Deutscher Bundestag
Innenausschuss

Ausschussdrucksache
17(4)584 E

Betreff: Stellungnahme für die Anhörungen am 22.10.
Von: "Gerrit Hornung" <gerrit.hornung@uni-passau.de>
Datum: 18.10.2012 14:56
An: <innenausschuss@bundestag.de>

Sehr geehrter Herr Heynkes,
sehr geehrte Damen und Herren,

anbei erhalten Sie meine schriftliche Stellungnahme für die beiden Anhörungen am kommenden Montag. Ich bitte die um einen Tag verspätete Übermittlung zu entschuldigen.

Da ich sowohl am Vormittag als auch am Nachmittag eingeladen bin und die beiden Bereiche eng miteinander verzahnt sind, habe ich eine einheitliche Stellungnahme angefertigt, die allerdings zwei Kapitel zu den beiden Teilen enthält. Das angefügte Dokument bezieht sich also auf beide Anhörungen.

Mit freundlichen Grüßen
Gerrit Hornung

Lehrstuhl für Öffentliches Recht, IT-Recht und Rechtsinformatik
Universität Passau
Innstr. 39
94032 Passau
0851 509 2380
gerrit.hornung@uni-passau.de
http://www.jura.uni-passau.de/hornung.html

Anhänge:

Hornung, Stellungnahme Datenschutzreform 121022.pdf 27 Bytes

Prof. Dr. Gerrit Hornung, LL.M.

Lehrstuhl für Öffentliches Recht, Informationstechnologierecht und Rechtsinformatik

UNIVERSITÄT PASSAU
Juristische Fakultät

Telefon Prof. Dr. Gerrit Hornung, LL.M.
0851 509-2380
Telefax 0851 509-2382
e-mail gerrit.hornung@uni-passau.de

Datum 17. Oktober 2011

Stellungnahme

zu den öffentlichen Anhörungen des Innenausschusses des Deutschen Bundestages am 22. Oktober 2012 zu den Vorschlägen der Europäischen Kommission für eine Reform des Datenschutzrechts,

insbesondere dem Vorschlag für eine Verordnung zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr (Datenschutz-Grundverordnung), KOM(2012)11 endg.

und dem Vorschlag für eine 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, KOM(2012)10 endg.

Gliederung

1 Vorbemerkungen

Die Vorschläge der Europäischen Kommission zu einer Reform des europäischen Datenschutzrechts gehören zu den derzeit am intensivsten diskutierten Gesetzgebungsvorschlägen sowohl auf der europäischen als auch auf der mitgliedstaatlichen Ebene, wie sich nicht zuletzt an dem Interesse an der interparlamentarischen Anhörung im Europäischen Parlament am 9./10. Oktober 2012 gezeigt hat.

Mit den beiden Vorschlägen für eine Datenschutz-Grundverordnung (im Folgenden: DS-GVO-E) und eine Richtlinie für den Bereich des Sicherheitsrechts (im Folgenden: RL-E) hat sich die Kommission an die Spitze der bis dahin – auch und gerade in Deutschland – intensiv geführten Diskussion um die Reform des Datenschutzrechts gestellt. Diese Diskussion ist in der Vergangenheit mit großer Intensität geführt worden, und dies hat seit der Vorlage der Vorschläge am 25. Januar 2012 nochmals erheblich zugenommen.

Angesichts der Vielzahl der Beiträge,[1] der Fülle der kontroversen Fragen und des erheblichen Umfangs der vorgeschlagenen Regelungswerke ist es im Rahmen dieser Stellungnahme nicht möglich, zu allen Einzelfragen der Entwürfe Stellung zu nehmen und diese im Detail zu diskutieren. Die folgenden Ausführungen beschränken sich deshalb auf wesentliche Grundprobleme der beiden Vorschläge sowie einige Regelungsbereiche, die trotz ihrer Spezialität meines Erachtens von hervorgehobener Bedeutung für die weitere Entwicklung des Datenschutzrechts sind.

Angesichts von Umfang und Komplexität der Vorschläge ist es überdies kaum möglich, eine zusammenfassende Bewertung abzugeben. In der Summe lässt sich sagen, dass die Kommission eine Vielzahl begrüßenswerter Einzelvorschläge unternommen hat und inso-

---

[1] Ohne Anspruch auf Vollständigkeit und unter Beschränkung auf die wissenschaftliche Diskussion: *Bäcker/Hornung*, ZD 2012, 147; *Boehm*, DuD 2012, 339; *Breinlinger/Scheuing*, RDV 2012, 64; *Costa/Poullet*, CLSR 2012, 254; *De Hert/Papakonstantinou*, CLSR 2012, 130; *Dix*, DuD 2012, 318; *Eckhardt*, CR 2012, 195; *Forst*, NZA 2012, 364; *Franzen*, DuD 2012, 322; *Giesen*, CR 2012, 550; *Gola*, RDV 2012, 60; *Gola*, EuZW 2012, 332; *Gürtler*, RDV 2012, 126; *Härting*, AnwBl 2012, 716; *Härting*, BB 2012, 459; *Hornung*, ZD 2011, 51; *Hornung*, ZD 2012, 99; *Hornung/Sädtler*, CR 2012, i.E.; *Jaspers*, DuD 2012, 571; *Jaspers/Reif*, RDV 2012, 78; *Kalabis/Selzer*, DuD 2012, 670; *Kipker/Voskamp*, DuD 2012, 737; *Koreng/Feldmann*, ZD 2012, 311; *Kort*, DB 2012, 1020; *Kramer*, DSB 2012, 57; *Kugelmann*, DuD 2012, 581; *Lang*, K&R 2012, 145; *Masing*, NJW 2012, 2305; *Münch*, RDV 2012, 72; *Nebel/Richter*, ZD 2012, 407; *Richter*, DuD 2012, 576; *Ritzer*, FS Scheuing, 2011, 387; *Rogall-Grothe*, ZRP 2012, 193; *Ronellenfitsch*, DuD 2012, 561; *Roßnagel*, DuD 2012, 553; *Schild/Tinnefeld*, DuD 2012, 312; *J.-P. Schneider*, Die Verwaltung 44 (2011), 499, 516 ff.; *J. Schneider*, ITRB 2012, 180; *J. Schneider/Härting*, ZD 2012, 199; *J. Schneider /Härting*, in: Redeker/Hoppen, DGRI Jahrbuch 2011, 15; *Schulz*, CR 2012, 204; *Schwartmann*, RDV 2012, 57; *Taupitz*, MedR 2012, 423; *Traung*, Cri 2012, 33; *von Lewinski*, DuD 2012, 564; *Wagner*, DuD 2012, 676; *Wuermeling*, NZA 2012, 368; *Wybitul/Fladung*, BB 2012, 509; *Wybitul/Rauer*, ZD 2012, 160. Zur eigenen Darstellung der zuständigen EU-Kommissarin s. *Reding*, ZD 2012, 195.

weit Unterstützung verdient hat, aber sowohl in wesentlichen Grundfragen als auch in speziellen Bereichen – zum Teil deutlicher – Verbesserungsbedarf besteht.[2]

2 Zur Datenschutz-Grundverordnung

2.1 Thesen

Zur DS-GVO-E lassen sich die wesentlichen Ergebnisse der folgenden Ausführungen wie folgt zusammenfassen:

1. Die mitgliedstaatlichen Spielräume sind – insbesondere hinsichtlich des öffentlichen Bereichs – auf Basis des Entwurfs nicht hinreichend klar und bedürfen einer Präzisierung.

