Bericht der Arbeitsgruppe des UA RV unter Beteiligung des UA FEK, UA IuK und der AG Kripo zur Darstellung und Bewertung der Auswirkungen des Vorschlags der Europäischen Kommission vom 25.01.2012 für eine

"Richtlinie des Europäischen Parlaments und des Rates 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 Strafverfolgung sowie zum freien Datenverkehr, KOM [2012] 10"

05.03.2013

Inhaltsverzeichnis

I. Anlass und Auftrag

1. Anlass

In der 32. Sitzung des UA RV am 21./22.03.2012 in Freiburg i. Br. wurde dazu unter TOP 10 folgender Beschluss gefasst:

1. Der UA RV nimmt den Bericht des Landes Bayern zur Kenntnis.
2. Er beschließt die Einrichtung einer Arbeitsgruppe, die unter Beteiligung des UA FEK, des UA IuK und der AG Kripo die Auswirkungen des Vorschlags der Europäischen Kommission vom 25.01.2012 einer "Richtlinie des Europäischen Parlaments und des Rates 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 Strafverfolgung sowie zum freien Datenverkehr, KOM (2012) 10" für die Polizeien der Länder und des Bundes in rechtlicher und polizeitaktischer Hinsicht darstellt und bewertet.
3. Nordrhein-Westfalen (Federführung), Bayern, Hamburg, der Bund sowie ggf. Sachsen-Anhalt entsenden Teilnehmer in die Arbeitsgruppe.
4. Der UA RV bittet seinen Vorsitzenden, den Beschluss zu Nrn. 1 bis 3 den Vorsitzenden des UA FEK, des UA IuK und der AG Kripo zur Kenntnis zu geben.
5. Der UA FEK, der UA IuK und die AG Kripo werden gebeten, je einen Vertreter in die Arbeitsgruppe zu entsenden.

2. Zusammensetzung der Arbeitsgruppe

Unter dem Vorsitz von Herrn RD Dr. Manuel Kamp (Ministerium für Inneres und Kommunales NRW) nahmen folgende Personen an der Arbeitsgruppe teil:
UA RV:
RD Martin Reinhard, Dr. Alexander Sindelar, Bayer. Staatsministerium des Innern
MR Eckhard Treptow, Ministerium für Inneres und Sport des Landes Sachsen-Anhalt
RR´ in Dr. Katharina Humbert, Behörde für Inneres und Sport der Freien und Hansestadt Hamburg

UA RV und UA IuK:
ORR Ralf Lesser, LL. M., Bundesministerium des Innern

UA FEK:
RR´ in Manja Barth,Bundespolizeipräsidium

AG Kripo:
RR Mirco Faßbender, Bundeskriminalamt
RR´in Elisabeth Braun, Landeskriminalamt Baden-Württemberg

3. Vorgehensweise der Arbeitsgruppe

Die Arbeitsgruppe hat Auswirkungen des Richtlinienentwurfs auf folgende Normen untersucht:

- BKAG, BPolG;
- StPO, soweit es um Regelungen geht, die unmittelbar für die Polizeiarbeit relevant sind;
- Landespolizeigesetze, exemplarisch die der an der AG teilnehmenden Länder (Bayern, Hamburg, NRW, Sachsen-Anhalt). Den MEPolG hält die AG angesichts der fehlenden Aktualität nicht für eine geeignete Grundlage einer Analyse;
- BDSG, daneben hält es die AG grundsätzlich für ausreichend, dass der jeweilige Bearbeiter exemplarisch das DSG seines Landes untersucht.

Es wurden folgende Prüfkriterien angewandt:

- Vergleich der Regelungen der Richtlinie mit den davon betroffenen Landes- und Bundesnormen: Existiert überhaupt eine entsprechende Norm im innerstaatlichen Recht? Ist sie ausreichend?
- Hieraus folgender Anpassungsbedarf?
- Folgen für Polizeitaktik?
- Folgen für Datenschutzniveau?
- Zusammenfassende Bewertung: kritische/ unkritische Richtliniennorm?

Der Bericht der vom UARV mit Umlaufbeschluss vom 12.11.2010 eingerichteten Arbeitsgruppe "Rahmenbeschluss Datenschutz: Umsetzungsbedarf und Verhältnis zu Ratsbeschluss Prüm und Rahmenbeschluss Schwedische Initiative" vom 22.08.2011 diente als wichtiges Grundlagendokument.
Neben dem Entwurf der Richtlinie wurde schon der von Herrn MdEP Droutsas, gefertigte Entwurf des Berichts des Ausschusses für bürgerliche Freiheiten, Justiz und Inneres des Europäischen Parlaments - LIBE(2012/0010 [COD]) vom 20.12.2012 und der Entwurf einer Stellungnahme des Rechtsausschusses des Europäischen Parlaments vom 04.01.2013 berücksichtigt.
Gemäß der vorstehenden Eckpunkte hat die Arbeitsgruppe die einzelnen Bestimmungen des Richtlinienentwurfs geprüft. Die Resultate sind im Detail aufgeführt (unten III.); in der Anlage sind sie tabellenförmig zusammengefasst. Die wesentlichen Ergebnisse sind um des besseren Überblicks willen vorangestellt (unten II.).
Mit Schreiben vom 05.03.2012 bat der Vorsitzende des AK II den UA RV (federführend), unter Beteiligung des UA FEK, UA IuK und der AG Kripo, um die Einrichtung einer Arbeitsgruppe. Der Prüfauftrag umfasst die Darstellung und Bewertung der Auswirkungen des Vorschlags der Europäischen Kommission vom 25.01.2012 einer "Richtlinie des Europäischen Parlaments und des Rates 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 Strafverfolgung sowie zum freien Datenverkehr, KOM [2012] 10" auf die Polizeien der Länder und des Bundes in rechtlicher und polizeitaktischer Hinsicht.

II. Wesentliche Ergebnisse

Der Entwurf der Europäischen Kommission vom 25.01.2012 für eine "Richtlinie des Europäischen Parlaments und des Rates 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 Strafverfolgung sowie zum freien Datenverkehr (KOM [2012] 10; nachstehend: RL-E) würde sich in seiner jetzigen Fassung sowohl in rechtlicher, als auch in polizeitaktischer Hinsicht deutlich spürbar auf die Tätigkeit der Polizeien von Bund und Ländern auswirken:

1) Von physischen Maßnahmen abgesehen, bedeutet Polizeiarbeit Kommunikation und Informationsaustausch. Damit ist nahezu die gesamte Tätigkeit der Polizei datenschutzrechtlichen Vorgaben unterworfen. **Eine Reformierung des Datenschutzrechts bedeutet deshalb immer auch eine Reformierung der Polizeiarbeit und ihrer Abläufe.**

2) Der RL-E soll an die Stelle des Rahmenbeschlusses 2008/977/JI treten, der nach umfassenden Beratungen erst vor wenigen Jahren in Kraft getreten ist.[1] Anders als der Rahmenbeschluss soll der RL-E nicht nur für den grenzüberschreitenden Datenaustausch innerhalb der EU gelten, sondern – deutlich weitergehend – auch verbindliche Vorgaben für innerstaatliche Datenverarbeitungen enthalten. **Die EU erhöht damit ihren Einfluss auf die Polizeiarbeit der Mitgliedstaaten in ganz erheblichem Maße.**

3) Soweit sich der Anwendungsbereich der Richtlinie auch auf innerstaatliche Datenverarbeitungen erstreckt, ist der Bundesrat der Auffassung, **dass der RL-E nicht auf die seitens KOM angegebene Rechtsgrundlage des Artikels 16 Abs. 2 des Vertrages über die Arbeitsweise der Europäischen Union (AEUV) gestützt werden kann.**[2]Die Arbeitsgruppe „EU-Datenschutzreform“ des UA RV schließt sich dieser Auffassung an.

4) Ungeachtet dieser kompetenzrechtlichen Problematik erscheint die mit dem RL-E angestrebte Harmonisierung des innerstaatlichen polizeilichen Datenschutzes auch aus fachlichen Gründen beinahe unmöglich angesichts der inhaltlichen Nähe zum Polizei- und Strafprozessrecht (siehe bereits Ziffer 1): Es besteht die **Gefahr, dass über die Vereinheitlichung des innerstaatlichen Datenschutzes eine schleichende Harmonisierung des Polizei- und Strafprozessrechts innerhalb der EU stattfindet, die weder politisch gewollt noch europarechtlich zulässig wäre. Lässt man das heterogen ausgestaltete Polizei- und Strafprozessrecht der Mitgliedstaaten hingegen unangetastet, stellt sich die Frage, wie die Har-**

[1] Der Rahmenbeschluss 2008/977/JI ist gemäß seinem Artikel 30 am 20. Januar 2009 in Kraft getreten.

[2] Beschluss des Bundesrates vom 30. März 2012 (Subsidiaritätsrüge), Drucksache 51/12.

monisierung des daran anknüpfenden polizeilichen Datenschutzrechts gelingen soll.[3] Die insoweit bestehenden Schwierigkeiten werden zu Schutzlücken führen (siehe sogleich Ziffern 9 und 10).

5) Der RL-E enthält gerade auch in seinen besonders praxisrelevanten Regelungen zahlreiche unbestimmte Rechtsbegriffe. Das erschwert seine Auslegung und in der Folge auch die Prognose des in Deutschland entstehenden gesetzgeberischen Handlungsbedarfs. Es ist wichtig zu verinnerlichen, dass hier nur auf den ersten Blick Gestaltungsfreiräume für den nationalen Gesetzgeber entstehen. Tatsächlich liegt die Interpretationshoheit beim EuGH. **Nicht der deutsche Gesetzgeber und auch nicht das BVerfG, sondern der EuGH werden darüber entscheiden, wie der RL-E auszulegen ist und ob das deutsche Recht seinen Vorgaben genügt.**

6) Zu den schwierigen, zugleich aber auch besonders praxisrelevanten Auslegungsfragen des RL-E zählt unter anderem, ob und inwieweit eine Vollharmonisierung erfolgen soll. Eine solche wäre abzulehnen. Stattdessen sollten Mindeststandards auf hohem Niveau festgelegt werden. In Fortführung der im Rahmenbeschluss 2008/977/JI.[4] verankerten Philosophie **sollten die Mitgliedstaaten auch künftig nicht daran gehindert sein, strengere nationale Datenschutzbestimmungen zu erlassen bzw. beizubehalten** als im RL-E vorgesehen. Auf diese Weise bliebe auch der in Deutschland entstehende gesetzgeberische Handlungsbedarf überschaubarer, **während im Falle einer Vollharmonisierung Bund und Länder zu Gesetzesreformen aufgefordert wären, die das bewährte Schutzniveau des deutschen Datenschutzrechts gezielt absenken müssten** (vgl. dazu etwa Ziffer 11).

7) Der Anwendungsbereich des RL-E erfasst ausschließlich Datenverarbeitungen, die „zum Zwecke der Verhütung, Aufdeckung, Untersuchung oder Verfolgung von Straftaten oder der Strafvollstreckung“ erfolgen.[5]Daraus resultieren selbst in alltäglichen Situationen polizeilicher Tätigkeit **schwierige Abgrenzungsfragen zum seitens KOM parallel vorgelegten Entwurf der Datenschutz-Grundverordnung (VO-E).** Wenn die abzuwehrende Gefahr nicht strafrechtlich relevant ist und folglich die Polizei im Rahmen ihrer Aufgabenwahrnehmung keine Straftat verhütet, bleibt der RL-E unanwendbar. Es ist davon auszugehen, dass in diesen Fällen der VO-E gelten soll, der unterschiedslos alle öffentlichen Stellen adressiert, für den Bereich der polizeilichen Datenverarbeitung jedoch völlig ungeeignet ist. **Die Tätigkeit der Polizei unterläge zwei Rechtsregimen, die in ihrer Zielrichtung, in ihrem normenhierarchischen Rang und in ihrer Bindungswirkung höchst unterschiedlich ausgestaltet sind. Komplexe Rechtsprobleme im Rahmen der Umsetzung wären die Folge.**

---

[3] Dass sich aus diesem Nebeneinander von Datenschutzrecht einerseits und Polizei- und Strafprozessrecht andererseits erhebliche praktische Schwierigkeiten ergeben können, verdeutlicht zum Beispiel Artikel 7 des Richtlinienentwurfs, der zur Beurteilung der Rechtmäßigkeit von Datenerhebungen nahezu ausschließlich an die nationalen, sehr heterogen ausgestalteten fachlichen Aufgaben und Befugnisse von Polizei und Justiz im datenverarbeitenden Staat anknüpft und damit die in diesem Bereich zwischen den Mitgliedstaaten bestehenden Unterschiede in das Datenschutzrecht inkorporiert, so dass insoweit eine datenschutzrechtliche Vereinheitlichung nicht stattfindet.

[4] Dort Artikel 1 Abs. 5 und 12.

[5] Siehe Artikel 2 Abs. 1 in Verbindung mit Artikel 1 Abs. 1 RL-E.

8) Der RL-E orientiert sich zum Teil zu stark am VO-E und dessen Regelungen zum allgemeinennicht-öffentlichen Datenschutz. An den entsprechenden Stellen lässt er infolgedessen den notwendigen polizeispezifischen Bezug vermissen. An anderer Stelle **werden Polizei und Justiz ohne ersichtlichen Grund schlechter gestellt als die vom VO-E adressierten privaten und (sonstigen) öffentlichen Stellen.**

9) Nach Artikel 1 Abs. 2 lit. b RL-E soll künftig die Berufung auf ein **abweichendes Datenschutzniveau kein zulässiges Argument mehr sein, um die Übermittlung personenbezogener Daten an einen anderen Mitgliedstaat zu verweigern oder einzuschränken**. Diese Vorschrift ist problematisch, weil sie ein EU-weit homogenes Datenschutzniveau voraussetzt, das so nicht erreichbar ist (vgl. oben Ziffer 4)(Seite 8).

10) Erschwerend kommt hinzu, dass die (weitere) Verarbeitung von zuvor EU-intern übermittelten Daten im RL-E nicht geregelt ist. Abweichend von der gegenwärtigen Rechtslage der Artikel 11 und 12 des Rahmenbeschlusses 2008/977/JI **könnten folglich personenbezogene Daten im Anschluss an eine EU-interne Übermittlung unabhängig von etwaigen, im übermittelnden Mitgliedstaat geltenden Verarbeitungsbeschränkungen genutzt werden.** Durch eine EU-interne Datenübermittlung **würden selbst zentrale Prinzipien des nationalen Gefahrenabwehr- und Strafprozessrechts „abgestreift"**, so etwa der im deutschen Recht etablierte Grundsatz, dass bestimmte Daten, die durch eine nur bei besonders schweren Straftaten zulässige geheime Maßnahme gewonnen wurden (z. B. im Rahmen einer Telefonüberwachung), in anderen Strafverfahren nur bei vergleichbar schweren Tatvorwürfen verwendet werden dürfen.

11) Die in Artikel 4 RL-E statuierten allgemeinen Grundsätze der Datenverarbeitung bedeuten **im Vergleich zu den bereichsspezifischen Regelungen** insbesondere der Artikel 3, 4, 5 und 11 **des Rahmenbeschlusses 2008/977/JI** einen Rückschritt, mit dem eine **Absenkung des Datenschutzniveaus** einhergeht. Das gilt insbesondere mit Blick auf die Zweckbindung, für die der Rahmenbeschluss 2008/977/JI strengere Vorgaben enthält. Zudem fehlen im RL-E Regelungen zur Archivierung und zur Festlegung von Lösch- und Prüffristen (Seite 10).

12) **Das in den Artikeln 8 und 9 Abs. 2 RL-E statuierte ausnahmslose Verbot einer automatisierten Verarbeitung sensibler Daten** würde zu massiven polizeitaktischen Einschränkungen führen und zur ersatzlosen Streichung der entsprechenden gesetzlichen Rechtsgrundlagen zwingen. Das Verbot derartiger Maßnahmen **würde wichtige und legitime Ermittlungsmaßnahmen wie etwa den automatisierten Abgleich von DNA-Identifizierungsmustern nach §§ 81g, 81h StPO oder den Datenabgleich zur Gefahrenabwehr ausschließen** (Seite 19 ff.).

13) In Artikel 11 Abs. 1 und Artikel 12 des Richtlinienentwurfs sind **sehr weitgehende Informations- und Auskunftspflichten** der Behörden vorgesehen, die dem Betroffenen keinen spürbaren Mehrwert bieten, gleichzeitig jedoch einen erheblichen zeitlichen und bürokratischen Aufwand bedeuten und das verwaltungsrechtliche Verfahren erschweren. Hier entstünde **ganz erheblicher gesetzlicher Änderungsbe-**

darf mit weitreichenden Auswirkungen auf den polizeilichen Alltag, der in hohem Maße bürokratisiert würde (Seite 24 ff.).

14) Die **Regelungen zur Datenübermittlung in Drittstaaten** (Artikel 33 ff. RL-E) gewähren der Kommission weitreichende Kompetenzen und **schränken** – spiegelbildlich hierzu – **die Befugnisse der Mitgliedstaaten und deren Polizeien in erheblichem Umfang ein.** Ob personenbezogene Daten an Empfänger in Drittstaaten übermittelt werden dürfen, soll künftig grundsätzlich allein und in abstrakt-genereller Weise von der Kommission entschieden werden. **Dies würde zu erheblichem gesetzlichen Änderungsbedarf und polizeitaktischen Beeinträchtigungen führen**. Bestehende Vorschriften des nationalen Rechts, die wie zum Beispiel § 14 BKAG eine Abwägung der im Einzelfall betroffenen Interessen durch die zuständige Behörde vorsehen, wären weitestgehend ausgeschlossen (Seite 55 ff.)

15) Nach Artikel 60 RL-E müssen die von den Mitgliedstaaten bisher geschlossenen internationalen Übereinkünfte „erforderlichenfalls“ innerhalb von fünf Jahren nach Inkrafttreten des RL-E geändert werden. Diese Vorschrift wird im Bereich der internationalen Zusammenarbeit in polizeitaktisch bedenklicher Weise zu Rechtsunsicherheit führen, da sie die Wirksamkeit bestehender internationaler Abkommen aktiv in Frage stellt. **Zudem droht eine arbeitsintensive Wiederaufnahme völkerrechtlicher Verhandlungen, die bestenfalls in Umsetzungsgesetze von Bund und Ländern münden, unter Umständen aber auch eine Verschlechterung des Status quo der internationalen polizeilichen Zusammenarbeit zum Ergebnis haben können** (Seite 75).

16) Mit den Artikeln 50 ff. RL-E soll ein **Verbandsklagerecht** eingeführt werden. Einrichtungen, Organisationen und Verbände soll es zukünftig möglich sein, Beschwerde zu erheben oder „im Namen einer oder mehrerer betroffenen Personen“ zu klagen. Ein vergleichbares Instrument ist **im deutschen Recht bislang nicht vorgesehen**, das für die Überprüfung polizeilicher Maßnahmen stets eine individuelle Betroffenheit voraussetzt. **Insoweit wären Bund und Länder zu Gesetzesanpassungen aufgefordert, die ihrerseits zu einem deutlich spürbaren Anstieg gerichtlicher Verfahren gegen die Polizei führen könnten** (Seite 70 ff.).

17) Der von Herrn **MdEP Droutsas**,gefertigte **Entwurf des LIBE-Berichts** (2012/0010 [COD]) ist sehr **kritisch** zu sehen. Er strebt eine **weitereAnnäherung an die Regelungen des VO-E** an, die jedoch naturgemäß den bereichsspezifischen Bezug missen lassen und **für den Polizei- und Justizbereich daher völlig ungeeignet** sind. In der Folge würden der Polizei wichtige Befugnisse genommen (z. B. auch die Möglichkeit automatisierter Abrufverfahren). Zudem würden die Vorschläge die ohnehin schon gegebene Bürokratielastigkeit des RL-E weiter verschärfen. Erschwerend kommt hinzu, dass die im Berichtsentwurf vorgeschlagenen Änderungen häufig kompliziert formuliert sind. Das Zusammenspiel der verschiedenen Vorschriften des RL-E würde noch unübersichtlicher. Insgesamt ergeben sich aus dem Berichtsentwurf daher sowohl für den deutschen Gesetzgeber, als auch in polizeitaktischer Hinsicht **zusätzlicheProbleme**.

III. Umsetzungsbedarf im Hinblick auf die Einzelregelungen
Kapitel I Allgemeine Bestimmungen

Artikel 1 Gegenstand und Ziele

Artikel 1 definiert den Gegenstand der Richtlinie, d. h. es werden die Bestimmungen für die Verarbeitung personenbezogener Daten zum Zwecke der Verhütung, Aufdeckung, Untersuchung oder Verfolgung von Straftaten festgelegt; ferner wird das zweifache Ziel der Richtlinie dargelegt, die Grundrechte und Grundfreiheiten natürlicher Personen und insbesondere ihr Recht auf den Schutz personenbezogener Daten zu schützen und gleichzeitig ein hohes Maß an öffentlicher Sicherheit sowie den Austausch personenbezogener Daten zwischen zuständigen Behörden in der Europäischen Union zu gewährleisten. Der Richtlinienentwurf wirkt sich somit u.a auf die in der StPO, den Datenschutzgesetzen und den Polizeigesetzen bereits bestehenden Regelungslagen aus. Das auch betroffene Strafvollstreckungsrecht wird bei der Bewertung im Hinblick auf die vorrangige Zuständigkeit der Justizverwaltung nicht berücksichtigt. Es wird ferner davon ausgegangen, dass auch die Verfolgung und Ahndung von **Ordnungswidrigkeiten** vom Anwendungsbereich der Richtlinie nicht erfasst wird. Der Begriff der Straftat dürfte eng auszulegen sein. Insoweit wird auf die Ausführungen im Bericht zum Rahmenbeschluss Datenschutz Bezug genommen (vgl. Bericht zum Rahmenbeschluss Datenschutz, Stand: 22.8.2011, S. 7).
Der Vorschlag der Richtlinie und somit auch der Anwendungsbereich stützt sich auf Artikel 16 Abs. 2 AEUV, einer durch den Lissabonner Vertrag eingeführten neuen, spezifischen Rechtsgrundlage für Vorschriften über den Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die Organe, Einrichtungen, Ämter und Agenturen der Europäischen Union und durch die Mitgliedstaaten sowie bei der Ausübung von Tätigkeiten, die in den Anwendungsbereich des Unionsrechts und der Vorschriften über den freien Datenverkehr fallen. Der Vorschlag zielt darauf ab, ein hohes, einheitliches Datenschutzniveau in diesem Bereich zu garantieren und damit das gegenseitige Vertrauen zwischen den Polizei- und Justizbehörden verschiedener Mitgliedstaaten zu stärken und den freien Datenverkehr und die Zusammenarbeit zwischen Polizei- und Justizbehörden zu erleichtern.
Rein innerstaatliche Datenverarbeitungsvorgänge liegen aber nach hiesiger Auffassung außerhalb der Gesetzgebungskompetenz der EU. Artikel 16 Abs. 2 AEUV gilt nur für Tätigkeiten, die in den Anwendungsbereich des Unionsrechts fallen. Dies ist für den Bereich der innerstaatlichen Datenverarbeitung zu Zwecken der Strafverfolgung oder der Gefahrenabwehr nicht der Fall, da Artikel 87 Abs. 2 Buchstabe a AEUV der EU lediglich Maßnahmen gestattet, die der Entwicklung einer polizeilichen Zusammenarbeit zwischen allen zuständigen Behörden der Mitgliedstaaten dienen(vgl. u.a. auch Ausführungen des Bundesrates in Drsn. 51/1/12, 51/12 und 51/12 [B] [2]).

Für eine Erstreckung der Richtlinie auf die innerstaatliche Datenverarbeitung von Polizei und Justiz besteht zudem kein fachlicher Bedarf. Unter anderem aus diesem Grund hat der Rahmenbeschluss Datenschutz für die ehemals 3. Säule bewusst hierauf verzichtet.

Neben der Verfolgung und Verhütung von Straftaten, die nach Artikel 1 Abs. 1 von dem Richtlinienentwurf umfasst sind, gehört zu den Aufgaben der Polizeibehörden auch die nichtstraftatenbezogene Gefahrenabwehr. Die Verhütung von Straftaten ist nur ein kleiner Teil der Gefahrenabwehr. Dieser sehr wichtige Teil der polizeilichen Aufgabenerfüllung ist nach hiesiger Lesart vom Anwendungsbereich der Richtlinie nicht umfasst. Zugleich hat die KOM aber einen Vorschlag für eine Verordnung zum Datenschutz und zum freien Datenverkehr (Datenschutz-Grundverordnung) vorgelegt, der neben nicht-öffentlichen auch öffentliche Stellen adressiert. Diesbezüglich ist nicht auszuschließen, dass Aufgaben der polizeilichen Gefahrenabwehr, die nicht in der Verhütung von Straftaten bestehen, von der für den Bereich der polizeilichen Datenverarbeitung nicht passenden Grundverordnung erfasst würden. Angesichts der Tatsache, dass bei der Gefahrenabwehr zwischen der Verhütung von Straftaten und „sonstigen" Gefahrenabwehr oftmals nicht trennscharf unterschieden werden kann, ist dies nicht hinnehmbar. Inwieweit je nach Tradition der Mitgliedstaaten Aufgaben als polizeiliche Aufgaben verstanden werden, dürfte innerhalb der Mitgliedstaaten auch unterschiedlich beurteilt werden. Es sollte vermieden werden, dass dieselbe Tätigkeit in einem Mitgliedstaat der Verordnung und in einem anderen Mitgliedstaat der Richtlinie unterfällt. **Hier ist eine klare Abgrenzung des Anwendungsbereichs der beiden Rechtsakte dringend erforderlich** (so auch BR-Drsn. 51/1/12, 51/12 und 51/12 (B) (2)). Der Rechtsausschuss des Europäischen Parlaments hat mit seinem Entwurf einer Stellungnahme vom 04.01.2013 auch bereits einen Änderungsantrag zu Artikel 1 Abs. 1 gestellt:

> *Diese Richtlinie enthält Bestimmungen zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die zuständigen Behörden zum Zwecke der Verhütung von Gefahren, der Aufdeckung, Untersuchung oder Verfolgung von Straftaten sowie der Strafvollstreckung.*

Er begründet dies wie folgt:

> *Bei der polizeilichen Gefahrenabwehr gibt es Schwierigkeiten bei der Abgrenzung der Anwendungsbereiche von Richtlinie und Verordnung. Wenn die abzuwehrende Gefahr nicht strafbewehrt ist und folglich die Polizei keine Straftat im Sinne von Artikel 1 Abs. 1 des Richtlinienentwurfs verhütet, bleibt die Richtlinie unanwendbar (Beispiele: Datei für vermisste Personen, Selbstmörder). Die Vorschriften der Datenschutz-Grundverordnung sind für die Gefahrenabwehr völlig unpassend.*

Nach Artikel 1 Abs. 2 lit. b soll künftig der Austausch personenbezogener Daten nicht mehr „aus Gründen des Schutzes natürlicher Personen bei der Verarbeitung personenbezogener Daten" eingeschränkt oder verboten werden können. Dies ist wohl so zu interpretieren, dass die Berufung auf ein abweichendes Datenschutzniveau zukünftig kein zulässiges Argument mehr sein soll, die Übermittlung personenbezogener Daten an einen anderen Mitgliedstaat zu verbieten oder einzuschränken. **Eine**

solche Vorschrift wäre problematisch, weil sie ein EU-weit homogenes Datenschutzniveau voraussetzt, das nur schwerlich zu erreichen sein dürfte. Folge wäre, dass das hohe deutsche Datenschutzniveau durch die Übermittlung an einen Mitgliedstaat mit geringerem Datenschutzniveau ausgehebelt werden könnte/würde. So könnten z.B. auch nach deutschem Recht geltende Verwendungsbeschränkungen (z.B. bei Daten aus der Telekommunikationsüberwachung) durch eine Übermittlung ins EU-Ausland „abgestreift" werden. Der Rahmenbeschluss hat diesbezüglich genaue Regelungen vorgesehen, nach denen Beschränkungen beachtet werden müssen.

Artikel 2 Anwendungsbereich

Artikel 2 bestimmt den Anwendungsbereich der Richtlinie. Der Anwendungsbereich der Richtlinie ist nicht auf grenzübergreifende Datenverarbeitung beschränkt, sondern umfasst alle Verarbeitungen, die von „zuständigen Behörden" (gemäß der Definition in Artikel 3 Nr. 14) für die Zwecke dieser Richtlinie durchgeführt werden. Die Richtlinie gilt weder für eine Verarbeitung im Rahmen von Tätigkeiten, die nicht in den Bereich des Unionsrechts fallen, noch für eine Verarbeitung durch die Organe, Einrichtungen, Ämter und Agenturen der Europäischen Union, die in der Verordnung (EG) Nr. 45/2001 und anderen spezifischen Rechtsvorschriften geregelt ist.
Artikel 2 Abs. 2 beansprucht, den Anwendungsbereich im Hinblick auf die Umstände der Verarbeitung zu bestimmen. Der Wortlaut zumindest der deutschen Fassung lässt es im Unklaren, ob auch Akten von dem Anwendungsbereich der Richtlinie umfasst sind. **Diesbezüglich bedarf es einer Klarstellung.**Der Rechtsausschuss des Europäischen Parlaments ergänzt mit dem Entwurf seiner Stellungnahme vom 04.01.2013 Art 2 Abs. 2 dahingehend, dass die *Richtlinie keine Anwendungfinden soll, wenn die personenbezogenen Daten in Akten oder Aktensammlungen gespeichert sind oder gespeichert werden sollen, die in Papierform geführt werden.*
Ebenso wie die Verordnung nach deren Artikel 2 Abs. 2 lit. a findet auch die Richtlinie gemäß Artikel 2 Abs. 3 lit. a keine Anwendung auf die Verarbeitung personenbezogener Daten im Rahmen einer Tätigkeit, die nicht in den Anwendungsbereich des Unionsrechts fällt, etwa im Bereich der nationalen Sicherheit. Weder die Verordnung oder die Richtlinie selbst, noch deren Begründungen geben jedoch Hinweise, wie der Begriff „nationale Sicherheit" verstanden werden soll. **Eine Präzisierung erscheint zwingend erforderlich.**
Nach Artikel 2 Abs. 3 lit. b ist die Verarbeitung personenbezogener Daten durch die Organe, Einrichtungen, Ämter und Agenturen der Europäischen Union nicht vom Anwendungsbereich der Richtlinie umfasst. **Dies weicht von Artikel 1 Abs. 2 des Rahmenbeschlusses 2008/977/JI ab und ist nicht nachvollziehbar**. Allein die Tatsache, dass die Regelungen für die im gefahrenabwehrrechtlichen und strafprozessualen Bereich tätigen EU-Institutionen rechtstechnisch nicht in die Richtlinie selbst, sondern in eine gesonderte weitere Verordnung eingehen müssten, ist kein Grund für eine inhaltliche Herausnahme aus den Vorgaben der Richtlinie. Gleiches gilt für die behauptete bestehende Existenz eines hohen Datenschutzniveaus in den Organen: Dies bedeutete lediglich, dass der Umsetzungsbedarf gering wäre.Der

Entwurf einer Stellungnahme des Rechtsausschusses des Europäischen Parlaments vom 04.01.2013 sieht bereits eine Streichung des Artikels 2 Abs. 3 lit. b vor.

Artikel 3 Begriffsbestimmungen

Artikel 3 enthält die Begriffsbestimmungen. Einige Begriffsbestimmungen wurden von der Richtlinie 95/46/EG und dem Rahmenbeschluss 2008/977/JI übernommen, andere wurden abgeändert, ergänzt oder neu eingeführt. Die neuen Begriffsbestimmungen sind: „Verletzung des Schutzes personenbezogener Daten“, „genetische Daten“, „zuständige Behörden“ (gemäß Artikel 87 AEUV und Artikel 2 lit. h des Rahmenbeschlusses 2008/977/JI) und „Kind“ (im Sinne der UN-Kinderrechtskonvention). Mit Ausnahme des Artikels 3 Nr. 13 („Kind“) werden im Hinblick auf die bereits geltende Rechtslage (vgl. Anlage) weder Regelungsdefizite gesehen, noch sind - jedenfalls durch die bloße Begriffsbestimmungen als solche - polizeitaktische Folgen erkennbar. Zwar enthalten die geltenden Datenschutzgesetze keine expliziten Definitionen von „genetischen, biometrischen und Gesundheitsdaten“, jedoch umfassen die geltenden Definitionen von personenbezogenen Daten unproblematisch auch diese Begrifflichkeiten (vgl. Anlage). Als äußerst problematisch erweisen sich jedoch die Datenverarbeitungsverbote der Artikel 8 und 9, die an die Legaldefinition der „genetischen Daten“ anknüpfen (siehe dazu dort).
Kritisch ist jedoch die im Richtlinienentwurf enthaltende Definition des „Kindes“ zu betrachten. Ungeachtet des von der deutschen Rechtslage grundsätzlich abweichenden Alters (vgl. Anlage), sind an den Entwurf der Richtlinie keine spezifischen Verarbeitungsregeln bzw. Schutzgarantien geknüpft. Lediglich Artikel 45 Abs. 2 erwähnt in einem anderen Zusammenhang die besondere Stellung des Kindes. Nach hiesiger Auffassung sollte die Definition des „Kindes“ gestrichen werden.
Soweit bekannt, sind im überarbeiteten Entwurf der Verordnung bereits Änderungen der Begriffsbestimmungen erfolgt. So wurden die Definitionen von „personenbezogenen Daten“ und „betroffener Person“ zusammengelegt und die Begriffsbestimmung von „Kind“ wurde gestrichen. Es steht zu erwarten, dass diese Änderungen auch in der Richtlinie Eingang finden.

Kapitel II Grundsätze

Artikel 4 Grundsätze in Bezug auf die Verarbeitung personenbezogener Daten

Ausweislich der Richtlinienbegründung enthält Artikel 4 RL-E die für die Verarbeitung personenbezogener Daten geltenden Grundsätze entsprechend Artikel 6 der Richtlinie 95/46/EG sowie Artikel 3 des Rahmenbeschlusses 2008/977/JI (Rahmenbeschluss). Im Vergleich zu den bereichsspezifischen Regelungen des Rahmenbeschlusses, insbesondere den Artikeln 3, 4, 5 und 11 hieraus, bedeutet diese Rückkehr zu den allgemeinen Formulierungen der Datenschutzrichtlinie für den polizeilichen und justiziellen Bereich einen Rückschritt, mit dem eine Absenkung des Schutzniveaus einherzugehen droht. Der RL-E bleibt in vielen Fällen ungenau und

wirft hierdurch Auslegungsfragen auf. Auch fehlen z. B. Regelungen zur Archivierung und zur Festlegung von Lösch- und Prüffristen.
Die in Artikel 4 des RL-E sehr allgemein gehaltenen Grundsätze sind im Wesentlichen bereits im deutschen Recht realisiert (vgl. StPO, BKAG, BDSG, PolG BW, LDSG BW, BPolG, SOG LSA, HmbPolDVG, PolG NRW) und würden jedenfalls bei einem Verständnis des RL-E als Mindeststandard grundsätzlich keinen gesetzgeberischen Handlungsbedarf in Deutschland begründen.

