Einwilligung oder Zustimmung der Erziehungsberechtigten nur bis zum vollendeten 13. Lebensjahr erforderlich, und in (problematischer) Abschwächung der Beweislastregel des Art. 7 Abs. 1 lässt Art. 8 Abs. 1 Satz 2 es ausreichen, dass unter Berücksichtigung der „vorhandenen Technologie angemessene Anstrengungen" unternommen werden, um eine nachprüfbare Einwilligung zu erhalten. Der Entwurf trägt der besonderen Schutzbedürftigkeit von Kindern (d.h. auch zwischen dem 13. und 18. Lebensjahr) an mehreren anderen Stellen Rechnung, so bei der Abwägung mit berechtigten Interessen (Art. 6 Abs. 1 lit. f, EG 38), den Transparenzanforderungen (Art. 11 Abs. 2: „adressatengerechte Sprache"; s.a. EG 46), dem Recht auf Vergessenwerden (Art. 17 Abs. 1; EG 53 betont zu Recht die Gefahr, dass im Kindesalter die mit der Verarbeitung verbundenen Gefahren noch nicht in vollem Umfang erkannt werden) und der Pflicht zur Datenschutz-Folgenabschätzung (Art. 33 Abs. 2 lit. d).[33] Dagegen wurde das vollständige Verbot von auf Profiling basierenden Maßnahmen bei Kindern aus dem Entwurf entfernt; der Gedanke findet sich nunmehr noch in EG 58.

3. Moderne Datenschutzinstrumente

Der Entwurf betont in EG 13 den Gedanken des technologieneutralen Schutzes, enthält aber in Art. 23 Regelungen zum Datenschutz durch Technik und zu datenschutzfreundlichen Voreinstellungen. Darin liegt ein dringend erforderlicher Schritt hin zu einer Verbindung rechtlicher und technischer Schutzinstrumente.[34] Allerdings enttäuscht der Entwurf, weil er sehr an der Oberfläche bleibt: „data protection by design" (EG 61) ist eine bloße Ankündigung. Der Verantwortliche hat zwar technische und organisatorische Maßnahmen und Verfahren zur Einhaltung der DS-GVO-E und Wahrung der Betroffenenrechte durchzuführen (Art. 23 Abs. 1) und insbesondere das Erforderlichkeitsprinzip technisch strikt einzuhalten (Art. 23 Abs. 2). Es fehlt aber jede verbindliche Aussage zur Technikgestaltung, und Grundprinzipien des technischen Datenschutzes wie Anonymisierung und Pseudonymisierung werden im gesamten Entwurf nicht erwähnt. Der normative Gehalt bleibt damit noch hinter dem von § 3a BDSG[35] zurück. Ob man insoweit auf die gem. Art. 23 Abs. 3 und 4 sowie Art. 30 Abs. 3 zulässigen Rechtsakte und Standards der *Kommission* vertrauen darf, ist völlig unklar.

Noch vager sind die Aussagen zu Zertifizierungen, Datenschutzsiegeln und -zeichen in Art. 39, die durch Mitgliedstaaten und *Kommission* „gefördert" werden sollen. Auch dieses Instrument – das in Schleswig-Holstein mit Erfolg eingesetzt wird[36] – hätte eine verbindliche Regelung verdient gehabt.[37] Es fehlt jede Aussage zu zertifizierenden Stellen, Zertifizierungsverfahren, anzulegenden Kriterien und Rechtsfolgen der Zertifizierung, sodass völlig unklar ist, nach welchen Maßgaben die *Kommission* ihre Ermächtigung zum Erlass delegierter Rechtsakte und technischer Standards (Art. 39 Abs. 2 und 3) ausfüllen soll.