2. Der Entwurf hält zu Recht am Grundsatz fest, dass jede Verwendung personenbezogener Daten einer gesetzlichen Grundlage oder Einwilligung bedarf. Die Diskussion um das so genannte „Verbotsprinzip“ erweist sich als nicht weiterführend für die aktuellen Probleme des Datenschutzrechts und seine Reform, weil es vor allem eine regelungstechnische Frage, kein materieller Grundsatz ist.

3. Die neuen Rechte auf „Vergessenwerden“ und „Datenübertragbarkeit“ bringen in ihrer derzeitigen Form normativ wenig Neues und bleiben deutlich hinter ihren kraftvollen Bezeichnungen zurück. Die vorgeschlagenen Begriffe (insbesondere das „Vergessenwerden“) sind deshalb weder für die öffentliche Wahrnehmung noch für die politische Debatte hilfreich.

4. Der Entwurf enthält einige sinnvolle neue Instrumente wie die Datenschutz-Folgenabschätzung. Die Regelungen zum Datenschutz durch Technik und zu Zertifizierungen, Datenschutzsiegeln und -zeichen sind jedoch viel zu vage und sollten in jedem Fall durch verbindliche Vorgaben (auch für Hersteller) ergänzt werden. Es ist kaum verständlich, dass der Entwurf wesentliche Grundbegriffe Anonymisierung und Pseudonymisierung noch nicht einmal erwähnt, geschweige denn regelt.

5. Die Europäische Kommission würde auf der Basis des Entwurfs erhebliche Kompetenzzuwächse im Bereich des so genannten Kohärenzmechanismus und hinsichtlich der delegierten Rechtssetzung erlangen. In der Summe stellt dies eine in ihrer Weite unangemessene, primärrechtlich problematische und im Verhältnis zu den Aufsichtsbehörden systemwidrige Befugnisfülle dar, die geändert werden sollte.

---

[2] Wesentliche Teile der folgenden Überlegungen gehen auf die Veröffentlichungen in *Hornung*, ZD 2011, 51; *Hornung*, ZD 2012, 99 sowie *Bäcker/Hornung*, ZD 2012, 147 zurück (alle abrufbar unter http://www.jura.uni-passau.de/2108.html).

2.2 Klarstellungsbedarf: Das Verhältnis zwischen Union und Mitgliedstaaten

Rechtlich bewirkt der Wechsel des Instruments von der Richtlinie zur Verordnung, 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 Europäische Gerichtshof nach den Regeln des Vorabentscheidungsverfahrens (Art. 267 Abs. 1 lit. b AEUV) zuständig wäre. Dies hat erhebliche Auswirkungen auf den Grundrechtsschutz.[3] Da die DS-GVO-E mit Ausnahme von Gefahrenabwehr und Strafverfolgung auch die staatliche Verwaltung erfasst, wäre darüber hinaus aber auch ein erheblicher Bereich der hoheitlichen Datenverarbeitung nicht mehr durch das Bundesverfassungsgericht kontrollierbar. Um es hart auszudrücken: Das betrifft – je nach Auslegung von Art. 6 DS-GVO-E und der durch diese Norm den Mitgliedstaaten gewährten Spielräume – auch den Fall der Volkszählung und hätte einer entsprechenden Verfassungsfortbildung des Bundesverfassungsgerichts in einer Entscheidung zu diesem Bereich entgegengestanden.[4]

2.2.1 Privatwirtschaft

Der Wechsel zur Verordnung erscheint im Bereich der datenverarbeitenden Wirtschaft als grundsätzlich sinnvoll, weil hier die Interessen an einer europaweit einheitlichen Rechtslage evident sind. Es ist beispielsweise kaum einzusehen, dass – wie es gegenwärtig der Fall ist – die Formerfordernisse für die datenschutzrechtliche Einwilligung in Europa uneinheitlich geregelt sind.

Die Verlagerung auf die europäische Ebene führt aber dazu, dass dem deutschen Gesetzgeber spezifische Ausformungs- und Konkretisierungsmöglichkeiten genommen werden. Eine Regelung spezieller 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 gemäß Art. 35 Abs. 1 lit. b DS-GVO-E erst ab 250 Mitarbeitern gelten,[5] das grundsätzliche Schriftformerfordernis für die Einwilligung (§ 4a Abs. 1 Satz 2 BDSG) ließe sich wegen des Widerspruchs mit Art.

---

[3] Zum Problem z.B. *Matz-Lück*, in: ders./Hong, Grundrechte und Grundfreiheiten im Mehrebenensystem – Konkurrenzen und Interferenzen, 2012, 161; zu den Auswirkungen des Entwurfs auf den Rechtsschutz im Bereich des Datenschutzrechts *Schwartmann*, RDV 2012, 57 ff.; *von Lewinski*, DuD 2012, 564, 567 ff.

[4] Weitere denkbare Beispiele sind der Bereich der Finanzverwaltung (zum Abruf von Kontostammdaten s. BVerfG 118, 168) oder der Auskunftsanspruch gegen Behörden (z.B. BVerfGE 120, 351). Ich danke *Matthias Bäcker* für die Anregungen zu diesem Punkt.

[5] Dazu *Jaspers/Reif*, RDV 2012, 78 ff.; zur Auswirkung auf die Datenschutzorganisation im Unternehmen allgemein *Jaspers*, DuD 2012, 571.

4 Abs. 8, Art. 6 Abs. 1 lit. a, Art. 7 DS-GVO-E 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 DS-GVO-E) und ein Überprüfungs- und Auditverfahren (Art. 22 DS-GVO-E) Entwicklungen aufgreift, die im Rahmen der Spielräume der Datenschutzrichtlinie durch die nationalen Rechtsordnungen entwickelt wurden, unter dem Gesichtspunkt der Ermöglichung innovativer Schutzinstrumente nur bedingt überzeugend.[6] Es wird hier sehr darauf ankommen, wie die Kommission die ihr zugedachte Rolle ausfüllt. Eine Mitwirkung der Mitgliedstaaten an der delegierten Rechtsetzung wäre insoweit durchaus sinnvoll, ist jedoch primärrechtlich kaum möglich.

