Univ.-Prof. Dr. Dieter Kugelmann

Leiter des Fachgebietes Öffentliches Recht
mit Schwerpunkt Polizeirecht
einschließlich des internationalen Rechts
und des Europarechts

Deutsche Hochschule der Polizei
Zum Roten Berge 18 - 24
D-48165 Münster

Tel.: 02501/806-437
Sekretariat: 02501/806-279
E-mail: Dieter.Kugelmann@dhpol.de

Deutscher Bundestag
Innenausschuss

Ausschussdrucksache
17(4)585 A

Stellungnahme

zur Anhörung vor dem Innenausschuss des Deutschen Bundestages

zu

a) dem Vorschlag für eine Richtlinie des Europäischen Parlaments und des Rates zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die zuständigen Behörden zum Zweck der Verhütung, Aufdeckung, Untersuchung oder Verfolgung von Straftaten oder der Strafvollstreckung sowie zum freien Datenverkehr
KOM (2012)10 endg.
Ratsdok.-Nr. 5833/12,

b) dem Bericht der Kommission an das Europäische Parlament, den Rat, den Europäischen Wirtschafts- und Sozialausschuss und den Ausschuss der Regionen auf der Grundlage von Artikel 29 Absatz 2 des Rahmenbeschlusses des Rates vom 27. November 20008 über den Schutz personenbezogener Daten, die im Rahmen der polizeilichen und justiziellen Zusammenarbeit in Strafsachen verarbeitet werden
KOM (2012)12 endg.
Ratsdok.-Nr. 5834/12,

c) der Mitteilung der Kommission an das Europäische Parlament, den Rat, den Europäischen Wirtschafts- und Sozialausschuss und den Ausschuss der Regionen
Der Schutz der Privatsphäre in einer vernetzten Welt
Ein europäischer Datenschutzrahmen für das 21. Jahrhundert
KOM (2012)9 endg.
Ratsdok.-Nr. 5852/12,

d) dem Antrag der Abgeordneten Dr. Konstantin von Notz, Volker Beck (Köln), Kai Gehring, weiterer Abgeordneter und der Fraktion BÜNDNIS 90/DIE GRÜNEN
EU-Datenschutzreform unterstützen
BT-Drucksache 17/9166.

1. Reichweite und Anwendungsbereich

Der Richtlinien-Vorschlag beruht auf der Kompetenz des Art. 16 Abs. 2 AEUV. Auf ihn ist das Datenschutz-Grundrecht des Art. 8 Grundrechte-Charta (GR-Ch) anwendbar, so dass die Richtlinie an den Maßstäben des europäischen Grundrechtsschutzes zu messen ist. Ziele der Richtlinie sind die Schaffung eines hohen Datenschutzniveaus und Stärkung des gegenseitigen Vertrauens der Polizei- und Justizbehörden der Mitgliedstaaten untereinander. Der Datenaustausch soll dadurch erleichtert werden, dass innerstaatliche wie grenzüberschreitende Datenverarbeitung denselben Regeln unterliegen. In der Erklärung Nr. 21 zum Vertrag von Lissabon haben die Vertragsstaaten bereits anerkannt, dass für die polizeiliche und justizielle Zusammenarbeit spezifische Vorschriften erforderlich sein können.

Die Richtlinie beabsichtigt eine *umfassende Harmonisierung* des Datenschutzes unabhängig von einem konkreten grenzüberschreitenden Bezug eines Datenvorgangs. Im Verbund mit der Datenschutz-Grundverordnung werden damit die Regelungen des Datenschutzes weitgehend europäisiert. Diesen Ansatz kann man insbesondere mit Blick auf die vereinheitlichende Wirkung der unmittelbar anwendbaren Verordnung kritisieren, weil Differenzierungen zwischen Sachbereichen für den Datenschutz produktiv sein können und auch die grundrechtlichen Anforderungen Unterschiede aufweisen können (*Masing*, NJW 2012, 2305, 3211). Auch der Bundesrat bezweifelt in seiner Subsidiaritätsrüge vom 29. März 2012 die Reichweite der Kompetenzgrundlagen (BR-Drs. 707/10 [B], Ziff. 8, 3. Abs.) und befürchtet Verletzungen der Prinzipien der Subsidiarität und der Verhältnismäßigkeit (so auch *Ronellenfitsch*, DuD 2012, 562 f.; zur Subsidiaritätsrüge gegen die Datenschutz-Grundverordnung *Nguyen*, ZEuS 2012, 277). Im Hintergrund steht die Befürchtung, dass über die Regelungen des Datenschutzes auch Kompetenzen zur Regelung von Sachgebieten beansprucht werden, für die der EU keine Kompetenzen zustehen (*Rogall-Grothe*, ZRP 2012, 193).