Im Einzelnen gibt es zu den verschiedenen Absätzen folgende Anmerkungen:

In Artikel 4 a RL-E wird der Grundsatz verankert, dass die Verarbeitung personenbezogener Daten nach Treu und Glauben und auf rechtmäßige Weise zu erfolgen hat. Der Grundsatz von Treu und Glauben entstammt dem Zivilrecht und ist dem Bereich der Eingriffsverwaltung fremd. Die Strafverfolgungsbehörden als Teil der vollziehenden Gewalt sind an Recht und Gesetz gebunden.[6] Es gelten die Grundsätze des Vorbehalts und des Vorrangs des Gesetzes. Polizeiliches und justizielles Handeln bedarf somit einerseits immer einer gesetzlichen Grundlage und andererseits dürfen die getroffenen Maßnahmen einem Gesetz nicht widersprechen. **Ein Regelungsdefizit ist nicht erkennbar**. Die vom Ausschuss für bürgerliche Freiheiten, Justiz und Inneres des Europäischen Parlaments (LIBE)[7]mit dem Änderungsantrag Nr. 52 geforderte Ergänzung von Artikel 4 a RL-E in der Weise, dass die Verarbeitung in einer für die betroffene Person nachvollziehbaren Weise zu erfolgen hat, können in der formu-lierten Absolutheit für den Bereich der Verfolgung und vorbeugenden Bekämpfung von Straftaten keine Anwendung finden. So widerspricht dies u. a. Sinn und Zweck von verdeckten Maßnahmen sowie deren Speicherungen in Dateien.
Die Regelung in der von der Kommission vorgelegten Form ist als unkritisch zu bewerten, die Ergänzung des LIBE jedoch abzulehnen.
Die Regelung des Artikels 4 b RL-E betrifft zum einen die Erhebung personenbezogener Daten für genau festgelegte, eindeutige und rechtmäßige Zwecke und zum anderen die Unzulässigkeit der Weiterverarbeitung in einer mit den festgelegten Zwecken nicht zu vereinbarenden Weise. Auch diese Grundsätze liegen der Datenerhebung und Datenverarbeitung im deutschen Recht zugrunde und sind in den einschlägigen Gesetzen realisiert (vgl. StPO, BKAG, BDSG, PolG BW, LDSG BW, BPolG, SOG LSA, HmbPolDVG, PolG NRW).
Die im deutschen Recht gesetzlich geregelten Zweckänderungen bzw. Zweckumwidmungen, werden hierbei nicht als unvereinbare Weiterverarbeitung im Sinne von Artikel 4 b 2 HS RL-E gewertet. Die umfassendere Formulierung des Rahmenbeschlusses, die speziell auf Zweckänderungen bzw. Zweckumwidmungen eingeht, wurde jedoch nicht übernommen. Bei einer an Artikel 3 des Rahmenbeschlusses an-

[6] Bundesrat Drucksache 51/12 (Beschluss) (2), Nr. 8.
[7] Entwurf eines Berichts über den Vorschlag für eine Richtlinie des Europäischen Parlaments und des Rates 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 Strafvollstre-ckung sowie zum freien Datenverkehr, - 2012/0010 [COD]) -

gelegten Auslegung wäre **kein Regelungsdefizit** für Artikel 4 b RL-E gegeben. Die von LIBE mit dem Änderungsantrag Nr. 11 geforderte Ergänzung der Erwägungen würde jedoch zu einer restriktiveren Auslegung des Artikel 4b RL-E führen. Dies hätte Auswirkungen auf die bestehenden gesetzlichen Vorschriften zu den Zweckänderungen bzw. Zweckumwidmungen und somit auch auf die polizeiliche Praxis. **Es würde beträchtlicher Regelungsbedarf bestehen.**
Die Auslegung in Anlehnung an den Änderungsantrag Nr. 57 wird somit als kritisch bewertet.
Der in Artikel 4 c RL-E geregelte Grundsatz der Verhältnismäßigkeit der Datenverarbeitung (angemessen, sachlich relevant und nicht exzessiv) ist ebenfalls ein dem deutschen Recht der Eingriffsverwaltung zugrundeliegender Grundsatz. Ein Regelungsdefizit ist nicht gegeben. Auch die mit dem Änderungsantrag Nr. 53 vom LIBE geforderte Ergänzung von Artikel 4 c RL-E wird als unkritisch bewertet. Sie trägt lediglich dem datenschutzrechtlichen Grundsatz der Erforderlichkeit Rechnung. **Die Regelung ist somit als unkritisch zu bewerten. Auswirkungen auf die polizeiliche Arbeit sind nicht zu erwarten.**
Artikel 4 d 1 HS RL-E regelt, dass personenbezogene Daten sachlich richtig und – wenn nötig – auf dem neuesten Stand sein müssen, und dass alle angemessenen Maßnahmen getroffen werden müssen, damit personenbezogene Daten, die im Hinblick auf die Zwecke ihrer Verarbeitung unzutreffend sind, unverzüglich gelöscht oder berichtigt werden. Dieser Grundsatz ist in der Weise realisiert, dass bei einem Fehlen der Datenrichtigkeit die Pflicht zur Löschung, Berichtigung oder Sperrung geregelt ist (vgl. § 489 StPO, §§ 32, 33 BKAG, § 20 BDSG, § 46 PolG BW, § 22 LDSG BW, § 35 BPolG, § 16 SOG LSA, § 24 HmbPolDVG, § 45 PAG BY, § 32 PolG NRW, § 27 HSOG). Eine Regelung der im deutschen Recht vergleichbaren Sperrung ist im RL-E nur in Artikel 3 Nr. 4 (Begriffsbestimmung) sowie in Artikel 16 Nr. 3 (im Hinblick auf die Rechte von Betroffenen) in Form der „Markierung“ vorgesehen. Artikel 4 d RL-E sieht hingegen keine generelle Regelung zur Markierung bzw. Sperrung als Ausnahmeregelung zur Löschung vor. Die in Artikel 16 Nr. 3 RL-E eingefügte Regelung zur Markierung ist darüber hinaus in ihrem Regelungsgehalt enger, als die in den deutschen Vorschriften enthaltenen gesetzlichen Normierungen zur Sperrung (vgl. u. a. § 33 Abs. 3 und 4 BKAG, § 35 Abs. 6 BPolG, § 23 Abs. 4 LDSG BW). Vergleiche hierzu im Detail auch die Ausführungen zu Artikel 16 RL-E.
Um die Regelungen zur Sperrung als Ausnahmeregelung zur Löschung vollumfänglich beibehalten zu können, wäre eine Änderung des RL-E erforderlich. Erfolgt dies nicht, würden die Handlungsbefugnisse der Polizei in diesen Fällen eingeschränkt. Praktisch relevant würde dies etwa werden, wenn eine Löschung unmöglich oder aber – z.B. mangels technischer Möglichkeit eines selektiven Zugriffs auf einzelne Datensätze innerhalb eines umfangreichen Backup – nur mit unverhältnismäßigem Aufwand durchführbar ist. Ungeklärt bleibt im RL-E desweiteren das Verhältnis der Löschungsverpflichtung zu etwaigen Aufbewahrungs- und Archivierungspflichten.**Es handelt sich nach polizeilicher Bewertung somit um eine kritische Vorschrift, die Auswirkungen auf die polizeiliche Praxis hätte**.

Artikel 4 e regelt die zeitliche Befristung der Verarbeitung im Rahmen der Erforderlichkeit mit Identifizierungsmöglichkeit des Betroffenen. Dieser Grundsatz ist in den Polizeigesetzen der Länder und des Bundes sowie der Strafprozessordnung durch die Vergabe von Prüffristen bzw. der Erforderlichkeit der Aufgabenwahrnehmung geregelt (vgl. u.a. §§ 37, 38 PolG BW, 29 BPolG, § 32 BKAG, § 489 Abs. 4 und 5 StPO). Eine Identifizierungsmöglichkeit des Betroffenen ist regelmäßig gegeben (vgl. § 37 Abs. 1 PolG BW). **Die Vorschrift wird als unkritisch bewertet auch unter Berücksichtigung der partiellen Neufassung durch den Änderungsantrag Nr. 55 von LIBE.**

Artikel 4 f regelt die Verantwortlichkeit des Datenverarbeiters. Auch dieser Grundsatz ist im deutschen Recht entsprechend umgesetzt. Ein Umsetzungsbedarf wird nicht gesehen (vgl. hierzu § 12 BKAG, § 490 StPO, § 3 Abs. 7 BDSG).Der LIBE-Änderungsvorschlag Nr. 56 verlangt darüber hinaus, dass für jeden Verarbeitungsvorgang ein Nachweis zu erbringen ist. Wie dieser Nachweis auszusehen hat, bleibt unklar, ebenso wie die Rechtsfolgen, die ein Verstoß gegen diese Vorschrift nach sich ziehen soll. Zwar besteht grundsätzlich die Pflicht zur Dokumentation polizeilichen Handelns, ob diese jedoch den von LIBE geforderten Anforderungen des Nachweises genügt, ist ungewiss. **Aus diesem Grund ist die Einfügung kritisch zu bewerten.**
Der Änderungsvorschlag Nr. 57 von LIBE, beschränkt den Zugriff personenbezogener Daten auf bevollmächtigte Mitarbeiter, die die Daten zur Aufgabenwahrnehmung benötigen. Da die Zugriffsberechtigung für Dateien üblicherweise durch eine entsprechende Berechtigungsvergabe geregelt ist und diese Ausfluss des Grundsatzes der Erforderlichkeit ist, **erscheint dieErgänzung unproblematisch.**

Artikel 4 a Zugang zu Daten, die ursprünglich zu anderen Zwecken als den in Artikel 1 Abs. 1 genannten Zwecken verarbeitet wurden

Die mit dem Änderungsantrag Nr. 58 geforderte Einfügung eines neuen Artikels 4 a, der den „Zugang“ zu Daten, die ursprünglich zu anderen Zwecken als den in Artikel 1 Abs. 1 genannten verarbeitet wurden (z. B. Melderegister, Waffenregister, Verkehrsregister etc.) regeln soll, **wird ebenfalls sehr kritisch bewertet.** Die Begrifflichkeit des „Zugangs“ wird in Artikel 3 RL-E nicht definiert, eine Ergänzung durch LIBE wurde nicht vorgenommen. Bei datenschutzrechtlicher Bewertung könnte es sich hierbei um die „Erhebung“ personenbezogener Daten aus polizeifremden und polizeilichen Dateien zur Gefahrenabwehr handeln. Automatisierte Abrufverfahren, die für viele Bereiche bereits gesetzlich geregelt sind, wären nach Nummer b unter Umständen nicht mehr zulässig, da die Anfragen schriftlich zu erfolgen haben. Ob eine Protokollierung der Anfrage die geforderte Schriftlichkeit erfüllt, darf bezweifelt werden, ist zumindest aber unklar. Darüber hinaus werden neben speziellen Rechtsgrundlagen für die Erhebung, weitere Voraussetzungen gefordert (z. B. geeignete Garantien), die in Ergänzung zu den ohnehin spezifischen Zugangsbedingungen zu gelten haben. **Die Einfügung dieser Vorschrift würde zu beträchtlichem Regelungsbedarf führen, die polizeiliche Arbeit erschweren und einen erheblichen verwaltungs-**

technischen Mehraufwand darstellen.Die Neueinfügung ist abzulehnen und wird als äußerst kritisch bewertet.

Artikel 4 b Fristen für die Speicherung und Überprüfung
Im LIBE - Änderungsantrag Nr. 59 wird zunächst gefordert, dass personenbezogene Daten zu löschen sind, wenn sie nicht länger für den Zweck, den die ursprüngliche Verarbeitung erfüllen sollte, erforderlich sind. Dies würde die bisherige Möglichkeit zur Weiterspeicherung nach Zweckumwidmung in erheblichem Maße einschränken und hätte **gravierende Auswirkungen für die polizeiliche Praxis (insbesondere für die Weiterspeicherung zur vorbeugenden Bekämpfung von Straftaten).**
Zum anderen sollen verschieden Personenkategorien unterschiedliche Speicherfristen zugewiesen sowie eine Überwachung dieser Fristen gewährleistet werden. Diese Forderung wurde bereits im Rahmenbeschluss realisiert und ist im deutschen Recht umgesetzt (vgl. hierzu auch die Anmerkungen zu Artikel 5). **Die Einfügung erscheint unproblematisch.**

Artikel 5 Unterscheidung verschiedener Kategorien von betroffenen Personen

Artikel 5 RL-E sieht vor, dass in Dateien „soweit wie möglich“ zwischen den personenbezogenen Daten fünf verschiedener Kategorien von Personen zu unterscheiden ist. Unterschieden wird hierbei nach den Personenrollen Tatverdächtige/Beschuldigte/potentielle Straftäter, verurteilte Straftäter, Opfer/potentielle Opfer, Zeugen/Hinweisgeber/Kontakt- und Begleitpersonen zu den genannten Kategorien und sonstige Personen, die keiner genannten Kategorie zugeordnet werden können.
Umgesetzt ist dies in den Polizeigesetzen der Länder durch Regelungen, die bei Speicherungen in Dateien die Erkennbarkeit der Personengruppen vorschreiben (vgl. explizit geregelt in § 37 Abs. 1 PolG BW, Voraussetzung für die Vergabe unterschiedlicher Aussonderungsprüffristen bzw. Speicherfristen z. B. § 32 BKAG, § 29 BPolG, § 15 HmbPolDVG, § 24 PolG NRW etc.). Darüber hinaus besteht bei automatisierten Dateien die Verpflichtung zur Erstellung von Verfahrensverzeichnissen bzw. Errichtungsanordnungen, in welchen der Kreis der von den Speicherungen Betroffenen auszuweisen ist (§ 490 StPO, § 34 BKAG, §§ 4d, e BDSG, §§ 37 Abs. 1, 38 Abs. 6 PolG BW bzw. § 48 i.V.m. § 11 LDSG BW, § 36 BPolG, § 14 DSG LSA, § 26 HmbPolDVG, Artikel 47 PAG BY, § 8 DSG NRW).
Problematisch erscheint jedoch, dass die Reichweite des Artikels 5 RL-E unklar bleibt. Die Vorschrift dürfte als allgemeiner Grundsatz weit über die eben genannten, im deutschen Recht bereits umgesetzten Fallkonstellationen hinausgehen. Insoweit droht ein im Einzelnen nicht überschaubarer Regelungsbedarf sowie daran anknüpfend eine polizeiliche Praxis, die unabhängig vom konkreten Nutzen für den Betroffenen zu sehr weitgehenden, bürokratischen Differenzierungen gezwungen wird. Ob und welche Rechtsfolgen sich aus der Kategorisierung oder dem Fehlen einer solchen Kategorisierung ergeben, ist bei alledem nicht erkennbar (im Unterschied hierzu werden z. B. in den aufgezählten Landes- und Bundesgesetzen an die unterschiedlichen Personenrollen u. a. unterschiedliche Speichervoraussetzungen, Fristen etc. geknüpft). Infolgedessen wird auch nicht deutlich, welche Rechtsfolgen

ein Verstoß gegen diese Vorschrift nach sich ziehen würde (z. B. mögliche Konsequenz: Verfahrensfehler im Strafprozess).
Soweit in den polizeilichen Dateien (z. B. in den Inpol-Fall-Dateien, in Inpol-Zentral, in den Inpol-Land-Dateien und in den Vorgangsbearbeitungssystemen) bereits heute überwiegend nach Personenrollen unterschieden wird, wird kein größerer Umsetzungsbedarf durch die Polizei gesehen. Ob der abstrakt-generellen Regelung des Artikel 5 RL-E ohne konkrete Rechtsfolgenverweisung bleibt die Erforderlichkeit einer solchen Regelung jedoch fraglich.
Aufgrund der Unbestimmtheit der Regelung und der zurzeit nicht absehbaren Rechtsfolgen bei Verstößen gegen den Artikel 5 RL-E kann der mögliche Umsetzungsbedarf für die Polizei nicht konkretisiert werden. Die Regelung wird deshalb aus polizeilicher Sicht kritisch bewertet.
Mit dem Änderungsantrag Nr. 61 fordert LIBE darüber hinaus eine Ergänzung des Artikels 5 dahingehend, dass spezifische Garantien für die Verarbeitung personenbezogener Daten im Hinblick auf Personen, die nicht verurteilte Straftäter sind oder im Hinblick auf Personen, gegen die kein begründeter Straftatverdacht vorliegt, eingesetzt werden. Was unter den spezifischen Garantien zu verstehen ist, bleibt unklar. Da zu den Speichervoraussetzungen dieser Personenkategorien u.a. restriktive höchstrichterliche Rechtsprechung existiert, könnte diese als entsprechende Garantie gewertet werden. Ob dies zur Umsetzung der geforderten Ergänzung ausreichen würde, ist offen. **Die vorgeschlagene Ergänzung ist somit ebenfalls kritisch zu bewerten.**

Artikel 6 Unterscheidung der personenbezogenen Daten nach Richtigkeit und Zuverlässigkeit

In Artikel 6 Abs. 1 RL-E wird geregelt, dass die Mitgliedstaaten dafür Sorge zu tragen haben, dass Datenkategorien „soweit wie möglich“ nach ihrer sachlichen Richtigkeit und Zuverlässigkeit unterschieden werden. Die Reichweite der Vorschrift bleibt unklar. Wie auch bei Artikel 5 RL-E wird zum einen keine konkrete Rechtsfolge an die Regelung geknüpft, zum anderen geht aus der Vorschrift nicht hervor, welche Datenkategorien überhaupt dem Anwendungsbereich des Artikels 6 unterfallen.
Eine entsprechende Differenzierung nach der sachlichen Richtigkeit und Zuverlässigkeit der Datenkategorien ist im deutschen Recht nicht vorhanden. Das strafrechtliche Ermittlungsverfahren sowie die Verfahren zur Gefahrenabwehr sind jedoch darauf angelegt, die sachliche Richtigkeit und Zuverlässigkeit der Erkenntnisse im Hinblick auf ihre Verwertbarkeit im Verfahren stetig zu überprüfen. Wie bereits unter Artikel 4 d 1 HS RL-E dargelegt, gilt im deutschen Recht bei einem Fehlen der Datenrichtigkeit die Pflicht zur Löschung, Berichtigung oder Sperrung der Daten.
Da die Vorschrift selbst sowie ihre Rechtsfolgen unbestimmt bleiben, ist der mögliche Umsetzungsbedarf für die Polizei schwer zu fassen. Da die Vorschrift aber – anders als Artikel 8 des Rahmenbeschlusses, der die Überprüfung der sachlichen Richtigkeit von Daten nur vor deren Übermittlung an Dritte verlangt –eine stetige, anlasslose (!) Aktualisierung anordnet, wird sie nach hiesiger Einschätzung zu einem erheblichen Mehraufwand führen. Auch die Frage, welche Kriterien für die Zuordnung der Kate-

gorien heranzuziehen sind, ist in der Regelung nicht konkretisiert. **Artikel 6 Abs. 1 RL-E wird daher kritisch bewertet.**
In Artikel 6 Abs. 2 RL-E wird geregelt, dass „so weit wie möglich“ zwischen Fakten und persönlichen Einschätzungen unterschieden werden soll. Auch hier bleiben die Reichweite der Regelung sowie mögliche Rechtsfolgen unklar. Die Vorschrift ist sehr unbestimmt formuliert.
Eine Differenzierung nach wertenden Aussagen und Fakten wird teilweise in der Weise aufgegriffen, dass bei wertenden Angaben die unterlagenführende Stelle feststellbar sein muss (§ 7 Abs. 4 BKAG, § 14 HmbPolDVG). Dies ist jedoch nicht durchgehend in allen Gesetzen geregelt. Ob eine solche Formulierung zur Umsetzung von Artikel 6 Abs. 2 RL-E ausreichen würde, darf bezweifelt werden, ist aber jedenfalls nicht rechtssicher zu beurteilen.**Auch Abs. 2 wird somit kritisch bewertet.**
Aus polizeilicher Sicht wird Artikel 6 RL-E insgesamt als kritisch bewertet. Aufgrund der unbestimmten Regelungen sowie möglicher Rechtsfolgen ist der Umsetzungsbedarf nicht absehbar.

Artikel 7 Rechtmäßigkeit der Verarbeitung

Artikel 7 enthält die zentrale Vorschrift zur Bestimmung der Rechtmäßigkeit von Datenverarbeitungen. Danach dürfen die Mitgliedstaaten eine Datenverarbeitung zulassen, wenn diese Verarbeitung erforderlich ist, damit eine zuständige Behörde eine gesetzliche Aufgabe auf den Gebieten der Verhütung oder Verfolgung von Straftaten oder der Strafvollstreckung wahrnehmen kann.
Grundsätzlich erscheint es aus hiesiger Sicht schwierig, das angestrebte Ziel einer Harmonisierung durch Artikel 7 zu erreichen, da die Vorschrift in den Buchstaben a und b an die jeweiligen nationalen Fachgesetze anknüpft. Diese Anbindung an das jeweilige Fachrecht ist zwar richtig, da für die Tätigkeit von Polizei und Justiz die polizeirechtlichen, strafrechtlichen und strafprozessualen Vorgaben maßgeblich sein müssen. Polizei-, Straf- und Strafprozessrecht sind aber EU-weit aus gutem Grund äußerst heterogen ausgestaltet und unterfallen, wie bereits beschrieben, nicht der Rechtsetzungskompetenz der EU. Wenn aber einerseits das Datenschutzrecht an das Fachrecht anzubinden ist, es andererseits diesem Fachrecht aber an Homogenität fehlt, zeigt sich insgesamt die Schwierigkeit, des mit der Richtlinie verfolgten Ansatzes einer vom Datenschutzrecht her gedachten Harmonisierung.
Die Bewertung der Vorschrift leidet unter dem wie oben beschrieben **unklaren Anwendungsbereich der gesamten Richtlinie**. Erst wenn die noch offenen Fragen geklärt sind, kann abschließend beurteilt werden, ob die in Artikel 7 statuierten Vorschriften zur Rechtmäßigkeit von Datenverarbeitungen ausreichend sind. Die fragliche Reichweite des Anwendungsbereichs ist zudem vor dem Hintergrund problematisch, dass Daten oftmals in gemeinsamen Datensammlungen geführt werden, die dann unterschiedlichen Rechtsregimen unterliegen könnten.
Nicht durchdacht erscheint der Regelungsgehalt des Artikels 7 insbesondere im Zusammenspiel mit Artikel 1 Abs. 2 lit. b. Nach Letzterem soll die Berufung auf Datenschutzgründe kein zulässiges Argument mehr sein, eine Übermittlung von Daten abzulehnen (s. o.). Artikel 7 regelt nunmehr – dem Anschein nach für alle Daten (un-

abhängig davon, ob sie im Inland erhoben wurden oder von einem anderen Mitgliedstaat übermittelt wurden) –, für welche Zwecke Daten verarbeitet werden dürfen. Die bisher u. a. im Rahmenbeschluss (dort Artikel 11 S. 1 lit. d) für von einem anderen Mitgliedstaat übermittelte Daten enthaltenen üblichen Einschränkungen, dass bestimmte Verarbeitungen nur bei einer Einwilligung des übermittelnden Mitgliedstaates zulässig sind, enthält die Richtlinie nicht. Dies würde wohl dazu führen, dass die im übermittelnden Mitgliedstaat geltenden Verwendungsbeschränkungen zukünftig dem empfangenden Mitgliedstaat nicht mehr mitgeteilt werden können bzw. von diesem nicht mehr zu beachten sind, soweit sein Rechtssystem den Vorgaben des Artikel 7 entspricht (s. diesbezüglich auch die Ausführungen zu Artikel 1). In der Konsequenz müssten z. B. Daten immer dann von der Staatsanwaltschaft des Empfängerstaates an dortige Verwaltungsbehörden weitergeleitet werden dürfen, wenn die Gesetze des Empfängerstaates dies vorsehen (unabhängig davon, ob die vergleichbare Verwaltungsbehörde des übermittelnden Staates nach dessen Rechtssystem die Daten bekommen hätte). Dies hätte Auswirkungen auf mannigfaltige Sachverhalte. So gibt es im deutschen Recht z. B. Vorschriften, nach denen bestimmte Daten, die durch eine nur bei besonders schweren Straftaten zulässige geheime Maßnahme (z. B. eine Telefonüberwachung) gewonnen wurden, in anderen Strafverfahren nur bei vergleichbar schweren Tatvorwürfen verwendet werden dürfen. Derartige Verarbeitungsbeschränkungen müssten – entgegen der derzeitigen Rechtslage nach dem Rahmenbeschluss - von dem Empfängerstaat nicht mehr berücksichtigt werden. Auch könnte eine Übermittlung nicht mehr unter Berufung auf Geheimhaltungsvorschriften (z.B. Amtsgeheimnisse, Berufsgeheimnisse, Steuergeheimnisse, Sozialgeheimnisse), möglicherweise bestehende Gefährdung einer Person (z. B. eines Zeugen) oder den Untersuchungszweck verweigert werden. **Es bedarf diesbezüglich dringend einer Klarstellung der Richtlinie,**dies insbesondere auch im Hinblick auf den augenscheinlich mit den Artikeln 1 und 7 in Widerspruch stehenden Artikel 37, nach dem:

> *Die Mitgliedstaaten [vor]sehen […], dass der für die Verarbeitung verantwortliche den Empfänger personenbezogener Daten auf Verarbeitungsbeschränkungen hinweist und alle vertretbaren Vorkehrungen trifft, um sicherzustellen, dass diese Beschränkungen eingehalten werden.*

Erläuterungsbedürftig ist weiterhin das Zusammenwirken des Artikels 7 mit den in Artikel 4 aufgeführten Prinzipien der Datenverarbeitung, insbesondere im Hinblick auf den Grundsatz der Zweckbindung.

Bedenken bestehen auch dahingehend, dass eine Einwilligung als Legitimation für die Datenverarbeitung im Bereich der Richtlinie jedenfalls nicht ausdrücklich vorgesehen ist. Da Ermittlungsmaßnahmen stets Eingriffe in die Grundrechte der betroffenen Personen sind, die einer hinreichend bestimmten gesetzlichen Grundlage bedürfen, spielt die Einwilligung als Voraussetzung z.B. für strafprozessuale Eingriffe naturgemäß eine nur untergeordnete Rolle. Dennoch ist sie aus hiesiger Sicht in wesentlichen Bereichen unabdingbar (z.B. bei der Entnahme von Blutproben, DNA-Analyse usw.). Sie sollte daher in rechtssicherer Weise im RL-Entwurf verankert werden. Anderenfalls wären die im deutschen Recht verankerten einwilligungs-

basierten Datenverarbeitungen durch gesetzliche Regelungen zu ersetzen. Aus polizeitaktischer Sicht könnte damit ein erhöhter Bürokratieaufwand einhergehen, wenn zum Beispiel – wie in den Fällen des §81g StPO – anstelle der Einwilligung stets eine richterliche Anordnung einzuholen wäre. Zudem bietet die Einwilligung des Betroffenen Raum für eine flexible Handhabung des Einzelfalls, wie sie durch gesetzliche, abstrakt-generelle Regelungen nicht immer möglich wäre.

Es ist nicht völlig ausgeschlossen, dass auch nach dem RL-E in der seitens KOM vorgelegten Fassung Einwilligungslösungen zulässig sind. So ließe sich argumentieren, dass Artikel 7 RL-E für die Rechtmäßigkeit einer Datenverarbeitung lediglich voraussetzt, dass die Datenverarbeitung „zur Wahrnehmung einer gesetzlichen Aufgabe“ (lit. a) oder „zur Erfüllung einer gesetzlichen Verpflichtung“ (lit. b) notwendig ist. Gesetzlich verankert sein muss – so ließe sich anführen – also nur der (übergeordnete) Zweck der Datenverarbeitung, nicht die konkrete Rechtsgrundlage der einzelnen Datenverarbeitung selbst. Solange die Datenverarbeitung der Erfüllung einer gesetzlichen Aufgabe (z.B. Gefahrenabwehr, Strafverfolgung) dient, könnte sie folglich auch auf Grundlage einer Einwilligung erfolgen. Diese Auslegung des RL-E scheint einerseits nicht unvertretbar, wird aber andererseits in der aktuellen Diskussion soweit ersichtlich nicht vertreten.

Aus diesem Grunde sollte auf eine ausdrücklich Kodifikation der Einwilligung im RL-E hingewirkt werden. Die Einwilligung ist für die polizeiliche Praxis zu bedeutsam, um es auf komplexe juristische Auslegungsfragen ankommen zu lassen. Hinzukommt, dass die Einwilligung des Betroffenen im Rahmenbeschluss 2008/977/JI legaldefiniert (Artikel 2 lit. g) und in dessen Artikel 11 (Verarbeitung personenbezogener Daten die von einem anderen Mitgliedstaat übermittelt oder bereitgestellt wurden) als eine von zwei Möglichkeiten zulässiger Datenverarbeitung ausdrücklich genannt wird. Bliebe die Einwilligung nunmehr im RL-E unerwähnt, könnten hieraus aus hiesiger Sicht ungünstige Rückschlüsse gezogen werden.

Gemäß dem Entwurf einer Stellungnahme des Rechtsausschusses des Europäischen Parlaments vom 04.01.2013 soll Artikel 3 Abs. 1 um eine Nr. 9a „Einwilligung der betroffenen Person“ ergänzt werden. Begründet wird dieser Vorschlag wie folgt:

> *Die Änderung führt die Einwilligung des Betroffenen innerhalb enger Grenzen ein. Auch wenn es grundsätzlich keine Augenhöhe zwischen Bürger und Staat geben kann, kann die Einwilligung im Einzelfall als Rechtfertigungsgrund dienen, zum Beispiel bei DNA-Massentests.*

Explizite Erwähnung findet die „Einwilligung“ entgegen dieser allgemeingültigen (und zutreffenden) Begründung aber lediglich bei der Verwendung personenbezogener Daten aus anderen Mitgliedstaaten. Nach der Stellungnahme des Rechtsauschusses soll folgender Artikel 7b Nr. 2 lit. d–neu eingefügt werden:

> *[Dürfen] Die personenbezogenen Daten […] unter den Voraussetzungen des Artikels 7 Abs. 3 nur für folgende andere Zwecke als diejenigen, für die sie übermittelt oder bereitgestellt wurden, weiter verarbeitet werden:*
>
> *jeden anderen Zweck nur mit der vorherigen Zustimmung des übermittelnden Mitgliedstaats oder mit Einwilligung der betroffenen Person, die sie im Einklang mit dem innerstaatlichen Recht erteilt hat*

Dieser Anwendungsbereich ist **deutlich zu eng gefasst**. Nicht umfasst wäre insbesondere auch der in der Praxis wohl wichtigste Fall: die Erhebung von Daten mit Einwilligung des Betroffenen sowie die daran anknüpfende weitere Verarbeitung dieser Daten zu spezifischen, in der Einwilligung genannten Zwecken.

Unklar bzw. zu eng erscheint die Regelung in Artikel 7 lit. a im Hinblick auf die Zulässigkeit von **Datenübermittlungen an andere Behörden**. Es fehlt an der Befugnis zur Datenübermittlung von Polizeibehörden, Staatsanwaltschaften und Gerichten, Daten auch an andere Behörden zur Erfüllung deren gesetzlicher Aufgaben, die nicht in der Verhütung oder Verfolgung von Straftaten bestehen, zu übermitteln. Informationen aus Strafakten werden für vielfältige weitere Zwecke der Rechtspflege, insbesondere für Zivilverfahren, Verwaltungsverfahren etc. verwendet. Auch besteht die Notwendigkeit einer Weitergabe zu Forschungs- und Archivzwecken. Artikel 7 lit. b scheint für diese Konstellationen in der Regel nicht einschlägig zu sein, da diese Regelung an eine „gesetzliche Verpflichtung“ anknüpft. In Deutschland bestehen für die Übermittlung polizeilicher Daten und von Daten aus Strafverfahren an andere innerstaatliche Behörden jedoch keine expliziten Übermittlungspflichten, sondern regelmäßig nur gesetzliche Befugnisnormen. Sämtliche dieser Befugnisnormen wären umzuformulieren in gesetzliche Verpflichtungen. Der damit einhergehende gesetzgeberische Aufwand wäre enorm. Ggf. drohen schwierige politische Debatten, wenn es darum geht, die heutigen Kann-Vorschriften zur Übermittlungen polizeilicher Informationen an andere Behörden verpflichtend auszugestalten.

Ebenfalls zu eng erscheint auch Artikel 7 lit. c, wonach eine Übermittlung nur zur Wahrung lebenswichtiger Interessen möglich ist. Eine Übermittlung muss auch zulässig sein, um sonstige schützenswerte Interessen einer anderen Person zu wahren, beispielsweise an den Geschädigten einer Straftat, damit dieser seine Schadensersatzansprüche gegenüber dem Täter geltend machen kann.

Ebenfalls evident zu eng gefasst ist Artikel 7 lit. d, der eine Verarbeitung personenbezogener Daten lediglich zur Abwehr einer unmittelbaren und ernsthaften Gefahr für die öffentliche Sicherheit vorsieht. Die Aufgabenerfüllung der Gefahrenabwehrbehörden dürfte hiermit zum Erliegen gebracht werden. Auch die Warnung des Opfers vor einem Stalker muss der zuständigen Behörde beispielsweise möglich sein, auch wenn noch keine unmittelbare und ernsthafte Gefahr für die öffentliche Sicherheit vorliegt. Es muss den zuständigen Behörden auch möglich sein, Maßnahmen zur Verhütung von Straftaten zu ergreifen, auch wenn gerade noch keine gegenwärtige Gefahr vorliegt (z. B. langfristig geplanter Bombenanschlag). Gleichwohl würde Artikel 7 lit. d dazu führen, dass die Verarbeitung personenbezogener Daten unzulässig wäre – ein in polizeitaktischer Hinsicht gravierender Einschnitt.

Aus polizeilicher Sicht ist Artikel 7 RL-E daher zumindest in Teilen als äußerst kritisch zu bewerten.