2.2.2 Die Spielräume im öffentlichen Bereich

Im öffentlichen Bereich ist der Übergang zur Verordnung deutlich weniger überzeugend, sofern – was eine durchaus offene Frage ist – mit ihm eine stärkere Harmonisierung als unter der gegenwärtigen Richtlinie bewirkt werden soll. Die DS-GVO-E erfasst den gesamten Bereich der Leistungsverwaltung und die Eingriffsverwaltung, soweit diese nicht den Sicherheitsbereich betrifft. Anders als im Bereich grenzüberschreitender wirtschaftlicher Tätigkeit ist das Harmonisierungsbedürfnis hier deutlich weniger ausgeprägt. Warum beispielsweise – um ein aktuelles Beispiel aus Deutschland aufzugreifen – europaweit einheitlich geregelt werden soll, unter welchen Voraussetzungen Private Zugriff auf staatliche Registerdaten haben sollen, ist wenig einsichtig.

Der Entwurf enthält hierfür eine Reihe von Öffnungsklauseln, ist aber deutlich präzisierungsbedürftig. Art. 6 Abs. 1 lit. e DS-GVO-E lässt die Verarbeitung zu, wenn sie für die „Wahrnehmung einer Aufgabe“ erforderlich ist, die im öffentlichen Interesse liegt oder in Ausübung hoheitlicher Gewalt erfolgt und die dem für die Verarbeitung Verantwortlichen übertragen wurde. „Rechtsgrundlagen“ hierfür können nach Art. 6 Abs. 3 lit b DS-GVO-E die Mitgliedstaaten vorsehen, wenn ein entsprechendes öffentliches Ziel vorliegt, der Wesensgehalt gewahrt bleibt und die Regelung verhältnismäßig ist. Nicht wirklich klar ist insoweit, was unter der „Aufgabe“ und der „Rechtsgrundlage“ zu verstehen ist. Dürfen die Mitgliedstaaten – um im genannten Beispiel zu bleiben – nur die „Aufgabe“ des staatlichen Betriebs eines Personenstands- oder Passregisters vorsehen, oder zusätzlich wie nach geltendem Recht detaillierte Erhebungsbefugnisse, Datenarten, Aufbewahrungs- und Löschungsfristen, Zugriffsregelungen etc.?

---

[6] S. näher *Hornung*, ZD 2011, 51, 55 f.

Im ersten Fall würden sich jenseits der mitgliedstaatlichen Aufgabenfestlegung alle weiteren Verwendungsregeln aus der DS-GVO-E ergeben. Dies wäre m.E. evident nicht mit deutschen verfassungsrechtlichen Bestimmtheitsanforderungen zu vereinbaren. Gegen eine solche Interpretation spricht auch, dass Art. 7 der aktuellen Datenschutzrichtlinie bereits eine fast wortgleiche Regelung enthält und so ausgelegt wird, dass mitgliedstaatliche Bestimmungen zulässig sind. Ob dies auch nach der „Hochzonung" von der Richtlinie auf eine Verordnung aufseiten des europäischen Gesetzgebers – und später durch den Europäischen Gerichtshof – genauso gesehen wird, ist nach meiner Wahrnehmung der bisherigen Diskussion jedoch nicht zu entnehmen.

2.3 Beizubehalten: Das „Verbotsprinzip"

Die Diskussion um das so genannte Verbotsprinzip – der Grundsatz, dass jede Erhebung, Verarbeitung und Nutzung personenbezogener Daten einer Rechtfertigung bedarf, die in einer normativen Ermächtigung oder einer Einwilligung liegen kann (§ 4 Abs. 1 BDSG, Art. 7 der Datenschutzrichtlinie) – ist zumindest in Deutschland derzeit Kontroversen ausgesetzt. Der Kommissionsentwurf behält diesen Grundsatz zu Recht bei.

Die Kritik am Verbotsprinzip[7] stützt sich vor allem auf das Argument, private Datenverarbeiter seien anders als der Staat Träger von (insbesondere Wirtschafts-)Grundrechten und müssten deshalb unter leichteren Bedingungen als der Staat zur Verarbeitung personenbezogener Daten befugt sein. Die Prämisse dieser Aussage ist korrekt, aber unvollständig. Die gezogenen Schlussfolgerungen sind in mehrfacher Hinsicht unzutreffend.

Erstens suggeriert das Argument, das geltende Datenschutzrecht behandle private und öffentliche Datenverarbeiter gleich. Dies ist angesichts der Vielzahl von Verarbeitungsbefugnissen der privaten Wirtschaft in den §§ 28 ff. BDSG unzutreffend. Diese Generalklauseln sind teils von extremer Weite und führen dazu, dass private Datenverarbeitungen bereits de lege lata zwar dem Anwendungsbereich des Datenschutzrechts unterfallen, im Ergebnis aber weithin – und teils ohne echte tatbestandliche Begrenzungen – zulässig sind. Hier mag es an der einen oder anderen Stelle (insbesondere im Verhältnis zum Äußerungsrecht)[8] Überarbeitungsbedarf geben. Das spricht aber nicht gegen das Grundprinzip an sich.

---

[7] S. *J. Schneider*, AnwBl 2011, 233; *Härting*, AnwBl 2012, 716; *Härting*, BB 2012, 459, 462 f.; *J. Schneider /Härting*, ZD 2012, 199 ff.; *J. Schneider /Härting*, in: Redeker/Hoppen, DGRI Jahrbuch 2011, 36 ff.; *Giesen*, CR 2012, 550, 553 f.; *Rogall-Grothe*, ZRP 2012, 193, 194 f.

[8] Dies wird an der so genannten „spickmich"-Entscheidung des Bundesgerichtshofs (BGHZ 181, 328) deutlich, in der trotz der genannten Generalklauseln kein Erlaubnistatbestand einschlägig war und das Gericht deshalb mit einer (angreifbaren) teleologischen Reduktion operierte.