Die *Erstreckung auf die innerstaatliche Datenverarbeitung* ist zur Erreichung des von der Richtlinie verfolgten Ziels unabdingbar. Anlass für die Reform des Datenschutzes war gerade die Erkenntnis, dass sich das Niveau des Datenschutzes zwischen den Mitgliedstaaten trotz der vorhandenen Rechtsakte deutlich unterscheidet. Nach der Konzeption der Richtlinie findet sie daher auf jede Datenverarbeitung der zuständigen Behörden zu den Zwecken der Verhütung, Aufdeckung, Untersuchung oder Verfolgung

von Straftaten oder der Strafvollstreckung Anwendung (Art. 2). Unter Verarbeitung ist auch das Erheben von Daten zu verstehen (Art. 3 Ziff. 3). Ob der Vorgang rein innerstaatlich ist, spielt keine Rolle. Eine Ausnahme bilden nur Tätigkeiten, die nicht in den Anwendungsbereich des Unionsrechts fallen, z. B. die Verteidigung (s. Art. 39 EUV) und die Datenverarbeitung durch Nachrichten- und Sicherheitsdienste. Aufgrund des in Deutschland geltenden Trennungsgebotes ist die Richtlinie daher auf die Ämter für Verfassungsschutz, den MAD oder den BND nicht anwendbar (*Bäcker/Hornung*, ZD 2012, 149), während sie auf das BKA und die Staatsschutzabteilungen der Polizeibehörden Anwendung findet.

Die Anwendbarkeit auf jede Datenverarbeitung der zuständigen Behörden wird von Art. 16 AEUV getragen. Die prinzipiellen Zweifel an der Kompetenz der EU greifen letztlich nicht durch, führen aber zu einer sorgfältigen Betrachtung der Kompetenzgrenzen. Datenschutz betrifft als Querschnittsmaterie nahezu jeden Bereich staatlicher Verwaltung. In der Informationsgesellschaft gehört die Erhebung und Verarbeitung von Daten bekanntlich zu den zentralen Aufgaben der Behörden. Eine Trennung der Vorgänge mit und ohne grenzüberschreitenden Bezug ist in diesem Zusammenhang kaum möglich, zumal schon der Standort der Server für die Übermittlung von Daten nicht immer klar ist. Die von Art. 16 Abs. 2 S. 1 AEUV umfasste Verarbeitung von Daten durch die Mitgliedstaaten, die in den Anwendungsbereich des Unionsrechts fallen, ist von der sonstigen Verarbeitung von Daten schwer zu unterscheiden. Der Anwendungsbereich des Unionsrechts kann aus Sicht der Behörden eng gefasst werden, weil Art. 87 AEUV nur die Europäische Polizeiliche Zusammenarbeit betrifft. Der Anwendungsbereich des Unionsrechts kann aber auch aus Sicht des Bürgers mit dem Ziel der Verbesserung des Datenschutzes betrachtet werden, wodurch ein weites Verständnis begründet wird. Folgt man der letzteren Sichtweise, können innerstaatliche Sachverhalte in der Richtlinie mitgeregelt werden, soweit nicht die Besonderheiten des Sachbereiches Justiz und Inneres Grenzen setzen.