Begrüßenswert sind demgegenüber die Regelungen zur Meldung von Schutzverletzungen („data breach notification"), die gegenüber der Aufsichtsbehörde (Art. 31) und der betroffenen Person (Art. 32) zu erfüllen sind. Hierin liegt nicht nur ein sinnvolles Instrument zur Herstellung von Transparenz für die Betroffenen, sondern auch ein Anreizmechanismus, um die Verantwortlichen zur Einhaltung rechtlicher und technischer Standards anzuhalten.[38] Überdies führt der Entwurf zu einer Harmonisierung, da an die entsprechende Regelung in Art. 2 lit. h, Art. 4 Abs. 3-5 der ergänzten RL 2002/58/EG angeknüpft wird.[39] Zweckmäßigerweise hätten allerdings deren Formulierungen

30 Gegen die Zulässigkeit eines Ausschlusses der Einwilligung im Beschäftigtendatenschutz z.B. *Forst*, RDV 2010, 150; *Thüsing*, RDV 2010, 147, 148 f.; *Rasmussen-Bonn/Raif*, GWR 2011, 80; ähnlich *Kort*, MMR 2011, 294, 299; a.A. zu Recht *Tinnefeld/Petri/Brink*, MMR 2010, 727, 729.

31 Dieser hatte eine – praktisch kaum realisierbare – Pflicht des Verantwortlichen enthalten, für eine Löschung aller Links und Internetkopien zu sorgen.

32 Zur bisherigen Rechtslage s. *Jandt/Roßnagel*, MMR 2011, 637.

33 S. ferner Art. 38 Abs. 1 lit. e (Verhaltensregeln), Art. 52 Abs. 2 Satz 2 (Aufgaben der Aufsichtsbehörde).

34 Näher *Hornung*, ZD 2011, 51; zum Konzept des technischen Datenschutzes *Borking*, DuD 1998, 636; *ders.*, DuD 2001, 607, sowie die Beiträge in *Roßnagel*, Allianz von Medienrecht und Informationstechnik, 2001.

35 Zu dessen umstrittener Rechtsnatur s. Simitis-*Scholz*, BDSG, § 3a Rdnr. 27 f. m.w.Nw.

36 S. *Bäumler*, DuD 2002, 325; *ders.*, DuD 2004, 80; *Schläger*, DuD 2004, 459.

37 Dazu *Roßnagel*, DuD 1997, 505; *ders.*, Datenschutzaudit. Konzeption, Durchführung, gesetzliche Regelung, 2000; *ders.*, in: Hempel/Krasmann/Bröckling, Sichtbarkeitsregime, Leviathan Sonderheft 25/2010, 263; *Bäumler*, CR 2001, 795; *ders.*, DuD 2002, 325; *ders.*, DuD 2004, 80.

38 S. zum Konzept *Gabel*, BB 2009, 2045; *Eckhardt/Schmitz*, DuD 2010, 390; *Ernst*, DuD 2010, 472; *Hanloser*, MMR 2010, 300; *Hornung*, NJW 2010, 1841.

39 Der deutsche Gesetzgeber hat bereits eine allgemeine Regelung in § 42a BDSG eingeführt.

übernommen werden sollen; die unterschiedliche Regelungssystematik ist wenig einsichtig, wenn damit keine inhaltlichen Abweichungen impliziert werden sollen. Dies scheint offenbar nur insoweit beabsichtigt zu sein, als die Benachrichtigung der Aufsichtsbehörde „nach Möglichkeit" binnen 24 Stunden zu erfolgen hat.