Zweitens ist die Schlussfolgerung unzutreffend, schon aus dem Eingreifen grundrechtlicher Schutzbereiche für private Datenverarbeiter folge zwingend, diese seien zumindest für bestimmte Gruppen von Daten vom Verbotsprinzip ausgenommen. Vielmehr hat der Gesetzgeber hier eine Einschätzungsprärogative, bei der er auch die besonderen Gefährdungen zu berücksichtigen hat, die in heutiger Zeit gerade durch private Datenverarbeiter für die Persönlichkeitsrechte der Bürger drohen.[9] Diese Schutzpflichtendimension zwingt den Gesetzgeber nicht zur Beibehaltung des geltenden Regelungsansatzes. Sie würde es aber ausschließen, weite Teile der Datenverarbeitung durch die private Wirtschaft von jedem datenschutzrechtlichen Schutz auszunehmen. Im Ergebnis könnten damit zwar die Abwägungsentscheidungen der §§ 28 ff. BDSG auf die Ebene des Anwendungsbereichs verlagert werden. Es muss aber betont werden, dass es ausgeschlossen wäre, diese Abwägung dort grundsätzlich anders durchzuführen und beispielsweise die Verarbeitung sensibler personenbezogener Daten grundsätzlich zuzulassen. Das Verbotsprinzip erweist sich damit im Kern nicht als materieller Grundsatz, sondern vielmehr als regelungstechnisches Problem.

Drittens würde eine Aufgabe des Verbotsprinzips dazu führen, dass Kriterien für bestimmte Arten von Daten oder Verarbeitungsbereiche angegeben werden müssten, die vom Datenschutzrecht ausgenommen, also per se „harmlos“ sein sollen. An handhabbaren Kriterien hierfür fehlt es in der Debatte weithin. Das liegt daran, dass – dies ist seit langer Zeit anerkannt – die Schutzbedürftigkeit eines personenbezogenen Datum eben nicht an und für sich, sondern nur in Bezug auf den jeweiligen Verwendungskontext beurteilt werden kann. Die Freistellung bestimmter Arten von Daten würde die Gefahr von Zweckänderungen und voraussetzungslosen Übermittlungen an andere Stellen mit sich bringen, bei denen eben doch Persönlichkeitsgefährdungen eintreten könnten. Überdies legt das Verbotsprinzip die Darlegungs- und Beweislast für die „Harmlosigkeit“ eines personenbezogenen Datums der verantwortlichen Stelle auf. Dies ist sinnvoll und sollte beibehalten werden.

Im Ergebnis sollte die Frage, ob Daten generell oder im Einzelfall keinen rechtlichen Schutz bedürfen, nicht auf der Ebene des Anwendungsbereichs des Datenschutzrechts, sondern innerhalb dieses Rechtsgebiets beantwortet werden. Dass in bestimmten Bereichen erleichterte Verarbeitungsbefugnisse sinnvoll, teils auch erforderlich sind, wird nicht ernsthaft bestritten. Hierfür liegen seit über zehn Jahren Vorschläge des Modernisierungsgutachtens von *Roßnagel/Pfitzmann/Garstka* vor, die beispielsweise für Datenverarbeitungen „ohne gezielten Personenbezug“ risikoadäquate Erleichterungen vorschlagen, sofern

---

[9] Zum grundrechtlichen „Informationsschutz gegen Private“ s. z.B. *Bäcker*, Der Staat 51 (2012), 91.

Daten einer strengen Zweckbindung unterliegen und nach der Verarbeitung sofort wieder gelöscht werden. In diesen Fällen sollen etwa die Unterrichtungspflicht und der Auskunftsanspruch entfallen und bestimmte generalisierte Transparenzanforderungen statt individueller Rechte eingreifen.[10] In Fortführung derartiger Ansätze ist eine angemessene Abwägung zwischen Persönlichkeitsrechten und wirtschaftlichen Interessen möglich, ohne das Grundprinzip der Begründungsbedürftigkeit der Verarbeitung aufzugeben.

2.4 Ausbaufähig: Die neuen Betroffenenrechte auf Datenübertragbarkeit und Vergessenwerden

Der Entwurf enthält zwei innovative neue Betroffenenrechte, nämlich das auf Datenübertragbarkeit und das auf Vergessenwerden.

Soweit personenbezogene Daten in „strukturierten gängigen elektronischen Formaten" verarbeitet werden, haben die betroffenen Personen nach Art. 18 DS-GVO-E das Recht, hiervon eine elektronische Kopie zu erhalten und bei einem Anbieterwechsel nicht behindert zu werden. Die Vorschrift dürfte in Teilen durch die Diskussion um soziale Netzwerke beeinflusst sein, geht aber weit darüber hinaus. Der Anspruch ist von 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 DS-GVO-E könnte dazu beitragen, derartige Lock-In-Effekte zu vermeiden. Gerade in sozialen Netzwerken wird er alleine diesen Effekt jedoch kaum haben, weil hier der Anbieterwechsel zumindest bislang dazu führt, dass die Kommunikation mit den bisherigen Kontakten unmöglich gemacht wird – der Nutzer kann zwar wechseln, seine „Freunde" bleiben jedoch zurück. Dieser Effekt könnte nur mittels Vorgaben für Interoperabilität und anbieter- und diensteübergreifende Kommunikation verhindert werden. Diese sind im Entwurf nicht enthalten und hätten Konsequenzen, die weit über das Datenschutzrecht hinaus in das Vertrags- und Wettbewerbsrecht reichen würden.[11]

Für das so genannte Recht auf Vergessenwerden scheint sich inzwischen als nahezu allgemeine Meinung herauszukristallisieren, dass der normative Inhalt des Vorschlags diesen kraftvollen Titel nicht verdient und sogar die Gefahr von Missverständnissen micht sich

---

[10] S. die Zusammenfassung in *Roßnagel/Pfitzmann/Garstka*, Modernisierung des Datenschutzrechts. Gutachten im Auftrag des Bundesministeriums des Innern, 2001, 14 f.; näher ebd., 68 ff., 113 ff., 172 ff. et passim.

[11] S.a. *De Hert/Papakonstantinou*, CLSR 2012, 130, 137 f.

bringt.[12] Vorgesehen sind die – schon im geltenden Recht enthaltenen – Löschungsbefugnisse sowie eine Nachberichtspflicht bei Löschungen. Auch Letztere ist für gezielte Übermittlungen im geltenden Recht enthalten und wird – dies ist die einzige Neuerung – nunmehr auf die Veröffentlichung von Daten erweitert.

Diese Informationspflicht steht unter Zumutbarkeitsvorbehalt und wird kaum praxisrelevant werden, weil – dies folgt aus dem Charakter einer „Veröffentlichung" – der Verpflichtete gerade im Internet praktisch keine Chance hat festzustellen, bei wem die Daten nunmehr verarbeitet werden. Das echte Problem eines Rechts auf Vergessenwerden liegt auf der materiellrechtlichen Ebene, nämlich in dem Verhältnis zwischen Persönlichkeitsrechten einerseits, Presse- und Meinungsfreiheit (wenn man so will, Rechten auf „Erinnern") andererseits. Der Vorschlag der Kommission versucht hier materiellrechtliche Probleme durch eine verfahrenstechnische Vorgabe zu lösen. Dies dürfte kaum von Erfolg gekrönt sein, solange nach Art. 80 Abs. 1 DS-GVO-E die Mitgliedstaaten weithin Sonderregeln für den – im europäischen Datenschutzrecht weit verstandenen – Bereich der Presse verabschieden dürfen. Zusammenfassend lässt sich sagen, dass sich ein gemeinschaftsweites Recht auf Vergessenwerden kaum konsistent mit mitgliedstaatlichen Derogationsbefugnissen im Bereich von Presse- und Meinungsfreiheit vereinbaren lässt.