Soweit es um die Verhütung und Verfolgung von Straftaten geht, sind die geltenden *Polizeigesetze* und insbesondere die *Strafprozessordnung* Gegenstand der Umsetzung der Richtlinie. Die Richtlinie enthält selbst in Art. 17 den Vorbehalt, dass das einzelstaatliche Strafprozessrecht für eine Reihe von Konstellationen zur Anwendung kommen kann. Angesichts der unklaren Fassung der Vorschrift sind hier viele Fragen offen (so auch die Stellungnahme der Konferenz der Datenschutzbeauftragten des Bundes und der Länder

vom 11. Juni 2012 zur 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, S. 7 f.). Auch nach einer notwendigen Präzisierung der Regelung verbleiben jedenfalls Umsetzungsspielräume, die eine Berücksichtigung nationaler Besonderheiten insbesondere im Ermittlungsverfahren erlauben.

Angesichts der zunehmenden europäischen Kooperation von Strafverfolgungsbehörden und Gerichten ist es nachhaltig zu begrüßen, dass der Flickenteppich an Einzelregelungen durch gemeinsame Grundregeln teilweise ersetzt wird (so auch die Stellungnahme der Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 11. Juni 2012 zur Richtlinie, S. 3). Allerdings ist nicht zu verkennen, dass die Datenschutzvorschriften in besonderen Rechtsakten für *Organe und Einrichtungen der EU* wie Europol, Eurojust oder Frontex oder auch für die polizeiliche Zusammenarbeit wie im Prüm-Beschluss 2008/615/JI unberührt bleiben sollen (Art. 59). Die allgemeine Verordnung 45/2001 über den Datenschutz bleibt ebenfalls bestehen. Dadurch ist dann, wenn eine EU-Agentur an den Informationsflüssen beteiligt ist, der Mindeststandard der Richtlinie nicht auf alle beteiligten Behörden anwendbar. Wünschenswert wäre daher, den Anwendungsbereich der Richtlinie auch auf Organe und Einrichtungen der EU zu erstrecken (so auch *Bäcker/Hornung*, ZD 2012, 149).

2. Allgemeine Regeln

Eine Unterscheidung nach den *Kategorien betroffener Personen* fordert Art. 5. Als Kategorien werden Personen, gegen die ein begründeter Verdacht besteht, Verurteilte, Opfer, Dritte (z.B. eventuelle Zeugen) und Sonstige genannt. Diese Unterscheidung kann nicht der Anwendungspraxis überlassen bleiben. Aufgrund der Wesentlichkeitstheorie muss in der Bundesrepublik Deutschland der Gesetzgeber die Unterscheidung treffen, da an diese Kategorien sehr unterschiedliche Rechtsfolgen geknüpft werden. Regelungsgegenstände können der Opferschutz durch die Geheimhaltung von Informationen oder die Verwendung von Daten zur Strafvollstreckung sein, indem geltende Regelungen gesichtet und weiter entwickelt werden.

Eine weitere Unterscheidung betrifft unterschiedliche *Kategorien von Daten* im Hinblick auf den Grad ihrer Richtigkeit und Zuverlässigkeit (Art. 6). Einschneidende Maßnahmen der Behörden, die Grundrechtseingriffe darstellen, bedürfen einer soliden Datengrundlage. In die Rechtssphäre des Bürgers darf nur eingegriffen werden, wenn dieser Eingriff auf einer tragfähigen tatsächlichen Informationsgrundlage fußt. Die zuständige Behörde muss gerade auch im Fall grenzüberschreitender Übermittlungen von Daten in der Lage sein, die Zuverlässigkeit der Daten abzuschätzen, um eine ermessensfehlerfreie Entscheidung zu treffen. Besonders deutlich wird dies bei Straftaten im Zusammenhang mit dem Urheberrecht oder von Cyber Crime. Maßnahmen, die ausschließlich auf automatisierter Datenverarbeitung zum Zweck der Bewertung einzelner Aspekte einer Person erfolgen (Profiling), sind grundsätzlich verboten, wenn nicht ein Gesetz die Interessen der Person wahrt (Art. 9).