Artikel 8 Verarbeitung besonderer Kategorien von personenbezogenen Daten

Artikel 8 sieht vor, dass besondere Kategorien von personenbezogenen Daten (z.B. ethnische Herkunft, politische Meinung, Religion oder Überzeugung, Gesundheit, genetische Daten) grundsätzlich nicht verarbeitet werden dürfen. Verarbeitung um-

fasst nach der Richtlinie jeden mit oder ohne Hilfe automatisierter Verfahren ausgeführten Vorgang oder jede Vorgangsreihe im Zusammenhang mit personenbezogenen Daten wie das Erheben, Erfassen, die Organisation, das Ordnen, die Speicherung, die Anpassung oder Veränderung, das Auslesen, das Abfragen, die Verwendung, die Weitergabe durch Übermittlung, die Verarbeitung oder jede andere Form der Bereitstellung, der Abgleich oder die Verknüpfung, das Löschen oder Vernichten der Daten sowie die Beschränkung des Zugriffs auf Daten.
Zweifelsohne sollten besonders sensible Daten einen besonderen Schutz genießen. Die Verarbeitung „besonderer Kategorien von Daten" ist für die polizeiliche Arbeit allerdings erforderlich. So sind genetische Daten zum einen für den eindeutigen Nachweis der Täterschaft, aber auch zum eindeutigen Ausschluss der Täterschaft und damit der frühzeitigen Einstellung von weiteren Ermittlungen gegen Unschuldige unerlässlich. Im Phänomenbereich Eigentumskriminalität z.B. spielt die DNA-Analysedatei bei der Fallaufklärung eine bedeutende Rolle und führt speziell beim automatisierten Spurenabgleich innerhalb der EU-Staaten immer wieder zu Fallzuordnungen oder Täteridentifizierungen. Personengebundene Hinweise wie „Ansteckungsgefahr“ oder „Betäubungsmittelkonsument“ oder „Sexualstraftäter" sind aus Eigensicherungsgründen und bei der Vorbereitung und Durchführung offener strafprozessualer Maßnahmen unerlässlich. Im Bereich des islamistischen Terrorismus sind Kenntnisse über die Religion des Betroffenen unabdingbar. Es ist von erheblicher Bedeutung zu wissen, welcher religiösen Strömung eine Person angehört. Eine Person, die dem jihadistischen Salafismus anhängt, hat ein großes Gefährdungspotential. Das Wissen um eine mögliche Fanatisierung sensibilisiert für zukünftige Ermittlungsverfahren und offenbart Ansatzpunkte für die „Deradikalisierung“. Solche Informationen sind nötig, um das Gefahrenpotential eines Täters einschätzen zu können. Ähnliches gilt für den Bereich des Rechtsextremismus. Hier ist es erforderlich, auf Informationen über die politische Gesinnung eines Betroffenen zurückgreifen zu können, um rassistische, antisemitische oder fremdenfeindliche Täter- oder Gruppenstrukturen erkennen zu können. In Deutschland werden die besonderen Kategorien von Daten durch verschiedene Rechtsvorschriften besonders geschützt und dürfen auch nur in diesen gesetzlich normierten Fällen verarbeitet werden. Dieser Schutz ist sinnvoll und wichtig.Ein grundsätzliches Verbot, wie in Artikel 8 RL-E vorgesehen, geht jedoch deutlich zu weit und droht die polizeiliche Arbeit in vielen Bereichen (z.B. durch rechtliche Einschränkung oder gar Verhinderung einer eindeutigen Identifizierung von Tätern) ernsthaft zu gefährden.
Artikel 8 Abs. 2 erlaubt zwar, im mitgliedstaatlichen Recht Ausnahmeregelungen zu schaffen, die geeignete "Garantien" enthalten müssen, auch soll die Verarbeitung möglich sein, wenn dieszur Wahrung lebenswichtiger Interessen erforderlich ist, oder aber die Daten durch den Betroffenen offenkundig öffentlich gemacht wurden. Diese Regelung trägt den polizeilichen Bedürfnissen insgesamt aber nicht in ausreichendem Maße Rechnung.
Zunächst sind hier schon die Bedeutung und der Inhalt des Begriffs "geeignete Garantien" unklar. Es bedarf zumindest der Erläuterung, inwieweit diese Garantien über das hinausgehen müssen, was für die Verarbeitung sonstiger Daten gilt. **Dar-**

über hinaus ist auch der Umsetzungsbedarf völlig unklar, ebenso ob und inwieweit innerhalb dieser Garantien Raum für Abwägungen bleibt, die auch gegenläufige Interessen angemessen berücksichtigen. Es wären aber Regelungen in erheblichem Umfang erforderlich, um die Vielfalt der denkbaren Fälle zu erfassen und im Einzelnen zu regeln. Es muss hierbei aber auch immer beachtet werden, dass es sichnach der Systematik des Artikels 8 RL-E lediglich um Ausnahmeregelungen handeln soll. Dies dürfte es verbieten, dass alle Fälle extensiv unter diese Ausnahmen subsumiert werden, sodass sich das Verhältnis von Regel und Ausnahme verkehrt. Dem nationalen Gesetzgeber stünden also nur in begrenztem Maße Möglichkeiten offen, unter Beachtung des in dem RL-E angelegten Grundsatz-Ausnahme-Schemas gesetzliche Regelungen zur Verarbeitung sensibler Daten zu erlassen. Daher wäre eine Überarbeitung des RL-E wünschenswert. Er sollte, statt des grundsätzlichen Verbots mit der Möglichkeit von Ausnahmeregelungen die Verarbeitung von sensiblen Daten zulassen, wenn dies auch unter Berücksichtigung der besonderen Sensibilität der Daten zur Erfüllung der Aufgaben der jeweiligen Stellen notwendig ist.Die dargestellte (Rechts-)Auffassung deckt sich mit der im Entwurf einer Stellungnahme des Rechtsausschusses des Europäischen Parlaments vom 04.01.2013 vorgeschlagenen Änderung des Artikels 8 Abs. 1 und der dazugehörigen Begründung:

> *Der Artikel wurde nach dem Vorbild von Artikel 6des Rahmenbeschlusses 2008/977/JI umformuliert. Auch wenn er in seiner Systematik vom Verbotsprinzip des RL-E abweicht, bleibt die Verarbeitung sensibler Daten jedoch nach wie vor nur unter strengen Voraussetzungen zulässig. Mit Blick auf die große Bedeutung von DNA-Beweisspuren ist das von der KOM neu etablierte grundsätzliche Verbot zur Verarbeitung genetischer Daten gestrichen.*

Nach dem o. g. Entwurf einer Stellungnahme des Rechtsausschusses des Europäischen Parlaments soll Artikel 8 Abs. 2 lit. b wie folgt geändert werden:

> *die Verarbeitung unbedingt notwendig und durch eine Vorschrift gestattet ist, die geeignete Garantien vorsieht.*

Es ist unklar, welche Maßstäbe an das Erfordernis der unbedingten Notwendigkeit gesetzt werden soll. Sofern das Erfordernis der unbedingten Notwendig nicht dem geltenden Grundsatz der Erforderlichkeit entspricht, sondern die Verarbeitung der entsprechenden Daten als ultima ratio verstanden werden würde, müssten selbst bei unverhältnismäßigem Aufwand erst sämtliche anderen denkbaren Möglichkeiten ausgeschöpft werden. Eine Lösung auf Basis einer Verhältnismäßigkeitsprüfung anstelle des ultima-ratio-Prinzips wäre in diesem Fall wünschenswert.

Ungeachtet o. a. Ausführungen erscheint die Ausnahmereglung in Artikel 8 Abs. 2 lit. b zu eng gefasst. Eine Ausnahme sollte nicht nur lediglich zur Wahrung lebensnotwendiger Interessen möglich sein, sondern auch dann, wenn andere hochrangige Rechtsgüter (z. B. dauerhafter Verlust des Sehvermögens oder andere schwere Körperverletzungen, Glaubwürdigkeit eines Politikers in Verleumdungsfällen, etc.) betroffen sein sollten.

Aus polizeilicher Sicht ist Artikel 8 RL-E daher als äußerst kritisch zu bewerten.

Artikel 9 Auf Profiling und automatischer Datenverarbeitung basierende Maßnahmen

Artikel 9 Abs. 1 bestimmt, dass die Mitgliedstaaten diejenigen Maßnahmen, die eine nachteilige Rechtsfolge für die betroffene Person haben oder sie erheblich beeinträchtigen und die ausschließlich aufgrund einer automatisierten Verarbeitung von personenbezogenen Daten zum Zwecke der Bewertung einzelner Aspekte ihrer Person ergehen, verbieten, es sei denn, dies ist durch ein Gesetz erlaubt, das Garantien zur Wahrung der berechtigten Interessen der betroffenen Person festlegt.
Zahlreiche Gesetze enthalten vergleichbare Regelungen für automatisierte*Entscheidungen*, die rechtliche Folgen nach sich ziehen (z. B. Artikel 15 Abs. 6 DSG BY, § 5a HmbDSG, § 37 BKAG i.V.m. § 6a BDSG, § 37 BPolG i.V.m. §6 a BDSG, § 4 Abs. 4 DSG NRW, § 4a DSG LSA).
Aus polizeilicher Sicht besteht für Artikel 9 Abs. 1 RL-E dennoch Umsetzungsbedarf. Im Gegensatz zu den oben aufgeführten Regelungen und zur Regelung des Artikels 7 des Rahmenbeschlusses, referenziert Artikel 9 Abs. 1 RL-E nicht auf die „*Entscheidung"*, sondern bereits auf die einzelne „*Maßnahme*". Wird von der BLAG zum Umsetzungsbedarf des Ratsbeschlusses Prüm und der Schwedischen Initiative für Artikel 7 des Rahmenbeschlusses unter Ziffer 5 noch dargelegt, dass im Bereich der polizeilichen und justiziellen Zusammenarbeit in Strafsachen Entscheidungen mit nachteiligen Rechtsfolgen immer auf das Tätigwerden einer natürlichen Person zurückgingen, die die Daten bewerte und eine Entscheidung treffe, ist dies bei den einzelnen Maßnahmen gerade nicht der Fall. So müsste u. a. jede Rechtsgrundlage, aufgrund derer eine Dateien-Überprüfung zulässig ist, entsprechende Garantien für den Betroffenen vorsehen. **Die Vorschrift wird als kritisch bewertet, da sie erheblichen Regelungs- und Umsetzungsbedarf nach sich ziehen würde.**
Artikel 9 Abs. 2 RL-E legt fest, dass die automatisierte Verarbeitung personenbezogener Daten zum Zwecke der Auswertung bestimmter persönlicher Aspekte der betroffenen Person sich nicht ausschließlich auf die in Artikel 8 genannten besonderen Kategorien personenbezogener Daten stützen darf.
Dieser weitgehende Nutzungsausschluss ist im deutschen Recht nicht verankert und ist für die polizeiliche Praxis z. B. im Hinblick auf die polizeiliche Ermittlungsarbeit bei Sexualstraftaten deutlich **zu eng.Die polizeiliche Analysetätigkeit** z. B. bei der Aufklärung von Sexualstraftaten würde **unangemessen eingeschränkt**[8].
Sollte der Richtlinienentwurf in der vorgelegten Fassung umgesetzt werden, würde ein **erheblicher Umsetzungsbedarf entstehen, der für die polizeiliche Auswertungspraxis weitreichende Folgen haben würde.**
Aus polizeilicher Sicht ist Artikel 9 RL-E als äußerst kritisch zu bewerten.

[8] Bundesrat Drucksache 51/12 (Beschluss) (2), Nr. 14.

Kapitel III Rechte der betroffenen Person

Artikel 10 Modalitäten für die Ausübung der Rechte der betroffenen Person

Artikel 10 Abs. 1 RL-E regelt, dass die Verarbeitung personenbezogener Daten und die der betroffenen Person zustehenden Rechte in transparenter Weise dargestellt werden und erfolgen soll. Vergleichbare Regelungen sind im deutschen Recht nicht explizit enthalten. Ob Artikel 10 Abs. 1 RL-E eigenständige Pflichten begründet, oder nur deklaratorischen Charakter hat, bleibt unklar, da dem für die Datenverarbeitung Verantwortlichen eine Transparenzpflicht auferlegt wird. Die Ausgestaltung hiervon bleibt jedoch unbestimmt. Jedenfalls kann es sich bei dieser Pflicht aus polizeilicher Sicht lediglich um die Darstellung allgemeiner Informationen zur Gesetzeslage handeln und nicht um die Preisgabe interner polizeilicher Arbeitsabläufe. **Die Vorschrift ist somit kritisch zu sehen und bedarf der Klarstellung.**
Der LIBE - Änderungsantrag Nr. 72 sorgt ebenfalls nicht für die gewünschte Klarstellung.
Artikel 10 Abs. 2 RL-E legt fest, dass die betroffenen Personen alle Informationen über die Datenverarbeitung in verständlicher Sprache erhalten. Auch dieser Grundsatz ist im deutschen Recht nicht ausdrücklich geregelt, ergibt sich jedoch aus Sinn und Zweck der Rechte der Betroffenen. Ein Umsetzungsbedarf wird nicht gesehen. **Die Regelung wird als unkritisch bewertet**.
Die Ergänzung des LIBE - Änderungsantrags Nr. 73 ist entbehrlich.
In Artikel 10 Abs. 3 RL-E ist geregelt, dass die Mitgliedstaaten Verfahrensregelungen zur Umsetzung der Rechte der Betroffenen einführen sollen. Da die einzelnen Rechte der Betroffenen im RL-E im Folgenden (Artikel 11 und 12 bis 17) detailliert geregelt sind, hat Artikel 10 Abs. 3 RL-E lediglich deklaratorischen Charakter.
Eine vergleichbare Regelung ist im deutschen Recht nicht explizit enthalten. Dass entsprechende Verfahren vorliegen müssen, ergibt sich jedoch aus den in den jeweiligen Gesetzen festgelegten Rechten der Betroffenen (z. B. auf Auskunft, Löschung, Sperrung, Benachrichtigung etc.). Ein Umsetzungsbedarf für diese Regelung wird daher nicht gesehen. **Die Vorschrift wird als unkritisch bewertet.**
Die Verknüpfung der automatisierten Verarbeitung von Daten und der elektronischen Antragsstellung, die mit dem LIBE - Änderungsantrag Nr. 74 eingebracht wird, erschließt sich nicht.
Artikel 10 Abs. 4 RL-E sieht vor, dass der Betroffene ohne unangemessene Verzögerung von den Maßnahmen Kenntnis erlangt, die im Zusammenhang mit etwaigen Anträgen getroffen wurden. Zwar gibt es im deutschen Recht keine vergleichbare Vorschrift, allerdings wird diesem Grundsatz z. B. für den Bereich der Anträge auf Auskunft dadurch Rechnung getragen, dass der Betroffene Untätigkeitsklage bei Gericht einreichen kann, wenn eine Bearbeitung seines Antrags nicht innerhalb von drei Monaten nach Eingang erfolgt (vgl. § 75 Abs. 1 VwGO). Ob eine solche Regelung der Vorschrift genügt, kann nicht beurteilt werden**. Ein Umsetzungsbedarf kann daher nicht bestimmt werden.Die Vorschrift ist folglich kritisch.**
Der LIBE - Änderungsantrag Nr. 75 sieht vor, dass der Antragseingang spätestens innerhalb eines Monats bestätigt werden muss und die Unterrichtung in elektroni-

scher Form zu erfolgen hat, wenn die Antragstellung auch elektronisch erfolgte. Entsprechende Regelungen sind bisher im polizeilichen Bereich nicht enthalten. Der elektronischen Übermittlung sensibler personenbezogener Daten ohne Verschlüsselung kann darüber hinaus aus datenschutzrechtlicher Sicht nicht zugestimmt werden. **Die Einfügung ist abzulehnen.**

Artikel 10 Abs. 5 RL-E sieht grundsätzlich eine Kostenfreiheit für die Anträge der Betroffenen vor. Nur ausnahmsweise kann unter bestimmten Umständen bei missbräuchlichen Anträgen ein Entgelt für die Maßnahmen verlangt werden. Ähnliche Regelungen zur Kostenfreiheit finden sich in allen Datenschutzgesetzen der Länder und des Bundes (vgl. § 19 Abs. 7 BDSG, Artikel10 Abs. 2 BayDSG, § 18 Abs. 2 DSG NRW, §15 Abs. 7 DSG LSA, §21 Abs. 1 LDSG BW, § 18 HDSG). In bestimmten Fällen wird allerdings die Gebührenfreiheit eingeschränkt (z. B. wegen hohen Verwaltungsaufwands Artikel10 Abs. 2 BayDSG, für bestimmte Daten §15 Abs. 1a, Abs. 7 DSG LSA).

Die Möglichkeit der Gebührenerhebung bei missbräuchlichen Anträgen ist bisher in den Landesdatenschutzgesetzen sowie dem Bundesdatenschutzgesetz nicht geregelt und grundsätzlich zu begrüßen. Die Definitionen sind unbestimmt und bedürfen einer Konkretisierung. Ein Umsetzungsbedarf ist zwar gegeben, dieser hat jedoch keine wesentlichen polizeitaktischen Folgen. **Somit wird die Vorschrift als unkritisch bewertet.**

Artikel 11 Information der betroffenen Person

Artikel 11 normiert eine Unterrichtungspflicht. Bereits Artikel 16 RB Datenschutz sah eine solche– allerdings in deutlich moderaterer Form – vor. Der RL-E brächte hier deutlich spürbare Verschärfungen: Während in Artikel 16 RB nur vorgesehen ist, dass die betroffene Person im Einklang mit dem innerstaatlichen Recht über die Erhebung oder Verarbeitung personenbezogener Daten informiert wird, nennt Artikel 11 RL-E einen umfassenden, äußerst detailliert formulierten und in der polizeilichen Praxis kaum erfüllbaren Katalog an Informationspflichten. Diese Informationspflichten sollten jedoch nicht nur in Fällen gelten, die für den Betroffenen besondere Risiken bereithalten, sondern für sämtliche Datenverarbeitungen der Polizei. **Im Ergebnis wird Artikel 11 daher zu einem erheblichen zeit- und personalintensiven Aufwand auch und gerade in den örtlichen Polizeidienststellen führen. Aus polizeilicher Sicht würde die Umsetzung der Norm an die Grenzen des Machbaren bzw. sogar darüber hinaus führen.** Alltägliche Aufgabenwahrnehmungen, wie bspw. Identitätsfeststellungen, wären mit umfangreichen Mitteilungspflichten verbunden, die regelmäßig bereits zum Zeitpunkt der Datenerhebung (!), d.h. sofort vor Ort, zu erfüllen wären.

Nach Artikel 11 Abs. 1 haben die Mitgliedstaaten dafür Sorge zu tragen, dass der für die Verarbeitung Verantwortliche alle geeigneten Maßnahmen ergreift, um einer Person, von der personenbezogene Daten erhoben werden, bestimmte in Artikel 11 Abs. 1 lit. a bis g näher genannte Daten mitzuteilen.

Wenn Daten beim Betroffenen oder bei Dritten erhoben werden, sehen die deutschen Polizeigesetze gegenwärtig zwar eine Hinweispflicht über die Rechtsgrundlage

der Datenerhebung sowie die beabsichtigte Verwendung der Daten vor (vgl. z.B. § 2 Abs. 4 S. 1 Nr. 1, 3 HmbPolDVG, § 9 Abs. 6 PolG NRW, § 15 Abs. 7 S. 2 SOG LSA, Artikel 30 Abs. 4 S. 1 Nr. 1 PAG BY, § 21 Abs. 4 S. 1 BPolG, § 20b Abs. 3 BKAG i.V.m. § 21 Abs. 4 BPolG). **Weitergehende Hinweispflichten in den Polizeigesetzen sind im Falle der Datenerhebung beim Betroffenen oder bei Dritten aber nicht ersichtlich, insofern gehen die Anforderungen des Artikels 11 Abs. 1 deutlich darüber hinaus und rufen folglich erheblichen Umsetzungsbedarf hervor.** Erfolgt die Datenerhebung nicht beim Betroffenen, sondern ohne dessen Wissen verdeckt, beispielsweise durch eine Telekommunikationsüberwachung oder durch den Einsatz technischer Mittel zur Anfertigung von Bildaufnahmen und Bildaufzeichnungen, ist die Person über die Maßnahme zu unterrichten (vgl. z.B. Artikel 33 Abs. 7, Artikel 34 Abs. 6 PAG BY, § 17 Abs. 7, § 18 Abs. 6 SOG LSA, § 9 Abs. 3, § 10 Abs. 2 S. 1, § 10a Abs. 6, § 10e Abs. 4 HmbPolDVG, § 16a Abs. 3, § 17 Abs. 5, § 18 Abs. 7, § 19 Abs. 3, § 20 Abs. 5 PolG NRW, § 28 Abs. 5 BPolG, § 20w BKAG). In den Polizeigesetzen ist der Inhalt der Information zumeist nicht festgelegt (vgl. aber § 17 Abs. 5 S. 3 PolG NRW). Um die mit der Benachrichtigung eröffnete Möglichkeit des nachträglichen Rechtsschutzes effektiv wahrnehmen zu können, dürfte es als erforderlich anzusehen sein, die Anordnung als solche, die Durchführung und auch den Umfang der Maßnahme mitzuteilen (vgl. zur Wohnraumüberwachung in § 100d StPO a.F. BVerfG, NJW 2007, S. 2753, 2757). **Auch insoweit, d.h. bei verdeckten Maßnahmen, bleibt das Landesrecht hinter den Vorgaben des Artikels 11 zurück.** Die StPO sieht in § 101 Abs. 4 Satz 2 vor, dass bei der Benachrichtigung auf die Möglichkeit nachträglichen Rechtschutzes und auf die dafür vorgesehene Frist hinzuweisen ist.

Zu Artikel 11 Abs. 1 lit. d): Zum Zeitpunkt der Datenerhebung ist es in vielen Fällen noch völlig unklar, in welchen Dateien die Daten gespeichert werden oder über welchen Zeitraum. Auch kann nicht gesagt werden, an wen Datenübermittlungen erfolgen werden.

Nach Abs. 2 ist ferner mitzuteilen, ob die Bereitstellung der Daten obligatorisch oder freiwillig ist und welche möglichen Folgen die Zurückhaltung der Daten hätte.

Teilweise sehen die Polizeigesetze vor, dass die betroffene Person darüber aufzuklären ist, ob eine Auskunftspflicht besteht oder die Auskunft freiwillig erfolgt (vgl. z.B. § 2 Abs. 4 S. 1 Nr. 2 HmbPolDVG, § 9 Abs. 6 PolG NRW, § 15 Abs. 7 S. 1 SOG LSA, Artikel 30 Abs. 4 S. 1 Nr. 2 PAG BY, § 21 Abs. 4 S. 1 BPolG, § 20b Abs. 3 BKAG i.V.m. § 21 Abs. 4 BPolG). Mitunter steht diese Belehrungspflicht unter dem Vorbehalt, dass der Betroffene sie verlangt (§ 21 Abs. 4 S. 1 BPolG). Eine Hinweispflicht zu den Folgen der Verweigerung der Auskunft ist bei den vorliegend untersuchten Polizeigesetzen nicht ersichtlich (vgl. aber § 36 Abs. 2 S. 4 SächsPolG).

Abs. 3 regelt, wann der für die Verarbeitung Verantwortliche die Auskünfte nach Abs. 1 erteilt. Soweit der Zeitpunkt für die oben stehenden Hinweispflichten in den Polizeigesetzen nicht bereits ausdrücklich normiert ist, ergibt sich dies jedenfalls aus dem Zusammenhang, da diese Hinweise jeweils bei der Datenerhebung beim Betroffenen vorzunehmen sind, mithin zum Zeitpunkt der Datenerhebung im Sinne des Artikels 11 Abs. 3 lit. a des RL-Entwurfs. Falls die Daten nicht bei der betroffenen Person er-

hoben werden, soll die Unterrichtung zum Zeitpunkt der Erfassung oder innerhalb einer angemessenen Frist nach der Erhebung unter Berücksichtigung der jeweiligen Umstände der Verarbeitung erfolgen (vgl. Abs. 3 lit. b RL-E). Dies gilt im Polizeirecht für verdeckte Maßnahmen. Der Betroffene ist dann von der Datenerhebung zu unterrichten, sobald die Maßnahme beendet ist und der Zweck der Maßnahme durch die Benachrichtigung nicht mehr gefährdet ist (vgl. z.B. Artikel 33 Abs. 7, Artikel 34 Abs. 6 PAG BY, § 17 Abs. 7, § 18 Abs. 6 SOG LSA, § 9 Abs. 3, § 10 Abs. 2 S. 1, § 10a Abs. 6, § 10e Abs. 4 HmbPolDVG, § 16a Abs. 3, § 17 Abs. 5, § 18 Abs. 7, § 19 Abs. 3, § 20 Abs. 5 PolG NRW, § 28 Abs. 5 BPolG, § 20w BKAG).
Abs. 4 sieht vor, dass die Mitgliedstaaten Ausnahmen von der Unterrichtungspflicht vorsehen dürfen. **Die Spielräume der nationalen Gesetzgeber sind hierbei jedoch wiederum begrenzt (vgl. bereits oben zu Artikel 8), da das in Artikel 11 RL-E angelegte Grundsatz-Ausnahme-Schema nicht aufgehoben werden darf.** Bund und Länder könnten somit einzelne Ausnahmeregelungen für spezifische Situationen schaffen, von der im RL-E vorgesehenen grundsätzlichen Informationspflicht aber im Kern gerade nicht abrücken.
Soweit die gegenwärtig in Bund und Ländern geltenden Polizeigesetze eine Unterrichtungspflicht normieren, sind dort auch Ausnahmen geregelt. Zumeist kann von entsprechenden Hinweisen abgesehen werden, wenn die Erfüllung der polizeilichen Aufgabe oder die schutzwürdigen Belange Dritter beeinträchtigt oder gefährdet würden (vgl. z. B. § 2 Abs. 4 S. 2 HmbPolDVG, § 9 Abs. 6 PolG NRW, § 15 Abs. 7 S. 5 SOG LSA, Artikel 30 Abs. 4 S. 2 PAG BY, § 21 Abs. 4 S. 2 BPolG, § 20b Abs. 3 BKAG i.V.m. § 21 Abs. 4 BPolG).
Nach Artikel 11 Abs. 5 können die Mitgliedstaaten Datenverarbeitungskategorien festlegen, für die die Ausnahmeregelung nach Abs. 4 vollständig oder teilweise zur Anwendung kommt. Weder den Erwägungsgründen noch den Erläuterungen des Vorschlages im Einzelnen ist zu entnehmen, was hiermit gemeint sein könnte. Zutreffend dürfte die Annahme sein, dass nach Artikel 11 Abs. 5 eine abstrakt-generelle Regelung ohne Rücksicht auf den Einzelfall getroffen werden kann (vgl. Bäcker/Hornung, ZD 2012, S. 147, 151). Unklar ist jedoch, wie Datenverarbeitungskategorien in diesem Zusammenhang definiert werden können, mithin welche Fallkonstellationen abstrakt generell geregelt werden könnten (Bäcker/Hornung, ZD 2012, S. 147, 151 verstehen darunter Datenverarbeitungsarten). Der Begriff taucht nachfolgend auch in Artikel 13 Abs. 2 auf. Dort sind Datenverarbeitungskategorien darüber hinaus „gesetzlich“ festzulegen. Artikel 8 regelt die Verarbeitung besonderer Kategorien personenbezogener Daten. Damit sind personenbezogene Daten gemeint, aus denen die Rasse und ethnische Herkunft, politische Meinungen, Religion oder Überzeugungen, die Gewerkschaftszugehörigkeit hervorgehen, sowie von genetischen Daten oder die Gesundheit oder das Sexualleben betreffende Daten. Das deutsche Recht kennt diese als sog. besondere Arten personenbezogener Daten (vgl. Legaldefinition in § 3 Abs. 9 BDSG). Allerdings besteht schon vom Wortlaut her ein Unterschied zwischen Datenverarbeitungskategorien und Kategorien von Daten. Hier ist zur Klärung die weitere Beratung in den europäischen Gremien abzuwarten. Der Begriff der Datenkategorie taucht durchgängig auch im VO-Entwurf auf. Daneben

gibt es dort aber auch sog. Kategorien von Empfängern und Übermittlungen (vgl. Artikel 15 Abs. 1 lit. c, Artikel 43 Abs. 2 lit. b VO-Entwurf).
Im Strafprozessrecht besteht kein allgemeiner Mitteilungsanspruch. Nach § 170 Abs. 2 S. 2 StPO setzt die Staatsanwaltschaft den Beschuldigten von der Einstellung des Verfahrens in Kenntnis, wenn er als solcher vernommen worden ist oder ein Haftbefehl gegen ihn erlassen worden ist; dasselbe gilt, wenn er um einen Bescheid gebeten hat oder wenn ein besonderes öffentliches Interesse an der Bekanntgabe ersichtlich ist. Die Benachrichtigung ist als grundrechtssichernde Verfahrensregelung im Übrigen bei verdeckten Maßnahmen nach § 101 Abs. 4 StPO vorgesehen.
Nach allem ist die Vorschrift äußerst kritisch zu betrachten.

Artikel 12 Auskunftsrecht der betroffenen Person

Artikel 12 normiert ein Auskunftsrecht. Die Mitgliedstaaten sollen sicherstellen, dass die betroffene Person Auskunft über ihre personenbezogenen Daten erhält. Der Anspruch basiert auf Artikel 12 lit. a der Richtlinie 95/46/EG, enthält jedoch einige Ergänzungen zum Umfang des Auskunftsrechts (Mitteilung zur Speicherfrist, zum Recht auf Berichtigung, auf Löschung oder Einschränkung der Verarbeitung sowie zum Beschwerderecht).
Artikel 12 Abs. 1 regelt, dass die betroffene Person ein Auskunftsrecht hat und legt den Umfang der Auskunft fest. Mitzuteilen ist der Zweck der Verarbeitung, die Kategorien personenbezogener Daten, die verarbeitet werden, die Datenempfänger, Speicherfristen, Berichtigungs- und Löschungsrechte, die Daten, die Gegenstand der Verarbeitung sind sowie alle verfügbaren Informationen über die Herkunft der Daten.
Die Polizei- bzw. Datenschutzgesetze der Länder sehen alle ein Recht auf Auskunft vor. Der Umfang der Auskunftserteilung ist jedoch differenziert ausgestaltet. **Die Landesgesetze regeln eine dem Artikel 12 Abs. 1 RL-E nur in Teilen entsprechende Auskunftspflicht** (vgl. § 25 HmbPolDVG i.V.m. § 18 HmbDSG, Artikel 48 Abs. 1 PAG BY, § 13a SOG LSA i.V.m. § 15 Abs. 1 S. 1 und 2 DSG LSA, § 18 Abs. 1 DSG NRW). So ist beispielsweise die Speicherfrist als solche sowie der Hinweis auf mögliche Berichtigungs- und Löschungsrechte durchgehend nicht Gegenstand der Auskunftspflicht, **schon deshalb dürfte ein Umsetzungsbedarf zu bejahen sein**.
Der Hinweis auf das Bestehen eines Beschwerderechts ist zumindest für den Fall vorgesehen, dass keine Auskunft erteilt wird (vgl. § 18 Abs. HmbDSG, Artikel 48 Abs. 3 S. 2 PAG BY, § 13a SOG LSA i.V.m. § 15 Abs. 5 DSG LSA, § 18 Abs. 6 DSG NRW). Gleiches gilt jeweils für das BKAG und das BPolG (vgl. § 19 Abs. 1 S. 1, Abs. 5 S. 2BDSG).
Welche personenbezogenen Daten genau damit gemeint sind, die Gegenstand der Verarbeitung sind, wird in Artikel 12 Abs. 1 lit. g nicht konkretisiert. Eine Verpflichtung zur Auskunft über die Herkunft der Daten besteht in Baden-Württemberg nicht und widerspricht geltendem Recht (vgl. § 45 PolG BW).
Anders als beispielsweise derzeit in § 19 Abs. 2 BDSG geregelt, dürften auch solche Daten von der Auskunftspflicht erfasst sein, die der Datensicherung oder der Datenschutzkontrolle dienen. Die Einbeziehung derartiger Daten erscheint jedoch entbehr-

lich, da schutzwürdige Interessen des Betroffenen dadurch nicht berührt werden (vgl. Gola/Schomerus, § 19 BDSG, Rn. 19f.).
Nach Abs. 2 kann die betroffene Person von dem für die Verarbeitung Verantwortlichen eine Kopie der verarbeiteten personenbezogenen Daten verlangen. Die Form der Auskunftserteilung wird von den zu untersuchenden Gesetzen nicht vorgegeben, sondern steht im Ermessen der Auskunft erteilenden Stelle. So heißt es in § 25 HmbPolDVG i.V.m. § 18 Abs. 1 S. 4 HmbDSG, dass die Daten verarbeitende Stelle die Form der Auskunftserteilung nach pflichtgemäßen Ermessen bestimmt (ebenso z.B. Artikel 48 Abs. 1 S. 3 PAG BY, § 13a SOG LSA i.V.m. § 15 Abs. 1 S. 4 DSG LSA, § 37 BPolG i.V.m § 19 Abs. 1 S. 4 BDSG, § 12 Abs. 5 BKAG i.V.m. § 19 Abs. 1 S. 4 BDSG).
Das Auskunftsrecht ist in Artikel 17 des RB Datenschutz deutlich reduzierter geregelt, denn dieser sieht entsprechend des ausdrücklichen Anwendungsbereiches (Datenverarbeitung zwischen den Mitgliedstaaten der EU) nur vor, dass die betroffene Person die Bestätigung erhält, dass sie betreffende Daten übermittelt oder bereit gestellt wurden, Informationen über die Empfänger oder Kategorien von Empfängern, an die die Daten weitergegeben wurden und eine Mitteilung über die Daten, die Gegenstand der Verarbeitung sind.
Im Strafprozess sind verschiedene Auskunftsrechte geregelt. Maßgeblich für die Einschlägigkeit ist die prozessuale Stellung des Antragstellers. Soweit die Erteilung oder Versagung einer Auskunft in der StPO nicht besonders geregelt ist, richtet sich die Auskunftserteilung – wie beim BPolG und dem BKAG – nach § 19 BDSG (vgl. § 491 Abs. 1 S. 1 StPO bzw. § 495 S. 1 StPO i.V.m § 19 BDSG). Besondere Regelungen für die Auskunftserteilung finden sich in §§ 147, 406e, 434 Abs. 1 Satz 2, § 442 Abs. 2 Satz 2, § 444 Abs. 2 Satz 2 StPO für besondere Verfahrensbeteiligte wie den unverteidigten Beschuldigten, den Verteidiger, den Verletzten, den Einziehungsbeteiligten. Der unverteidigte Beschuldigte hat selbst keinen generellen Anspruch auf Akteneinsicht. Er hat jedoch auf seinen Antrag hin einen Anspruch auf Auskünfte und Abschriften aus den Akten, wenn er sich ansonsten nicht angemessen verteidigen könnte; diesen Anspruch hat er allerdings nur, soweit der Untersuchungszweck auch in Bezug auf andere Strafverfahren nicht gefährdet werden kann und nicht überwiegende schutzwürdige Interessen Dritter entgegenstehen. Akten dürfen dem Beschuldigten grundsätzlich nicht überlassen werden. Der Verteidiger kann im gesamten Verfahren die Akten einsehen, im Vorverfahren kann dies jedoch beschränkt werden. Zwar ist die Erteilung von Abschriften und Ablichtungen ein Unterfall der Akteneinsicht, der Verteidiger hat allerdings keinen Anspruch darauf, dass ihm Abschriften oder Ablichtungen ausgehändigt werden (Meyer-Goßner, StPO, Kommentar, § 147, Rn. 6 m.w.N). Die Form der Auskunftserteilung wie auch der Umfang weichen zwar insoweit von den Vorgaben des Artikels 12 des RL-E ab. Die Beschränkung des strafprozessualen Auskunftsrechtes ist aber mit Blick auf Artikel 13 Abs. 1 lit. b zulässig.
Die bestehenden landesrechtlichen Regelungen, die das Auskunftsrecht als solches statuieren, werden als ausreichend angesehen. Insbesondere erscheint es nicht erforderlich, wie Artikel 12 Abs. 2 möglicherweise suggerieren mag und die

Kommission in den Beratungen auch zu verstehen gegeben hat, dass der betroffenen Person Auszüge in Form von Kopien der Akten- bzw. Dateieinträge zu übermitteln sind.Hierbei ist zu berücksichtigen, dass damit ggfs. auch andere personenbezogene Daten wiederum geschwärzt werden müssten. Hiermit würde ein erheblicher Bürokratieaufwand erzwungen werden, der zu dem dadurch erlangten Nutzen in keinem Verhältnis stünde. Schließlich würden so mitunter auch Verknüpfungen offenbar, die Rückschlüsse auf die polizeiliche Erkenntnisgewinnung ermöglichen.
Ungeachtet dieser grundsätzlichen Kritik, ist allerdings festzuhalten, dass ein Umsetzungsbedarf bestünde, wenn Artikel 12 in der derzeitigen Form verabschiedet werden würde.