2.5 Stark ausbaufähig: Moderne Datenschutzinstrumente[13]

Der Entwurf enthält in Art. 23 DS-GVO-E Regelungen zum Datenschutz durch Technik und zu datenschutzfreundlichen Voreinstellungen. Darin liegt ein dringend erforderlicher Schritt hin zu einer Verbindung rechtlicher und technischer Schutzinstrumente.[14] 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 DS-GVO-E) und insbesondere das Erforderlichkeitsprinzip technisch strikt einzuhalten (Art. 23 Abs. 2 DS-GVO-E). Es fehlt aber jede verbindliche Aussage zur Technikgestaltung, und Grundprinzipien des technischen Datenschutzes wie Anonymisierung und Pseudonymisierung werden im gesamten Entwurf

---

[12] S. schon *Hornung*, ZD 2012, 99, 103; mit unterschiedlich starker Kritik: *Costa/Poullet*, CLSR 2012, 254, 256 f.; *Jaspers*, DuD 2012, 571, 572 f.; *Koreng/Feldmann*, ZD 2012, 311; *Kort*, DB 2012, 1020, 1022 f.; *Lang*, K&R 2012, 145, 149; *Wybitul/Fladung*, BB 2012, 509, 510 f.; mit umgekehrter Richtung (zu weitgehende Pflichten mit „unübersehbarem Risiko" für Internetveröffentlichungen): *Härting*, BB 2012, 459, 464; zu mehr konzeptionellen Grundüberlegung s. *Mayer-Schönberger*, Delete: The Virtue of Forgetting in the Digital Age, 2009; *Koops*, SCRIPTed 2011, 229; *Ausloos*, CLSR 2012, 143.

[13] Dieser Abschnitt basiert im Wesentlichen auf *Hornung*, ZD 2012, 99, 103 f.

[14] 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.

nicht erwähnt. Der normative Gehalt bleibt damit noch hinter dem von § 3a BDSG[15] zurück. Ob man insoweit auf die gemäß Art. 23 Abs. 3 und 4 sowie Art. 30 Abs. 3 DS-GVO-E zulässigen Rechtsakte und Standards der Kommission vertrauen darf, ist völlig unklar.[16]

Noch vager sind die Aussagen zu Zertifizierungen, Datenschutzsiegeln und -zeichen in Art. 39 DS-GVO-E, die durch Mitgliedstaaten und Kommission „gefördert" werden sollen. Auch diese Instrumente – die in Schleswig-Holstein mit Erfolg eingesetzt werden[17] – hätte eine verbindliche Regelung verdient gehabt.[18] 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 DS-GVO-E) ausfüllen soll.

Begrüßenswert sind demgegenüber die Regelungen zur Meldung von Schutzverletzungen („data breach notification"), die gegenüber der Aufsichtsbehörde (Art. 31 DS-GVO-E) und der betroffenen Person (Art. 32 DS-GVO-E) 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.[19] 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.[20] Zweckmäßigerweise hätten allerdings deren Formulierungen übernommen werden sollen; die unterschiedliche Regelungssystematik ist wenig einsichtig, wenn damit keine inhaltlichen Abweichungen impliziert werden sollen.

Auch die Einführung der Datenschutz-Folgenabschätzung (data protection impact assessment, DPIA) ist ein sinnvolles neues Instrument.[21] Sie tritt anstelle der bisherigen Meldepflicht und ist nach Art. 33 Abs. 1 DS-GVO-E bei Verarbeitungsvorgängen erforderlich, die „konkrete Risiken für die Rechte und Freiheiten betroffener Personen bergen". Diese kaum operationalisierbare Formulierung wird in Art. 33 Abs. 2 DS-GVO-E durch Regelbeispiele

---

15 Zu dessen umstrittener Rechtsnatur s. Simitis-*Scholz*, BDSG, § 3a Rn. 27 f. m.w.N.

16 Ebenfalls kritisch *Richter*, DuD 2012, 576 ff.

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

18 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.

19 S. zum Konzept *Gabel*, BB 2009, 2045; *Eckhardt/Schmitz*, DuD 2010, 390; *Ernst*, DuD 2010, 472; *Hanloser*, MMR 2010, 300; *Hornung*, NJW 2010, 1841; in Bezug auf den Entwurf *De Hert/Papakonstantinou*, CLSR 2012, 130, 139 f.

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

21 *De Hert/Papakonstantinou*, CLSR 2012, 130, 140 f. Zur Technikfolgenabschätzung s. etwa *Ropohl*, Ethik und Technikbewertung, 1996; *Grunwald*, Technikfolgenabschätzung, 2. A. 2010; aus allgemeinerer rechtlicher Perspektive *Roßnagel*, Rechtswissenschaftliche Technikfolgenforschung, 1993.

präzisiert. Diese umfassen unter anderem auf Profiling basierende Maßnahmen, bestimmte Kategorien von Daten, die „weiträumige“ Überwachung öffentlich zugänglicher Bereiche, vor allem mittels Videoüberwachung, 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 DS-GVO-E.

Schließlich ist das neuartige Verbandsklagerecht positiv zu würdigen. Entsprechende Interessensorganisationen haben das Recht, im Namen der betroffenen Personen (Art. 73 Abs. 2 DS-GVO-E) und im eigenen Namen (Art. 73 Abs. 3 DS-GVO-E) Beschwerde bei einer Aufsichtsbehörde zu erheben. Im Namen der betroffenen Personen können derartige Organisationen nach Art. 76 Abs. 1 DS-GVO-E auch gerichtliche Verfahren anstrengen. Derartige Instrumente könnten zu einer erheblichen Effektivierung des Datenschutzrechts beitragen, bei dem nach wohl allgemeiner Meinung ein erhebliches Vollzugsdefizit in der Praxis zu beobachten ist. Hier sind durchaus weitere Schritte vorstellbar, insbesondere eine Regelung zur wettbewerbsrechtlichen Relevanz von Datenschutzverstößen, die derzeit uneinheitlich beurteilt wird,[22] jedoch einen Beitrag zur Durchsetzung leisten könnte.