Der Grundsatz der *Zweckbindung* ist in Art. 7 festgeschrieben. Die Vorschrift enthält eine Aufgabenzuschreibung an die Mitgliedstaaten und damit die Möglichkeit, Umsetzungsspielräume zu nutzen. Die bloße Aufgabenwahrnehmung einer Behörde sollte nicht für jede Datenverarbeitung genügen, sondern bedarf der Differenzierung. Anknüpfungspunkte in der Richtlinie sind die Unterscheidungen nach Kategorien von Personen und Zuverlässigkeit von Daten. Daran könnten und sollten differenzierende Vorschriften der Zweckbindung und Zweckänderung anknüpfen.

3. Betroffenenrechte

Die Richtlinie errichtet einen Mindeststandard für die Betroffenen. Die Einschränkungen des Auskunftsrechts sind durch die besonderen Aufgaben der Justiz- und Polizeibehörden zu rechtfertigen (Art. 12 ff.), die aber auch die Grenzen der Einschränkungsmöglichkeiten ziehen. So kann die Mitteilung bei heimlichen Ermittlungsmaßnahmen aufgeschoben oder ausgeschlossen werden, aber nur solange und soweit der Ermittlungserfolg gefährdet wird. Der Betroffene kann immer auch die Aufsichtsbehörde darum ersuchen, die Rechtmäßigkeit der Verarbeitung zu prüfen (Art. 14).

Die Rechte auf Berichtigung und Löschung (Art. 15, 16) sind überzeugend gefasst. Statt der Löschung können die personenbezogenen Daten markiert werden, insbesondere wenn ihre Richtigkeit überprüft werden muss. Die Kommission will den Begriff der Sperrung

nicht nutzen. Jedoch sollte die Rechtsfolge einer Markierung klar gestellt werden. Sie muss insbesondere darin bestehen, die Daten grundsätzlich nicht zu nutzen, um Grundrechtseingriffe auf der Grundlage unrichtiger Daten zu vermeiden. Ausnahmen könnten bei der unmittelbaren Gefahr der Begehung einer erheblichen Straftat erforderlich sein. Im Gegensatz zur Verordnung enthält die Richtlinie zwar kein ausdrückliches Recht auf Vergessen. Die Rechte der Betroffenen sind aber insgesamt effektiv ausgestaltet und stehen in Einklang mit Art. 8 GR-Ch (s. auch *Kugelmann*, DuD 2012, 582).

4. Grundrechtsschutz

Im Hinblick auf die Datenschutz-Grundverordnung sind erhebliche Bedenken geäußert worden, weil durch den Querschnittscharakter des Datenschutzes weite Bereiche dem Grundrechtsschutz durch das Bundesverfassungsgericht entzogen würden (*Masing*, Süddeutsche Zeitung Nr. 6 vom 9. Januar 2012, S. 10). Diese Bedenken machen an dem Charakter als Verordnung mit seiner Rechtsfolge der unmittelbaren Anwendbarkeit fest.

Demgegenüber kommen bei der Datenschutz-Richtlinie die Grundzüge des Grundrechtsschutzes zur Geltung, die das Bundesverfassungsgericht etwa in seinen Entscheidungen zum Europäischen Haftbefehl (BVerfGE 113, 273) oder zur Vorratsdatenspeicherung (BVerfGE 125, 260) entwickelt hat.

> BVerfGE 113, 273 vom 18.07.2005, DVBl. 2005, 1119 = EuGRZ 2005, 387 = DÖV 2005, 868 = NJW 2005, 2289; dazu *Tomuschat*, Ungereimtes, EuGRZ 2005, 453; *Vogel*, Europäischer Haftbefehl und deutsches Verfassungsrecht, JZ 2005, 801; vgl. Urteil des polnischen VerfG vom 27.4.2005, Az. P 1/05, EuR 2005, 494; das geänderte deutsche EuHBG vom 2.8.2006, BGBl. I, S. 1721; dazu *Böhm*, NJW 2006, 2592.
>
> BVerfGE 125, 260 vom 02.03.2010, NJW 2010, 833 = DVBl. 2010, 503 = JZ 2010, 611; dazu *Roßnagel*, Die „Überwachungs-Gesamtrechnung“ – Das BVerfG und die Vorratsdatenspeicherung, NJW 2010, 1238; *Bäcker*, Solange IIa oder BastaI?, Das Vorratsdaten-Urteil des Bundesverfassungsgerichts aus europarechtlicher Sicht, EuR 2011, 103.