Auch die Einführung der Datenschutz-Folgenabschätzung (data protection impact assessment, DPIA) ist ein sinnvolles neues Instrument.[40] Sie tritt anstelle der bisherigen Meldepflicht und ist nach Art. 33 Abs. 1 bei Verarbeitungsvorgängen erforderlich, die „konkrete Risiken für die Rechte und Freiheiten betroffener Personen bergen". Diese kaum operationalisierbare Formulierung wird in Art. 33 Abs. 2 durch Regelbeispiele präzisiert. Diese umfassen u.a. auf Profiling basierende Maßnahmen (lit. a, dessen umständliche Formulierung an Art. 20 anschließt), bestimmte Kategorien von Daten (lit. b, der indes nicht alle Kategorien aus Art. 9 Abs. 1 übernimmt), die „weiträumige" Überwachung öffentlich zugänglicher Bereiche, v.a. mittels Videoüberwachung (lit. c), die Verarbeitung personenbezogener Daten „aus umfangreichen Dateien" über Kinder, genetische und biometrische Daten sowie den Fall der „Zurateziehung" der Aufsichtsbehörde nach Art. 34 Abs. 2 lit. b. Im Folgenden werden der Inhalt und das Verfahren präzisiert (Art. 33 Abs. 3, 4) und eine Pflicht zur Information der Aufsichtsbehörde festgeschrieben, sofern die Folgenabschätzung „hohe konkrete Risiken" ergibt (Art. 34 Abs. 2 lit. a). EG 70 ff. enthalten überdies weiterführende Überlegungen. So soll die Folgenabschätzung in bestimmten Fällen nicht nur auf ein Projekt bezogen, sondern thematisch breiter angelegt sein.

Schließlich ist das neuartige Verbandsklagerecht positiv zu würdigen. Entsprechende Interessensorganisationen haben das Recht, im Namen der betroffenen Personen (Art. 73 Abs. 2) und im eigenen Namen (Art. 73 Abs. 3) Beschwerde bei einer Aufsichtsbehörde zu erheben. Im Namen der betroffenen Personen können derartige Organisationen nach Art. 76 Abs. 1 auch gerichtliche Verfahren anstrengen.

4. Institutionelle Aspekte

Institutionelle und organisatorische Regelungen machen einen erheblichen Teil des Entwurfs aus. Während bislang nationale Regeln über interne (behördliche und betriebliche) Datenschutzbeauftragte nach Art. 18 Abs. 2 DSRL fakultativ waren, ist dies nunmehr nach Art. 35 Abs. 1 für alle Behörden (lit. a), Unternehmen mit mindestens 250 Beschäftigten (lit. b) und solche mit bestimmten Kerntätigkeiten (lit. c) verpflichtend. Gem. Art. 35 Abs. 2 kann im Fall von Abs. 1 lit. b (nicht jedoch lit. c) eine Gruppe von Unternehmen einen gemeinsamen Datenschutzbeauftragten benennen. Dieser muss in allen Fällen besonders qualifiziert sein und genießt arbeitsrechtlichen Schutz (Art. 35 Abs. 5 ff.); er kann nach Art. 35 Abs. 8 beim Verantwortlichen beschäftigt oder extern beauftragt sein. Art. 36, 37 regeln Stellung (insbesondere Unabhängigkeit) und Aufgaben des Datenschutzbeauftragten, die vielfach an das BDSG erinnern.

Die detaillierten Regelungen sind im Grundsatz begrüßenswert. Die Grenze von 250 Beschäftigten (die der EU-Definition kleinerer und mittlerer Unternehmen entspricht) ist jedoch nicht überzeugend. Nach Angaben von *eurostat* fallen im Bereich des nichtfinanziellen Sektors der gewerblichen Wirtschaft 99,8% der Unternehmen unter diese Grenze,[41] sodass die Alternative in der Praxis vernachlässigbar ist. Überdies ist die abstrakte Zahl wenig sinnvoll: Sie führt dazu, dass lit. b ein produzierendes Unternehmen mit 250 Mitarbeitern und einer sehr kleinen Abteilung für Kunden- und Mitarbeiterdaten erfasst, nicht aber einen Adresshändler, dessen 200 Mitarbeiter sich ausschließlich mit dem An- und Verkauf personenbezogener Daten beschäftigen. Die Regelung in § 4f BDSG ist hier sowohl hinsichtlich der Mitarbeiterzahl als auch hinsichtlich des Kriterium der Beschäftigung der Personen mit der automatisierten Datenverarbeitung sinnvoller.