2.6 Primärrechtlich bedenklich und datenschutzrechtlich systemwidrig: Die Rolle der Kommission[23]

Eine der gravierendsten Veränderungen des Entwurfs liegt auf der institutionellen Ebene, nämlich in der Rolle der Kommission, die bislang nur in ausgewählten Bereichen Entscheidungskompetenzen hat,[24] 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 DS-GVO-E, s. Art. 290 AEUV) und/oder Durchführungsrechtsakten (Art. 87 Abs. 2 und 3 DS-GVO-E, 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.[25] Auch wird es vielfach sinnvoll sein, europaweit einheitliche Vorgaben und Leitlinien für die Praxis zu machen. Der Entwurf enthält aber so viele Ermächti-

---

22 Unter bestimmten Bedingungen bejahend OLG Köln, CR 2011, 680; OLG Köln, NJW 2010, 90; OLG Stuttgart GRUR-RR 2007; OLG Frankfurt, NJW-RR 2005, 1280; a.A. OLG München, ZD 2012, 330; einschränkend KG Berlin, NJW-RR 2011, 1264; näher *Conrad*, in: Auer-Reinsdorff/Conrad, Beck'sches Mandatshandbuch IT-Recht, 2011, 1277 ff.; *Schröder*, ZD 2012, 331f.; *Ohly*, in: Piper/Ohly/Sosnitza, UWG, 5. Aufl. 2010, UWG § 4 Rn. 11.79.

23 S. zu diesem Abschnitt schon *Hornung*, ZD 2012, 99, 104 ff.

24 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.

25 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.

gungen (die langen Kataloge in Art. 86 DS-GVO-E 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.[26] 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 DS-GVO-E) und den Zertifizierungen (Art. 39 DS-GVO-E) der Fall ist[27] – 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 DS-GVO-E),[28] andererseits dennoch der Kommission diesen Bereich zur Regulierung mittels tertiären Rechtsakten zu überantworten (Art. 82 Abs. 3 DS-GVO-E).

Die Entscheidungsbefugnis 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.[29] 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 Europäischen Datenschutzausschuss als Nachfolger der derzeitigen Art. 29-Datenschutzgruppe) vorsehen, die ebenso wie die Aufsichtsbehörden gerichtlicher Kontrolle (nunmehr des Europäischen Gerichtshofes) unterliegen sollte. Die Kommission könnte sich dann auf die Erarbeitung allgemein geltender

---

[26] Die Regelung ist allerdings nicht mit der Wesentlichkeitslehre des deutschen Verfassungsrecht gleichzusetzen; vielmehr kommt es auf die wesentlichen politischen Grundentscheidungen der Materie an, s. EuGH, Rs. C-240/90, Slg. 1992, I-5383, Rn. 37 (Deutschland/Kommission); dies impliziert einen erheblichen Spielraum, s.a. *Gärditz*, DÖV 2010, 453, 456; *Möllers/v. Achenbach*, EuR 2011, 39, 48 f.; zum Verfahren der europäischen exekutiven Rechtssetzung nach dem Vertrag von Lissabon s. *Sydow*, JZ 2012, 157.

[27] S.o. 2.5.

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

[29] Im Ergebnis ebenfalls kritisch *Costa/Poullet*, CLSR 2012, 254, 560 f.; *Roßnagel*, DuD 2012, 553; *Schild/Tinnefeld*, DuD 2012, 312, 316 f.; *Traung*, Cri 2012, 33, 34 f.; zur Datenschutzaufsicht im Mehrebenensystem grundsätzlicher *Dix*, DuD 2012, 318.

Leitlinien beschränken und hier eine sinnvolle Aufgabe der Präzisierung einheitlicher europäischer Standards erfüllen.

3 Zum Richtlinienentwurf

3.1 Thesen

Zum RL-E lassen sich die wesentlichen Ergebnisse der folgenden Ausführungen wie folgt zusammenfassen:

1. Die Union verfügt mit Art. 16 Abs. 2 AEUV über eine Kompetenzvorschrift für die geplanten Bestimmungen. Eine umfassende Regelung der informationsbezogenen Ermittlungs- und Gefahrenabwehrmaßnahmen in der Union wäre nicht zulässig, wird mit dem Vorschlag aber auch nicht vorgenommen.
2. Trotz des Anspruchs, ein einheitliches Rahmenwerk für den Datenschutz in Europa vorlegen zu wollen, weichen die Bestimmungen des RL-E in vielen Punkten zum Nachteil der Betroffenen von denen des DS-GVO-E ab. Problematisch ist also weniger die Aufteilung in zwei verschiedene Regelungsinstrumente, sondern die Tatsache, dass bestimmte Prinzipien der Verarbeitung, der Betroffenenrechte und der Befugnisse der Aufsichtsbehörden abweichend geregelt werden sollen.
3. Die Übermittlungsbefugnisse in Drittstaaten enthalten viele Erlaubnistatbestände und noch mehr Ausnahmen. Letztere sind so weit gefasst, dass der Vorschlag in seiner jetzigen Form teilweise sogar noch hinter dem geltenden Rahmenbeschluss zurückbleibt. Dieser Rückschritt ist vor dem Hintergrund der Zielrichtung der Reform grundsätzlich abzulehnen.
4. Es ist nicht überzeugend, dass die Kommission nicht zeitgleich mit dem RL-E einen Vorschlag für die Fortentwicklung des Datenschutzrechts bei Europol und Eurojust vorgelegt hat. Ohne eine Harmonisierung mit den Verarbeitungsvorgaben bei diesen Institutionen bleibt die Reform grundsätzlich fragmentarisch und gerade an den Stellen lückenhaft, die im Rahmen einer intensivierten Zusammenarbeit von Polizei und Justiz immer wichtiger werden.

3.2 Kompetenz

Eine gewisse stärkere Vereinheitlichung des Datenschutzrechts in Europa ist zur Gewährleistung vergleichbarer datenschutzrechtlichen Standards sinnvoll. Sie ist überdies unabdingbare Voraussetzung für eine weitere Intensivierung der polizeilichen und justiziellen Zusammenarbeit in Europa. Diese Zusammenarbeit bedingt weithin den Austausch personenbezogener Daten, der ohne gemeinsame – hohe – datenschutzrechtliche Anforderun-

gen nicht zu rechtfertigen ist. Hierfür bietet Art. 16 Abs. 2 AEUV eine entsprechende Grundlage. Diese erfasst zumindest im Grundsatz auch innerstaatliche Verarbeitungsvorgänge, die sich vielfach ohnehin im Rahmen der zunehmenden Kooperation der Kriminalbehörden in der Union nicht mehr vollständig von Vorgängen mit internationalen und grenzüberschreitenden Bezügen (einschließlich der Datenübermittlungen an europäische und internationale Organisationen) abgrenzen lassen.