Das Bundesverfassungsgericht hat seine Kontrolle auf die Vereinbarkeit der in den Umsetzungsspielraum fallenden Inhalte einer Richtlinie mit dem Grundgesetz konzentriert (*Calliess*, JZ 2009, 113, 118 f.; *Matz-Lück*, EuGRZ 2011, 207 jeweils

m.w.N.). Die Besonderheiten des Rahmenbeschlusses zum Europäischen Haftbefehl sind nach Abschaffung des Rahmenbeschlusses als Rechtsinstrument nicht mehr von Bedeutung. Das Gesetz zur Umsetzung einer Richtlinie unterliegt demnach der weit reichenden Kontrolle des Bundesverfassungsgerichts. Dieser Grundsatz gilt auch für die Umsetzung der Datenschutz-Richtlinie über Polizei und Justiz.

Über die Einzelheiten der Ausgestaltung dieses Grundsatzes besteht allerdings keine letztliche Einigkeit (*Matz-Lück*, in: dies./Hong, Hrsg., Grundrechte und Grundfreiheiten im Mehrebenensystem – Konkurrenzen und Interferenzen, 2012, S. 161, 184 ff.). Hier spielen schwierige Fragen des Grundrechtsschutzes eine Rolle. Materiell geht es um die Möglichkeit und Reichweite der parallelen Anwendbarkeit von Grundgesetz und Grundrechte-Charta. Institutionell geht es um das Verhältnis der Rechtsprechung des Bundesverfassungsgerichts zu der des EuGH. Aus der Warte des Bürgers ist die Gewährleistung des gerichtlichen Rechtsschutzes von zentraler Bedeutung, da auf europäischer Ebene kein der Verfassungsbeschwerde vergleichbares Instrument besteht, aber der Weg über das Vorabentscheidungsverfahren zum EuGH offensteht (Art. 267 AEUV).

Diese generellen Fragen könnten für die Datenschutz-Richtlinie dadurch eine besondere Note erhalten, dass der Datenschutz als Querschnittsmaterie in vielen Zusammenhängen eine Rolle spielt und die Richtlinie auch auf innerstaatliche Sachverhalte Anwendung finden soll (vgl. *Bäcker/Hornung*, ZD 2012, 152). Zur Klarstellung könnte eine Regelung in Art. 53 der Richtlinie aufgenommen werden, die eine Rahmenregelung zur Abgrenzung gerichtlicher Zuständigkeiten vornimmt, indem die Zuständigkeit des EuGH in Vorabentscheidungsverfahren über die Auslegung der Richtlinie näher beschrieben wird. Hier könnte eine Synchronisierung mit Art. 276 AEUV erfolgen, indem auf den Gebieten von Polizei und Justiz auch im Datenschutz eine Begrenzung der Zuständigkeiten des EuGH festgeschrieben wird.

5. Behördenpflichten

Die Richtlinie schreibt umfassende Informations-, Auskunfts- und Dokumentationspflichten vor. Diese müssen in der Umsetzung auf ihre praktische Durchführbarkeit und die Minimierung bürokratischen Aufwandes geprüft werden. Sie

sind aber dem Grunde nach zu begrüßen, da damit in allen Mitgliedstaaten der Union die Rechte der Betroffenen gleich effektiv sein werden.