Im Rahmen von Art. 35 Abs. 1 wird es damit entscheidend auf lit. c ankommen, der nach dem Willen der *Kommission* sicher Fälle wie den des Adresshändlers erfassen würde. Unglücklicherweise fallen die diesbezüglichen Formulierungen im Entwurfstext auseinander. Während die Einleitung (S. 12) und EG 75 auf Verarbeitungsvorgänge abstellen, „die einer regelmäßigen, systematischen Überwachung bedürfen", formuliert Art. 35 Abs. 1 lit. c, es ginge um solche Vorgänge, „welche aufgrund ihres Wesens, ihres Umfangs und/oder ihrer Zwecke eine regelmäßige und systematische Beobachtung von betroffenen Personen erforderlich machen". Im einen Fall werden also Verarbeitungsvorgänge, im anderen Fall Personen regelmäßig und systematisch beobachtet (der Widerspruch findet sich auch in der englischen Fassung, ist also kein Übersetzungsfehler). Beide Varianten sind denkbare Anknüpfungspunkte, wobei EG 75 die weitere Formulierung ist. Da auch jenseits einer systematischen Beobachtung von Personen besondere Interessen betroffen sein können (etwa bei der Verarbeitung einzelner, sehr sensibler Daten), sollte Art. 35 Abs. 1 lit. c in diesem Sinne geändert werden. Unabhängig davon kann für die Praxis allerdings schon wegen der erweiterten Haftungsregeln und Bußgeldtatbestände nur angeraten werden, ein internes Compliance-Management unter Einbeziehung eines Datenschutzbeauftragten einzurichten.

Neben der internen Selbstkontrolle werden die Aufsichtsbehörden (Art. 4 Abs. 19) geregelt, deren Einrichtung in Art. 46 verbindlich vorgeschrieben wird.[42] Die bisher in Art. 28 Abs. 1 Satz 2 DSRL knapp vorgegebene „völlige Unabhängigkeit" wird in Anlehnung an die Rechtsprechung des *EuGH*[43] in Art. 47 ausführlich geregelt und um die Pflicht zur angemessenen personellen, technischen und finanziellen Ausstattung erweitert. Art. 48 macht Vorgaben zur Bestimmung der Mitglieder, die entweder durch nationale Parlamente gewählt oder durch Regierungen ernannt werden können.

Aufgaben und Befugnisse der Aufsichtsbehörden wurden gegenüber der DSRL erweitert. Die detaillierte Regelung zu den Aufgaben in Art. 52 umfasst verschiedene Überwachungs-, Beschwerde-, Informations-, Untersuchungs-, Beratungs-, Genehmigungs- und Mitwirkungsaufgaben. Die in Art. 53 normierten Befugnisse sind präziser als in der DSRL gefasst und umfassen eine Vielzahl von Einflussnahmen auf die Datenverarbeitung sowie im nationalen Recht zu regelnde Zugangsrechte zu Geschäftsräumen. Die Verantwortlichen sind nach Art. 29 zur Zusammenarbeit verpflichtet. Art. 79 regelt in abgestufter Form die Möglichkeit, verwaltungsrechtliche Vergehen (Ordnungswidrigkeiten) zu ahnden. Die Bußgelder können bis zu € 1 Mio. oder 2% des weltweiten Jahresumsatzes erreichen, müssen aber „in jedem Einzelfall wirksam, verhältnismäßig und abschreckend sein". Die einzelnen Tatbestände erfassen eine Vielzahl von Verstößen gegen die DS-GVO-E.

Art. 74 regelt den Rechtsschutz gegen Aufsichtsbehörden sowohl in der Anfechtungs- als auch in der Verpflichtungssitua-

40 Zur Technikfolgenabschätzung s. etwa *Ropohl*, Ethik und Technikbewertung, 1996; *Grunwald*, Technikfolgenabschätzung, 2. Aufl. 2010; aus allgemeinerer rechtlicher Perspektive *Roßnagel*, Rechtswissenschaftliche Technikfolgenforschung, 1993.

41 S. für 2005 unter: http://epp.eurostat.ec.europa.eu/cache/ITY_OFFPUB/KS-SF-08-031/DE/KS-SF-08-031-DE.PDF.

42 Das deutsche Modell der Einrichtung mehrerer Behörden ist explizit zugelassen, es ist aber nach Art. 46 Abs. 2 eine „zentrale Kontaktstelle" einzurichten.