Artikel 13 Einschränkung des Auskunftsrechts

Artikel 13 Absätze 1 und 2 sehen vor, unter welchen Voraussetzungen das Auskunftsrecht eingeschränkt werden kann. Nach Abs. 3 sind die Gründe für eine eingeschränkte oder teilweise Auskunftsverweigerung schriftlich mitzuteilen, es sei denn, dies liefe den eigentlichen Verweigerungsgründen zuwider. Unterbleibt eine schriftliche Begründung, so ist dies gemäß Abs. 4 zu dokumentieren.
Artikel 13 Abs. 1 listet Fallgruppen auf, welche die Mitgliedstaaten als Begründung für eine teilweise oder vollständige Einschränkung des Auskunftsrechtes in Rechtsvorschriften vorsehen können. Diese Fallgruppen überschneiden sich teilweise. So erfasst die öffentliche Sicherheit in Artikel 13 Abs. 1 lit. c auch die nationale Sicherheit sowie den Schutz der Rechte und Freiheiten anderer.
Eine Artikel 13 Abs. 1 vergleichbare Regelung fand sich bereits in Artikel 17 Abs. 2 des RB Datenschutz. Artikel 13 Abs. 1 lit. a, c-e entsprechen Artikel 17 Abs. 2 lit. a, c-e RB Datenschutz bereits nahezu im Wortlaut. In Artikel 13 Abs.1 lit. b heißt es, dass eine Beschränkung möglich ist, um die Aufdeckung oder Untersuchung von Straftaten zu gewährleisten. In Artikel 17 Abs. 2 lit. b heißt es stattdessen, dass die Auskunftsbeschränkung möglich ist, um die Feststellung und Ermittlung von Straftaten nicht zu beeinträchtigen. Letztlich kann hierin nur ein sprachlicher Unterschied erkannt werden, so dass Artikel 13 Abs. 1 lit. a-e mit Artikel 17 Abs. 2 lit. a-e RB Datenschutz identisch ist. Dies wird in den Erläuterungen zum Richtlinienentwurf ebenfalls so dargestellt (vgl. KOM [2012] 10, S. 9). Insoweit kann auf die Ausführungen des Berichts der BLAG zum Umsetzungsbedarf des RB Datenschutz (Stand: 22.8.2011, S. 36f.) zurückgegriffen werden: „Die Ausgestaltung der Verweigerungsgründe ist in den Ländern im Einzelnen unterschiedlich. Zumeist dürften die landesrechtlichen Bestimmungen bereits rahmenbeschlusskonform sein. Dies gilt insbesondere für die Länder, in denen als Ausschlussgründe die Gefährdung der Aufgabenerfüllung, die Gefährdung der öffentlichen Sicherheit oder Ordnung, Nachteile für das Wohl des Bundes oder eines Landes sowie Geheimhaltungsbedürftigkeit angeführt sind (…)“ (vgl. Artikel 48 Abs. 2 PAG BY, § 13a SOG LSA i.V.m. § 15 Abs. 4 DSG LSA, § 18 Abs. 3 DSG NRW, § 18 Abs. 3 i.V.m. § 12a Abs. 3 S. 2 Nrn. 3 - 5 HmbDSG; für den Bund vgl. § 19 Abs. 4 BDSG).
Darüber hinaus sieht Artikel 13 Abs. 1 vor, dass die Auskunftsbeschränkung in einer demokratischen Gesellschaft notwendig und verhältnismäßig sein und den berechtig-

ten Interessen der betroffenen Person Rechnung tragen muss. Dass eine Maßnahme erforderlich und angemessen sein muss, ist dem in Deutschland geltenden Verhältnismäßigkeitsgrundsatz immanent und hätte, wie schon beim RB Datenschutz, insofern keine eigenständige Bedeutung für eine mögliche Umsetzungsverpflichtung.
Nach Artikel 13 Abs. 2 können die Mitgliedstaaten Datenverarbeitungskategorien festlegen, für die die Ausnahmeregelung nach Abs. 1 vollständig oder teilweise zur Anwendung kommt. Der Begriff wird ebenfalls in Artikel 11 Abs. 5 verwendet. Anders als in Artikel 13 Abs. 2 wird dort auf den Begriff „gesetzlich" verzichtet. **Es ist unklar, was mit der Regelung bezweckt wird** (vgl. dazu bereits oben zu Artikel 11 Abs. 5).
Nach Artikel 13 Abs. 3 sind eine Verweigerung der Auskunft, wozu auch eine nur eingeschränkte Verweigerung gehört, sowie die Gründe dafür der betroffenen Person schriftlich mitzuteilen. Hiervon kann nur abgesehen werden, wenn dies einem der in Abs. 1 genannten Verweigerungsgründe zuwiderliefe. In jedem Fall ist die betroffene Person darüber zu unterrichten, dass sie bei der Aufsichtsbehörde eine Beschwerde einlegen oder den Rechtsweg beschreiten kann. Diese Regelung soll wiederum derjenigen in Artikel 17 Abs. 3 RB Datenschutz entsprechen(vgl. KOM [2012] 10, S. 9). Beide Normen statuieren zunächst die Schriftform soweit die Auskunft verweigert wird oder nur eingeschränkt erfolgt. Es sind auch jeweils die Gründe hierfür mitzuteilen. Davon kann nur abgesehen werden, wenn dies einem der in Artikel 13 Abs.1 lit. a bis e genannten Zwecke zuwiderliefe bzw. ein Grund nach Artikel 17 Abs. 2 lit. a bis e RB Datenschutz vorliegt. Die dort jeweils genannten Fallgruppen sind im Wesentlichen identisch (vgl. bereits oben zu Artikel 13 Abs. 1).
Für die Frage der Umsetzung kann insoweit aufgrund der dargelegten Vergleichbarkeit wiederum auf den Bericht zur Umsetzung des RB Datenschutz (Stand: 22.8.2011, S. 37) Bezug genommen werden. Danach stünden die Vorschriften in den Landesgesetzen, die von einer Begründungspflicht nur dann dispensieren, wenn durch die Begründung der Zweck der Ablehnung gefährdet würde (vgl. § 18 Abs. 4 S. 1 DSG NRW, § 25 HmbPolDVG i.V.m. § 18 Abs. 4 Satz 1 HmbDSG, § 13a SOG LSA i.V.m. § 15 Abs. 5 S. 1 DSG LSA; für den Bund vgl. § 19 Abs. 5 S. 1 BDSG) mit dem Richtlinienentwurf im Einklang. **Dies ist seinerzeit auch für enger gefasste Vorschriften vertreten worden, nach denen die Ablehnung der Auskunftserteilung generell keiner Begründung bedarf (vgl. z.B. Artikel 48 Abs. 3 Satz 1 PAG BY). Zwingend ist diese Annahme allerdings nicht.**
Nicht ganz unproblematisch ist, dass bei – auch teilweiser – Versagung der Auskunft Mitteilungen der Polizei schriftlich zu erfolgen haben, während die Landesgesetze jedenfalls überwiegend ein solches Erfordernis nicht ausdrücklich aufführen. Teilweise ist die Schriftform durch untergesetzliche Regelungen, etwa in polizeilichen Richtlinien, festgeschrieben. In diesen Fällen dürfte den Vorgaben des Richtlinienentwurfes ausreichend Rechnung getragen sein. Fehlt es auch hieran, kann ggf. darauf hingewiesen werden, dass die Versagung der Auskunft durchweg, d.h. in ständiger Praxis, schriftlich erfolgt und vor diesem Hintergrund eine Regelung entbehrlich ist.
In den Landesgesetzen ist ferner vorgesehen, dass bei Versagung der Auskunft der Betroffene darauf hinzuweisen ist, dass er sich an den Landesbeauftragten für den

Datenschutz wenden kann (vgl. § 18 Abs. 6 DSG NRW, § 18 Abs. 6 HmbDSG, § 13a SOG LSA i.V.m. § 15 Abs. 5 S. 2 DSG LSA, Artikel 48 Abs. 3 S. 2 PAG BY, § 48 PolBW i.V.m § 21 Abs. 4 LDSG BW; für den Bund vgl. § 19 Abs. 5 S. 2 BDSG). Dieser ist Aufsichtsbehörde im Sinne des Artikels 13 Abs. 3. Da der Hinweis hinsichtlich einer Rechtsschutzmöglichkeit genügt, besteht insoweit kein Umsetzungsbedarf (vgl. hierzu ebenfalls Bericht der BLAG zur Umsetzung des RB Datenschutz, Stand: 22.08.2011, S. 37).
Abs. 4 normiert eine Dokumentationspflicht für die Entscheidung, der betroffenen Person, die Gründe für die Verweigerung der Auskunft nicht mitzuteilen. Das Dokumentieren bzw. aktenkundig Machen wird als landesgesetzliche Vorgabe im Zusammenhang mit einer Auskunftsverweigerung nur in Teilen ausdrücklich geregelt, z. B. § 18 Abs. 4 S. 2 DSG NRW, wonach die wesentlichen Gründe für die Entscheidung aufzuzeichnen sind. Eine Umsetzungspflicht dürfte gleichwohl zu verneinen sein, denn für die öffentliche Verwaltung besteht eine Pflicht zur Aktenführung auch dann, wenn dies nicht ausdrücklich bestimmt ist (vgl. BVerfG, Beschluss vom 06.06.1983, NJW 1983, 2135 - stRspr.). Diese Pflicht wird durch die Gebote der Vollständigkeit, Aktenmäßigkeit und der wahrheitsgetreuen Aktenführung ausgefüllt. Die Aktenführung dient als Erkenntnisquelle für das Verwaltungshandeln und als Grundlage für die Nachprüfung der Verwaltungsentscheidungen durch übergeordnete Behörden und Gerichte. Im Zusammenhang mit dem - andernfalls nicht erfüllbaren - Akteneinsichtsrecht nach § 29 VwVfG wird die vorausgesetzte Pflicht zur Aktenführung / Dokumentation ebenfalls deutlich (so zur Dokumentationspflicht bei Datenübermittlung bereits im Bericht zur Umsetzung des RB Datenschutz [Stand: 22.08.2011, S. 18].

Artikel 14 Modalitäten der Wahrnehmung des Auskunftsrechts

Nach Artikel 14 Abs. 1 haben die Mitgliedstaaten festzulegen, dass die betroffene Person das Recht hat, die Aufsichtsbehörde um Prüfung der Rechtmäßigkeit der Verarbeitung zu ersuchen. Über dieses Recht besteht nach Abs. 2 eine Unterrichtungspflicht seitens des für die Verarbeitung Verantwortlichen.
Im Falle einer Überprüfung durch die Aufsichtsbehörde hat diese die betroffene Person mindestens darüber zu informieren, ob alle erforderlichen Überprüfungen vorgenommen wurden und welches Ergebnis diese hatten (Artikel 14 Abs. 3).
Der Regelungsgehalt des Artikels 14 ist aus sich heraus nicht schlüssig. So erweckt die Überschrift den Eindruck als regele Artikel 14 die Art und Weise der Ausübung des Auskunftsrechtes. Dem Wortlaut nach könnte dagegen angenommen werden, dass Artikel 14 nicht allein regelt, wie das Auskunftsrecht durch den Betroffenen wahrgenommen wird, sondern vielmehr, dass dem Betroffenen ein weiteres Recht einzuräumen ist, nämlich bei der Aufsichtsbehörde zu jeder Zeit um Prüfung der Rechtmäßigkeit der Datenverarbeitung nachsuchen zu können. Dafür spricht die Verwendung des Zusatzes „besonders“. In der hiesigen Rechtstechnik erfolgt eine derartige Verwendung, um einzelne Elemente einer Vorschrift zu erläutern oder zu konkretisieren und um deutlich zu machen, dass auch andere gleichartige Fälle, die nicht im Zusatz genannt werden, von der Vorschrift erfasst werden sollen (vgl. BMJ, Handbuch der Rechtsförmlichkeit, 2. Aufl. Rn. 71). Dies ist aber, wie sich aus den

Erläuterungen zu Artikel 14 ergibt, offenbar nicht gemeint. Danach regele Artikel 14, dass in Fällen, in denen das direkte Auskunftsrecht eingeschränkt sei, die betroffene Person über die Möglichkeit unterrichtet werden müsse, über die Aufsichtsbehörde mittelbar Auskunft zu erhalten, die das Recht an ihrer Stelle ausüben könne und die betroffene Person über das Ergebnis ihrer Nachforschungen informieren müsse (vgl. KOM (2012) 10, S. 9). Dieser Regelungsgehalt des Artikels 14 wird aus der Überschrift allerdings nicht deutlich.
Ein allgemeines Anrufungsrecht im Sinne des Artikel 14 Abs. 1 statuiert bereits Artikel 25 Abs. 3 RB Datenschutz.
Die Datenschutzgesetze gewähren jedermann das Recht, den Landesbeauftragten für den Datenschutz anzurufen (vgl. z.B. Artikel 9 DSG BY, § 25 DSG NRW, § 26 HmbDSG, § 13a SOG LSA i.V.m. § 19 DSG LSA; für den Bund vgl. § 37 BKAG i.V.m. § 21 BDSG, § 37 BPolG i.V.m § 21 BDSG). Damit ist dem Regelungsgehalt des Artikels 14, auch bei Zuhilfenahme der Erläuterungen, bereits hinreichend genüge getan. Teilweise existieren für den Fall einer nur eingeschränkten oder verweigerten Auskunft sogar spezielle Regelungen. So heißt es in § 15 Abs. 6 Satz 1 DSG LSA, der über § 13a SOG LSA zur Anwendung kommt, dass dem Betroffenen, dem keine Auskunft erteilt worden ist, diese auf sein Verlangen dem Landesdatenschutzbeauftragten zu erteilen ist, soweit nicht die jeweils zuständige oberste Landesbehörde im Einzelfall feststellt, dass dadurch die Sicherheit des Bundes oder des Landes gefährdet würde. Sowohl das allgemeine Anrufungsrecht wie auch spezielle Ausgestaltungen entsprechen den Vorgaben des Artikel 14 Abs. 1. **Ein Umsetzungsbedarf bestünde daher nicht.**
Dies gilt auch für die in Abs. 2 geregelte Unterrichtungspflicht. Im Zusammenhang mit einer nur eingeschränkten oder verweigerten Auskunft ist zu Artikel 13 bereits ausgeführt worden, dass die untersuchten Gesetze bei Versagen der Auskunft eine Hinweispflicht gegenüber dem Betroffenen enthalten, dass er sich an den Landesbeauftragten für den Datenschutz wenden kann. Dies macht allerdings zugleich deutlich, dass entweder Artikel 13 Abs. 3 Satz 1 a. E. oder Artikel 14 Abs. 2 entbehrlich ist, denn beide haben in der Sache den gleichen Regelungsgehalt.
Zwar ist Artikel 14 Abs. 3, der die Mitteilungspflicht über das Ergebnis der Rechtmäßigkeitsprüfung durch den Datenschutzbeauftragten zum Gegenstand hat, durch die Verwendung des Begriffs „sollte“ nicht als zwingende Vorgabe formuliert, tatsächlich entspricht dies aber ebenfalls bereits dem status quo. Aus den zum Petitionsrecht entwickelten Grundsätzen ergibt sich, dass der Datenschutzbeauftragte die Anrufung durch den Betroffenen entgegenzunehmen, zu bearbeiten und ihn in geeigneter Weise über das Ergebnis zu unterrichten hat (vgl. Gola/Schomerus, § 21 BDSG, Rn. 6).

Artikel 15 Recht auf Berichtigung

Artikel 15 Abs. 1 statuiert ein Berichtigungsrecht bei unzutreffenden personenbezogenen Daten. Mit „unzutreffend“ sind vermutlich unrichtige Daten gemeint. In den Erwägungsgründen zu Artikel 15 wird insoweit auch von unrichtigen personenbezogenen Daten gesprochen.

Nach Abs. 1 Satz 2 kann bei unvollständigen Daten eine Vervollständigung verlangt werden. Die hierfür gewählte Bezeichnung „Korrigendum“ ist im deutschen Polizeirecht allerdings nicht gebräuchlich. Ferner erschließt sich die Sinnhaftigkeit des Satzes 2 nicht, denn die Vervollständigung ist ein Unterfall der Berichtigung und daher bereits von Satz 1 erfasst. Insofern bedürfte es der Regelung in Satz 2 nicht.
Der Rahmenbeschluss des Rates 2008/977/JI vom 27.11.2008 über den Schutz personenbezogener Daten, die im Rahmen der polizeilichen und justiziellen Zusammenarbeit in Strafsachen verarbeitet werden (ABl. L 350, S. 60), enthält in Artikel 18 eine ähnliche Regelung. Hier wie dort wird **ein Umsetzungsbedarf nicht gesehen**, denn die in den Landesgesetzen enthaltene Verpflichtung zur Berichtigung (vgl. Artikel 45 Abs. 1 PAG BY, § 24 Abs. 1 HmbPolDVG, § 32 Abs. 1 PolG NRW, § 13a SOG LSA i.V.m. § 16 Abs. 1 DSG LSA) gibt dem Betroffenen zugleich einen entsprechenden Anspruch gegen die Polizei. Für die Bundespolizei und das BKA gilt dies ebenfalls (vgl. § 37 BPolG i.V.m. § 35 Abs. 1 BDSG, §§ 32, 33 BKAG).
Im Falle einer Verweigerung der Berichtigung haben die Mitgliedstaaten hierüber sowie über die Gründe schriftlich zu informieren. Die betroffene Person ist ferner auf die Möglichkeit hinzuweisen, eine Beschwerde bei der Aufsichtsbehörde einzulegen oder den Rechtsweg zu beschreiten (vgl. Artikel 15 Abs. 2).
Auch insoweit sieht der RB Datenschutz in Artikel 18 eine ähnliche Regelung vor. Eine Entsprechung von Artikel 15 Abs. 2 sieht das deutsche Landespolizeirecht nicht vor. Zu Artikel 18 des RB Datenschutz ist seinerzeit zutreffend wie folgt argumentiert worden: „Sofern man die Ablehnung entsprechender Anträge als Verwaltungsakt auffasst[9], ergibt sich aus § 37 Abs. 2 Satz 2 VwVfG eine Verpflichtung zur Schriftform, die allerdings nur bei berechtigtem Interesse eingreift und von dem Betroffenen unverzüglich verlangt werden muss. Ob dies den Anforderungen des Rahmenbeschlusses genügt, ist fraglich. Ausreichend wäre aber möglicherweise eine ständige Verwaltungspraxis, die den Vorgaben des Artikels 18 Satz 3 bereits entspricht. Hinsichtlich des erforderlichen Hinweises kommt dabei sowohl ein Hinweis auf die Rechtsschutzmöglichkeiten nach der Verwaltungsgerichtsordnung als auch – wie Satz 5 zeigt – ein Hinweis auf die Möglichkeit der Anrufung des Landesbeauftragten für den Datenschutz in Betracht.
Insbesondere aus Transparenzgründen liegt es nahe, zur Umsetzung eine ausdrückliche (neue) Regelung zu schaffen.“[10]

Artikel 16 Recht auf Löschung

Im RB Datenschutz ist wiederum in Artikel 18 eine ähnliche Regelung vorgesehen.

[9] Gola/Schomerus, BDSG, § 20 Rn. 40. Vgl. zum ähnlich gelagerten Fall der Verweigerung der Auskunft nach § 19 BDSG auch Gola/Schomerus, BDSG, § 19, Rn. 31; Mallmann in: Simitis, BDSG, § 19, Rn. 55; a.A. BayVGH, NVwZ 1990, 775.
[10] PG Rahmenbeschluss Datenschutz: Umsetzungsbedarf und Verhältnis zu Ratsbeschluss Prüm und Schwedische Initiative (Stand: 22.08.2011) S. 38; vgl. dort auch den Regelungsvorschlag. Soweit die Schaffung einer neuen Regelung für erforderlich gehalten wird, ist allerdings der Anwendungsbereich der Richtlinie zu beachten (Stichwort: keine Rechtsetzungskompetenz für rein innerstaatliche Datenverarbeitung).

Artikel 16 Abs. 1 des Richtlinienentwurfes normiert ein Löschungsrecht, wenn die Verarbeitung personenbezogener Daten mit Artikel 4 lit. a bis e sowie Artikel 7 oder 8 nicht vereinbar ist. **Die in den Landesgesetzen enthaltene Verpflichtung zur Löschung** (vgl. Artikel 45 Abs. 2 PAG BY, § 24 Abs. 2 HmbPolDVG, § 32 Abs. 2 PolG NRW, § 13a SOG LSA i.V.m. § 16 Abs. 2 DSG LSA; für den Bund vgl. § 35 Abs. 2 BDSG) **gibt dem Betroffenen zugleich einen Anspruch gegen die Polizei, so dass auch insoweit kein Umsetzungsbedarfbesteht**.[11]
Diese Löschung ist nach Artikel 16 Abs. 2 unverzüglich vorzunehmen. Die untersuchten Landesgesetze und das BDSG schreiben keine Frist vor, innerhalb derer die Löschung zu erfolgen hat, jedoch wird sie innerhalb zumutbarer Zeit durchgeführt werden müssen (vgl. Gola/Schomerus, § 35 Rn. 6). **Ein Umsetzungsbedarf wird daher nicht gesehen**.
In bestimmten in Artikel 16 Abs. 3 beschriebenen Fällen kann der für die Verarbeitung Verantwortliche statt der Löschung eine sog. Markierung vornehmen. Die Markierung gibt es als Rechtsbegriff im deutschen Recht nicht. Im RB Datenschutz konnte für den Fall, dass die Richtigkeit eines personenbezogenen Datums von der betroffenen Person bestritten wird und nicht ermittelt werden kann, ob diese richtig ist oder nicht, eine Kennzeichnung erfolgen. Eine Kennzeichnung ist im RB Datenschutz in Artikel 2 lit. j legaldefiniert als eine Markierung gespeicherter personenbezogener Daten, ohne dass damit das Ziel verfolgt wird, ihre künftige Verarbeitung einzuschränken. Eine solche Legaldefinition fehlt im RL-E. Die Markierung wird allerdings im Zusammenhang mit der Legaldefinition für eine „Einschränkung der Verarbeitung“ in Artikel 3 Abs. 4 erwähnt. Danach ist die „Einschränkung der Verarbeitung“ die Markierung gespeicherter personenbezogener Daten mit dem Ziel, ihre künftige Verarbeitung einzuschränken. Die Markierung ist Mittel zum Zweck und Voraussetzung, dass erkennbar ist, für welche Daten die Verarbeitung künftig eingeschränkt ist. Da in Artikel 16 Abs. 3 nicht die Einschränkung der Verarbeitung, sondern nur die Markierung vorgesehen ist, bleibt unklar, welche Rechtsfolge mit der Markierung verbunden ist. In den Erläuterungen des Vorschlages wird die Intention deutlich, mit dem Begriff Markierung den in Artikel 12 lit. b RL 95/46/EG und in Artikel 18 RB Datenschutz verwendeten mehrdeutigen Ausdruck „Sperrung“ zu ersetzen (vgl. KOM [2012] 10, S. 9). Aber auch dabei bleibt offen, inwiefern der Ausdruck mehrdeutig ist und welche Rechtsfolge vorliegend bezweckt ist, denn „Sperrung“ wäre zwar wieder ein im deutschen Recht gebräuchlicher Rechtsbegriff, dieser sähe allerdings als Rechtsfolge sehr wohl auch die Einschränkung der Verarbeitung vor (vgl. § 13a SOG LSA i.V.m. § 16 Abs. 3, 4 DSG LSA, § 24 Abs. 4 HmbPolDVG, § 32 Abs. 5 PolG NRW, Artikel 45 Abs. 3 BayPAG; gleiches gilt für die Bundespolizei und das BKA, vgl. § 35 Abs. 3, 4 BDSG). Wenn der Begriff Sperrung aber gerade ersetzt werden soll, möchte man mitunter die damit einhergehende Rechtsfolge gerade nicht. **Nach allem besteht an dieser Stelle noch Nachbesserungsbedarf.**

[11] Vgl. Ausführungen in PG Rahmenbeschluss Datenschutz: Umsetzungsbedarf und Verhältnis zu Ratsbeschluss Prüm und Schwedische Initiative (Stand: 22.08.2011) S. 37.

Besonders problematisch ist darüber hinaus, dass die Gründe, bei denen statt einer Löschung eine Markierung erfolgen kann, deutlich zu eng gefasst sind. Hier sind weitere Konstellationen in Artikel 16 (3) RL-E aufzunehmen, in denen Daten nicht gelöscht werden müssen, sondern lediglich zu markieren sind. Abs. 3 sollte dazu insbesondere wie folgt ergänzt werden:

> „(d) gesetzliche Dokumentations- oder Aufbewahrungspflichten einer Löschung entgegenstehen; in diesem Fall sind die Daten entsprechend der gesetzlichen Dokumentations- oder Aufbewahrungspflichten zu behandeln;
> (e) soweit sie nur zu Zwecken der Datensicherung oder der Datenschutzkontrolle gespeichert sind;
> (f) die Löschung technisch nur mit unverhältnismäßig hohem Aufwand möglich ist, z. B. wegen der besonderen Art der Speicherung;
> (g) schutzwürdige Interessen einer anderen betroffenen Person beeinträchtigt würden".

Würde auf eine ausdrückliche Regelung dieser Ausnahmegründe verzichtet, wären die Bundes- und Landesgesetze, die entsprechende Ausnahmeregelungen vorsehen, zwingend abzuändern. Dies wiederum hätte gravierende Folgen für die Tätigkeit der Polizei. Die Vorschrift ist insoweit als sehr kritisch anzusehen. Bedeutsam ist insbesondere die Schaffung einer Ausnahme für den Fall, dass eine Löschung wegen der besonderen Art der Speicherung nicht oder nur mit unverhältnismäßigem Aufwand möglich ist. Polizeipraktischer Hintergrund ist, dass in Back-up-Dateien gespeicherte Daten in der Regel nicht oder nur mit sehr großem technischem Aufwand individuell (selektiv) gelöscht werden können. Eine Löschungsverpflichtung wäre in diesen Fällen äußerst kontraproduktiv und in der Praxis kaum umsetzbar, weshalb sich hier eine Markierung/Sperrung anbietet, bis die komplette Back-up-Datei überspielt oder ggf. vernichtet wird.
Im Falle einer Verweigerung der Löschung oder der Markierung haben die Mitgliedstaaten hierüber sowie über die Gründe schriftlich zu informieren. Die betroffene Person ist ferner auf die Möglichkeit hinzuweisen, eine Beschwerde bei der Aufsichtsbehörde einzulegen oder den Rechtsweg zu beschreiten (vgl. Artikel 16 Abs. 4). Für das Verfahren im Falle der Weigerung der Löschung oder Markierung gilt das zu Artikel 15 Abs. 2 (Recht auf Berichtigung) Gesagte.

Artikel 17 Rechte der betroffenen Person in strafrechtlichen Ermittlungen und in Strafverfahren

1. Inhalt und Auslegungsprobleme
Die Norm räumt den Mitgliedstaaten ein, hinsichtlich der Ausübung der in Artikel 11 bis 16 genannten Rechte das einzelstaatliche Strafverfahrensrecht anzuwenden, wenn es „um personenbezogene Daten in einem Gerichtsbeschluss oder einem Gerichtsdokument geht, die in strafrechtlichen Ermittlungen und in Strafverfahren verarbeitet werden."
Entgegen diesem Wortlaut soll die Vorschrift nach Auffassung der KOM den Mitgliedstaatenkeine generelle Befugnis zur eigenständigen strafprozessualen Rege-

lung der Rechte des Betroffenen und insbesondere auch keine Abweichungsmöglichkeit von Artikel 11 bis 16 RL-E gewähren (anders aber Bäcker/Hornung, ZD 2012, 147, 148, wenn dort vertreten wird, dass Artikel 17 die Befugnis enthalte, die Betroffenenrechte im einzelstaatlichen Strafprozessrecht zu regeln, sofern es um strafrechtliche Ermittlungen oder Strafverfahren gehe).

2. Relevanz für die Polizei

Die Norm hat keine Auswirkungen auf präventiv-polizeiliche Regelungen, da nach dem eindeutigen Wortlaut lediglich „strafrechtliche Ermittlungen und Strafverfahren" erfasst werden. Auch für den repressiven Bereich hat die Norm für die Polizei keine Relevanz. Denn soweit Strafverfahren inmitten stehen, besteht grundsätzlich keine polizeiliche Zuständigkeit für die Erfüllung der in Artikel 11 bis 16 genannten Rechte, zumal wenn es um die Verarbeitung personenbezogener Daten in einem Gerichtsbeschluss oder einem Gerichtsdokument geht. Die Zuständigkeit liegt vielmehr bei den Strafgerichten bzw. den Staatsanwaltschaften (vgl. etwa §§ 147, 406e, 478 StPO).

3. Ergebnis

Es handelt sich um eine für die Polizei **unkritische Regelung**,die entgegen dem ersten Anschein allerdings auch keine Spielräume bei der Umsetzung der Artikel 11 bis 16 RL-E in nationales Recht schafft.

Kapitel IV Für die Verarbeitung Verantwortlicher und Auftragsverarbeiter

Artikel 18 Pflichten des für die Verarbeitung Verantwortlichen

Nach Anforderung des Artikels**18 Abs. 1** RL-E sind „geeignete" Strategien und Maßnahmen einzuführen, um die Einhaltung der in dem RL-E vorgesehenen, datenschutz-rechtlichen Bestimmungen zu gewährleisten. Das deutsche Datenschutzrecht hingegen sieht mit Ausnahme von § 7 DSG NRW nur vor, dass solche Maßnahmen getroffen werden, die erforderlich sind (vgl. § 9 BDSG,Artikel 7 BayDSG, § 9 Abs. 2 LDSG BW, § 10 Abs. 1 HDSG, § 8 Abs. 1 HmbDSG, § 6 DSG LSA). Welche Maßnahmen erforderlich sind, ist in den einzelnen Vorschriften legaldefiniert. Dies sind solche Maßnahmen, die in einem angemessenen Verhältnis zu dem jeweiligen Schutzzweck stehen. § 7 DSG NRW statuiert hingegen sehr generell die Pflicht, die Einhaltung der datenschutzrechtlichen Bestimmungen sicherzustellen. Grundsätzlich wird also **im deutschen Recht** ein Stufenverhältnis dergestalt begründet, dass je sensibler die Datenverwendung ist, desto höher der Aufwand sein muss, der zur Sicherstellung der Einhaltung der datenschutzrechtlichen Standards erforderlich ist. Es gilt also das **Verhältnismäßigkeitsprinzip**.

Diese Unterscheidung findet sich im RL-E nicht. Vielmehr sind nach dem Wortlaut alle geeigneten Maßnahmen zu ergreifen. Nach deutscher Rechtsprechung sind geeignete Maßnahmen solche, die der Förderung des Zwecks dienen. **Dies würde in qualitativer und quantitativer Hinsicht deutlich über den nach den datenschutzrechtlichen Vorschriften bisher geforderten Maßnahmen liegen**. Inwiefern hier Umsetzungsbedarf entsteht, der zu einer Einstufung des Artikels als **umset-**

zungskritisch führen würde, hängt im Ergebnis allerdings maßgeblich von der Frage ab, wie streng der RL-E ausgelegt wird. Neu ist jedenfalls, dass der RL-E ausdrücklich auch Strategien fordert. Zu bedenken ist, dass Artikel 18 Abs. 1 RL-E sämtliche Regelungen des RL-E in Bezug nimmt. Insofern haben sämtliche Abweichungen des RL-E vom deutschen Recht mittelbar Auswirkungen auf die Frage, welche Strategien und Maßnahmen zu ergreifen sind. Anders gesprochen, dürften sich Unterschiede zwischen gegenwärtig geltendem deutschen Recht einerseits und den datenschutzrechtlichen Bestimmungen des RL-E andererseits in der Praxis bei den nach Artikel 18 Abs. 1 RL-E zu ergreifenden Strategien und Maßnahmen besonders deutlich zeigen (z.B. kostenmäßig, aber etwa auch in Form eines steigenden Bürokratie- und Zeitaufwands). Dies gilt es bei der Prüfung aller Artikel des RL-E im Auge zu behalten. Sofern der RL-E eine Vollharmonisierung anstrebt, würde sich dies ebenfalls in erheblichem Maße auf die zu ergreifenden Strategien und Maßnahmen auswirken.

Artikel 18 Abs. 1 Auswirkungen der Änderungsvorschläge des LIBE-Ausschussberichtentwurfs:

Nach dem Änderungsvorschlag des Droutsas-Berichtsentwurfs soll, über die in Artikel 18 Abs. 1 RL-E statuierte Pflicht der Maßnahmenergreifung zur Einhaltung der Datenschutzbestimmungen hinaus, für jeden einzelnen Verarbeitungsvorgang der Nachweis durch die verarbeitende Stelle erbracht werden, dass alle datenschutzrechtlichen Standards bei der Datenverarbeitung eingehalten wurden. **Eine solche Dokumentationspflicht ist dem deutschen Recht bisher fremd.** Sie würde zu einem erheblichen Dokumentations- und Bürokratieaufwand führen und ist daher **sehrumsetzungskritisch** zu bewerten.

Der Richtlinienentwurf verweist in Artikel **18 Abs. 2 lit.d** auf Artikel 30, der wiederum festlegt, dass der Verantwortliche für die Datenverarbeitung einen Datenschutzbeauftragten benennen muss. Das deutsche Recht sieht auf landesrechtlicher Ebene zum Teil lediglich Ermessensnormen vor (vgl. § 10 LDSG BW; § 10a HmbDSG). Dies steht im Widerspruch zum RL-E, der eine gebundene Entscheidung normiert.

Insoweit wäre der RL-E **umsetzungskritisch** zu betrachten. Allerdings sind in tatsächlicher Hinsicht bereits bei allen Sicherheitsbehörden Datenschutzbeauftragte bestellt, so dass sich Umsetzungsbedarf lediglich in rechtlicher Hinsicht ergeben würde, der aber in der Praxis keinen Mehraufwand zur Folge hätte (vgl. Anlage, Gesamtbewertung zu Artikel 30).