Die Union hat jedoch keine umfassende Rechtssetzungskompetenz im Bereich von Polizei und Justiz, insbesondere hinsichtlich der Datenerhebungsbefugnisse im Bereich von Gefahrenabwehr und Strafverfolgung. Diese zutreffende Überlegung steht hinter den Überlegungen des Bundesrats in seinem Beschluss vom 30. März 2012.[30] Im Ergebnis werden – wie der Kollege *Matthias Bäcker* zu Recht in seiner Stellungnahme ausführt, der ich mich in Ergebnis und Begründung anschließe – die Anforderungen und Beschränkungen von Art. 16 Abs. 2 AEUV jedoch gewahrt. Insbesondere die sehr weiten Regelungen in Art. 7 RL-E gewähren einen europarechtlich materiell praktisch kaum begrenzten Spielraum für entsprechende Erhebungsbefugnisse der Mitgliedstaaten. Dieser ist zwar wiederum in seiner Weite unter rechtsstaatlichen Gesichtspunkten zu kritisieren,[31] würde aber auch im Fall einer Präzisierung hinreichende Spielräume lassen. Für die im RL-E enthaltenen Regelungen, die im Kern datenschutzrechtlicher Natur sind, bietet Art. 16 Abs. 2 AEUV hingegen die erforderliche europarechtliche Kompetenz.

3.3 Abweichung nach „unten“: Unterschiede zum Entwurf der DS-GVO-E

Der RL-E enthält an einigen Stellen Abweichungen vom gleichzeitig vorgelegten DS-GVO-E. Anders als angemessen und zu erwarten wäre, beziehen sich diese Abweichungen nicht nur auf Besonderheiten der Datenverarbeitung bei Polizei und Justiz, sodass die Unterschiede zumindest insoweit dem selbstgesetzten Ziel der Kommission zuwiderlaufen, einen einheitlichen „europäischen Datenschutzrahmen für das 21. Jahrhundert“[32] zu schaffen.

Beispiele für derartige Abweichungen sind insbesondere:

- Das Fehlen einer Regelung zur Datenschutz-Folgenabschätzung, die in Art. 33 DS-GVO-E für deren Anwendungsbereich geregelt ist (anders noch Art. 31 des Zwischenstands der Vorarbeiten zum RL-E vom November 2011),

---

30 BR-Drs. 51/12(B).
31 S. auch dazu die Stellungnahme des Kollegen *Bäcker* sowie *Bäcker/Hornung*, ZD 2012, 147, 149 f.
32 KOM(2012) 9 endg.

- Das Fehlen von Bestimmungen zum Einsatz zertifizierter Technologien. Art. 39 DS-GVO-E folgt der Idee, dass diese sich am Markt leichter durchsetzen werden, was im Bereich des RL-E keine direkte Rolle spielt. Wie das Beispiel der schleswig-holsteinischen Regelung zeigt, sind aber Verpflichtungen von Behörden denkbar und sinnvoll, bevorzugt zertifizierte Technologien einzusetzen. Hinzu kommt, dass entsprechende Prüfverfahren auch im Interesse der Sicherheitsbehörden sind, die sich zunehmend der Kritik ausgesetzt sehen, bei informationstechnischen Maßnahmen keine hinreichend sicheren Systeme einzusetzen.[33] Überdies werden nachprüfbare Maßnahmen zur Datensicherheit in Zukunft vor dem Hintergrund der Anforderungen in der jüngeren Rechtsprechung des Bundesverfassungsgerichts[34] eine größere Rolle als bisher spielen,
- Die deutlich eingeschränkten Befugnisse der Aufsichtsbehörden (Art. 46 RL-E enthält nicht nur erheblich weniger, sondern auch viel offener formulierte Befugnisvorgaben als Art. 53 DS-GVO-E).

Demgegenüber ist es ausdrücklich zu begrüßen, dass die Informationspflichten bei „Datenpannen“[35] auch auf die Kriminalbehörden erstreckt werden. Hinsichtlich der Datensicherheit wird in Art. 27 Abs. 2 RL-E sogar detaillierter als in der DS-GVO-E formuliert;[36] offenbar hat die Kommission hier Regelungen aufgenommen, die sie im Anwendungsbereich der DS-GVO-E erst nachträglich aufgrund ihrer Befugnis zum Erlass delegierter Rechtsakte erlassen will.

3.4 Rechtsstaatlich problematisch: weitgehende Generalklauseln

Ein weiterer Punkt, in dem der RL-E vom DS-GVO-E abweicht, ist die Aufnahme einer Reihe von Generalklauseln im Bereich allgemeiner datenschutzrechtlicher Prinzipien. Mit dieser Regelungstechnik werden allgemeine Prinzipien in Teilen für den Anwendungsbereich des RL-E deutlich aufgeweicht.

Beispiele für derartige Normen sind unter anderem:

- Art. 4 lit. a RL-E verzichtet, anders als Art. 5 lit. a DS-GVO-E, auf die Vorgabe, die Verarbeitung müsse für die betroffene Person nachvollziehbar sein. Eine solcher

---

33 Insbesondere in der Diskussion um so genannte „Staatstrojaner“; s. dazu zuletzt *Der Bayerische Landesbeauftragte für den Datenschutz*, Prüfbericht Quellen-TKÜ, 30.7.2012.

34 S. insbesondere die Anforderungen in der Entscheidung zur Vorratsdatenspeicherung: BVerfGE 125, 260; zu diesem Aspekt der Datensicherheit *Hornung/Schnabel*, DVBl 2010, 824, 829; s. zuvor schon *Roßnagel/Bedner/Knopp*, DuD 2009, 536

35 Dazu *Gabel*, BB 2009, 2045; *Eckhardt/Schmitz*, DuD 2010, 390; *Ernst*, DuD 2010, 472; *Hanloser*, MMR 2010, 300; *Hornung*, NJW 2010, 1841.

36 S. bisher Art. 22 des Rahmenbeschlusses.

Verzicht lässt sich nur (und unter bestimmten Bedingungen) in Einzelfällen rechtfertigen, nicht aber als allgemeiner „Grundsatz“ in Art. 4 RL-E,

- Die Zweckbindung der Daten wird dadurch abgeschwächt, dass die Verarbeitung nicht wie in Art. 5 lit. c DS-GVO-E auf ein Mindestmaß beschränkt wird, sondern lediglich mit Blick auf den Zweck der Datenverarbeitung „nicht exzessiv“ (Art. 4 lit. c) sein darf,
- Statt eine nachvollziehbare und jedermann leicht zugängliche Strategie für die Umsetzung der Betroffenenrechte vorzugeben (Art. 11 DS-GVO-E) steht dies nach Art. 10 Abs. 1 RL-E unter dem Vorbehalt, dass nur „vertretbare Schritte“ unternommen werden müssen. Auch hier gilt, dass dies in begründbaren Einzelfällen gerechtfertigt werden kann, nicht aber im Bereich einer allgemeinen Strategie zur Umsetzung wesentlicher Rechte der Betroffenen.
- Auch der Ausnahmevorbehalt in Art. 11 Abs. 4 und Abs. 5 RL-E erscheint unangemessen weit. Danach ist es aus einer Vielzahl von Gründen zulässig, eine Information der betroffenen Person hinauszuzögern, einzuschränken oder ganz zu unterbinden. Diese Regelung steht zwar unter dem Vorbehalt der Verhältnismäßigkeit, der richtigerweise eine einschränkende Auslegung erfordert.[37] Dennoch sollte schon auf tatbestandlicher Ebene eine deutliche Einschränkung erfolgen.