43 *EuGH*, Rs. C-518/07, MMR 2010, 352 m. Anm. *Petri/Tinnefeld*.

tion, erfasst also auch einen gerichtlich durchsetzbaren Anspruch auf Einschreiten der Behörde. Anders als im Entwurf ist bei ausländischen Aufsichtsbehörden keine Klage vor einem Gericht des Heimatlands zulässig; stattdessen kann fakultativ anstelle einer eigenen Klage im Ausland die eigene Aufsichtsbehörde „ersucht" werden, im Namen der betroffenen Person dort Klage zu erheben.

Bedeutsam ist die Regelung zur Zuständigkeit: Diese erstreckt sich nach Art. 51 auf das jeweilige Hoheitsgebiet, allerdings mit Ausnahme von Unternehmen mit mehreren Niederlassungen in der Union: Hier ist nach Art. 51 Abs. 2 die Aufsichtsbehörde am Ort der Hauptniederlassung (Art. 4 Abs. 13) für das gesamte Unternehmen ausschließlich zuständig. Dies wird mutmaßlich zu Konflikten mit Aufsichtsbehörden und Gerichten anderer Mitgliedstaaten führen. Gem. Art. 75 Abs. 2 Satz 2 sind Klagen gegen Verantwortliche mit Sitz im Ausland auch vor Gerichten des Heimatlands möglich. Dadurch kann es zu dem Fall kommen, dass die zuständige Aufsichtsbehörde eine Verarbeitungsmaßnahme akzeptiert, ein ausländisches Gericht sie jedoch verwirft.

Im Verhältnis zwischen den Aufsichtsbehörden greift in den Fällen des Art. 51 Abs. 2 regelmäßig Art. 56 und ordnet gemeinsame Maßnahmen an, bei denen Behörden aller Staaten mitwirkungsberechtigt sind, in denen voraussichtlich Personen betroffen sind. Die Bediensteten der eingeladenen Behörden können vor Ort an Kontrollen mitwirken, wobei die einladende Aufsichtsbehörde für ihr Handeln haftet. Die Bündelung der Zuständigkeit bei einer zentralen Aufsichtsbehörde wäre aus Sicht der datenverarbeitenden Unternehmen sicher eine enorme Erleichterung. Sie kann inhaltlich aber nur gerechtfertigt werden, wenn in den Mitgliedstaaten nicht nur hohe einheitliche Rechtsstandards gelten, sondern diese auch in einheitlicher Art und Weise durch die jeweiligen Aufsichtsbehörden angewendet werden. Zumindest bislang ist die Praxis der Behörden davon weit entfernt, weil diese ihre Rollen i.R.d. bisherigen Vorgaben der DSRL sehr unterschiedlich interpretieren. Sollte dies weiterhin der Fall sein, besteht das Risiko einer Abwärtsspirale, bei der sich Unternehmen durch die Wahl ihrer Hauptniederlassung eine Aufsichtsbehörde „aussuchen", die die DS-GVO-E in ihrem Sinne interpretiert.

In bestimmten Fällen sieht der Entwurf neben der allgemeinen Pflicht der Aufsichtsbehörden zur Zusammenarbeit untereinander und mit der *Kommission* (Art. 46 Abs. 1 Satz 3) ein sog. „Kohärenzverfahren" (Art. 57 ff.) vor. Dieses ist (mit Ausnahme geringer Anklänge in Art. 26 Abs. 3 DSRL) völlig neuartig und findet in einer Vielzahl von Fällen Anwendung: Art. 58 Abs. 2 nennt Datenverarbeitungen für betroffene Personen in mehreren Mitgliedstaaten oder die Beobachtung ihres Verhaltens, eine Beeinträchtigung des freien Datenverkehrs, die Festlegung von Standard-Datenschutzklauseln, die Genehmigung von Vertragsklauseln und die Annahme verbindlicher unternehmensinterner Vorschriften.