Artikel 18 Abs. 2 Auswirkungen der Änderungsvorschläge des LIBE-Ausschussberichtentwurfs:

Nach dem Vorschlag des Ausschusses soll nach Artikel 18 Abs. 2 lit. aa als Maßnahme zur Sicherstellung der Datensicherheit im Sinne des Artikel 18 Abs. 1 eine Pflicht zur Durchführung einer **Datenschutz-Folgenabschätzung** eingeführt werden. Da eine Datenschutz-Folgenabschätzung im deutschen Recht bisher nicht vorgesehen ist, würde dieser Vorschlag mit Mehraufwand, insbesondere in organisatorischer Hinsicht, verbunden sein. Der Änderungsantrag 92 führt daher zu einer weiteren Verschärfung des Umsetzungsbedarfs und ist damit insgesamt als **umsetzungskritisch** zu bewerten.

Nach Artikel **18 Abs. 3** Satz 1 des RL-E soll der für die Datenverarbeitung Verantwortli-che geeignete Maßnahmen einführen, um die Wirksamkeit der von ihm getroffenen Strategien und Maßnahmen zu überprüfen. Das BDSG, sowie die einzelnen Landesgesetze sind zu dieser Frage sehr allgemein gehalten. Es ist lediglich geregelt, dass der Auftraggeber sich regelmäßig von der Einhaltung der beim Auftragnehmer getroffenen Maßnahmen überzeugen muss. Dies setzt nicht zwingend voraus, dass der Verantwortliche (dauerhafte) Maßnahmen zur Kontrolle zu etablieren hat. Vielmehr ist im deutschen Recht eine physische Überprüfung von Zeit zu Zeit jedenfalls auch denkbar. Ob eine solche Maßnahme auch als „geeigneter Mechanismus“ im Sinne des RL-E verstanden werden kann, scheint fraglich. Es ist nicht fernliegend, dass der RL-E hier strengere Maßstäbe normiert. Insoweit dürfte im deutschen Recht Umsetzungsbedarf entstehen, so dass die Vorschrift als **umsetzungskritisch** einzustufen ist. Eindeutiger Regelungsbedarf resultiert aus Artikel 18 Abs. 3 S. 2, der eine Überprüfung durch unabhängige interne oder externe Prüfer vorsieht, sofern dies verhältnismäßig ist. Eine solche Regelung findet sich im deutschen Datenschutzrecht nicht. Vorgesehen ist bei der eigenständigen Datenverarbeitung lediglich die Möglichkeit eines (freiwilligen) Datenschutzaudits zur Verbesserung des Datenschutzes gemäß § 9a BDSG. Darüber hinaus besteht bei der Auftragsdatenverarbeitung eine allgemeine Kontrollbefugnis der Aufsichtsbehörden, die jedoch nach freiem Ermessen erfolgt. Eine zwingende Prüfpflicht, wie sie der RL-E etablieren will, findet sich im deutschen Recht hingegen nicht. In tatsächlicher Hinsicht ergibt sich nach deutschem Recht allerdings ein Interesse an der Überprüfung aus der Verantwortlichkeit des Auftraggebers für die Einhaltung der datenschutzrechtlichen Bestimmungen gemäß § 11 Abs. 1 S. 1 BDSG. Auch im Landesrecht finden sich entsprechende Regelungen (vgl. Artikel 6 Abs. 1 S. 1 BayDSG, § 7 Abs. 1 S. 1 LDSG BW, § 4 Abs. 1 S. 1 HDSG, § 3 Abs. 1 S. 1 HmbDSG, § 6 Abs. 1 S. 1 DSG LSA, § 11 Abs. 1 S. 1 DSG NRW) Der RL-E dürfte in seinem Regelungsgehalt aber hierüber hinausgehen, so dass im Ergebnis **Umsetzungsbedarf** entstünde**, der für die Praxis zu erheblichen negativen Konsequenzen führen kann.**

Artikel 18 Abs. 3 S. 2 ist **daher** als **umsetzungskritisch** zu bewerten, weil er zu immensem Prüfaufwand führt. Da sich die Notwendigkeit der Einsetzung interner oder externer Prüfernach dem unbestimmten Begriff der Verhältnismäßigkeit bemisst, ist mit Rechtsunsicherheit zu rechnen.

Artikel 18 Abs. 3 Auswirkungen der Änderungsvorschläge des LIBE-Ausschussberichtsentwurfs:

Keine, da kein Änderungsantrag.

Artikel 19 Datenschutz durch Technik und durch datenschutzfreundliche Voreinstellungen

Artikel **19 Abs. 1** des RL-E legt fest, dass der Verantwortliche unter anderem durch technische und organisatorische Maßnahmen sicherstellt, dass die Datenverarbeitung rechtmäßig erfolgt und dürfte bereits hinreichend durch § 9 BDSG und die entsprechenden, vergleichbaren Regelungen des Landesrechts umgesetzt sein (vgl.Artikel 7 BayDSG, § 9 Abs. 2 LDSG BW, § 10 Abs. 1 HDSG, § 8 Abs. 1

HmbDSG, § 6 DSG LSA, § 7 DSG NRW). Exemplarisch für einen möglicherweise gleichwohl zumindest vereinzelt bestehenden Handlungsbedarf der Landesgesetzgeber sei jedoch auf § 7 DSG NRW verwiesen, der sehr allgemein gefasst ist und entgegen den Vorgaben des RL-E nicht explizit auf die technischen Anforderungen eingeht. Da es sich insoweit bei den Vorgaben des RL-E aber **wohl lediglich um Konkretisierungen des bereits bestehenden Schutzniveaus**handelt, ist der RL-E insoweit **nicht** als **umsetzungskritisch** einzustufen.

Artikel 19 Abs. 1 Auswirkungen der Änderungsvorschläge des LIBE-Ausschussberichtentwurfs:

Keine, da kein Änderungsantrag.

Artikel **19 Abs. 2** des RL-E regelt, dass Maßnahmen zu etablieren sind, die sicherstellen, dass nur die notwendigen Daten verarbeitet werden. Im deutschen Recht findet sich hierzu zumeinen die Verantwortlichkeit der verarbeitenden Stelle für die Einhaltung datenschutzrechtlicher Vorschriften, als auch der Grundsatz der Datensparsamkeit und Datenvermeidung. Die Regelungen sind jedoch sehr allgemein gefasst und stellen nicht auf bestimmte „Mechanismen“ ab. Sofern der RL-E dies fordert, entsteht Handlungsbedarf für die deutschen Gesetzgeber. Insbesondere durch die Notwendigkeit der Einführung besonderer Mechanismen ist die Vorschrift als **umsetzungskritisch** zu bewerten.

Artikel 19 Abs. 2 Auswirkungen der Änderungsvorschläge des LIBE-Ausschussberichtsentwurfs:

Der Änderungsantrag 93 konkretisiert die vom RL-E geforderten Mechanismen, die einzuführen sind. Da diese wie gesehen bisher im deutschen Recht nicht explizit geregelt sind, entstünde durch die Konkretisierung kein nennenswerter gesetzgeberischer Mehraufwand im Vergleich zum RL-E.

Artikel 20 Gemeinsam für die Verarbeitung Verantwortliche

Der RL-E sieht die Möglichkeit vor, dass mehrere Stellen gemeinsam für die Datenverarbeitung verantwortlich sind und untereinander eine Aufteilung der Verantwortung vereinbaren können und müssen. Auf Bundesebe findet sich eine solche Regelung nicht. Im BDSG wird eine Verbunddatei nur versteckt in § 6 Abs. 2 und § 8 Abs. 4 BDSG vorausgesetzt (ebenso §15 HDSG, § 4a DSG NRW, § 11a HmbDSG). In den einzelnen fachspezifischen Gesetzen des Bundes finden sich ebenso Vorschriften zu Verbunddateien (vgl. §§ 9a, 11 BKAG, § 486 StPO). Gleiches gilt vereinzelt auch für Landesrecht (vgl.§ 48a Polg BW, § 27 HmbPolDVG). Teilweise ist diesen Regelungen gemein (vgl. etwa § 11 BKAG), dass die Aufteilung der Verantwortlichkeit per Gesetz und nicht durch privatautonome Vereinbarung unter den verantwortlichen Stellen vorgenommen wird**. Insoweit entsteht Umsetzungsbedarf**. Dies gilt zunächst für den Fall einer Vollharmonisierung. Aber auch soweit der RL-E lediglich Mindeststandards formuliert, stellt sich die Frage, ob die gesetzlichen Lösungen des deutschen Rechts im Vergleich zur privatautonomen Systematik des RL-E ein „plus“ darstellen (dann kein Umsetzungsbedarf) oder aber ein „aliud“ (dann Umsetzungsbedarf). Inhaltlich ginge mit der Umstellung von der gesetzlich vorgesehenen Aufteilung der Verantwortlichkeiten hin zu einem vertragsorientierten System eine Verrin-

gerung des Datenschutzniveaus und ein Verlust an Rechtsklarheit einher. Artikel 20 ist daher insgesamt **sehr kritisch** zu sehen.

Artikel 20 Auswirkungen der Änderungsvorschläge des LIBE-Ausschussberichtsentwurfs:

Änderungsantrag 94 sieht unter 1. vor, dass die Bedingungen zwischen den Verantwortlichen schriftlich oder im Rahmen eines Rechtsakts erlassen werden können. Da dies nach deutschem Recht, wie soeben gesehen, bereits der Fall ist, würde der Änderungsantrag den Umsetzungsaufwand im Vergleich zum RL-E reduzieren.

Unter 2. sieht die Richtlinie vor, dass die betroffene Person ihre Rechte im Fall der Verantwortlichkeit mehrerer Stellen gegen alle gemeinsam ausüben kann. Dieser Grundsatz der Gesamtschuld ist bereits geltendes deutsches Recht und bedarf keiner weiteren Umsetzung, so dass hier kein Mehraufwand im Vergleich zum RL-E entsteht.

Artikel 21 Auftragsverarbeiter

Bezüglich Artikel**21 Abs.1** des RL-E besteht kein Regelungsbedarf. Die Prüfpflichten des Verantwortlichen bei der Auswahl eines Auftragsverarbeiters sind bereits in gleichem Maße, sowohl im deutschen Bundesrecht (vgl.§ 11 Abs. 2 BDSG), als auch in den einzelnen Landesgesetzen festgelegt (vgl. § 7 Abs. 2 LDSG BW, § 4 Abs. 2 HDSG, §§ 3, 8 HmbDSG, §§ 8 Abs. 2, 6 DSG LSA, §§ 11 Abs. 1, 10 DSG NRW). Der RL-E ist insoweit als **umsetzungsunkritisch** zu bewerten.

Artikel 21 Abs. 1 Auswirkungen der Änderungsvorschläge des LIBE-Ausschussberichtsentwurfs:

Der Änderungsantrag 95 konkretisiert den RL-E insoweit, als dass der für die Verarbeitung Verantwortliche im Rahmen der Auftragsdatenverarbeitung nur solche Auftragsverarbeiter auszuwählen hat, die insbesondere aufgrund technischer Sicherheitsvorkehrungen und organisatorischer Maßnahmen die Datensicherheit gewährleisten können. Da es sich hier lediglich um eine Klarstellung des RL-E handelt und dem Verantwortlichen keine zusätzlichen Prüfpflichten auferlegt werden, ist der Änderungsantrag nicht mit Mehraufwand verbunden und insoweit nicht umsetzungskritisch zu beurteilen.

Anders beurteilt sich dies jedoch hinsichtlich Artikel**21 Abs. 2 RL-E**. Darin ist zum einen vorgesehen, dass die Verbindung zwischen Verantwortlichem und Auftragsdatenverarbeiter auf Grund eines Rechtsakts erfolgen muss. Geregelt ist im deutschen Recht lediglich die Schriftlichkeit der Auftragsvergabe (vgl. § 11 Abs. 2 S. 2 BDSG, Artikel 6 Abs. 2 S. 2 BayDSG, § 7 Abs. 2 S. 2 LDSG BW, § 4 Abs. 1 S. 2 HDSG, § 3 Abs. 2 S. 2 HmbDSG, § 8 Abs. 2 S. 2 DSG LSA, § 11 Abs. 1 S. 4 DSG NRW). Zum anderen bestimmt der RL-E, dass in dem Rechtsakt insbesondere für Fälle, in denen eine Übermittlung der personenbezogenen Daten nicht zulässig ist, festgelegt wird, dass nur auf Weisung des Verantwortlichen gehandelt werden darf.

Grundsätzlich unterliegt jeder Auftragsverarbeiter nach deutschem Recht den Weisungen der für die Datenverarbeitung verantwortlichen Stelle. Gemäß § 11 Abs. 3 BDSG besteht die Befugnis zur Datenverarbeitung „im Rahmen der Weisungen“ (vgl. zum Landesrecht die regelungsidentischen Vorschriften: Artikel 6 Abs. 3 S. 2

BayDSG, § 7 Abs. 3 S. 2 LDSG BW, § 4 Abs. 2 S. 2 HDSG, § 3 Abs. 2 S. 2 HmbDSG, § 8 Abs. 3 DSG LSA, § 11 Abs. 1 S. 2 DSG NRW), wobei der RL-E explizit Handeln „auf Weisung“ vorsieht. Bei strenger Auslegung dieser Formulierung könnte die Frage aufgeworfen werden, ob beide Begriffe tatsächlich identisch sind. Der RL-E könnte eine Weisung des für die Datenverarbeitung Verantwortlichen in jedem Einzelfall regeln wollen, was augenscheinlich so im deutschen Recht nicht vorgesehen ist. Sollte mit dem RL-E tatsächlich eine solche Weisung des Auftraggebers für jede einzelne Datenverarbeitung des Auftragsverarbeiters eingeführt werden, würde die Auftragsdatenverarbeitung insgesamt ad absurdum geführt, da ihr Zweck ja gerade in der Übertragung der Datenverarbeitung auf einen Dritten und der damit einhergehenden organisatorischen Entlastung des Verantwortlichen besteht. Daher ist wohl eher davon auszugehen, dass die Formulierung „auf Weisung“ identisch mit der deutschen Formulierung „im Rahmen der Weisung“ ist.
Insgesamt ist Artikel 21 Abs. 2 somit als **umsetzungskritisch** zu beurteilen. Das Ausmaß des entstehenden Umsetzungsbedarfs ist schwer zu prognostizieren und hängt von der Auslegung des RL-E ab:
Sofern der RL-E dahingehend verstanden wird, dass in Artikel 21 Abs. 2 HS 1 eine Verpflichtung des deutschen Gesetzgebers statuiert wird, die Beziehung zwischen dem Auftragsdatenverarbeiter und dem Verantwortlichen auszugestalten, bestünde Um-setzungsbedarf, sowohl auf Bundes-, als auch auf Landesebene. Der RL-E wäre insofern als **umsetzungskritisch** einzustufen.
Für den Fall, dass Artikel 21 Abs. 2 HS 2 so verstanden werden sollte, dass in dem (entsprechend den Vorgaben des HS 1 erlassenen) Gesetz eine Pflicht des Verantwortlichen statuiert werden muss, dass insbesondere im Bezug auf Daten, deren Übermittlung unzulässig ist, nur auf Einzelweisung des Verantwortlichen gehandelt werden darf, bestünde erheblicher Umsetzungsbedarf; dies gilt sowohl materiellrechtlich, als auch organisatorisch und personell bei den jeweiligen verantwortlichen Stellen. Insofern wäre der RL-E als **sehr umsetzungskritisch** einzustufen.
Artikel 21 Abs. 2 Auswirkungen der Änderungsvorschläge des LIBE-Ausschussberichtsentwurfss:
Der Änderungsantrag 96 ist in diesem Zusammenhang zumindest teilweise zu begrüßen. Er legt zunächst fest, dass die Beziehungen zwischen dem Verantwortlichen und dem Auftragsverarbeiter auch „durch Vertrag“ geregelt werden können. Dies ist in Deutschland so bereits gesetzlich geregelt und **würde im Unterschied zum RL-E daher keinen Umsetzungsaufwand mit sich bringen** (vgl. § 11 Abs. 2 S. 2 BDSG, Artikel 6 Abs. 2 S. 2 BayDSG, § 7 Abs. 2 S. 2 LDSG BW, § 4 Abs. 1 S. 2 HDSG, § 3 Abs. 2 S. 2 HmbDSG, § 8 Abs. 2 S. 2 DSG LSA, § 11 Abs. 1 S. 4 DSG NRW).
Des Weiteren konkretisiert der Änderungsantrag die erforderlichen Inhalte des Rechtsaktes oder Vertrages.
Da nach deutschem Recht die Vertragsbeziehungen bereits in der Praxis vertraglich festgelegt sind, wäre hier zu prüfen, inwieweit gesetzlich bereits Inhaltsanforderungen an die Verträge gestellt werden müssten, um die Vorgaben des RL-E umzusetzen. Die entsprechenden Vorschriften enthalten bereits Regelungen, die im Kern denen des Änderungsvorschlages entsprechen (vgl. § 11 Abs. 2 BDSG, Artikel 6 Abs. 2

BayDSG, § 7 Abs. 2 LDSG BW, § 4 Abs. 1 HDSG, § 3 Abs. 2 HmbDSG, § 8 Abs. 2 DSG LSA, § 11 Abs. 1 DSG NRW). Insoweit müsste eventuell lediglich vereinzelt eine gesetzliche Klarstellung erfolgen.
In gesetzgeberischer Hinsicht bestünde daher Handlungsbedarf, so dass die Vorschrift als **umsetzungskritisch** anzusehen ist.
Insgesamt ist der Änderungsantrag 96 **im Vergleich zum RL-E allerdings** als **wenigerumsetzungskritisch** zu beurteilen.
Hinsichtlich Artikel **21 Abs. 3** besteht Handlungsbedarf. Es wird abermals auf die Regelungen einer Verbunddatei verwiesen, die im deutschen Recht (s.o. Anmerkungen zu Artikel 20) so nicht vorgesehen ist.
Artikel 21 Abs. 3 Auswirkungen der Änderungsvorschläge des LIBE-Ausschussberichtsentwurfs:
Keine, da kein Änderungsantrag.

Artikel 22 Verarbeitung unter der Aufsicht des für die Verarbeitung Verantwortlichen und des Auftragsverarbeiters

Es sollen sowohl Personen, die Zugang zu personenbezogenen Daten haben, als auch der Auftragsdatenverarbeiter selbst nur „auf Weisung“ des für die Datenverarbeitung Verantwortlichen handeln dürfen oder, wenn dies besonders gesetzlich vorgesehen ist.
Bezüglich des Weisungsrechts an den Auftragsdatenverarbeiter sei nach oben zu den Anmerkungen hinsichtlich Artikel 21 Abs. 2 RL-E verwiesen. Die gleiche Problematik ergibt sich hier. Sollte an dieser Stelle ein Einzelweisungsrecht des Verantwortlichen für Datenverarbeitung für seine Beschäftigten, den Auftragsdatenverarbeiter selbst sowie dessen Beschäftigte statuiert werden, würde dies in der Praxis zu erheblichen Schwierigkeiten führen. Sollte der Passus „auf Weisung“ entsprechend der deutschen Formulierung „im Rahmen der Weisung“ zu verstehen sein, entstünde kein Umsetzungsbedarf. Der Auftragsverarbeiter selbst handelt schon aufgrund des Vertrages mit dem Verantwortlichen im Rahmen von dessen Weisung, seine Beschäftigten können sich naturgemäß nur in dem Rahmen der Weisung bewegen, da sie die Datenverarbeitung für den Auftragsdatenverarbeiter ausführen und die Beschäftigten des Verantwortlichen sind ebenso im Rahmen des Arbeits-/Dienstverhältnisses an dessen Weisungen gebunden.Allerdings ist im deutschen Recht kein datenschutzspezifisches Weisungsrecht vorgesehen.
Abschließend beurteilt dürfte bei strenger Auslegung des RL-E Umsetzungsbedarf für die deutschen Gesetzgeber entstehen, so dass der RL-E für diesen Fall als **umsetzungskritisch** anzusehen wäre.
Artikel22Auswirkungen der Änderungsvorschläge des LIBE-Ausschussberichtsentwurfs:
Der Ausschussbericht führt einen neuen Abs. 1a ein, nach dem das nicht ausschließlich auf Weisung des Verantwortlichen rückführbare Handeln, sowie die Erhaltung von Entscheidungsbefugnissen beim Auftragsverarbeiter hinsichtlich Zweck, Mittel oder Methoden der Datenverarbeitung dazu führen soll, dass dieser als gemeinsam Verantwortlicher im Sinne des Artikels 20 gilt.

Eine vergleichbare gesetzliche Regelung gibt es weder auf Bundes-, noch auf Landesebene. Insoweit es um Artikel 20 geht, sei nach oben verwiesen. Soweit es um das Handeln auf Weisung geht, besteht wie oben ausgeführt wiederum die Frage der Auslegung des RL-E.
Es bestünde **gesetzgeberischer Handlungsbedarf (zumindest in klarstellender Hinsicht), so dass der Änderungsvorschlag als im Verhältnis zum RL-E kritischer zu betrachten wäre.**

Artikel 23 Dokumentation

Der RL-E bestimmt in Artikel **23 Abs. 1**eine weitreichende Dokumentationspflicht über Datenverfahren und Datensysteme.
Weder im Bundesrecht, noch in den verschiedenen landesrechtlichen Vorschriften ist eine solche Pflichtausdrücklich vorgesehen. Im BDSG ist geregelt, dass vor Inbetriebnahme der Datenverarbeitung die Pflicht besteht, das jeweilige Vorhaben mit detaillierten Angaben an die zuständige Aufsichtsbehörde zu melden(vgl. §§ 38 Abs. 2 i.V.m. 4d, 4e, 24 BDSG). Selbige führt dann ein Register über die Verarbeitungen. Der Betroffene hat zudem unter anderem gemäß § 19 Abs. 1 BDSG das Recht, Auskunft über die zu ihm gespeicherten Daten zu erlangen.Im Ergebnis ist eine Dokumentation über die Datenaufzeichnung in Deutschland auf Bundesebene daher zwar im Gesetz impliziert, jedoch nicht ausdrücklich normiert. Auch reichen der Auskunftsanspruch und die Aufzeichnungspflicht nicht annähernd so weit wie die Regelungen des RL-E.
Im Unterschied hierzu ist in den einzelnen Landesgesetzen die Verpflichtung des Datenverarbeitenden ein Verfahrensverzeichnis anzulegen ausdrücklich geregelt (vgl. § 11 Abs. 2 LDSG BW, § 6 Abs. 1 HDSG, § 26 HmbPolDVG, § 14 Abs. 3 DSG LSA, § 8 Abs. 1 DSG NRW), wobei deren jeweilige Detailgenauigkeit unklar ist. In Bayern ist ein solches Verzeichnis beim Datenschutzbeauftragten zu führen (vgl. Artikel 27 i.V.m. Artikel 26 BayDSG),
Daher besteht insgesamt umfassender Handlungsbedarf der deutschen Gesetzgeber. Der RL-E ist damit als **umsetzungskritisch** zu bewerten.
Inhaltlich bedarf es weiterer Prüfung, ob und inwieweit mit den Dokumentationspflichten des RL-E eine Anhebung des Datenschutzniveaus einhergeht und inwieweit diese in einem angemessenen Verhältnis zum ansteigenden Bürokratieaufwand steht.
Artikel **23 Abs. 2** des RL-E legt Mindestangaben fest, die in den, nach Artikel 23 Abs. 1 zu erstellenden, Verzeichnissen enthalten sein sollen. Insoweit wird auf die Ausführung zu Artikel 23 Abs. 1 verwiesen. Die Mindestangaben korrespondieren weder im Bundes-, noch im Landesrecht zur Gänze mit den Vorgaben zu den zu erstellenden Verzeichnissen, so dass auch hier **Umsetzungsbedarf für den Gesetzgeber** entstünde und damit einhergehend ein **gesteigerter Dokumentationsaufwand** bei den verantwortlichen Stellen. Artikel 23 Abs. 2 des RL-E ist damit als **umsetzungskritisch** einzustufen.
Artikel 23 Abs. 2 Auswirkungen der Änderungsvorschläge des LIBE-Ausschussberichtentwurfs:

Die Änderungsanträge 99-104 legen weitere inhaltliche Anforderungen an die zu führenden Verzeichnisse fest, die in ihrem Umfang weit über das hinausgehen, was der RL-E bereits fordert. Insoweit wird der Umsetzungsbedarf im Verhältnis zum RL-E sowohl im gesetzgeberischen Bereich, als auch vor allem im Rahmen der Dokumentation bei den verantwortlichen Stellen noch stark erhöht. **Die Änderungsanträge sind folglich im Verhältnis zu dem RL-E als umsetzungskritischer zu bewerten.**
Gemäß Artikel**23 Abs. 3 RL-E** sind die Verzeichnisse nach Artikel23 Abs. 1 der Aufsichtsbehörde auf Anforderung zur Verfügung zu stellen. Auf Bundesebene dürfte diese Regelung für öffentliche Stellen gemäß §§ 11 Abs. 4 Nr. 1 i.V.m. 24 Abs. 4 BDSG, für nicht-öffentliche Stellen gemäß §§ 38 Abs. 3 i.V.m. 11 Abs. 4 Nr. 2 BDSG bereits hinreichend klar normiert sein. Es dürfte somit kein zusätzlicher gesetzgeberischer Handlungsbedarf entstehen. In Bayern ist ein solches Verzeichnis beim Datenschutzbeauftragten selbst zu führen (vgl. Artikel 27 i.V.m. Artikel 26 BayDSG). Darüber hinaus besteht ein umfassendes Auskunftsrecht der Aufsichtsbehörde gemäß Artikel 32 BayDSG. Entsprechendes regeln auch die übrigen Landesgesetze (vgl. § 29 Abs. 1 HDSG, § 29 LDSG BW, § 23 Abs. 5 HmbDSG, § 23 Abs. 1 DSG LSA, § 22 Abs. 2 DSG NRW)
Der RL-E ist insoweit demnach nicht als umsetzungskritisch zu bewerten.
Artikel 23 Abs. 3 Auswirkungen der Änderungsvorschläge des LIBE-Ausschussberichtsentwurfs:
Der Änderungsantrag 105 konkretisiert inhaltlich die Informationspflichten. Da im deutschen Recht bereits umfassende Informationspflichten gegenüber der Aufsichtsbehörde bestehen, dürfte insoweit kein weiterer gesetzgeberischer Handlungsbedarf entstehen, so dass der Änderungsantrag ebenso als **umsetzungsunkritisch** zu bewerten ist.

Artikel 24 Aufzeichnung von Vorgängen

Der RL-E bestimmt in Artikel**24 Abs. 1** welcher Art die Daten sein müssen, die bei der Datenverarbeitung zu dokumentieren sind. Eine solch allgemeine und umfassende Protokollierungspflicht ist dem deutschen Datenschutzrecht fremd. Insbesondere ist entgegen der Regelung im RL-E nicht normiert, dass Zweck, Datum und Uhrzeit jeder Datenabfrage oder Datenweitergabe gespeichert werden müssen.
Nach § 19 BDSG hat der Betroffene allerdings ein Recht auf umfassende Auskunft über zu ihm gespeicherten und weitergeleiteten Daten. Die einzelnen Landesgesetze enthalten ebenfalls einen Auskunftsanspruch des Betroffenen (vgl. § 21 LDSG BW, Artikel 10 BayDSG, § 18 HDSG, § 18 HmbDSG, § 15 DSG LSA, § 18 DSG NRW). Voraussetzung für die Beantwortung solcher Auskunftsbegehren ist die vorherige Dokumentation der Daten. Im Umfang bleiben die Auskunftsansprüche im Bundes- und Landesrecht allerdings hinter den Dokumentationspflichten nach Artikel 24 Abs. 1 RL-E bei weitem zurück, so dass aus dem Vorhandensein dieser Ansprüche nicht auf eine bereits implizit bestehende Dokumentationspflicht im Sinne des Artikel 24 Abs. 1 RL-E geschlossen werden kann. Exemplarisch für eine besonders geregelte Dokumentationspflicht sei jedoch auf §§ 11 Abs. 6 und 9 Abs. 3 BKAG verwiesen.

In der Gesamtschau entsteht folglich **umfassender Regelungsbedarf**. Vor allem der **Bürokratieaufwand** in der Praxis dürfte ganz erheblich sein, was im Ergebnis zu einer Bewertung dieses Artikels als **umsetzungskritisch** führt.

Artikel 24 Abs. 1 (Auswirkungen der Änderungsvorschläge des LIBE-Ausschussberichtsentwurfs:

Änderungsantrag 106 verschärft die Anforderungen an die Dokumentationspflicht bezüglich der Identität des Empfängers. Insoweit entsteht im Vergleich zum RL-E ein nochmals **marginal erhöhter Handlungsbedarf**.

Ähnlich wie die Bewertung zu Artikel 24 Abs. 1 fällt auch die Bewertung hinsichtlich **Artikel 24 Abs. 2** aus, wonach die aufgezeichneten Daten nur zu eng bestimmten Zwecken verwendet werden dürfen. Eine derart spezifische Regelung findet sich im deutschen Recht nicht wieder. In der Gesamtschau der datenschutzrechtlichen Normen ließe sich zwar argumentieren, dass die dokumentationsspezifischen Vorgaben des RL-E bereits insoweit im deutschen Recht aufgegriffen sind, als nach den allgemeinen Grundsätzen insbesondere des BDSG jede Datenverarbeitung einer gesetzlichen Ermächtigung bedarf und nur in den eng vom Gesetz vorausgesetzten Grenzen zulässig ist. Allerdings ist fraglich, ob diese allgemeinen Normen zur Umsetzung der Vorgaben des RL-E den erforderlichen konkreten Bezug gerade zu solchen Daten aufweisen, die zu Dokumentationszwecken erhoben wurden. Zumindest unter dem Aspekt der Normenklarheit und notwendigen Bestimmtheit der Regelungen dürfte insoweit wohl ein Regelungsdefizit bestehen. Bei dessen Behebung wäre zu beachten, dass letztlich sämtliche Grundsätze zur Datenverarbeitung dokumentationspflichtenspezifisch ergänzt bzw. geändert werden müssten. Dies betrifft letztlich die Gesamtstruktur des BDSG und der entsprechenden Landesgesetze, so dass sich hier äußerst komplexe Fragestellungen ergeben können.

Artikel 24 Abs. 2 RL-E ist daher als **umsetzungskritisch** zu bewerten.

Artikel 24 Abs. 2 Auswirkungen der Änderungsvorschläge des LIBE-Ausschussberichtsentwurfs:

Der Änderungsantrag 107 will eine weitere Auskunftspflicht des Verantwortlichen und des Auftragsdatenverarbeiters gegenüber der Aufsichtsbehörde bezogen auf die nach Artikel 24 Abs. 2 RL-E zu speichernden Daten statuieren.

Es gilt entsprechend das zu Artikel 23 Abs. 3 RL-E Gesagte, so dass der Änderungsantrag als **umsetzungsunkritisch** zu bewerten ist.

Artikel 25 Zusammenarbeit mit der Aufsichtsbehörde

Der RL-E sieht in Artikel **25 Abs. 1** eine Pflicht des Verantwortlichen und des Auftragsdatenverarbeiters zur „Zusammenarbeit“ mit der Aufsichtsbehörde vor, insbesondere in Form umfassender Informationsübermittlung. Gemäß §§ 11 Abs. 4 Nr. 1 i.V.m. 24 Abs. 4 BDSG besteht für öffentliche Stellen die Verpflichtung, die Aufsichtsbehörde bei ihrer Aufgabenwahrnehmung zu „unterstützen“. Gleiches gilt für die Landesgesetze, die allerdings nicht zwischen der Art der Stelle unterscheiden (vgl. §§ 11 Abs. 4 i.V.m. 38 Abs. 3 und 24 Abs. 4 BDSG, Artikel 32 BayDSG, § 29 Abs. 1 HDSG, § 29 LDSG BW, § 23 Abs. 5 HmbDSG, § 23 Abs. 1 DSG LSA, § 22 Abs. 2 DSG NRW). Mit „Unterstützung“ und „Zusammenarbeit“ dürfte das Gleiche

gemeint sein. Lediglich auf Bundesebene ist eine solche Vorschrift in Bezug auf nicht-öffentliche Stellen nicht vorhanden. Insoweit bestünde Umsetzungsbedarf, da der RL-E nicht nach Art der Stelle zu differenzieren scheint. Zwar erstreckt sich der Anwendungsbereich des RL-E gemäß Artikel 1 Abs. 1 nur auf die Datenverarbeitung durch Behörden, mithin den öffentlichen Sektor. In Artikel 3 Abs. 7 des RL-E wird jedoch der Auftragsverarbeiter unter anderem definiert als natürliche oder juristische Person oder als Behörde.
Es bestünde demnach **Umsetzungsbedarf nur in geringem Maße auf Bundesebene**.
Artikel 25 Abs. 1 Auswirkungen der Änderungsvorschläge des LIBE-Ausschussberichtsentwurfs:
Änderungsantrag 108 konkretisiert zunächst die Informationspflichten betreffend alle personenbezogenen Daten und Informationen, die die Aufsichtsbehörde zur Erfüllung ihrer Aufgaben benötigt. Da diese, wie gesehen, bereits vom bestehenden Auskunftsanspruch nach deutschem Recht erfasst sind, ergibt sich insoweit **kein weiterer Umsetzungsbedarf.**
Des Weiteren schreibt der Änderungsantrag vor, dass die Mitgliedstaaten explizit regeln, dass der Aufsichtsbehörde Zugang zu allen Räumlichkeiten, Anlagen und Mitteln der Verantwortlichen oder der Auftragsdatenverarbeiter gewährt wird. Der Anspruch auf Zutritt zu den Diensträumen ist vom BDSG und den einzelnen Landesgesetzen jeweils explizit erfasst (vgl. §§ 24 Abs. 4, 38 Abs. 4 BDSG, § 29 Nr. 2 HDSG, Artikel 32 BayDSG, § 29 LDSG BW, § 23 Abs. 5 HmbDSG, § 23 Abs. 1 DSG LSA, § 22 Abs. 2 DSG NRW) Im Übrigen sollten die Vorgaben von der grundsätzlichen Pflicht umfasst sein, die Aufsichtsbehörde zu unterstützen.
Es ergäbe sich demnach nur weiterer Umsetzungsbedarf, wenn man den Zugang zu Anlagen und Mitteln nicht von den bisherigen Vorschriften als umfasst ansehen würde, beziehungsweise eine Regelung zur Klarstellung einführen wollte.
Insgesamt wäre aber auch für diesen Fall der **zusätzliche Umsetzungsaufwand** als **gering** anzusehen.
Gemäß Artikel**25 Abs. 2** Satz 1 ist der Aufsichtsbehörde in angemessener Frist zu antworten. Im deutschen Recht findet sich lediglich in. § 38 Abs. 3 BDSG eine vergleichbare Regelung, die auf den Auftragsverarbeiter über § 11 Abs. 4 BDSB Anwendung findet. § 38 Abs. 3 BDSG sieht eine „unverzügliche“ Mitteilung vor
Jedoch findet sich im vorliegend relevanteren öffentlichen Bereich weder auf Bundesnoch auf Landesebene eine vergleichbare Norm, auch wenn verwaltungsintern eine allgemeine, nicht normierte Pflicht zur guten und zügigen Zusammenarbeit bestehen mag.
Als nicht unkritisch ist zu bewerten, dass der RL-E davon ausgeht, dass die Aufsichtsbehörde auch im öffentlichen Bereich anordnungsbefugt ist (vgl. Artikel 25 Abs. 2 in Verbindung mit Art 46 lit. b RL-E). Das geltende deutsche Recht sieht in §§ 24, 25 BDSG nur ein Beanstandungsrecht und kein Weisungsrecht vor. Darauf sei im Zusammenhang mit Artikel 46 lit. b RL-E näher eingegangen (siehe unten).
Folglich ist im Ergebnis ein deutlicher Regelungsbedarf vorhanden und die **Gesamtbewertung des Artikels fällt umsetzungskritisch aus.**

Die nach Artikel 25 Abs. 2 S. 2 des RL-E vorausgesetzte Dokumentation von Maßnahmen, die nach Rüge der Aufsichtsbehörde erfolgt sind, ist u.a. in § 25 Abs. 3 BDSG für den öffentlichen Sektor implementiert und teilweise vergleichbar auf landesrechtlicher Ebene. Für den nicht-öffentlichen Bereich findet sich keine explizite Normierung. Insoweit dürfte **Umsetzungsbedarf** bestehen.