Schließlich kommt hinzu, dass weitere etablierte Schutzbereiche der Datenverarbeitung bei Polizei und Justiz fehlen: So enthält der RL-E beispielsweise keine Vorgaben für den Schutz von Berufsgeheimnisträgern.

Im Ergebnis erweisen sich die materiellrechtlichen Anforderungen des Richtlinienentwurfs in einer Reihe von Fragen zwar als Erweiterung des Schutzes der Betroffenen gegenüber dem bisher geltenden Rahmenbeschluss 2008/977/JI.[38] Die Regelungen bleiben aber weithin hinter den deutschen verfassungsrechtlichen Standards zurück. Im Gesetzgebungsprozess sollte deshalb entweder auf eine Angleichung auf hohem Niveau oder – wohl realistischer – auf entsprechende Spielräume für die Mitgliedstaaten hingewirkt werden, einen bisher höheren Datenschutzstandard im Bereich von Polizei und Justiz beibehalten zu dürfen.

---

[37] *Bäcker/Hornung*, ZD 2012, 147, 150 f.
[38] ABl. EU Nr. L 350/60 v. 30.12.2008.

3.5 Echte Grenzen erforderlich: Übermittlungsbefugnisse in Drittstaaten

Ein erhebliches Problem des Entwurfs sind die Regelungen zur Datenübermittlung in Drittstaaten.[39] Grundvoraussetzung für alle Übermittlungen ist gemäß Art. 33 lit. a RL-E, dass die Übermittlung zur Verhütung, Aufdeckung, Untersuchung oder Verfolgung von Straftaten oder zur Strafvollstreckung erforderlich ist. Hinzutreten muss nach Art. 33 lit. b RL-E ein Erlaubnistatbestand, nämlich ein Angemessenheitsbeschluss (Art. 34 RL-E), geeignete Garantien (Art. 35 RL-E) oder weitere Ausnahmetatbestände (Art. 36 RL-E).

Schon die Regelung zu geeigneten Garantien enthält eine zu weitgehende Bestimmung: Nach Art. 35 Abs. 1 lit. b RL-E soll es für eine Übermittlung ausreichen, dass „der für die Verarbeitung Verantwortliche oder der Auftragsverarbeiter alle Umstände beurteilt hat, die bei der Übermittlung personenbezogener Daten eine Rolle spielen, und zu der Auffassung gelangt ist, dass geeignete Garantien zum Schutz personenbezogener Daten bestehen". Eine derartige versubjektiverte ex ante-Perspektive ist bei weltweiten Datenübermittlungen abzulehnen.

Noch gravierender sind die Ausnahmen in Art. 36 RL-E, die sich als der Sache nach unangemessen weit erweisen. Allein Art. 36 lit. d RL-E lässt alle übrigen Übermittlungsvorschriften von Kapitel V überflüssig werden. Danach soll es als „Ausnahme" möglich sein, Daten in ein Drittland oder an eine internationale Organisation zu übermitteln, wenn dies zur „Verhütung, Aufdeckung, Untersuchung oder Verfolgung von Straftaten oder zur Strafverfolgung erforderlich ist". Dies ist jedoch bereits nach dem wortgleichen Art. 33 lit. a RL-E erforderlich (s.o.) und letztlich der Sache nach sogar Voraussetzung für jede Datenverwendung im Bereich des Entwurfs. Mit anderen Worten kann immer dann, wenn eine Datenübermittlung zur Gefahrenabwehr oder Strafverfolgung – und zwar sowohl innerhalb als auch außerhalb des Geltungsbereichs des RL-E – erforderlich ist, auch eine Übermittlung stattfinden.

Dieser Vorschlag verzichtet auf jede Berücksichtigung des Datenschutzniveaus im Empfängerstaat. Regelungstechnisch führt er überdies dazu, dass die übrigen Regelungen des Kapitels rechtsstaatlich geradezu schädlich sind. Beim unbefangenen Lesen gewinnt man zunächst den Eindruck, der Entwurf enthalte Sicherungsmechanismen, die de facto nicht bestehen. Im Ergebnis verzichtet die RL-E damit auf echte materielle Anforderungen an die datenschutzrechtlichen Regelungen in den Drittländern, an die die Sicherheitsbehörden personenbezogene Daten übermitteln. Dies ist durch eine Beschränkung der Ausnahmeregelungen in Art. 36 RL-E zu ändern.

---

[39] S. zum Folgenden schon *Bäcker/Hornung*, ZD 2012, 147, 151.

3.6 Notwendige Ergänzung: Europol und Eurojust

Nach Art. 2 Abs. 3 lit. b RL-E gilt der Entwurf nicht für Organe, Einrichtungen, Ämter und Agenturen der Union. Dieses Vorgehen erscheint einerseits regelungstechnisch verständlich, da insoweit andere Rahmenbedingungen gelten. Es ist allerdings kaum nachvollziehbar, dass die Kommission – die immerhin mit dem Anspruch eines „europäischen Datenschutzrahmens für das 21. Jahrhundert“[40] auftritt – nicht zugleich einen Vorschlag für die Institutionen der Union vorgelegt hat. Insbesondere die Datenschutzregeln für Europol sind in der Vergangenheit vielfach und zu Recht als ungenügend kritisiert worden.[41] Zumindest mittelfristig sind hier einheitliche Regeln für die nationalen Kriminalbehörden einerseits und für Europol und Eurojust andererseits erforderlich.[42]

---

[40] KOM(2012) 9 endg.

[41] Näher *Böhm*, Information Sharing and Data Protection in the Area of Freedom, Security and Justice, 2011, 177 ff. (zu Europol), 214 ff. (Eurojust); s. zur Rechtslage vor dem 1.1.2010 auch *Matz*, Europol – Datenschutz und Individualrechtsschutz im Hinblick auf die Anforderungen der EMRK, 2003; *Beaucamp*, DVBl 2007, 802; *Hilger/Ruthig/Schenke/Wolter/Zöller*, Alternativentwurf Europol und europäischer Datenschutz, 2008.

[42] S. schon *Bäcker/Hornung*, ZD 2012, 147, 149; ausführlich *Boehm*, DuD 2012, 339.