Eine dem Grunde nach zielführende Regelung betrifft die Meldung einer Verletzung des Datenschutzes an die Aufsichtsbehörde innerhalb von 24 Stunden nach der Feststellung (Art. 28, sog. data breach notification). Sie sollte aber praxisnah ausgestaltet werden, indem etwa gestufte Zeiträume festgelegt werden. Die inhaltlichen und organisatorischen Anforderungen gehen durchaus weit. So soll die Meldung u.a. eine Beschreibung der möglichen Folgen beinhalten, Verletzungen sind zu dokumentieren. Für kleinere Polizeibehörden oder auch für Staatsanwaltschaften und Gerichte dürften derart umfassende Meldepflichten innerhalb kürzester Zeit zu praktischen Schwierigkeiten führen. Die Kommission kann zudem Durchführungsvorschriften erlassen. Zur Meldung tritt die Benachrichtigung der Person über die Datenschutzverletzung hinzu (Art. 29). Die behördlichen Datenschutzbeauftragten sollen im Rahmen ihrer starken Stellung auch die Dokumentation und die Meldung überwachen (Art. 30 ff.). In § 42a BDSG (Informationspflichten bei unrechtmäßiger Kenntniserlangung von Daten) findet sich eine zu Art. 28 der Richtlinie vergleichbare Meldepflicht, allerdings für nichtöffentliche Stellen, die den Regelungen der Art. 31, 32 DS-GVO bereits vorgreift. Im Hinblick auf öffentliche Stellen der Polizei und Justiz können aber auch Sicherheitsbelange einer unverzüglichen Meldung entgegenstehen.

6. Zuständigkeiten der Kommission, insbesondere Übermittlung von Daten an Drittstaaten

Nach der Verordnung und der Richtlinie verfügt die Europäische Kommission künftig über die Befugnis, eine Reihe von delegierten Rechtsakten und Durchführungsrechtsakten zu erlassen (Art. 56, 57 DS-RL, s. Art. 86, 87 DS-GVO). Damit wird auf Art. 290 AEUV und auf das allgemeine Komitologie-Verfahren zum Erlass abgeleiteten Rechts verwiesen (Verordnung 182/2011). Das auf Ermächtigungen aus dem Sekundärrecht der Richtlinien und Verordnungen beruhende sog. *tertiäre Recht* dient regelmäßig der insbesondere verfahrensrechtlichen Durchführung und Konkretisierung des Rechtsaktes.

Im Zusammenhang des Datenschutzes ist aber zu beachten, dass der *Grundrechtsschutz durch Organisation und Verfahren* ein wichtiges Element der Rechtswahrung des Einzelnen ist. Dies gilt für Art. 8 GR-Ch ebenso wie für das Recht auf informationelle

Selbstbestimmung nach Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG. Die Befugnisse der Kommission bedürfen der Prüfung auf ihre Vereinbarkeit mit diesen Vorgaben.

Grundsätzliche Bedenken gegen die Rolle der Kommission folgen insbesondere aus Art. 290 AEUV, wonach die *wesentlichen Aspekte* eines Bereichs dem Gesetzgebungsakt vorbehalten sind und nicht in Durchführungsrechtsakten geregelt werden dürfen (so auch *Hornung*, ZD 2012, 105 zur DS-GVO). Wesentliche politische Grundentscheidungen muss der Gesetzgeber treffen. Die Befugnisse der Kommission sind daraufhin zu prüfen und zu beschneiden (s. auch *Rogall-Grothe*, ZRP 2012, 194).

Die Berechtigung der Kommission zur tertiären Rechtssetzung betrifft z.B. die Meldepflichten (Art. 28 Abs. 5). Hier dürfte eine zulässige Durchführungsregelung vorliegen, weil die Meldepflicht in der Richtlinie ausführlich vorgegeben ist und Einzelheiten der verfahrensmäßigen Realisierung durchaus regelungsfähig sind. Dagegen geht der Erlass von Durchführungsbestimmungen, die auch Verschlüsselungsstandards regeln können (Art. 27 Abs. 3), über eine Durchführungsregelung hinaus. Derartige Regelungen sind mit eigenständigen Grundrechtseingriffen verbunden. Aus Art. 8 GR-Ch und aus Art. 290 AEUV folgt daher die Notwendigkeit einer gesetzgeberischen Entscheidung.