Artikel 25 Abs. 2 Auswirkungen der Änderungsvorschläge des LIBE-Ausschussberichtsentwurfs:

Änderungsantrag 109 sieht vor, dass die angemessene Frist im Sinne des RL-E von der Aufsichtsbehörde selbst zu setzen ist. Insoweit dürfte zusätzlich zu dem o.a. Regelungsbedarf ein solcher auch auf Bundesebene in Bezug auf nicht-öffentliche Stellen bestehen. **Der Änderungsvorschlag ist insofern als umsetzungskritischer einzuschätzen.**

Artikel 25 a NEU Auswirkungen der Änderungsvorschläge des LIBE-Ausschussberichtsentwurfs:

Änderungsantrag 110 sieht die Einführung einer **Datenschutzfolgenabschätzung** für solche Datenverarbeitungsvorgänge vor, die wahrscheinlich mit besonderen Risiken verbunden sind. Bisher ist im deutschen Recht keine solche Datenschutzfolgenabschätzung geregelt. Zwar sieht auf Bundesebene § 4d BDSG eine Vorabkontrolle in bestimmten Fällen vor, aber auch diese bleibt in Inhalt und Umfang deutlich hinter dem Vorschlag des Ausschusses zurück. Entsprechende Regelungen finden sich auch in den Landesgesetzen (Artikel 26 BayDSG, § 12 LDSG BW, § 14 Abs. 2 DSG LSA, § 10 Abs. 3 DSG NRW, § 8 HmbDSG, § 7 Abs. 4 HDSG).Sowohl mit Blick auf das Erfordernis einer gesetzgeberischen Tätigkeit auf Bundes- und Landesebene, als auch und vor allem mit Rücksicht auf den enormen Bürokratie- und Organisationsaufwand, den die Einführung einer solchen Vorschrift mit sich bringen würde, ist der Änderungsantrag als **sehr umsetzungskritisch** einzustufen.

Artikel 26 Vorherige Zurateziehung der Aufsichtsbehörde

In Artikel**26 Abs. 1** RL-E ist ausführlich geregelt, wann der Verantwortliche und der Auftragsdatenverarbeiter die zuständige Aufsichtsbehörde zu Rate zu ziehen haben. Eine solche gesetzliche Regelung existiert in Deutschland derzeit nicht. Es besteht lediglich sowohl auf Bundes-, als auch auf Landesebene die Möglichkeit einer Vorabkontrolle, die allerdings deutlichen Einschränkungen unterliegt (§ 4d BDSG, Artikel 26 BayDSG, § 12 LDSG BW, § 14 Abs. 2 DSG LSA, § 10 Abs. 3 DSG NRW, § 8 HmbDSG, § 7 Abs. 4 HDSG). Die Vorgabe des RL-E, gerade bei der Verwendung neuer Technologien die Aufsichtsbehörde anzurufen, findet sich im deutschen Recht nicht wieder.

Zusammenfassend ist deshalb anzumerken, dass die Umsetzung einen nicht zu vernachlässigenden Aufwand bedeuten würde. Die Einbindung der Aufsichtsbehörde würde den Verwaltungsaufwand stark erhöhen, auch gerade vor dem Hintergrund einer nicht allzu umfassenden Erhöhung des Datenschutzniveaus. Gesetzgeberischer Handlungsbedarf besteht gleichwohl. Der Artikel ist daher als **umsetzungskritisch** zu bewerten.

Artikel 26 Abs. 1 Auswirkungen der Änderungsvorschläge des LIBE-Ausschussberichtsentwurfs:
Änderungsvorschlag 111 sieht vor, dass eine Zurateziehung der Aufsichtsbehörde nach Artikel 26 Abs. 1 RL-E nur in bestimmten, risikoreichen Fällen vorgesehen wird. Insbesondere wenn eine Risikofolgenabschätzung diese hohen Risiken bescheinigt.
Insgesamt ist damit festzuhalten, dass der Änderungsantrag, soweit er die Notwendigkeit einer vorherigen Absprache schmälert, im Umsetzungsaufwand hinter dem RL-E zurückbleibt. Jedoch nimmt der Vorschlag Bezug auf die Risikofolgenabschätzung. Insoweit ist er als **sehr umsetzungskritisch**anzusehen (vgl. oben unter Artikel 25a NEU).
Artikel 26 Abs. 1a NEU Auswirkungen der Änderungsvorschläge des LIBE-Ausschussberichtentwurfs:
Änderungsantrag 112 sieht vor, dass die Aufsichtsbehörde im Rahmen der vorherigen Zurateziehung bei Zweifeln an der Rechtmäßigkeit der geplanten Verarbeitung diese untersagen kann. Auch eine solche Eingriffsbefugnis mit unter Umständen weitreichenden praktischen Auswirkungen für die Polizeiarbeit ist im deutschen Recht bisher nicht geregelt, da wie oben festgestellt nicht einmal eine vorherige Zurateziehung vorgeschrieben ist. Im Vergleich zum RL-E würde der Änderungsvorschlag daher zu größerem Umsetzungsaufwand führen und ist damit als**sehrumsetzungskritisch** einzustufen.
Artikel**26 Abs. 2** stellt es ins Ermessen des Mitgliedstaates, eine Liste mit Datenverarbeitungsvorgängen zu erstellen, die einer Pflicht zur vorherigen Zurateziehung der Aufsichtsbehörde unterliegen. Angesichts der Ausgestaltung als Ermessensvorschrift entsteht insoweit kein zwingender gesetzgeberischer Handlungsbedarf.
Artikel 26 Abs. 2 Auswirkungen der Änderungsvorschläge des LIBE-Ausschussberichtsentwurfs:
Im Gegensatz zum RL-E stellt der Änderungsantrag 113 unter anderem das Erstellen einer Liste nach Artikel 26 Abs. 2 nicht ins Ermessen der Mitgliedstaaten. Diese Liste ist zu erstellen und von der Aufsichtsbehörde an die für die Verarbeitung Verantwortlichen und den Europäischen Datenschutzausschuss zu übermitteln. Hier besteht zusätzlicher Umsetzungsaufwand in rechtlicher, aber vor allem in organisatorischer Hinsicht, so dass der **Antrag als im Vergleich zu dem RL-E umsetzungskritischer** einzuschätzen ist.

Artikel 27 Sicherheit der Verarbeitung

Artikel 27 enthält die Regelungen zum **technischen und organisatorischen Datenschutz**, die bereits in der Artikel 17 Abs. 1 der Richtlinie 95/46/EG und Artikel 22 des Rahmenbeschlusses 2008/977/JI enthalten waren. Die Ausgestaltung des technisch-organisatorischen Datenschutzes auf normativer Ebene entspricht somit der bisherigen Ausgestaltung auf europäischer Ebene. Neu ist lediglich, dass diese Verpflichtung auch auf den Auftragsdatenverarbeiter erstreckt wird.
Im Verhältnis zum Bundesdatenschutzgesetz besteht **kein Handlungsbedarf**, da die Regelungen des § 9 BDSG und dessen Anlage, also die vorzusehenden technisch-organisatorischen Maßnahmen, den Regelungen des Richtlinienentwurfs entspre-

chen. Fraglich könnte dies bei einzelnen landesgesetzlichen Regelungen sein, die anstelle von einzelnen Maßnahmen Datenschutzziele definieren, da sich die Kommission gegen das Formulieren von Datenschutzzielen entschieden hat, wie es beispielsweise von der Konferenz der Datenschutzbeauftragten des Bundes und der Länder gefordert wird.[12] Soweit nunmehr auch der Auftragsdatenverarbeiter einbezogen ist, ist dies in der Praxis unproblematisch, da dies durch § 11 BDSG über die vertragliche Regelung mit dem Auftragsdatenverarbeiter bereits sicherzustellen war.
Das **Datenschutzniveau** wird durch diese Vorschriften **weder abgesenkt noch erhöht.**Auch aus **polizeitaktischer Sicht ist die Regelung unkritisch**, zumal bei den Sicherheitsbehörden von jeher besondere Anforderung an die Sicherheit der Datenverarbeitung gestellt werden.
Zu begrüßen ist, dass die Regelung auf den Stand der Technik abstellt und auch den Aufwand für Schutzmaßnahmen in ein Verhältnis zu den Risiken der Verarbeitung setzt. Die Regelung bleibt technikneutral, was im Hinblick auf die schnelle Entwicklung der Technik auch sinnvoll ist. Im Gegensatz zur dieser Technikneutralität steht allerdings die der **Kommission** eingeräumte **Möglichkeit, Durchführungsbestimmungen zur situationsabhängigen Konkretisierung** zu erlassen. Dieser Vorbehalt für die Kommission ist **unnötigund könnte zudem (in Abhängigkeit von den konkreten Durchführungsbestimmungen) zu gesetzgeberischem Handlungsbedarf führen**. Gerade soweit beispielsweise die explizit genannte Verschlüsselung betroffen ist, hat der deutsche Gesetzgeber die Auswahl des Verschlüsselungsverfahrens und die verwendeten Schlüssellängen bewusst der Entscheidungsfreiheit der verantwortlichen Stelle überlassen, weil abhängig von dem jeweils ausgewählten Verschlüsselungsverfahren eine Reihe zusätzlicher Aspekte zu berücksichtigen seien, so z.B. Schlüsselgenerierung, Schlüsselverteilung, Performance der Verschlüsselung, Schlüsselsicherheit und Handhabbarkeit.[13] Detaillierte Vorgaben durch delegierte Rechtsakte sind bei Regelungen des technischen Datenschutzes wenig sinnvoll.[14]

Artikel 28 Meldung einer Verletzung des Schutzes personenbezogener Daten an die Aufsichtsbehörde

Wird der **Schutz persönlicher Daten** durch die verantwortliche Stelle **verletzt**, so hat die verantwortliche Stelle dies innerhalb von **24 Stunden der Aufsichtsbehörde zu melden**. Kommt es bei einem Auftragsdatenverarbeiter zu einer solchen Datenpanne, so hat dieser die verantwortliche Stelle zu unterrichten. Für die Meldung an die Aufsichtsbehörde ist detailliert vorgegeben, welchen Inhalt die Meldung haben muss. Zudem müssen die Verletzung des Schutzes personenbezogener Daten und die entsprechenden Abhilfemaßnahmen dokumentiert werden. Die Kommission ist

[12] Eckpunktepapier der Konferenz der Datenschutzbeauftragten des Bundes und der Länder „Ein modernes Datenschutzrecht für das 21. Jahrhundert“ S. 18 ff.
[13] Ernestus in Simitis, Bundesdatenschutzgesetz, 7. Auflage 2010, § 9 Rnr. 176.
[14] So beispielsweise auch die Stellungnahme des Deutschen Richterbundes zum Datenschutzpaket der Europäischen Kommission vom Februar 2012, S. 22 zum Pendant der Regelung in der Datenschutz-Grundverordnung.

ermächtigt, die Kriterien und Anforderungen für die Feststellung der genannten Verletzungen und die konkreten Umstände, unter denen die Meldung zu erfolgen hat, festzulegen und ggf. eine Standardvorlage zu erlassen.
Bei dieser Regelung besteht bei den Datenschutzgesetzen der Länder **erheblicher Umsetzungsbedarf**, da eine solche Regelung für öffentliche Stellen bisher nicht besteht. Zwar enthält das BDSG mit § 42a BDSG eine Benachrichtigungspflicht für den Fall, dass Daten unrechtmäßig übermittelt werden oder auf sonstige Weise Dritten unrechtmäßig zur Kenntnis gelangen. Diese Vorschrift gilt allerdings nur für nichtöffentliche Stellen. Insoweit ist die **Regelung vollständig umzusetzen.**
Aus **polizeitaktischer Sicht ist die Regelung ebenfalls kritisch**, weil datenschutzrechtliche Verletzungen üblicherweise nur mit sehr großem Aufwand aufgeklärt werden können und es infolgedessen unmöglich sein dürfte, die Meldung binnen der nach dem RL-E vorgesehenen 24-Stunden-Frist vorzunehmen. Gerade bei größeren Sicherheitsbehörden verlangt allein die verlässliche Aufklärung eines solchen Vorgangs, dass verschiedene Stellen (Leitung, örtliche Ebene, IT-Sicherheit, Datenschutz ggf. Innenrevision) beteiligt werden, so dass eine Frist von 24 Stunden vor diesem Hintergrund deutlich zu kurz ist. Hinzukommt, dass die Meldung nach Artikel 28 Abs. 3 RL-E nicht nur Informationen zur erfolgten Verletzung enthalten soll, sondern auch eine Beschreibung der möglichen Folgen sowie Empfehlungen zu deren Eindämmung. Hier droht eine Informationsbürokratie, die die eigentlich vordringlichen Arbeiten – die tatsächliche Eindämmung des entstandenen oder noch im Entstehen begriffenen Schadens – zu Unrecht in den Hintergrund rückt.
Hinzu kommt, dass bei einer Umsetzung in das deutsche Recht geregelt werden muss, wie mit diesen Meldungen bei den Aufsichtsbehörden umzugehen ist, insbesondere in den entsprechenden Tätigkeitsberichten. Gerade bei technischen Datenpannen ist denkbar, dass eine Veröffentlichung, insbesondere von Einzelheiten kritisch sein kann. Die polizeilichen Belange und Aufgabenwahrnehmung dürfen ebenso wie die schutzwürdigen Interessen Dritter durch die Meldepflicht nicht gefährdet werden; eine entsprechende Ausnahmeregelung fehlt im RL-E indes. Hier müsste bei einer Umsetzung sichergestellt werden, dass keine Veröffentlichung erfolgt oder ausschließlich in abstrakter Form. Vor diesem Hintergrund ist auch der Änderungsvorschlag im Berichtsentwurf des Ausschusses für bürgerliche Freiheiten, Justiz und Inneres problematisch, der verlangt, dass die Aufsichtsbehörde ein öffentliches Register über die Art der gemeldeten Verletzungen führt.[15]
Das Ansinnen der Regelung ist eine **Erhöhung des Datenschutzniveaus**, da durch die Benachrichtigung der Aufsichtsbehörde gewährleistet wird, dass eine externe Kontrollinstanz über Verletzungen des Schutzes personenbezogener Daten, informiert wird.

[15] Änderungsantrag 116 im Berichtsentwurf des Ausschusses für bürgerliche Freiheiten, Justiz und Inneres (LIBE-Ausschuss) über den Vorschlag für eine Richtlinie des Europäischen Parlaments und des Rates 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 (COM(2012)0010 – C7-0024/2012 – 2012/0010(COD)).

Die Regelung birgt allerdings **eine erhebliche Gefahr**:
Aus der Stellung der Regelung ist zu schließen, dass diese Benachrichtigungspflicht nur dann greift, wenn durch einen Verstoß gegen die Vorgaben des technischen Datenschutzes der Schutz personenbezogener Daten verletzt wurde, also bei sogenannten Datenpannen. Dies ergibt sich allein aus der Stellung und Systematik der Norm und nicht aus dem Wortlaut. Hätte die Regelung zur Folge, dass **jede Verletzung des Rechts auf Schutz der persönlichen Daten**, beispielsweise durch eine rechtswidrige Speicherung, **mitzuteilen** wäre, hätte dies gravierende Konsequenzen. Dies würde dazu führen, dass die ggf. unterschiedlich zu beurteilende Rechtsfrage, ob eine Nutzung bzw. Speicherung der Daten zulässig ist, eine entsprechende Benachrichtigungspflicht auslösen würde. Dies müsste deshalb auch im Wortlaut entsprechend klargestellt werden, da ansonsten das Risiko besteht, dass die Norm durch den EuGH dahingehend ausgelegt wird, dass tatsächlich über jede rechtswidrige Datennutzung zu informieren ist.
Auch bei dieser Regelung ist die **Möglichkeit der Kommission, detaillierte Vorgaben zu machen**, **verfehlt**. Der Verwaltungsablauf ist in den Mitgliedstaaten unterschiedlich, es tut nicht Not, hier durch detaillierte Vorgaben unter Umständen systemfremde Verfahrensvorgaben zu machen. Zudem drohen möglicherweise weitere bürokratische Hindernisse, die heute noch nicht absehbar sind.
Insgesamt ist Artikel 28 aus verschiedenen Gründen (kurze Frist, Umfang der Meldepflicht, Fehlen geeigneter Ausnahmen zur Wahrung polizeilicher Belange) kritisch zu sehen.

Artikel 29 Benachrichtigung der betroffenen Person von einer Verletzung des Schutzes personenbezogener Daten

Artikel 29 sieht vor, dass auch die betroffene Person ohne unangemessene Verzögerung von der Verletzung des Schutzes personenbezogener Daten zu benachrichtigen ist, wenn die Wahrscheinlichkeit besteht, dass der Schutz der personenbezogenen Daten oder der Privatsphäre der betroffenen Person beeinträchtigt wird. Die Verpflichtung entfällt, wenn die verantwortliche Stelle nachweist, dass sie geeignete Schutzmaßnahmen getroffen hat und diese nach Auffassung der Aufsichtsbehörde ausreichend waren. Die Benachrichtigungspflicht kann entsprechend der Vorgaben des Artikels 11 Abs. 4 ausgeschlossen werden.
Auch hier besteht im **deutschen Recht** mit Ausnahme einzelner Landesdatenschutzgesetze für die öffentlichen Stellen noch **keine vergleichbare Regelung**, so dass diese **Regelung umzusetzen** wäre. Auch soweit einzelne Landesgesetze bereits eine Benachrichtigungspflicht vorsehen, sind diese nicht ausreichend, da lediglich schwerwiegende Beeinträchtigungen die Benachrichtigungspflicht auslösen.[16] Im Gegensatz dazu macht der Richtlinienentwurf diese Einschränkung nicht. Es ist dort lediglich von Beeinträchtigungen die Rede.
Inwieweit die Regelung **polizeitaktische Folgen** hat, hängt letztlich von der **Umsetzung des Artikels 11 Abs. 4 des Richtlinienentwurfs** ab. Wenn tatsächlich ge-

16 so beispielsweise § 18a LDSG Rheinland-Pfalz; § 23 LDSG Mecklenburg-Vorpommern .

währleistet würde, dass die Aufgabenwahrnehmung der Sicherheitsbehörden nicht beeinträchtigt wird und die Regelungssystematik der Strafprozessordnung nicht ausgehebelt wird, bestünden**keine polizeitaktischen Bedenken**. Es kommt bei der **Umsetzung insoweit darauf an, den von Artikel11 Abs. 4 vorgegeben Rahmen auszuschöpfen** und an die Besonderheiten polizeilicher und strafverfahrensrechtlicher Erfordernisse anzupassen. Sollte Artikel 11 Abs. 4 nicht entsprechend umgesetzt werden oder kommt es nach der Umsetzung in nationales Recht zu einer engeren Auslegung des Artikels 11 Abs. 4 durch den EuGH, so **können polizeitaktische Konsequenzen nicht ausgeschlossen werden.**Dies scheint die wahrscheinlichere Variante, da der in Artikel 29 Abs. 4 RL-E vorgesehene Verweis auf Artikel 11 Abs. 4 RL-E als Ausnahmeregelung zu betrachten und dementsprechend restriktiv auszulegen ist.

Die Regelung dient der **Transparenz des Datenschutzes**, insbesondere für die Betroffenen. Durch die Regelung wird ein Sanktionsinstrument auf Sicherheitsbehörden übertragen, das der deutsche Gesetzgeber lediglich für nicht-öffentliche Stellen vorgesehen hat: Für den nicht-öffentlichen Bereich wird davon ausgegangen, dass die Verpflichtung, Betroffene zu informieren, aufgrund der negativen Publizität zu einer Stärkung des Datenschutzes führe.[17]Dies entspricht der Tendenz, die Ausgestaltung des Datenschutzes im öffentlichen und nicht-öffentlichen Bereich zu vereinheitlichen.[18] Damit soll der Schutz verbessert werden. Zu hinterfragen ist allerdings, ob der Ansatz – Sanktion durch „negative Publicity“ - bei Sicherheitsbehörden sinnvoll bzw. notwendig ist. Die öffentliche Verwaltung ist an Recht und Gesetz gebunden,auch existiert durch die Rechts- und die Fachaufsicht und die Kontrolle der Gerichte bereits ein Kontrollsystem, das auch die Einhaltung datenschutzrechtlicher Regelungen gewährleistet.

Insgesamt ist Artikel 29 daher kritisch zu sehen.

Artikel 30 Benennung eines Datenschutzbeauftragten

Artikel 30 regelt die **Verpflichtung** der verantwortlichen Stelle einen **Datenschutzbeauftragten zu benennen** und formuliert die Grundanforderungen an die **Qualifikation** des Datenschutzbeauftragten.

Diese **Regelung** ist aus **deutscher Sicht unbedenklich**. Im Bundesdatenschutzgesetz ist die Bestellung eines Datenschutzbeauftragten für öffentliche Stellen bereits verpflichtend vorgeschrieben, so dass insoweit kein Umsetzungsbedarf besteht. Dies sieht bei den Ländern teilweise anders aus, da die Bestellung eines Datenschutzbeauftragten nicht in allen Landesdatenschutzgesetzen verpflichtend vorgeschrieben ist, sondern als Kann-Bestimmung ausgestaltet ist.[19] Aus praktischer Sicht ist dies

[17] Dix, in Simitis (Hrsg.), Bundesdatenschutzgesetz, 7. Aufl. 2010, § 42a Rnr. 1; ebenso Hornung, zur Datenschutzgrundverordnung, ZD 2012, S. 99, 103.

[18] So auch im Berichtsentwurf (siehe FN 10), in dem an anderer Stelle ausdrücklich klargestellt wird, dass zwei unterschiedliche Systeme im Falle einer Verletzung des Schutzes personenbezogener Daten nicht zu rechtfertigen sind.

[19] So beispielsweise in § 10 LDSG Baden-Württemberg.

unbedenklich, da bei den Sicherheitsbehörden auch in den Ländern durchweg Datenschutzbeauftragte bestellt sind.
Ebenso **unbedenklich sind die Anforderungen an die Qualifikation**, die sich bereits heute im deutschen Recht finden, da die entsprechende Fachkunde vorausgesetzt wird. Die Fachkunde nach dem Bundesdatenschutzgesetz setzt rechtliche, organisatorische und technische Kenntnisse voraus und entspricht somit den Forderungen des Richtlinienentwurfs. Im Gegensatz zum Richtlinienentwurf verlangt das Bundesdatenschutzgesetz neben der Fachkunde auch die Zuverlässigkeit. Dies ist auch sinnvoll, da über dieses Kriterium sowohl die persönliche Zuverlässigkeit sowie mögliche Interessenkollision berücksichtigt werden können. Soweit die Richtlinie keine Vollharmonisierung anstrebt (vgl. Wesentliche Ergebnisse, 6)), kann dieses Kriterium auch beibehalten werden, was zu begrüßen ist.

Artikel 31 Stellung des Datenschutzbeauftragten

Artikel 31 verlangt eine frühzeitige Einbindung in die Behandlung aller mit dem Schutz personenbezogener Daten zusammenhängenden Fragen, wobei sowohl von der verantwortlichen Stelle als auch vom Auftragsdatenverarbeiter sicherzustellen ist, dass der Datenschutzbeauftragte die Mittel erhält, die er zur wirksamen Erfüllung seiner Pflichten und Aufgaben gemäß Artikel 32 benötigt. Gleichzeitig wird festgeschrieben, dass der Datenschutzbeauftragte keine Weisungen bezüglich seiner Tätigkeit erhält.
Die Vorschrift ist im **deutschen Recht** bereits **umgesetzt**. Insoweit besteht **kein Anpassungsbedarf.** Das Bundesdatenschutzgesetz geht aber weiter als der Richtlinienvorschlag, da der Beauftragte dem Leiter der verantwortlichen Stelle direkt unterstellt ist und zusätzlich ein Benachteiligungsverbot festgeschrieben ist, einschließlich eines spezifischen Kündigungsschutzes.[20]
Auch soweit festgelegt ist, dass der Datenschutzbeauftragte frühzeitig einzubinden ist, hat diese Regelung bereits jetzt im deutschen Recht eine Entsprechung, da im Bundesdatenschutzgesetz bereits eine Unterrichtungspflicht bei Vorhaben der automatisierten Verarbeitung personenbezogener Daten vorgesehen ist.
Aus **polizeilicher Sicht** ist die Regelung **unkritisch** und aufgrund der Rechtslage in Deutschland **ohne Folgen für das Datenschutzniveau**.

Artikel 32 Aufgaben des Datenschutzbeauftragten

Artikel 32 enthält einen Katalog an Aufgaben des behördlichen Datenschutzbeauftragten. So hat der behördliche Datenschutzbeauftragte die verantwortliche Stelle bei der Umsetzung und Anwendung datenschutzrechtlicher Vorgaben und Vorschriften zu beraten und zu überwachen. Eingeschlossen von der Überwachungspflicht sind auch die Strategien zum Schutz personenbezogener Daten.
Geht man von der Ausgestaltung im Bundesdatenschutzgesetz aus, so sind die Beratungs- und Überwachungsaufgaben des Richtlinienentwurfs bereits erfasst, da der

[20] Dieser Punkt wird auch im Berichtsentwurf des Europäischen Parlamtents (s. FN 10) aufgegriffen; siehe Änderungsantrag 121.

behördliche Datenschutzbeauftragte nach § 4g BDSG auf die Einhaltung des BDSG hinzuwirken und entsprechende Beratungs- und Kontrollpflichten hat. Soweit **Überwachungspflichten hinsichtlich der Einhaltung datenschutzrechtlicher Vorgaben** und Vorschriften vorgegeben werden, besteht deshalb **kein Umsetzungsbedarf**.

Im Gegensatz dazu besteht **Umsetzungsbedarf**, soweit **Regelungen** aufgrund des Richtlinienentwurfs **neu** aufzunehmen sind. Dies wären folgende Regelungen:

- Sicherstellung, dass die in Artikel 23 vorgesehene Dokumentation vorgenommen wird,
- Meldung an die Aufsichtsbehörde und Benachrichtigung der betroffenen Personen bei Verletzung des Schutzes persönlicher Daten (Artikel 28 und 29),
- Tätigkeit als Ansprechpartner für die Aufsichtsbehörde.

Viel wesentlicher ist allerdings **folgende Konsequenz** des Richtlinienentwurfs, die allerdings allein Auswirkungen auf Bundesebene hat, da eine vergleichbare Regelung in den Landesdatenschutzgesetzen nicht besteht.

Die bisherige Regelung **des § 4g Abs. 3 Satz 2 BDSG**, (ähnlich auch § 14 1 Abs. 2 S. 2 DSG LSA), nach der der behördliche Datenschutzbeauftragte von Sicherheitsbehörden sich außerhalb der Vorabkontrolle nicht direkt an die Aufsichtsbehörde wenden kann, ist **teilweise nicht** mit den Vorgaben des Richtlinienentwurfs **vereinbar**. § 4g Abs. 3 Satz 2 BDSG beschränkt das Recht des behördlichen Datenschutzbeauftragten sich außerhalb der Vorabkontrolle an die Aufsichtsbehörde zu wenden. Der behördliche Datenschutzbeauftragte hat zunächst das Benehmen mit der Behördenleitung herzustellen. Bei Unstimmigkeiten entscheidet die oberste Dienstbehörde, ob die Aufsichtsbehörde angerufen werden kann. Diese Regelung wäre nicht richtlinienkonform und wäre abzuändern.

Aus **polizeitaktischer Sicht** ist die Regelung **unkritisch**.

Insgesamt wird durch die Regelung die Stellung des Datenschutzbeauftragten, insbesondere bei Polizei und Staatsanwaltschaften gestärkt, auch da die Regelung des Bundesdatenschutzgesetzes zur Frage, wie die Aufsichtsbehörde anzurufen ist, abgeschafft werden müsste und so auch die externe Kontrolle intensiviert wird. Zudem werden ihm spezifische Zuständigkeiten, insbesondere die Meldung von Verletzungen des Schutzes von personenbezogenen Daten an die Aufsichtsbehörde und die Tätigkeit als Ansprechpartner für die Aufsichtsbehörde zugewiesen.

Die Stärkung der Rolle des Datenschutzbeauftragten dient dazu, das **Datenschutzniveau zu verbessern**. Gerade bei Sicherheitsbehörden kommt der Datenverarbeitung auch aus Sicht des Bürgers eine besondere Bedeutung zu. Die Stärkung der internen Kontrollinstanz dient somit auch der Gewährleistung datenschutzrechtlicher Vorschriften und Vorgaben und ist deshalb zu begrüßen. Kritisch ist anzumerken, dass bewährte deutsche Instrumente zum Schutz des behördlichen Datenschutzbeauftragten nicht übernommen werden, wie beispielsweise der besondere Kündi-

gungsschutz oder das Benachteiligungsverbot. Dies wurde allerdings auch im Bericht des LIBE-Ausschusses des Europäischen Parlamentes gerügt.[21]

Kapitel V Übermittlung personenbezogener Daten in Drittländer oder an internationale Organisationen

Kapitel V enthält abschließende Regelungen zur Übermittlung in Drittländer und an internationale Organisationen. Von diesen sind Übermittlungen zwischen den Mitgliedstaaten sowie an oder von Stellen der EU abzugrenzen, deren Zulässigkeit sich nach den allgemeinen Verarbeitungsgrundsätzen des Richtlinienentwurfs und den Bestimmungen gesonderter Rechtsakte richtet, die nach Artikel 59 unberührt bleiben (Bäcker/Hornung, ZD 2012, 147, 148). Zu denken ist insoweit insbesondere an die Regelungen des Rahmenbeschlusses 2006/960/JI vom 18.12.2006 über die Vereinfachung des Austauschs von Informationen und Erkenntnissen zwischen den Strafverfolgungsbehörden der Mitgliedstaaten der Europäischen Union (zur Umsetzung auf Bundesebene vgl. BGBl. 2012 I, 1566).

Artikel 33 bis 36

1. Inhalt

a) Überblick

Die Regelungen der Artikel 33 bis 36 sind als zusammenhängende Regelung zur Datenübermittlung in Drittländer oder internationale Organisationen zu sehen. Sie weichen deutlich von dem Konzept des Rahmenbeschlusses 2008/977/JI ab und sind **im Ergebnis kritisch zu sehen**. Übereinstimmung zwischen den Artikeln 33 ff. und dem insoweit maßgeblichen Artikel 13 des Rahmenbeschlusses besteht noch darin, dass die Übermittlung zur Verhütung, Aufdeckung, Untersuchung oder Verfolgung von Straftaten oder zur Strafvollstreckung erforderlich sein muss. Die weiteren Voraussetzungen divergieren allerdings, wobei KOM zulasten der Mitgliedstaaten und deren nationalen Stellen in abzulehnender Weise Kompetenzen zugewiesen werden.

Anders als Artikel 13 des Rahmenbeschlusses enthalten die Artikel 33 ff. ein dreistufiges Konzept aus Angemessenheitsbeschlüssen, geeigneten Garantien und Ausnahmen. Artikel 13 des Rahmenbeschlusses bindet die Zulässigkeit der Datenübermittlung dagegen an vier kumulative Voraussetzungen (Erforderlichkeit, Zuständigkeit, Zustimmung und angemessenes Schutzniveau). Bedeutsam ist dabei insbesondere der eingeschränkte Anwendungsbereich des Artikels 13 des Rahmenbeschlusses. Danach ist eine Regelung zur Datenübermittlung an die zuständigen Behörden in Drittstaaten oder an internationale Einrichtungen nur für den Fall vorgesehen, dass der übermittelnde Mitgliedstaat die zu übermittelnden personenbezogenen Daten seinerseits von der zuständigen Behörde eines anderen Mitgliedstaats übermittelt oder bereitgestellt bekommen hat. Mit der geplanten Ausweitung des Anwendungsbereichs der Richtlinie sind die Artikel 33 ff. demgegenüber bei jeder (straftatbezoge-

[21] Siehe Änderungsantrag 121 des Berichtsentwurfs des LIBE-Ausschusses (FN 10)

nen) Übermittlung in ein Drittland oder eine internationale Organisation zu beachten. Im Übrigen verlangte Artikel 13 des Rahmenbeschlusses zwar grundsätzlich ebenfalls ein angemessenes Datenschutzniveau im Drittstaat oder in der internationalen Einrichtung. Für die Feststellung desselben war aber der übermittelnde Mitgliedstaat selbst zuständig (vgl. Artikel 13 Abs. 4 des Rahmenbeschlusses), **während nach dem RL-E künftig KOM (!) eine abstrakte, d.h. vom konkreten Einzelfall losgelöste Prüfung des Datenschutzniveaus vornehmen wird. Hierin liegt ein in der polizeilichen Praxis nicht zu unterschätzender Unterschied in den Konzeptionen von RB und RL-E.**

Der RL-E stellt wesentliche Prozesse des Bewilligungsverfahrens im Rechtshilfeverkehr in Frage (insbesondere hinsichtlich Entscheidungen bezüglich des Datenschutzniveaus in Drittstaaten). Dies könnte auch bedeutende Anpassungen der Abläufe zwischen Bund und Ländern bei der internationalen Rechtshilfe in Strafsachen erfordern. Aufgrund der Vereinbarung zwischen dem Bund und den Ländern zur Zuständigkeit im Rechtshilfeverkehr mit dem Ausland in strafrechtlichen Angelegenheiten vom 28.04.2004 (sog. Zuständigkeitsvereinbarung) und die daran anknüpfenden landesinternen Delegationserlasse sowie die Richtlinien für den Verkehr mit dem Ausland in strafrechtlichen Angelegenheiten (RiVASt) wird die Bewilligungsbefugnis für die Stellung und Beantwortung von Rechtshilfeersuchen auf verschiedene Behörden und Gerichte im Bund und in den Ländern verteilt, die neben anderen Aspekten auch das Datenschutzniveau in dem jeweiligen Drittstaat bei ihrer Bewilligungsentscheidung zu berücksichtigen haben (für das BKA: vgl. § 14 Abs. 7 BKAG).