Insbesondere wegen der ersten beiden Varianten wird das Verfahren mutmaßlich in einer Vielzahl von Fällen Anwendung finden. Es beginnt auf Antrag einer Aufsichtsbehörde, des *Europäischen Datenschutzausschusses* oder der *Kommission*. Die letzteren beiden können nach Art. 58 Abs. 7, 59 Stellungnahmen abgeben. Die zuständige Aufsichtsbehörde muss der Stellungnahme des *Ausschusses* „Rechnung", der Stellungnahme der *Kommission* nach Art. 59 Abs. 2 „so weit wie möglich" (also stärker) Rechnung tragen und über eine etwaige Änderung der Maßnahme berichten. Im Anschluss endet die Beteiligung des *Datenschutzausschusses*. Entspricht das Ergebnis nicht dem Willen der *Kommission*, kann diese demgegenüber die Behörde nach Art. 60 auffordern, die Maßnahme für maximal zwölf Wochen auszusetzen, um eine eigene Maßnahme nach Art. 62 Abs. 1 lit. a zu erlassen. Diese Vorschrift gestattet Durchführungsakte zur „ordnungsgemäßen Anwendung" der DS-GVO-E, über die i.R.d. Kohärenzmechanismus folglich abschließend die *Kommission* entscheidet.

Dies leitet über zu der gravierendsten institutionellen Verschiebung des Entwurfs, nämlich der Rolle der *Kommission*, die bislang nur in ausgewählten Bereichen Entscheidungskompetenzen hat,[44] nunmehr aber in allen wichtigen Regelungsfeldern tätig werden soll. In einer Vielzahl von Artikeln des Entwurfs finden sich Kompetenzen zum Erlass von delegierten Rechtsakten (Art. 86, s. Art. 290 AEUV) und/oder Durchführungsrechtsakten (Art. 87 Abs. 2 und 3, s. Art. 291 AEUV). Angesichts des schnellen Fortschritts der technischen Entwicklung liegt in diesen Instrumenten zwar durchaus ein sinnvoller Ansatz, um mit flexiblen und schnelleren Regelungsinstrumenten reagieren zu können.[45] Auch wird es vielfach sinnvoll sein, europaweit einheitliche Vorgaben und Leitlinien für die Praxis zu machen. Der Entwurf enthält aber so viele Ermächtigungen (die langen Kataloge in Art. 86 sprechen hier Bände), die überdies auch wichtige Fragen betreffen, dass im Gesamtbild Art. 290 Abs. 1 UA 1 AEUV kaum als gewahrt angesehen werden kann, wonach sich delegierte Rechtsakte auf „nicht wesentliche" Vorschriften des betreffenden Gesetzgebungsakts beziehen müssen.[46] Das gilt insbesondere für Bereiche, in denen die DS-GVO-E sich auf die Nennung von Grundsätzen beschränkt und alle wichtigen Rechtsfragen der *Kommission* überlässt, wie das beim Datenschutz durch Technik (Art. 23) und den Zertifizierungen (Art. 39) der Fall ist[47] – diese und andere Normen werden vor Erlass delegierter Rechtsakte in der Praxis nicht einmal anwendbar sein. Schlicht nicht akzeptabel ist es schließlich, einen ganzen Regelungsbereich wie den Beschäftigtendatenschutz einerseits komplett auszuklammern und der Kompetenz der Mitgliedstaaten zu überlassen (Art. 82 Abs. 1),[48] andererseits dennoch der *Kommission* diesen Bereich zur Regulierung zu überantworten (Art. 82 Abs. 3).

Die Endscheidungsbefugnis der *Kommission* im Kohärenzmechanismus steht schließlich in scharfem Widerspruch zur Stellung der nationalen Aufsichtsbehörden. Der Entwurf zwingt die Mitgliedstaaten, diesen vollständige Unabhängigkeit einzuräumen. Auf europäischer Ebene hingegen soll mit der *Kommission* eine Institution das letzte Wort haben, die in Besetzung, Organisation und Arbeitsweise in keiner Weise dem Leitbild einer unabhängigen Datenschutzkontrolle entspricht.