Ein wichtiger und schwieriger Regelungskomplex ist die *Übermittlung von Daten an Drittstaaten*. Nach Art. 41 der DS-GVO trifft die Kommission insoweit einen Angemessenheitsbeschluss. Dann ist keine weitere Genehmigung erforderlich. Ohne einen allgemeinen Beschluss prüft die Kommission das Schutzniveau und kann einen besonderen Beschluss für den Anwendungsbereich der Richtlinie fassen (Art. 34). Soweit die Übermittlung von Daten an Drittstaaten auf Vertrag beruht, führt die Kommission die Vertragsverhandlungen. Die Erfahrungen mit den Passagierdaten (PNR) und Bankdaten (SWIFT) machen deutlich, dass hier die Grundrechtssphäre der Bürger wesentlich betroffen wird. Eine alleinige Befugnis der Kommission wäre insoweit mit den Vorgaben europäischer Rechtsstaatlichkeit nicht vereinbar.

Die Übermittlung von Daten *an Drittstaaten durch Behörden der Mitgliedstaaten* im Fall des Fehlens eines Angemessenheitsbeschlusses der Kommission unterliegt dem Regime der Art. 35, 36, 37 DS-RL. Hier bestehen Unklarheiten, die noch ausgeräumt werden sollten. Nach Art. 35 ist eine Übermittlung nach den dortigen Voraussetzungen möglich.

Diese Bestimmung betrifft den regelmäßigen Datenaustausch aufgrund von Verträgen oder nach Vorschriften des innerstaatlichen Rechts (z.B. § 14 BKAG). Dagegen stellt Art. 36 eine Ausnahmebestimmung dar, die eine Datenübermittlung im Einzelfall aufgrund des Vorliegens einer qualifizierten Gefahrenlage zulässt. Allerdings wären nach dieser Konzeption die Voraussetzungen streng zu fassen und etwa Buchstabe d zu streichen. Da Art. 36 unabhängig von Art. 34 zur Anwendung gelangen soll, könnte auch gemeint sein, dass Art. 36 bei einem ablehnenden Beschluss der Kommission greift. Dann wäre erst recht eine sehr viel engere Fassung angezeigt. Auf die restriktive Handhabung der Ausnahmen ist spätestens in der Umsetzung besonderes Augenmerk zu legen.

7. Aufsichtsbehörden und Verbandsklage

Die Unabhängigkeit der Aufsichtsbehörden (Art. 40) folgt als Grundsatz aus der EuGH-Rechtsprechung.

> EuGH, Rs. C-518/07 (Kommission / Deutschland), EuGRZ 2010, 58 = K&R 2010, 326 m.Anm. *Taeger* = EuZW 2010, 296 m.Anm. *Roßnagel*; JZ 2010, 784 m. Anm. *Spiecker*; dazu *Bull*, EuZW 2010, 488.

Die Vorschriften über die personellen Voraussetzungen der Mitglieder (Art. 41) und das Errichten der Behörde (Art. 42) beeinflussen die innerstaatliche Verwaltungsorganisation und das Benennungsverfahren in erheblichem Ausmaß. Hier könnte die auf Art. 16 AEUV beruhende Kompetenz überschritten sein, da das Verwaltungsverfahren grundsätzlich der innerstaatlichen Kompetenz unterfällt. Die Befugnisse der Aufsichtsbehörden umfassen das Recht der Untersuchung, wirksame Einwirkungsbefugnisse und ein eigenständiges Klagerecht (Art. 44 ff.). Einwirkungsbefugnis bedeutet nicht notwendig ein Weisungsrecht, dies verdeutlichen die Beispiele der Stellungnahme und der Verwarnung (Art. 46).

Das *System der Datenschutzkontrolle*, das der Richtlinie zu Grunde liegt, beruht auf der Amtshilfe der Datenschutzbeauftragten und auf dem Datenschutzausschuss (Art. 48, 49). Deren Zusammenwirken soll unter der Aufsicht der Kommission stehen. Eine solche horizontale Datenschutzkontrolle in der EU hebelt die innerstaatlichen Kontrollwege aus. Infolge der Unabhängigkeit der Datenschutzbeauftragten würde ein Defizit an demokratischer Legitimation die Folge sein. Die Kontrolle der Exekutive muss aber in der Legislative verankert sein. Die innerstaatlichen Parlamente müssen ihre Verantwortung

behalten und wahrnehmen können. Eine konstruktive Teilung der Verantwortung mit dem Europäischen Parlament bedürfte der Begründung.