Sollte die Entscheidung, ob in einem Drittstaat ein hinreichendes Datenschutzniveau sichergestellt ist, von der KOM getroffen werden, gäbe Deutschland im Kern mit dem hier in Rede stehenden Richtlinienentwurf auch Teile seiner Entscheidungskompetenzen und seines Entscheidungsspielraums für den Bereich der internationalen Zusammenarbeit in strafrechtlichen Angelegenheiten auf.

Grundvoraussetzung für alle Übermittlungen in Drittländer oder an internationale Organisationen auf der Basis des Richtlinienentwurfs ist gemäß Artikel 33 lit. a, dass die Übermittlung zur Verhütung oder Verfolgung von Straftaten oder zur Strafvollstreckung erforderlich ist. Zusätzlich erforderlich ist, dass der für die Verarbeitung Verantwortliche und (natürlich nur wenn ein solcher eingeschaltet ist) der Auftragsverarbeiter die in den Artikeln 34 ff. niedergelegten Bestimmungen einhalten. Erforderlich ist nach Artikel 33 lit. b also, dass ein Erlaubnistatbestand hinzutritt, nämlich ein Angemessenheitsbeschluss nach Artikel 34, geeignete Garantien nach Artikel 35 oder ein Ausnahmetatbestand nach Artikel 36.

Konkreter Adressat in dem Drittland oder der internationalen Organisation soll nach Erwägungsgrund 45 nur eine Behörde sein, die für die Verhütung, Aufdeckung, Untersuchung oder Verfolgung von Straftaten oder die Strafvollstreckung zuständig ist. Bezogen auf internationale Organisationen muss das wohl dahingehend ausgelegt werden, dass der jeweilige Empfänger und damit letztlich auch die Organisation selbst einen unmittelbaren Bezug zu Fragen der Straftatenverhütung und Straftatenverfolgung aufweisen muss.

b) Einzelheiten zu den Artikeln 34 bis 36

aa) Zu Artikel 34: Diese Bestimmung regelt die Datenübermittlung auf der Grundlage eines Angemessenheitsbeschlusses. Sofern die Kommission einen solchen Beschluss hinsichtlich des betreffenden Drittlandes oder der internationalen Organisation gefasst hat, ist die Angemessenheit des Datenschutzniveaus verbindlich festgestellt und die fragliche Datenübermittlung bedarf dann keiner weiteren Genehmigung (vgl. Absätze 1 bis 3). **Die Kommission kann nach Abs. 5 aber auch feststellen, dass ein Drittland oder eine internationale Organisation keinen angemessenen Datenschutz bietet (sog. Negativbeschluss). In diesem Fall haben die Mitgliedstaaten Datenübermittlungen nach dorthin – unbeschadet allerdings der Artikel 35 Abs. 1 und Artikel 36 – zu untersagen (vgl. Abs. 6).** Die Kommission hat im Amtsblatt der EU eine Liste der Drittländer und internationalen Organisationen zu veröffentlichen, bei denen sie im Beschlusswege die bestehende oder fehlende Angemessenheit festgestellt hat (vgl. Abs. 7). Die Frage der Angemessenheit kann hinsichtlich der Drittländer jeweils auch bezogen auf einzelne Landesteile oder Verarbeitungssektoren festgestellt werden. So kann z.B. ein nach Artikel 38 des Entwurfs der Datenschutz-Grundverordnung erlassener Angemessenheitsbeschluss auch im Rahmen der Richtlinie anwendbar sein.

bb) Zu Artikel 35: Diese Bestimmung regelt die Datenübermittlung auf der Grundlage geeigneter Garantien.

Liegt ein Beschluss nach Artikel 34 nicht vor, dürfen gleichwohl personenbezogene Daten an einen Empfänger oder an eine internationale Organisation übermittelt werden, wenn (a) in einem rechtsverbindlichen Instrument geeignete Garantien für den Schutz personenbezogener Daten vorgesehen sind oder (b) der Übermittelnde nach umfassender Interessenabwägung zu der – nach Abs. 2 zu dokumentierenden – Auffassung gelangt, dass geeignete Garantien zum Schutz personenbezogener Daten bestehen.

Hinsichtlich des rechtsverbindlichen Instruments i.S.d. Artikels 35 Abs. 1 lit. a werden in erster Linie völkerrechtliche Abkommen, z. B. der deutsch-schweizerische Polizeivertrag (vgl. die datenschutzrechtlichen Regelungen dort in Artikel 26 bis 28), in Betracht kommen.

cc) Zu Artikel 36: Liegen die Voraussetzungen einer zulässigen Datenübermittlung nach den Artikeln 34 und 35 nicht vor, kommt nur noch eine Datenübermittlung aufgrund der Ausnahmeregelung in Artikel 36 in Betracht. Insoweit werden fünf alternativ geltende Ausnahmen statuiert. Danach ist die Übermittlung zulässig, wenn sie

(a) zur Wahrung lebenswichtiger Interessen der betroffenen Person oder einer anderen Person erforderlich ist,
(b) nach dem Recht des Mitgliedstaats, aus dem die personenbezogenen Daten übermittelt werden, zur Wahrung der berechtigten Interessen der betroffenen Person notwendig ist,
(c) zur Abwehr einer unmittelbaren und ernsthaften Gefahr für die öffentliche Sicherheit eines Mitgliedstaats oder eines Drittstaats unerlässlich ist,
(d) zur Verhütung, Aufdeckung, Untersuchung oder Verfolgung von Straftaten oder zur Strafvollstreckung erforderlich ist oder
(e) in Einzelfällen zur Begründung, Geltendmachung oder Abwehr von Rechtsansprüchen im Zusammenhang mit der Verhütung, Aufdeckung, Untersuchung

oder Verfolgung einer bestimmten Straftat oder der Vollstreckung einer bestimmten Strafe notwendig ist.

dd) Zusammenfassung: Im Ergebnis hat somit die KOM die Frage nach der Zulässigkeit von Datenübermittlungen an Drittstaaten in der Hand. Sie kann solche Übermittlungen durch sog. Angemessenheitsbeschlüsse in abstrakt-genereller Form und ohne Ansehung von konkreten Einzelfällen gestatten, aber auch verbieten. Eine eigenständige Einschätzung des Datenschutzniveaus im Empfängerstaat durch die übermittelnde Behörde ist künftig nur noch möglich, wenn und solange die KOM keinen Angemessenheitsbeschluss gefasst hat. Ohne Ansehung des Datenschutzniveaus des Empfängerstaates dürfen Daten nur in den Ausnahmefällen des Artikel 36 RL-E übermittelt werden.

c) Hinweis zur nicht-straftatbezogenen Gefahrenabwehr

Sofern man für den Bereich der nicht-straftatbezogenen Gefahrenabwehr und die diesbezüglich bestehenden Fragen der Datenübermittlung in Drittländer oder an internationale Organisationen die geplante Datenschutz-Grundverordnung (GVO) für anwendbar erachtet, ergeben sich aus den Artikeln 40 bis 44 GVO-E im Ausgangspunkt weitgehend den Artikeln 33 bis 36 RL-E vergleichbare Bestimmungen. Allerdings sind die Regelungen der geplanten GVO nicht näher auf die spezifischen Bedürfnisse der Gefahrenabwehr abgestimmt, die Worte „Abwehr“ oder „Verhütung von Gefahren“ tauchen in der Entwurfsfassung nicht auf. Das gilt insbesondere für die wichtige Regelung des Artikels 44 GVO-E, wo sich allein mittels der Ausnahmeregelung in Abs. 1 lit. d (Übermittlung aus Gründen des öffentlichen Interesses) die Besonderheiten der Gefahrenabwehr berücksichtigen ließen. Die Regelungen zur Übermittlung sind primär auf den unternehmensbezogenen Datenaustausch bezogen. Dies zeigt erneut, dass die geplante GVO für die nicht-straftatbezogene Gefahrenabwehr keine adäquaten Regelungen vorhält.
Das Datenschutzpaket ist insofern aus polizeitaktischer Sicht als äußerst kritisch zu beurteilen.
2. Regelungen in den Polizeigesetzen, Umsetzungsbedarf und Auslegungsfragen
Nach den im Einzelnen divergierenden Regelungen der Polizeigesetze (vgl. etwa § 20 Abs. 3 HmbPolDVG, Artikel 40 Abs. 5 PAG BY, § 28 Abs. 4 PolG NRW, § 27 Abs. 3 SOG LSA, § 32 Abs. 3 BPolG, § 14 Abs. 1 BKAG) darf die Polizei personenbezogene Daten in Drittstaaten und an internationale Organisationen im Wesentlichen dann übermitteln, soweit dies zur Erfüllung polizeilicher Aufgaben erforderlich ist, sie hierzu aufgrund über- oder zwischenstaatlicher Rechtsakte berechtigt oder verpflichtet ist oder dies zur Abwehr einer erheblichen Gefahr durch den Empfänger erforderlich erscheint. Da die (geplante) Richtlinie einer Umsetzung bedarf und die Polizei nicht aus ihr heraus zur Übermittlung berechtigt oder verpflichtet wird, **lässt sich das von der Kommission geplante Konzept zur Übermittlung in Drittstaaten und an internationale Organisationen nicht harmonisch in das bestehende Polizeirecht eingliedern**. Die Regelungen der Artikel 33 bis 36 rufen daher Änderungsbedarf in den Polizeigesetzen hervor. Zu beachten ist, dass die Vorgaben der

(geplanten) Richtlinie insoweit auch deutlich von dem Regelungskonzept des Rahmenbeschlusses 2008/977/JI (konkret Art. 13) abweichen (näher s.o. unter 1. a). Die Länder, die (wie etwa Hamburg, vgl. § 18a Abs. 3 HmbPolDVG) bereits den Rahmenbeschluss 2008/977/JI umgesetzt haben, müssten die getroffene Regelung wieder ändern.

Die umzusetzende Regelung wird das dreistufige Konzept (Angemessenheitsbeschlüsse, geeignete Garantien, Ausnahmen) und damit in erheblichem Umfang die Bestimmungen der Artikel 33 bis 36 zu übernehmen haben. Dabei ist zu beachten, dass die Datenschutzgesetze auf Bundes- und Länderebene im Anschluss an die Regelungen in Artikel 25 und 26 der Richtlinie 95/46/EG insoweit bereits ähnlich differenzierende Regelungen vorhalten, nach denen eine fehlende Angemessenheit beim Datenschutzniveau die Übermittlung grundsätzlich ausschließt, insoweit aber (Gegen-)Ausnahmen greifen können (vgl. § 4b Abs. 2 BDSG, Artikel 21 Abs. 2 DSG BY). **Neu und insoweit umsetzungsbedürftig ist aber, dass die Frage der Angemessenheit des Datenschutzniveaus künftig von KOM entschieden werden darf und somit alle bisher bekannten Ermessensspielräume der Mitgliedstaaten und deren nationaler Behörden entfallen. Dies wird zu gesetzgeberischem Handlungsbedarf führen und ist in polizeitaktischer Hinsicht – insbesondere im Zusammenhang mit der Bekämpfung der organisierten Kriminalität und anderer grenzüberschreitender Phänomene – als äußerst kritisch zu betrachten.**

Die Regelungen der Artikel 33 bis 36 enthalten einige Unklarheiten und Ungereimtheiten:

- Zum zu weit geratenen Wortlaut bei Artikel 35 Abs. 1 hinsichtlich der Worte „Beschluss nach Artikel 34“ siehe bereits oben.
- Schwierigkeiten bereitet eine Konkretisierung der recht unbestimmten Regelung des Artikels 35 Abs. 1 lit. b. Danach 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.“ Zwar wird der Begriff der geeigneten Garantien im Richtlinienentwurf auch an anderen Stellen verwendet (vgl. z.B. Artikel 8 Abs. 2 lit. a), der sachliche Gehalt wird jedoch nicht näher konkretisiert. Das muss indes nicht unbedingt ein Nachteil sein, da insoweit den Mitgliedstaaten Auslegungsspielräume verbleiben.

  Kritisiert wird im Übrigen die subjektive Ausrichtung der Bestimmung (s. Hornung, Schriftliche Stellungnahme vom 17.10.2012 zur öffentlichen Anhörung des Innenausschusses des Deutschen Bundestages am 22.10.2012 zum Richtlinienentwurf, S. 17: „Eine derartige versubjektivierte ex ante-Perspektive ist bei weltweiten Datenübermittlungen abzulehnen.“).
- Wirft man einen Blick auf die allgemeinen Anforderungen nach Artikel 33, so ist festzustellen, dass sich aus der Ausnahmeregelung des Artikels 36 lit. d keine weitergehenden Einschränkungen („Bedingungen“ i.S.d. Artikels 33 lit. b) ergeben. Damit ließe die Vorschrift unter Verzicht auf jede Berücksichtigung des Datenschutzniveaus im Empfängerstaat alle übrigen Übermittlungsvorschriften nach Artikel 33 ff. überflüssig werden. Diese Ausnahmeregelung ist aus diesem Grund bereits heftig kritisiert worden (vgl. etwa die Stellungnah-

men von Hornung und Bäcker zur öffentlichen Anhörung des Innenausschusses des Deutschen Bundestages am 22.10.2012 zum Richtlinienentwurf).Sie scheint die zuvor statuierten Grundsätze wieder auszuhebeln, so dass der genaue Bedeutungsgehalt des V. Kapitels insgesamt im Ergebnis unklar bleibt.

- Fraglich bleibt zudem, in welchen Fällen des Artikels 36 lit. e zugleich die Voraussetzungen des Artikels 33 lit. a vorliegen können und erstgenannte Regelung damit ein praktischer Anwendungsbereich verbleibt.

Aus diesen Befunden sowie aus dem Stufenkonzept der Übermittlungsvorschriften ergeben sich Bedenken an dem vorgeschlagenen Regelungssystem der Artikel 33 ff.

Nach den Vorstellungen der Kommission soll die Übermittlung auf der Grundlage von Angemessenheitsbeschlüssen nach Artikel 34 Abs. 1 bzw. 3 im Vordergrund stehen, also gleichsam den Regelfall darstellen. Zu bedenken ist insoweit, dass von den 190 INTERPOL-Staaten ein großer Teil über keinen im Sinne der EU ausreichenden „angemessenen“ Datenschutzstandard verfügen dürfte. Soll die Übermittlung auf der Grundlage von Angemessenheitsbeschlüssen den Regelfall darstellen, so besteht die Gefahr, dass die verbleibenden Erlaubnistatbestände der Artikel 35 und 36 als Ausnahmebestimmungen (zu) restriktiv interpretiert werden. Dies wiederum dürfte zu praktischen Problemen führen und könnte insbesondere den internationalen Nachrichtenverkehr im Bereich des internationalen Terrorismus oder der organisierten Kriminalität erheblich schwächen. Das hauptsächlich für den Datenverkehr mit dem Ausland zuständige Bundeskriminalamt (vgl. § 3 BKAG) führt täglich im Rahmen der weltweiten INTERPOL-Personenfahndung in großem Umfang Schriftverkehr mit Drittländern. Jährlich werden rund 2.000 deutsche INTERPOL-Personenfahndungen übermittelt (vgl. Ziercke, Schriftliche Stellungnahme vom 19.10.2012 zur öffentlichen Anhörung des Innenausschusses des Deutschen Bundestages am 22.10.2012 zum Richtlinienentwurf, S. 8 f.). Für die effektive Bekämpfung von Schwerkriminalität im Einzelfall muss in weitem Umfang auch eine Übermittlung personenbezogener Daten an diejenigen Staaten möglich sein, die nicht über ein angemessenes Datenschutzniveau verfügen. Die derzeitige Regelung in § 14 Abs. 7 BKAG ermöglicht dem BKA insoweit eine hinreichend flexible Handhabung, anhand der auch sich verändernden Umständen auch des jeweils zugrunde liegenden konkreten Einzelfalls Rechnung tragen lässt. Dagegen lassen Angemessenheitsbeschlüsse im Rahmen des Artikels 34 weder eine abweichende nationale Abwägungsentscheidung zu, es handelt sich vielmehr um „starre“ Vorgaben, noch eine zeitnahe Anpassung an sich verändernde Bedingungen des Einzelfalls. Letzteres ist aber für den hiesigen Bereich von besonderem Interesse, um schnell und effektiv auf Straftaten reagieren zu können. Aus polizeilicher Sicht müssen zudem bei der Entscheidung, ob Daten in einen Drittstaat übermittelt werden, auch Belange nicht-datenschutzrechtlicher Art Berücksichtigung finden können (z.B. Zeugenschutz, Gefährdungen von Leib und Leben, etc.). Das System der Angemessenheitsbeschlüsse ist insoweit zu eindimensional gehalten, weil es diese Belange unberücksichtigt lässt und die Zulässigkeit von Datenübermittlungen grundsätzlich allein aus datenschutzrechtlicher Perspektive beurteilt.

Bei dem dann neben Artikel 36 verbleibenden Erlaubnistatbestand des Artikels 35 stellt sich die Frage nach einem relevanten Anwendungsbereich. In den Fällen des Artikels 35 Abs. 1 lit. a dürfte angesichts des dort vorausgesetzten Bestehens rechtsverbindlicher Datenschutzregelungen regelmäßig ein (positiver) Angemessenheitsbeschluss nach Artikel 34 vorliegen, sodass für Artikel 35 Abs. 1 lit. a in der Praxis kaum Anwendungsbereich verbleiben dürfte. Die Regelung des Artikels 35 Abs. 1 lit. b bereitet demgegenüber praktische Anwendungsschwierigkeiten.
Von daher steht zu erwarten, dass die Praxis Datenübermittlungen auf die bislang noch sehr weitgehenden Ausnahmeregelungen des Artikels 36 stützen wird, was allerdings mit dem gewollten Ausnahmecharakter der Regelung kaum zu vereinbaren wäre. Auf der anderen Seite würde, wie dargelegt, eine zu restriktive Fassung und Auslegung der Übermittlungsregelungen außerhalb der Angemessenheitsbeschlüsse gewichtige Interessen der Straftatenverhütung und -verfolgung beeinträchtigen.Insgesamt zeigt sich damit, dass das System der Artikel 33 ff. RL-E nicht hinreichend durchdacht ist.
Teilweise sehen die Polizeigesetze bestimmte Schranken der Datenübermittlung vor, die sich nicht oder jedenfalls nicht ausdrücklich in der Regelung des Richtlinienentwurfs finden. Das gilt etwa für mögliche Verstöße gegen den Zweck eines deutschen Gesetzes oder eine Beeinträchtigung überwiegender schutzwürdiger Interessen des Betroffenen (vgl. § 20 Abs. 3 S. 3 HmbPolDVG, Artikel 40 Abs. 5 S. 2 PAG BY, § 28 Abs. 4 S. 2 PolG NRW, § 14 Abs. 7 S. 6, 7 BKAG). Teilweise mögen diese Schranken mit den auslegungsfähigen Regelungen der Artikel 35 Abs. 1 lit. b und Artikel 36 in Übereinstimmung gebracht werden können. Es bleibt jedoch eine im Gesetzgebungsprozess zu klärende Frage, inwieweit die Mitgliedstaaten befugt sind, eigene Ausnahmen zu den Übermittlungsregelungen der Artikel 33 bis 36 zu schaffen.Dies wiederum hängt eng mit der allgemeinen, den gesamten RL-Entwurf betreffenden Frage zusammen, ob eine Vollharmonisierung beabsichtigt ist oder aber lediglich Mindeststandards (mit der Möglichkeit zum Erlass strengerer datenschutzrechtlicher Bestimmungen im nationalen Recht) geschaffen werden sollen.
3. Relevanz für die Polizei
Im (derzeitigen) präventiv-polizeilichen Anwendungsbereich des Richtlinienentwurfs, mithin im Bereich der straftatbezogenen Gefahrenabwehr, könnte die Regelung der Richtlinie vor dem Hintergrund der sehr weitgehenden Ausnahmeregelung in Artikel 36 lit. d nicht zu einer Erhöhung der bisher in den Polizeigesetzen bestehenden Voraussetzungen für eine Datenübermittlung, teilweise sogar zu einer Erleichterung führen (vgl. etwa § 28 Abs. 4 S. 1 PolG NRW, nach dem die Datenübermittlung zur Abwehr einer erheblichen Gefahr erforderlich sein muss). Dies wäre allerdings nur der Fall, wenn die Ausnahmeregelung des Artikels 36 lit. d RL-E weit ausgelegt und damit faktisch zum eigentlichen Grundsatz der Datenübermittlung in Drittstaaten erhoben würde. Die Frage, ob und inwieweit eine solche Interpretation zulässig ist, wird allerdings nicht vom deutschen Gesetzgeber zu beantworten sein, dem insoweit keine eigenständigen Interpretations- und Gestaltungsspielräume erwachsen, sondern in letzter Konsequenz vom EuGH entschieden. Ungeachtet dieser Problematik wird jedenfalls das schwer überschaubare mehrstufige Regelungskonzept die praktische

Rechtsanwendung im Vergleich zu den bisherigen, klarer strukturierten Regelungen der nationalen Polizeigesetze erschweren.

4. Folgen für das Datenschutzniveau

In politischer Hinsicht lässt sich hinterfragen, ob es sachgerecht ist, dass die Kommission weitgehend eigenständig für die Feststellung der Angemessenheit des Datenschutzniveaus zuständig sein soll (vgl. Kugelmann, DuD 2012, 581, 583, der unter Verweis auf die Erfahrungen mit den Passagierdaten und den Bankdaten eine Rückbindung der Entscheidung an das Europäische Parlament befürwortet, was allerdings zu zeitlichen Verzögerungen führen würde; ebenso Aden, Schriftliche Stellungnahme zur öffentlichen Anhörung des Innenausschusses des Deutschen Bundestages am 22.10.2012 zum Richtlinienentwurf, S. 5 f., dort auch mit der Forderung, bei der Übermittlung sensibler Daten mindestens ein „hohes“ Datenschutzniveau zur Voraussetzung zu machen). Die durch die Kommission vorzunehmende abstrakte Prüfung der Angemessenheit des Schutzniveaus ist in der Praxis schwierig. Geht es um die Abwehr schwerwiegender Gefahren oder dringende Maßnahmen der Strafverfolgung, muss die Polizei oft binnen kürzester Zeit entscheiden, ob ein Datum zu dem konkreten Zweck übermittelt werden darf. Für ein bürokratisches Verfahren ist dann kein Raum.

Auch politisch könnte sich das vorgesehene Prüfverfahren als höchst brisant erweisen. Die Feststellung der Kommission, dass ein bestimmtes Land nicht über das aus Sicht der EU angemessene Datenschutzniveau verfügt, dürfte mitunter zu erheblichen politischen Spannungen führen. Es ist nicht ausgeschlossen, dass die Angemessenheit im Einzelfall aus politischer Opportunität bejaht werden könnte.

5. Zusammenfassende Bewertung

Das Regelungssystem ist bislang nicht hinreichend überdacht, teilweise unklar und wohl auch von der Struktur her noch vereinfachungsfähig.Den polizeilichen Belangen wird nicht, jedenfalls nicht in der erforderlichen Klarheit und Rechtssicherheit Rechnung getragen. **Das Regelungssystem ist daher als äußerst kritisch anzusehen.**

Artikel 37 Besondere Bedingungen für die Übermittlung personenbezogener Daten

1. Inhalt

Artikel 37 regelt die Pflicht zur Benachrichtigung des Empfängers über Verarbeitungsbeschränkungen und zur Sicherstellung von deren Einhaltung. Auf Adressatenseite erfasst werden alle Empfänger personenbezogener Daten in dem jeweiligen Drittland oder der jeweiligen internationalen Organisation. Die Regelung lehnt sich im Ausgangspunkt an Artikel 12 Abs. 1 des Rahmenbeschlusses 2008/977/JI an, dort allerdings bezogen auf den Datenaustausch zwischen Mitgliedstaaten.

2. Regelungen in den Polizeigesetzen und Umsetzungsbedarf

a) Hinweispflicht auf Verarbeitungsbeschränkungen

Die Vorschriften der Polizeigesetze enthalten zwar weithin Hinweispflichten hinsichtlich der Zweckbindung (vgl. etwa § 18 Abs. 4 S. 2 HmbPolDVG, Artikel 39 Abs. 2 S. 2 PAG BY, § 26 Abs. 4 S. 2 PolG NRW, § 33 Abs. 6 S. 2 BPolG, § 14 Abs. 7 S. 3 BKAG), ganz überwiegend jedoch nicht hinsichtlich von (sonstigen) „Verarbeitungs-

beschränkungen“ bei der Datenübermittlung an Drittstaaten und internationale Organisationen (vgl. für den Datenaustausch innerhalb der EU nunmehr jedoch § 18a Abs. 2 S. 1 HmbPolDVG). Verarbeitungsbeschränkungen gelten z.B. für Daten, die einem besonderen Berufs- oder Amtsgeheimnis unterliegen (§ 18 Abs. 3 HmbPolDVG, Artikel 39 Abs. 3 PAG BY, § 26 Abs. 2 PolG NRW, § 26 Abs. 2 SOG LSA, vgl. aber auch § 27 Abs. 1 S. 1 Nr. 2 BKAG) oder mit besonderen Mitteln und Methoden erhoben worden sind (vgl. § 14 Abs. 2 HmbPolDVG, Artikel 34c Abs. 4 S. 2 PAG BY; darüber hinaus vgl. § 26 Abs. 4 SOG LSA, § 32 Abs. 5 BPolG). In den angeführten Fällen sind die Verarbeitungsbeschränkungen allerdings schon von der übermittelnden Stelle zu beachten. Fälle, in denen es einer – über die Zweckbindung hinausgehenden – Mitteilung an den Empfänger und damit einer weitergehenden gesetzlichen Regelung in den Polizeigesetzen bedarf, ergeben sich in manchen Polizeigesetzen (z.B. § 23 Abs. 7 PolG BW; § 20v Abs. 3 BKAG) für personenbezogene Daten, die im Rahmen bestimmter verdeckter Ermittlungsmaßnahmen erhoben worden sind. Hier ist zur Sicherung der Zweckbindung (vgl. BVerfGE 100, 313, 360; 109, 279, 379 f.; BT-Drs. 16/10121, S. 36) nicht nur vorgesehen, dass die Daten besonders zu kennzeichnen sind, sondern auch, dass diese Kennzeichnung nach einer Übermittlung durch den Empfänger aufrechtzuerhalten ist.

Zu beachten ist, dass der Richtlinienentwurf anders als der Rahmenbeschluss 2008/977/JI(Artikel 5 und 9) keine Regelungen zur Festlegung von Löschungs- und Prüffristen und zur Mitteilung dieser Fristen an die empfangende Stelle im Drittstaat oder die internationale Organisation enthält. Mit Blick darauf, dass der europäische Gesetzgeber insoweit zu differenzieren weiß, er auf entsprechende Regelungen im Richtlinienentwurf aber (bislang) verzichtet hat, wird man die Hinweispflicht des Artikels 37 nicht auch auf die Mitteilung von (im Richtlinienentwurf nicht geregelten) Löschungs-, Sperrungs- und Prüffristen beziehen können.

Anders als in Artikel 12 Abs. 1 Satz 1 des Rahmenbeschlusses 2008/977/JI fehlt im Übrigen eine Anknüpfung an „nach dem innerstaatlichen Recht des übermittelnden Mitgliedstaates unter besonderen Umständen geltende besondere Verarbeitungsbeschränkungen“, die bei der Übermittlung zu beachten wären. Ob mit dem knapperen Wortlaut in Artikel 37 ein abweichender Bedeutungsgehalt verknüpft ist, etwa dahingehend, dass die Mitgliedstaaten über die innerstaatlich geltenden Beschränkungen hinaus solche nach eigenem Ermessen vorsehen können, ist nicht ganz klar, aber mit Blick auf den Wortlaut („hinweist“) wohl eher abzulehnen. Erläuterungen hierzu lassen sich dem Kommissionsentwurf nicht entnehmen.

b) Einhaltung der Verarbeitungsbeschränkungen

Neben der Hinweispflicht hat der übermittelnde Mitgliedstaat „alle vertretbaren Vorkehrungen“ zu treffen, um sicherzustellen, dass die „Verarbeitungsbeschränkungen“ eingehalten werden. Hierin liegt eine Umkehrung der Pflichtenstellung im Vergleich zum Rahmenbeschluss 2008/977/JI. Nach dessen Artikel 12 Abs. 1 Satz 2 hat dort der Empfänger sicherzustellen, dass diese Verarbeitungsbeschränkungen eingehalten werden. Allerdings betraf diese Regelung den Datenaustausch zwischen den Mitgliedstaaten, so dass es unproblematisch war, diese als Adressaten des Rahmenbeschlusses zu verpflichten. Anderes gilt aber vorliegend. Die als Empfänger der

Daten vorgesehenen Drittstaaten und internationale Organisationen sind nicht Adressaten der (geplanten) Richtlinie, so dass ihnen gegenüber bereits aus völkerrechtlichen Grundsätzen keine Pflichten auferlegt werden können. Der Forderung des Bundesrates (vgl. BR-Drs. 51/12 [Beschluss 2], S. 12), dem Empfänger der Daten die Verpflichtung von Verfügungsbeschränkungen aufzuerlegen, ist daher nicht zu folgen. Allerdings dürfte dem Bundesrat (a.a.O.) jedenfalls darin Recht zu geben sein, dass die Regelung weder effektiv noch verlässlich und selbst bei außerordentlich hohem Verwaltungs- und damit Zeit- und Kostenaufwand praktisch kaum durchsetzbar ist. Die Formulierung „alle vertretbaren Vorkehrungen“ entschärft die Problematik nicht entscheidend, zumal offen bleibt, was hierunter zu verstehen ist.
Eine dem Artikel 37 Hs. 2 entsprechende Pflicht fehlt in den Polizeigesetzen der Länder, so dass insoweit Umsetzungsbedarf bestünde, falls eine gesetzliche Regelung zum Hinweis auf Verarbeitungsbeschränkungen für erforderlich gehalten wird.
3. Relevanz für die Polizei
Sie ist abhängig von der Beurteilung des Umsetzungsbedarfs. Ein solcher unterstellt, ist zu bedenken, dassdie Regelung des Artikels 37 zu zusätzlichen (Verwaltungs-)Pflichten für die Polizei führt. Während die Erfüllung der Hinweispflicht ohne erheblichen Aufwand zu erfüllen sein dürfte und nachvollziehbaren datenschutzrechtlichen Belangen dient, lässt sich dies für die Sicherstellungspflicht mit Blick auf ihre problematische Um- und Durchsetzbarkeit nicht sagen. Jedenfalls auf sie sollte in einer (zukünftigen) Richtlinie verzichtet werden.
4. Folgen für das Datenschutzniveau
Die Regelung des Artikels 37 dient einer Verbesserung des Datenschutzniveaus. Ob eine solche Verbesserung tatsächlich erwirkt wird, hängt davon ab, inwieweit nach dem jeweiligen Landes- bzw. Bundesrecht Anwendungsfälle gesehen werden.
5. Zusammenfassende Bewertung
Ob die Norm Umsetzungsbedarf in den Polizeigesetzen hervorruft, ist nicht ganz eindeutig und wohl nach der jeweiligen Landes- bzw. Bundesregelung zu beurteilen. **Jedenfalls ist sie hinsichtlich der Sicherstellungspflicht nach Artikel 37 Hs. 2 sehr kritisch zu sehen.**

Artikel 38 Internationale Zusammenarbeit zum Schutz personenbezogener Daten

1. Inhalt
Artikel 38 hält die Kommission sowie die Mitgliedstaaten an, geeignete Maßnahmen in der internationalen Zusammenarbeit zum Schutz personenbezogener Daten zu treffen. Damit soll insbesondere die grenzüberschreitende Zusammenarbeit bei der Anwendung von Datenschutzgesetzen gefördert werden (zu näheren Überlegungen siehe Erwägungsgrund 50).
2. Relevanz für die Polizei
Die unmittelbaren Auswirkungen für die polizeiliche Arbeit oder die Polizeigesetze sind abhängig von den konkreten einzelnen Maßnahmen, die von Seiten der Kommission oder den Mitgliedstaaten auf der Grundlage des Artikels 38 getroffen werden. Die durch Artikel 38 ermöglichten Maßnahmen können einerseits im Interesse

der Polizei liegen, etwa wenn es um die Verbesserung der internationalen Zusammenarbeit geht. Sie können andererseits aber auch – z.B. im Zusammenhang mit der Erleichterung der Durchsetzung datenschutzrechtlicher Vorschriften – neue bürokratische Hindernisse etablieren, die die polizeiliche Tätigkeit beeinträchtigen. Problematisch ist in diesem Zusammenhang, dass .Artikel 38 RL-E nicht regelt, auf welche Weise und von wem Maßnahmen ergriffen werden können. Die Vorschrift könnte in vertretbarer Weise dahingehend verstanden werden, dass Maßnahmen auch einseitig von KOM ergriffen werden können; in Artikel 38 Abs. 2 ist dies für einen Teilbereich sogar ausdrücklich vorgesehen. Angesichts der praktischen Bedeutung der in Artikel 38 ermöglichten Maßnahmen, ist dies aus Sicht der Mitgliedstaatenhöchst problematisch.

3. Ergebnis

Es handelt sich im Ergebnis um eine Regelung, die zumindest Klarstellungsbedarf bezüglich der – wohl zu weitreichenden – Befugnisse der KOM mit sich bringt und auf deren Grundlage Maßnahmen getroffen werden können, die die Tätigkeit der Polizei beeinträchtigen. **Die Vorschrift ist daher in ihrer jetzigen Fassung kritisch zu sehen.**

Kapitel VI Unabhängige Aufsichtsbehörden

Artikel 39 bis 47

Kapitel VI des Richtlinienentwurfs trifft in Artikel 39 bis 47 Regelungen zu nationalen Aufsichtsbehörden für den Datenschutz. Die Vorschriften regeln vor allem die Einrichtung, die Aufgaben und die Befugnisse der Aufsichtsbehörden. Daneben werden Vorgaben zur Unabhängigkeit, zur Leitung und zur personellen Ausstattung der Aufsichtsbehörden getroffen. Den Status von Aufsichtsbehörden i. S. des RL-Entwurfs haben in Deutschland die für die Kontrolle des Datenschutzes im öffentlichen Bereich eingerichteten Datenschutzbeauftragten des Bundes und der Länder.

Sollten Artikel 39 bis 47 des Richtlinienentwurfs **unverändertRecht werden**, wäre der sich daraus ergebende **Änderungsbedarf im nationalen Recht marginal.**

Dies ergibt zum einen bereits daraus, dass nach Artikel 39 Abs. 2 des Richtlinienentwurfs die Aufsichtsbehörde mit der Aufsichtsbehörde nach Kapitel VI des Entwurfs der Datenschutz-Grundverordnung identisch sein kann. In Deutschland sind schon jetzt der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit sowie die Landesbeauftragten für den Datenschutz für die Kontrolle des Datenschutzes im öffentlichen Bereich zuständig. Dabei findet eine Unterscheidung danach, ob staatliches Handeln im Anwendungsbereich der künftigen Richtlinie oder außerhalb davon liegt, nicht statt.