Im Gesamtbild würde die *Kommission* so eine in ihrer Weite unangemessene, primärrechtlich problematische und im Verhältnis zu den Aufsichtsbehörden systemwidrige Befugnisfülle erlangen. Der Entwurf sollte deshalb an mehreren Stellen inhaltlich präzisere Vorgaben für die delegierten Rechtsakte enthalten und – soweit europaweite Einzelentscheidungen erforderlich sind – eine unabhängige, effektiv ausgestattete europäische Institution (etwa einen mit mehr Kompetenzen ausgestatteten

44 S. Art. 25 Abs. 4 und 6, Art. 31 Abs. 2 DSRL zur Befugnis zum Erlass von Angemessenheitsentscheidungen und Art. 26 Abs. 4 zur Anerkennung von Standardvertragsklauseln.

45 S. *Europäischer Datenschutzbeauftragter*, Opinion on the Communication from the Commission, http://www.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consultation/Opinions/2011/11-01-14_Personal_Data_Protection_EN.pdf, S. 24; *Roßnagel*, FAZ v. 1.6.2011, 7; *Hornung*, ZD 2011, 51, 56.

46 Die Regelung ist allerdings nicht mit der Wesentlichkeitslehre des deutschen Verfassungsrechts gleichzusetzen; vielmehr kommt es auf die wesentlichen politischen Grundentscheidungen der Materie an, s. *EuGH*, Rs. C-240/90, Slg. 1992, I-5383, Rdnr. 37 (Deutschland/Kommission); dies impliziert einen erheblichen Spielraum, s.a. *Gärditz*, DÖV 2010, 453, 456; *Möllers/v. Achenbach*, EuR 2011, 39, 48 f.

47 S.o. IV.3.

48 Ein Anlauf der *Kommission* für eine europäische Regelung zu diesem Bereich war in den Jahren nach 2001 nicht weiter verfolgt worden.

Europäischen Datenschutzausschuss) vorsehen, der ebenso wie die Aufsichtsbehörden gerichtlicher Kontrolle unterliegen sollte. Die *Kommission* könnte sich dann auf die Erarbeitung allgemein geltender Leitlinien beschränken.

V. Vorläufiges Fazit

Die *Kommission* hat sich der Herkulesaufgabe einer grundsätzlichen Reform des europäischen Datenschutzrechts gestellt; allein dies verlangt Anerkennung in einer Materie, vor deren grundsätzlicher Reform z.B. der deutsche Gesetzgeber seit vielen Jahren zurückschreckt. Der enorme Anstieg des Umfangs verdeutlicht – da keine Regelungsmaterie des Entwurfs überflüssig erscheint – die gestiegene Komplexität des Datenschutzes in der Informationsgesellschaft.

Inhaltlich bietet der Entwurf Licht und Schatten. Wesentliche Neuerungen zu Betroffenenrechten, technischen und organisatorischen Pflichten, Befugnissen der Aufsichtsbehörden, Auftragsdatenverarbeitung und Sanktionen erscheinen gelungen. An anderen Stellen (insbesondere den modernen Schutzinstrumenten) liegen begrüßenswerte Grundregelungen vor, die im weiteren Gesetzgebungsverfahren ausgebaut werden sollten. Dagegen ist die überaus starke Stellung der *Kommission* nicht gerechtfertigt. Mutmaßlich werden deshalb an dieser Stelle sowie bei der Grundentscheidung über den Wechsel zur Verordnung die wesentlichen Weichen der künftigen Entwicklung des europäischen Datenschutzrechts gestellt.

Prof. Dr. Gerrit Hornung, LL.M.
ist Inhaber des Lehrstuhls für Öffentliches Recht, IT-Recht und Rechtsinformatik an der Universität Passau, der auch in das Institute of IT-Security and Security Law (ISL) der Universität eingebunden ist.