Verbände, deren Tätigkeit den Datenschutz zum Ziel haben, sollen Klage gegen die Aufsichtsbehörde oder die verarbeitende Behörde erheben können und zwar mit oder ohne Vollmacht des Betroffenen (Art. 50 Abs. 2, Art. 53 Abs. 1). Die Einführung der Verbandsklage führt zu der Frage, ob die Kompetenz des Art. 16 Abs. 2 AEUV das Prozessrecht umfasst, zumal auch einstweiliger Rechtsschutz gewährt werden muss (Art. 53 Abs. 3: „rasch"). Vorzugswürdig ist eine Lösung über das Verwaltungsverfahren, indem Verbände die Aufsichtsbehörden aktivieren können. Ein praktisches Bedürfnis für eine Verbandsklage besteht immerhin dann, wenn die Mitteilung an den Betroffenen unterbleibt oder zumindest beschränkt ist. Der nationale Gesetzgeber kann insoweit reagieren.

8. Fazit und Umsetzungsstrategie

Die Festlegung eines Mindeststandards an Datenschutz ist gerade auch zur Absicherung des Datenaustausches zwischen den Mitgliedstaaten ein Fortschritt. Der Grundrechtsschutz wird inhaltlich und organisatorisch verbessert. Für eine Reihe von Mitgliedstaaten dürfte dies zu einer spürbaren Verbesserung des Datenschutzes führen, diesen Vorteil gilt es zu bedenken und zu sichern. Auf die Ausgestaltung der Meldepflichten sollte in der Umsetzung besonderes Augenmerk gelegt werden, um die Regelungen für die Behörden mit angemessenem bürokratischem Aufwand durchführbar zu gestalten.

Eine Verbandsklage auf dem Gebiet des Datenschutzes kann punktuell sinnvoll sein, um den Rechtsschutz in Fällen zu ergänzen, in denen Mitteilungspflichten gegenüber dem Betroffenen ausgesetzt oder beschränkt sind. Der Kommission wird eine zu starke Rolle zugemessen. Ihre Befugnisse zum Erlass von Durchführungsrechtsakten sind mit dem europäischen Rechtsstaatsprinzip nicht vereinbar, weil sie insbesondere die Rolle des Europäischen Parlaments empfindlich berühren. Wesentliche Regelungen muss der europäische oder innerstaatliche Gesetzgeber treffen.

Die Richtlinie greift punktuell über die Gesetzgebungskompetenz des Art. 16 Abs. 2 AEUV hinaus, soweit sie im Hinblick auf Justiz und Polizei Fragen der Verwaltungsorganisation und des Prozessrechts zu stark regelt. Unklarheiten bestehen über den Anwendungsbereich, weil die verwendeten Begriffe in den Mitgliedstaaten nicht einheitlich verwendet werden.

Ein weit reichendes Verständnis des Anwendungsbereiches der Richtlinie führt dazu, dass diese Bereiche dem Anwendungsbereich der Verordnung entzogen sind (Art. 2 Ziff. 2 lit. e DS-GVO). Je mehr Einzelpunkte als Teil der Richtlinie verstanden werden, desto weniger Punkte unterfallen der vereinheitlichenden Wirkung der Verordnung. Soweit die Richtlinie umgesetzt wird, soweit bestehen auch grundrechtlich vom Bundesverfassungsgericht überprüfbare Umsetzungsspielräume. Daher sollte etwa das staatsanwaltschaftliche Ermittlungsverfahren ebenso mitgeregelt werden wie bestimmte Fragen der Gefahrenabwehr. Eine offensive Herangehensweise an die Umsetzung stärkt die spezifische Rolle und Bedeutung des Sachgebietes Polizei und Justiz.

Dieter Kugelmann

(Diese Datei wurde elektronisch versendet und ist nicht unterschrieben)