Zum anderen stimmen die meisten Regelungen zu Aufsichtsbehörden im Entwurf der Richtlinie und im Entwurf der Datenschutz-Grundverordnung überein. **Sollte Änderungsbedarf bei den nationalen Regelungen zu Aufsichtsbehörden bestehen, würde es regelmäßig ausreichen, diese Änderungen im allgemeinen Daten-**

schutzrecht des Bundes und der Länder vorzunehmen, nicht aber im Polizei-, Strafprozess- oder Strafvollzugsrecht.
Die **Übereinstimmung** der Vorschriften zu den Aufsichtsbehörden besteht allerdings **nicht bei den Regelungen zu den Befugnissen in Artikel 46 des Richtlinienentwurfs und Artikel 53 des Entwurfs der Datenschutz-Grundverordnung.** Dabei ist **festzustellen, dass Artikel 46 des Richtlinienentwurfs dem Artikel 28 Abs. 3 der Richtlinie 95/46/EG entspricht**. **Letztgenannte Vorschrift ist im nationalen Recht umgesetzt, so dass im Anwendungsbereich der künftigen Richtlinie eine Änderung der bestehenden Befugnisse der Aufsichtsbehörde wohl nicht vorgenommen werden müsste.**

Artikel 46 lit. a

Artikel 46 lit.a des Richtlinienentwurfs sieht vor, dass die Aufsichtsbehörden über Untersuchungsbefugnisse verfügen, wie das Recht auf Zugang zu Daten, die Gegenstand von Verarbeitungen sind, und das Recht auf Einholung aller für die Erfüllung ihrer Aufsichtspflichten erforderlichen Informationen. Diese **Regelung stimmt im Wortlaut weitgehend mit Artikel 28 Abs. 3 Satz 1, 1. Anstrich der Richtlinie 95/46/EG überein und deckt sich inhaltlich mit den Informationsbefugnissen bzw. Zugangsrechten der Aufsichtsbehörde nach Artikel 53 Abs. 1 lit. c und Abs. 2 lit. a und b des Entwurfs der Datenschutz-Grundverordnung.**

Artikel 46 lit. b

Nach Artikel 46 lit. b des Richtlinienentwurfs haben die Mitgliedstaaten dafür Sorge zu tragen, dass die Aufsichtsbehörde über wirksame Einwirkungsbefugnisse verfügen, wie beispielsweise die Möglichkeit, vor der Durchführung der Verarbeitung Stellungnahmen abzugeben und für eine geeignete Veröffentlichung der Stellungnahmen zu sorgen, oder die **Befugnis, die Beschränkung, Löschung oder Vernichtung von Daten oder das vorläufige Verbot einer Verarbeitung anzuordnen** oder die Befugnis, eine Verwarnung oder eine Ermahnung an den für die Verarbeitung Verantwortlichen zu richten oder die nationalen Parlamente oder andere politische Institutionen zu befassen. Diese Regelung entspricht Artikel 28 Abs. 3 Satz 1, 2. Anstrich der Richtlinie 95/46/EG. Außerdem muss die Aufsichtsbehörde nach Artikel 46 lit. c des Richtlinienentwurfs das Klagerecht oder eine Anzeigebefugnis bei Verstößen gegen die nach Maßgabe dieser Richtlinie erlassenen Vorschriften haben. Diese Regelung entspricht Artikel 28 Abs. 3 Satz 1, 3. Anstrich der Richtlinie 95/46/EG.
Der Katalog der Einwirkungsbefugnisse nach Artikel 46 lit. b des Richtlinienentwurfs bzw. nach Artikel 28 Abs. 3 Satz 1, 2. Anstrich der Richtlinie 95/46/EG nennt mögliche Einwirkungsmöglichkeiten beispielhaft, ohne davon einzelne zwingend vorzugeben. Es muss nur gewährleistet sein, dass die der Aufsichtsbehörde eröffneten Einwirkungsbefugnisse in ihrer Summe wirksam sind**. In Deutschland verfügen der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit und die Landesbeauftragten für den Datenschutz als Datenschutzkontrollinstitutionen im öffentlichen Bereich grundsätzlich nicht über Weisungs- oder Untersagungsrechte** einschließlich der Befugnis zur Ahndung durch Bußgeldzahlungen.

Dies wäre nach deutschem Verfassungsrecht und deutscher Rechtstradition höchst problematisch. Es sei hierzu auf die Nr. 51 der Stellungnahme des Bundesrates (BR-Drs. 52/12 [Beschluss] [2]) verwiesen. Grundsätzlich werden Behörden gegenüber Hoheitsträgern nicht obrigkeitlich tätig. Auch ist es generell ausgeschlossen, dass eine in ministerielle Weisungsstränge nicht eingebundene Aufsichtsbehördehoheitliche Befugnisse gegenüber einer anderen öffentlichen Stelle ausübt. So stehen z. B. auch den Rechnungshöfen, die eine vergleichbar unabhängige Rechtsstellung wie die Datenschutzbeauftragten des Bundes und der Länder haben, keine Eingriffsbefugnisse gegenüber den ihrer Kontrolle unterliegenden öffentlichen Stellen zu.Zu gleichen Feststellungen kommt der Hessische Datenschutzbeauftragte; siehe Ausführungen vom 19. April 2012 auf seiner Homepage unter dem Fachthema „Europa“ zum Thema „Neue Vorschläge der Europäischen Kommission zum Datenschutz in Europa“, Einzelfragen der Verordnung, 7. Unterpunkt. Darin heißt es:

> „Den Datenschutzaufsichtsbehörden sind nicht nur gegenüber privaten Unternehmen sondern auch gegenüber öffentlichen Stellen die Befugnisse eingeräumt, bestimmte Anweisungen und Anordnungen zu treffen, verwaltungsrechtliche Sanktionen zu erlassen sowie Klage zu erheben (Artikel 53). Dies wirft verfassungsrechtliche Probleme auf, da nach deutschem Staatsverständnis ein Hoheitsträger einem anderen Hoheitsträger auf gleicher Hierarchieebene nicht unterworfen werden kann. Nach dem Prinzip der Einheit der Verwaltung können durchsetzbare, sanktionsbewehrte Hoheitsakte gegenüber anderen öffentlichen Stellen nicht erlassen werden.“ (http://www.datenschutz.hessen.de/ft-europa.htm)

Trotz des Verzichts auf Weisungs- und Untersagungsrechte verfügen in Deutschland die für den öffentlichen Bereich zuständigen Datenschutzkontrollinstitutionen schon jetzt in ausreichendem Maße über wirksame Einwirkungsbefugnisse,sodass kein Bedürfnis für die im Zusammenhang mit der EU-Datenschutzreform diskutierten weitergehenden Befugnisnormen besteht. Nach deutschem Recht lassen sich nämlich im öffentlichen Bereich mit den Rechten auf Beanstandung, auf Unterrichtung zuständiger Aufsichtsbehörden, auf Anrufung des Parlaments, auf Unterrichtung der Öffentlichkeit usw. datenschutzrechtlich bedenkliche Verarbeitungen leichter und vor allem auch schneller abstellen, als mit Verbotsverfügungen. Keine öffentliche Stelle darf auf Grund ihrer Bindung an Gesetz und Recht rechtswidrig personenbezogene Daten verarbeiten. Zu rechtskonformem Handeln werden öffentliche Stellen mit Mitteln der Dienst-, Rechts- und Fachaufsicht, durch parlamentarische Kontrolle, durch gerichtliche Kontrolle ggf. auch durch Druck der Medien angehalten. Im öffentlichen Bereich würde der Verzicht auf eigene Durchsetzungsbefugnisse der Datenschutzkontrollinstitutionen diese Stellen von zusätzlichen Aufgaben entlasten.

Die Bundesrepublik Deutschland hat im Vertragsverletzungsverfahren zur Ausgestaltung der Datenschutzkontrolle im nicht-öffentlichen Bereich, das mit der Entscheidung des EuGH vom 10. März 2010 - C 518/07 – endete, gegenüber der Europäischen Kommission nachrichtlich auch das deutsche System der Datenschutzkontrolle im öffentlichen Bereich, das ohne die Befugnis zur Untersagung von Datenverar-

beitungen durch die Datenschutzkontrollinstitution auskommt, dargestellt. Die Vereinbarkeit dieses Systems mit den Vorgaben des Artikels 28 Abs. 1 Satz 1, 2. Anstrich der Richtlinie 95/46/EG stand nie zur Diskussion, auch nicht seitens der Europäischen Kommission.
Dagegen müsste nach der bisherigen Konzeption die Aufsichtsbehörde im Anwendungsbereich der Datenschutz-Grundverordnung künftig über echte Eingriffsbefugnisse (z. B.die Befugnis zur Untersagung von Datenverarbeitungen) auch gegenüber öffentlichen Stellen verfügen. Dies wäre – wie vorstehend ausgeführt - höchst problematisch. **In gleicher Weise problematisch wäre es, wenn Artikel 46 lit. b RL-E aufgrund der dort beispielhaft genannten sehr weitgehenden Eingriffsbefugnisse in dem Sinne verstanden würde, dass wirksame Einwirkungsbefugnisse immer auch mit echten Eingriffsbefugnissen einhergehen müssen**.
Sollten die Aufsichtsbehörden nach der Richtlinie und der Verordnung unterschiedliche Befugnisse erhalten, hätte dies auch für die Polizei und die Strafverfolgungsbehörden weitreichende und fatale Folgen. Diese Behörden sind nämlich regelmäßig auch mit Aufgaben betraut, die dem Anwendungsbereich der Datenschutz-Grundverordnung unterfallen würden. Abgesehen davon, dass kaum vermittelbar wäre, warum die Aufsichtsbehörde im öffentlichen Bereich - abhängig von der Art der zu kontrollierenden Verwaltungstätigkeit - unterschiedliche Befugnisse haben soll, gäbe es erhebliche Auslegungs- und Anwendungsprobleme. Da sich insbesondere die Aufgabenfelder der Polizei häufig überschneiden, dürfte die eindeutige Zuordnung einer Aufgabe zum Anwendungsbereich der Richtlinie oder der Verordnung nicht immer möglich sein. An dieser Stelle zeigt sich einmal mehr das grundlegende Problem, dass das Zusammenspiel von Datenschutz-Grundverordnung und Richtlinie nicht hinreichend durchdacht ist, zu Wertungswidersprüchen führen kann und in der polizeilichen Praxis Schwierigkeiten bereiten würde.
Die aufgezeigten Probleme bestünden nicht, wenn die Aufsichtsbehörden gegenüber öffentlichen Stellen im Anwendungsbereich der Richtlinie und der Verordnung über gleiche Befugnisse verfügen würden. **Daher sollte die deutsche Delegation bei der Verhandlung über beide Regelungswerke das Ziel verfolgen, die Befugnisse der Aufsichtsbehörden gegenüber öffentlichen Stellen auch im Anwendungsbereich der Datenschutz-Grundverordnung entsprechend Artikel 46 des Richtlinienentwurfs zu beschränken.**
Kontraproduktiv wäre es, wenn sich der Ausschuss für bürgerliche Freiheiten, Justiz und Inneres des Europäischen Parlaments mit seinen gegenläufigen Änderungsanträgen 142 (zu Artikel 46) und 144 (zu Artikel 48 Abs. 2), wie sie im Entwurf des Berichts vom 20.12.2012 (2012/0010 [COD]) dargestellt sind, durchsetzen würde, dass die Eingriffs- und Sanktionsbefugnisse gegenüber öffentlichen Stellen entsprechend Artikel 53 des Entwurfs der Datenschutz-Grundverordnung geregelt werden.

Artikel 46 lit. c

Nach Artikel 46 lit. c hat die **Aufsichtsbehörde** bei Verstößen gegen die nach Maßgabe der Richtlinie erlassenen Vorschriften **entweder** das **Klagerecht oder** eine **Anzeigebefugnis.** Zu dieser Regelung**im Widerspruch steht Artikel 53 Abs. 2, wo-**

nach die Aufsichtsbehörde das Klagerecht hat. Gegen das Klagerecht bestehen aus den zu Artikel 53 Abs. 2 genannten Gründe erhebliche Bedenken.
Abschließend bleibt zu Kapitel VI **anzumerken**:
Sofern einzelne weitere Regelungen zur Aufsicht im Entwurf der Richtlinie problematisch erscheinen oder im nationalen Recht Umsetzungsbedarf auslösen würden, ist dies der Anlage zu entnehmen. Solcher **Umsetzungsbedarf bestünde - wegen der weitgehenden Parallelität der Regelungen zur Aufsicht im Entwurf der Datenschutz-Grundverordnung – aber grundsätzlich nicht im Polizeirecht, sondern regelmäßig im allgemeinen Datenschutzrecht des Bundes und der Länder.**

Kapitel VII Zusammenarbeit

Artikel 48 Amtshilfe

Artikel 48 verpflichtet, ebenso wie Artikel 45 Abs. 1 lit. d) zu einer wirksamen Regelung der gegenseitigen Amtshilfe unter den Aufsichtsbehörden (siehe auch schon Artikel 28 Abs. 6 Richtlinie 95/46/EG). Die Norm entspricht zum Teil Artikel 55 der Datenschutz-Grundverordnung.
Die deutschen Aufsichtsbehörden sind europäischen Behörden bereits jetzt über §§ 8a ff. der VwVfGe zur Hilfeleistung verpflichtet. **Regelungsdefizite** in den hier untersuchten Gesetzen **bestehen nicht**.
Polizeibehörden sind nicht Adressaten der Norm. Auf ihre Tätigkeit sind daher **nur mittelbare Auswirkungen** möglich, die sich bei grenzüberschreitenden Bezügen durch von europäischen Aufsichtsbehörden veranlasste Anfragen der jeweiligen LfD/BfDI ergeben können. Ob hierbei ein qualitatives oder quantitatives Mehr an Arbeitsbelastung im Vergleich zur bisherigen Rechtslage entstehen wird, ist momentan schwer abschätzbar.
Der von MdEP Droutsas gefertigte Entwurf des LIBE-Berichts (2012/0010 [COD]) enthält Änderungsvorschläge zu Artikel 48 des Kommissionsentwurfs. Diese enthalten keine weiteren kritischen Punkte. Der ebenfalls vorgeschlagene neue Artikel 48a betrifft gemeinsame Durchsetzungsmaßnahmen und andere gemeinsame Einsatzformender Aufsichtsbehörden. Die Norm ist unnötig, sie kann zudem mittelbare Auswirkungen im oben beschriebenen Sinne haben.

Artikel 49 Aufgaben des Europäischer Datenschutzausschuss

Der nach der Datenschutz-Grundverordnung vorgesehene Europäische Datenschutzausschuss nimmt gemäß Artikel 49 seine Aufgaben auch in Bezug auf Verarbeitungsvorgänge wahr, die in den Anwendungsbereich des Richtlinienentwurfs fallen.
Die Aufgabenbeschreibung entspricht derjenigen in Artikel 66 Datenschutz-Grundverordnung. **Umsetzungsakte** der Mitgliedstaaten sind **nicht nötig**.
Für die Polizeiarbeit hat die Norm **keine unmittelbaren Auswirkungen**.

Der von MdEP Droutsas gefertigte Entwurf des LIBE-Berichts (2012/0010 [COD]) enthält Änderungsvorschläge zu Artikel 49 des Kommissionsentwurfs, die keine weiteren kritischen Punkte enthalten.

Kapitel VIII Rechtsbehelfe, Haftung und Sanktionen

Artikel 50 Recht auf Beschwerdebei der Aufsichtsbehörde

a) Abs. 1 regelt ein Recht des Einzelnen, sich bei der Aufsichtsbehörde über ihn betreffende Verstöße gegen die Richtlinie (vgl. bereits Artikel 28 Abs. 4 Richtlinie 95/46/EG) zu beschweren.
Ein solches Beschwerderecht ist in allen Datenschutzgesetzen enthalten. Ein **Regelungsdefizitbesteht nicht**.
Unmittelbare polizeitaktische **Folgen bestehen nicht**. Wie unter der derzeit geltenden Rechtslage sind allenfalls mittelbare Auswirkungen denkbar, die ein vom Beschwerdeführer veranlasstes Tätigwerden der LfD/BfDI betreffen.
b) In Abs. 2 erhalten Einrichtungen, Organisationen und Verbände das Recht, im Namen und mit Vollmacht des Einzelnen Beschwerde gegenüber der Aufsichtsbehörde bei Verstößen gegen die Richtlinie (betreffend den Einzelnen) zu führen. Um eine Popularbeschwerde handelt es sich – anders als im Fall des Abs. 3 - wegen des Erfordernisses einer Vollmacht nicht.
Auch diese Norm ist nicht an Polizeibehörden adressiert. Sie bedarf **keiner weiteren Umsetzung**, da die Vorschriften in den Verwaltungsverfahrensgesetzen (§§ 14 ff.) über das Auftreten von Bevollmächtigten im Verwaltungsverfahren Entsprechendes ermöglichen.
Polizeitaktische Folgen sind auch hier **nurmittelbar** denkbar und nicht in einem über das geltende Recht hinausgehenden Umfang.

Der von MdEP Droutsas gefertigte Entwurf des LIBE-Berichts (2012/0010 [COD]) schlägt eine Änderung von Artikel 50 Abs. 2 des Kommissionsentwurfs dahingehend vor, dass eine Vollmacht für die Einrichtungen, Organisationen und Verbände nicht erforderlich ist. Das ist äußerst kritisch, weil es zum Individualrechtsschutz nicht erforderlich ist und eine Steigerung der Beschwerden erwarten lässt.

c) **Demgegenüber sieht Abs. 3 eine Popularbeschwerde für Einrichtungen, Organisationen und Verbände bei den Aufsichtsbehörden vor, die im Falle einer Verletzung des Schutzes personenbezogener Daten auch unabhängig von einer Beschwerde der betroffenen Person tätig werden können. Diese Vorschrift ist als besonders kritisch einzustufen**. Für eine Popularbeschwerde gibt es kein nachvollziehbares datenschutzrechtliches Erfordernis. Anders als im nichtöffentlichen Bereich des Datenschutzes ist nicht ersichtlich, welche Verbände im Polizei- und Justizbereich „stellvertretend“ klagen sollten. Bei polizeilichen Maßnahmen kommt es stets auf die individuelle Betroffenheit an.

Die Schaffung einer Popularbeschwerde würde zunächst zu erheblichem gesetzgeberischen Anpassungsbedarf führen, da die deutschen Gesetze nurdemBetroffenen

selbst das Recht geben, sich an die Aufsichtsbehörde zu wenden (z.B. § 25 DSG NRW).Als gravierender dürfte indes die faktischen Auswirkungen auf die Tätigkeit der Polizeien einzuschätzen sein:
Hier droht ein hoher Aufwand für die Bearbeitung von verstärkt zu erwartenden Prüfungen und Anfragen der LfD/ BfDI und der Verbände, die „popular“ angestoßen werden.

Artikel 51 Recht auf gerichtlichen Rechtsbehelf gegen eine Aufsichtsbehörde

Mit Artikel 51 wird ein Recht auf gerichtlichen Rechtsbehelf gegen eine Aufsichtsbehörde normiert (vgl. bereits Abs. 28 Abs. 3 Richtlinie 95/46/EG). Er entspricht Artikel 74 der Datenschutz-Grundverordnung.
Während Abs.1 einen Rechtsbehelf gegen Entscheidungen der Aufsichtsbehörde verlangt, sieht Abs. 2 eine „Untätigkeitsbeschwerde“ vor, mit der die Aufsichtsbehörde gezwungen werden soll, im Fall einer Beschwerde tätig zu werden. In beiden Fällen ist unklar, wie das Verhältnis mehrfacher Klageerhebungen (gegen Aufsichtsbehörde und datenverarbeitende Stelle) ist.
Umsetzungsbedarf besteht, ebenso wie bei der Zuständigkeitsregelung des Abs. 3 **nicht**. Die allgemeinen Regeln der VwGO erfassen auch diesen Bereich.
Relevante **polizeitaktische Folgen** sind **nicht** auszumachen.

Artikel 52 Recht auf gerichtlichen Rechtsbehelf gegen für die Verarbeitung Verantwortliche oder Auftragsverarbeiter

Die Norm zielt darauf, ein Recht auf gerichtlichen Rechtsbehelf gegen einen für die Verarbeitung Verantwortlichen oder einen Auftragsverarbeiter zu schaffen (siehe schon Artikel 22 Richtlinie 95/46/EG, Artikel 20 Rahmenbeschluss 2008/977/JI).
Das deutsche Recht enthält in StPO, EGGVG und VwGO mit den allgemeinen Regelungen ein ausreichendes Instrumentarium bereit. **Regelungslücken** sind **nicht ersichtlich**. Soweit die Richtlinie neue klagefähige Rechtspositionen enthält, müssen diese ggf. separat umgesetzt werden.
Polizeitaktische Folgen gibt es im Vergleich zur geltenden Rechtslage **nicht** zu bedenken.

Artikel 53 Gemeinsame Vorschriften für Gerichtsverfahren

Artikel 53 legt gemeinsame Vorschriften für Gerichtsverfahren fest, er entspricht Artikel 76 Datenschutz-Grundverordnung.
a) Abs.1 verlangt ein Klagerecht für Einrichtungen, Organisationen und Verbände im Namen betroffener Person sowohl im Hinblick auf Klagen gegen die Aufsichtsbehörde als auch gegen die datenverarbeitende Behörde.
Diese Regelung ist rechtspolitisch verfehlt, weil ein Bedarf an besonderer Unterstützung nicht erkennbar ist, und aus den bereits genannten Gründen äußerst kritisch zu sehen (vgl. oben zu Artikel 50 Abs. 3 RL-E und auch BR-Drs. 51/12 (B) (2), S. 14).

b) Auch die Aufsichtsbehörden sollen nach Abs. 2 ein Recht erhalten, um die Einhaltung der Vorgaben der Richtlinie im Klageweg durchzusetzen (vgl. auch Artikel 46 lit. c).
Ein solches Klagerecht ist aus den oben genannten Gründenüberflüssig: Die Strafverfolgungsbehörden sind an Recht und Gesetz gebunden. Die bestehenden Regeln der Dienstaufsicht und Ministerverantwortlichkeit genügen zur Durchsetzung der Datenschutzvorschriften. Daneben reichen die sonstigen Untersuchungs- und Einwirkungsbefugnisse der Aufsichtsbehörden aus (vgl. auch BR-Drs. 51/12 [B] [2], S. 14).
Es besteht **Umsetzungsbedarf**, den sinnvollerweise der Bund in Ausübung seiner Gesetzgebungskompetenz nach Artikel 74 Nr. 1 GG) in der VwGO erfüllen könnte.
Für die Polizeiarbeit sind **möglicherweise erheblicheAuswirkungen** zu erwarten. Die Belastung mit verwaltungsgerichtlichen Streitverfahren dürfte in nicht näher bezifferbarer Weise zunehmen. Ermittlungsverfahren können verzögert und durch die Tätigkeit der Aufsichtsbehörden inhaltlich beeinträchtigt werden.
c) Abs. 3 verlangt von den Mitgliedstaaten die Sicherstellung, dass die Klagemöglichkeiten rasch (vgl. insoweit bereits Artikel 18 Abs. 1 Richtlinie 2000/31/EG über den elektronischen Geschäftsverkehr) und auch einstweilig wirken.
Umsetzungsbedarf besteht **nicht**. Das Instrumentarium von StPO, EGGVG und VwGO reicht aus.
Folgen für die Polizeiarbeit stehen somit **nicht** an.

Artikel 54 Haftung und Recht auf Schadenersatz

Artikel 54 verpflichtet die Mitgliedstaaten, Regelungen zu Haftung und Schadensersatzverpflichtungen zu treffen. Er entspricht Artikel 77 Datenschutz-Grundverordnung.
Die in Abs. 1 vorgesehene Verpflichtung zu Schadensersatzregelungen bei Verstößen gegen die Vorgaben der Richtlinie ist im deutschen Datenschutzrecht wohl **nur zum Teil erfüllt**. Dieses enthält zwar Regelungen zum Schadensersatz bei Verletzung von Datenschutzvorschriften, nicht jedoch zu einer unmittelbaren Haftung des Auftragsverarbeiters gegenüber der betroffenen Person (vgl. etwa § 20 DSG NRW).Allerdings könnte Artikel 54 Abs. 1 RL-E in dem Sinne interpretiert werden, dass es dem nationalen Gesetzgeber überlassen bleibt, ob nur der für die Verarbeitung Verantwortliche und/oder der Auftragsverarbeiter haftet, solange er nur einen der beiden eine Haftung auferlegt.
Der von MdEP Droutsas gefertigte Entwurf des LIBE-Berichts (2012/0010 [COD]) schlägt vor, den Ersatzanspruch auch auf immaterielle Schäden zu erstrecken.

Auch die im Abs. 2 verlangte gesamtschuldnerische Haftung des Verantwortlichen und des Auftragsverarbeiters ist nicht umgesetzt.

Aus Abs. 3 folgt, dass die Haftung aufgrund vermuteten Verschuldens eintreten soll. Verantwortlicher und Auftragsverarbeiter können ganz oder teilweise von der Haftung

befreit werden, wenn sie fehlendes Vertretenmüssen nachweisen können. Dies sehen die Datenschutzgesetze des Bundes und der Länder bereits vor.
Für die **Polizeiarbeit** hat eine Umsetzung des Artikels 54 im Vergleich zur bisherigen Rechtslage **keine unmittelbaren Auswirkungen**. Die nach außen gerichtete Inpflichtnahme des Auftragsverarbeiters wird für die Polizei voraussichtlich keine negativen Folgen haben.

Artikel 55 Sanktionen

Die Mitgliedstaaten werden in Artikel 55 (entspricht Artikel 58 Datenschutz-Grundverordnung, Artikel 24 Rahmenbeschluss 2008/977/JI) aufgefordert, festzulegen, welche Sanktionen bei Verstößen gegen die Richtlinie zu verhängen sind. Die Norm enthält nur die Verpflichtung, wirksame, verhältnismäßige und abschreckende Sanktionen vorzusehen.
Umsetzungsbedarf dürfte insoweit **nicht** bestehen. Ob die Befugnisse der Dienst- und Fachaufsicht als ausreichende Umsetzung angesehen werden kann, ist zwar fraglich, kann aber offen bleiben: Bestimmte Verstöße gegen Vorschriften der Datenschutzgesetze sind mit Strafen oder Bußgeldern belegt.

Der von MdEP Droutsas gefertigte Entwurf des LIBE-Berichts (2012/0010 [COD]) enthält als Änderungsvorschlag zum Kommissionsentwurf die Einfügung eines neuen **Artikel 55a**, wonach die Übermittlung personenbezogener Daten an andere Behörden oder nicht-öffentliche Stellen innerhalb der Union unter bestimmten Voraussetzungen möglich ist. Das ist zu begrüßen; der Kommissionsentwurf ist demgegenüber deutlich enger (vgl. Artikel 7).

Kapitel IX Delegierte Rechtsakte und Durchführungsakte

Artikel 56 Befugnisübertragung

Mit Artikel 56 wird die Übertragung der Befugnis zum Erlass delegierter Rechtsakte gemäß Artikel 290 AEUV umgesetzt (entspricht Artikel 86 Datenschutz-Grundverordnung). Danach wird der Kommission die Befugnis übertragen, Rechtsakte ohne Gesetzescharakter mit allgemeiner Geltung zur Ergänzung oder Änderung bestimmter nichtwesentlicher Vorschriften eines Gesetzgebungsaktes zu erlassen. Vorliegend wird die Befugnis übertragen, Kriterien und Anforderungen für Meldungen von Verletzungen des Schutzes von personenbezogenen Daten an die Aufsichtsbehörden festzulegen.
Die Ermächtigung der Kommission istkritisch. Zum einen erhält die KOM auf diese Weise eine Art „Blankoscheck“ der Mitgliedstaaten, die Vorgaben der RL zu konkretisieren. Insoweit **drohen weitestgehend einseitige Festlegungen durch KOM, die häufig nicht erforderlich sowie in Inhalt, Umfang und Reichweite heute nicht vorhersehbar sind, gegebenenfalls aber zu erheblichem Mehraufwand und Beeinträchtigungen der Polizei führen können**. Es ist kein Grund dafür ersichtlich, etwaig bestehenden Ergänzungs- oder Konkretisierungsbedarf durch entsprechende Regelungen im RL-E selbst zu beheben; auf diese Weise könnten die

Mitgliedstaatendiese Regelungen aktiv mitgestalten. Alternativ könnte die Beantwortung von im RL-E offen gelassenen Detailfragen den Mitgliedstaatenselbst überlassen bleiben.

Zum anderen kann es bis zu einem Tätigwerden der Kommission ggf. zu **Rechtsunsicherheiten** kommen.Wohl vor diesem Hintergrund enthält der von MdEP Droutsas gefertigte Entwurf des LIBE-Berichts (2012/0010 [COD]) als Änderungsvorschlag zum Kommissionsentwurf einen neuen **Artikel 56a**, der eine Frist zum Erlass des delegierten Rechtsakts vor dem Zeitpunkt der Umsetzung der Richtlinie enthält.

Artikel 57 Ausschussverfahren

Artikel 57 regelt das Ausschussverfahren für die Übertragung von Durchführungsbefugnissen auf die Kommission. Er entspricht Artikel 87 Datenschutz-Grundverordnung.
Der Bundesrat hat vorgeschlagen, in den Absätzen 2 und 3 jeweils einzufügen, dass Durchführungsakte der Kommission ohne Stellungnahme des Ausschusses nicht erlassen werden dürfen (Drs. 51/12 [Beschluss] [2], S. 15). Die Arbeitsgruppe teilt diese Einschätzung.
Umsetzungsbedarf im mitgliedstaatlichen Recht **besteht nicht**.
Für die Polizeiarbeit hat Artikel 57 **keine relevanten Auswirkungen**.

Kapitel X Schlussbestimmungen

Artikel 58 Aufhebung

Die in Artikel 58 RL-E vorgesehene Aufhebung des Rahmenbeschlusses 2008/977/JI ist einerseits folgerichtig. Andererseits stellt sich aus politischer Sicht die Frage, warum der erst am 20. Januar 2009 nach umfassenden Beratungen in Kraft getretene-Rahmenbeschluss zum jetzigen Zeitpunkt überhaupt ersetzt werden soll. Solange der Rahmenbeschluss noch nicht hinreichend erprobt und der Nachweis seiner Unzulänglichkeit nicht geführt ist, erscheint es aus fachlicher Sicht wenig sinnvoll, neue EU-weite Regelungen für den Polizei- und Justizbereich zu diskutieren. Sofern eine solche Diskussion, wie gegenwärtig zum seitens KOM vorgelegten RL-E, gleichwohl geführt wird, sollte nicht ohne Grund von den durchdachten Regelungen des Rahmenbeschlusses abgewichen werden.
Für das Recht der Bundesländer, die den Rahmenbeschluss bereits umgesetzt haben, ergeben sich aus der Norm keine eigenständigen Folgen. Soweit die entsprechenden Vorschriften der Richtlinie nicht widersprechen, bleibt ihr Bestand auch bei Wegfall des Rahmenbeschlusses unangetastet. Im Übrigen sind sie anzupassen.Ob und inwieweit hier gesetzgeberischer Handlungsbedarf entsteht, hängt maßgeblich davon ab, ob der RL-E als Vollharmonisierung zu begreifen ist oder aber lediglich Mindeststandards (mit der Möglichkeit, nationale strengere Vorgaben zu erlassen oder beizubehalten) vorgeben soll.

Artikel 59 Verhältnis zu bestehenden Rechtsakten der Union im Bereich der polizeilichen und justiziellen Zusammenarbeit in Strafsachen

Die Norm ordnet an, dass bisherige Regelungen im thematischen Anwendungsbereich der Richtlinie (betreffend die Verarbeitung personenbezogener Daten und den Zugang zu Informationssystemen) bestehen bleiben. Das sind etwa:
- Beschluss 2002/348/JI des Rates vom 25. April 2002 (und Änderungsrechtsakte) – Sicherheit bei Fußballspielen von internationaler Bedeutung;
- Beschluss 2008/617/JI des Rates vom 23. Juni 2008 – Zusammenarbeit zwischen den Spezialeinheiten der Mitgliedstaaten in Krisensituationen;
- Beschluss 2008/633/JI des Rates vom 23. Juni 2008 – Zugang der benannten Behörden der Mitgliedstaaten und von Europol zum Visa-Informationssystem (VIS) zum Zwecke der Verhütung, Aufdeckung und Ermittlung terroristischer und sonstiger schwerwiegender Straftaten.

Wegen des von Artikel 61 formulierten Prüfauftrags an die Kommission ist sichergestellt, dass etwaiger Anpassungsbedarf an die bestehenden Rechtsakte zukünftig festgestellt wird.
Umsetzungsbedarf hat dies für den Bund und die Länder **nicht** zur Folge. Für die Polizeiarbeit sind keine Auswirkungen zu erwarten.

Artikel 60 Verhältnis zu bestehenden internationalen Übereinkünftenim Bereich der polizeilichen und justiziellen Zusammenarbeit in Strafsachen

Die Mitgliedstaaten werden zur Prüfung und ggf. Abänderung von vor Inkrafttreten der Richtlinie geschlossenen internationalen Übereinkünften innerhalb von fünf Jahren nach Inkrafttreten der Richtlinie verpflichtet.
Die **Norm** ist**äußerst kritischzu betrachten**. Der Zwang zur Abänderung bestehender bi- oder multilateraler Polizeiabkommen berührt u. a. die Regelungen der Wiener Vertragsrechtskonvention sowie die außenpolitische Kompetenz der Mitgliedstaaten (vgl. auch BR-Drs. 51/12 [B] [2], S. 15).
Der auf den Bund und die Länder zukommende Aufwand wäre enorm. Zudem ist völlig unklar, ob sich die Vertragspartner zu Neu-/Nachverhandlungen bereit sehen und Änderungen im Sinne der Richtlinie akzeptieren.**Hier drohen erhebliche Lücken und Effektivitätseinbußen in bewährten Bereichen der internationalen Zusammenarbeit zu entstehen.**

Artikel 61 Bewertung

Die Kommission wird verpflichtet, die Anwendung der Richtlinie zu evaluieren und eine Anpassung anderer Rechtsakte der Europäischen Union über die Verarbeitung personenbezogener Daten (Artikel 59) an die Richtlinie zu prüfen. **Kritisch** ist zu sehen, dass anders als bei Artikel 27 des Rahmenbeschlusses 2008/977/JI eine ausdrückliche Beteiligung der Mitgliedstaaten an der Evaluierung nicht vorgesehen ist.
Für die Mitgliedstaaten folgt hieraus noch **kein Umsetzungsbedarf**.

Demnach sind **Auswirkungen** auf die Polizeiarbeit erst denkbar, wenn aufgrund der Feststellungen und Berichte der Kommission Rechtsänderungen vorgenommen werden.

Artikel 62 Umsetzung

Die zweijährige Frist zur Umsetzung der Richtlinie ist sehr knapp bemessen. Mit der Bewerkstelligung des nötigen Anpassungs- und Umstellungsaufwands können die Polizeibehörden erst nach Verkündung bzw. Inkrafttreten der Änderungsgesetze auf Bundes- und Landesebene beginnen. Wie viel zeitlichen Spielraum sie dazu haben werden, ist nicht abzusehen.
Artikel 62 enthält im Übrigen übliche Regelungen zur Kennzeichnung der nationalen Vorschriften, die die Richtlinie umsetzen und Mitteilungspflichten gegenüber der Kommission.

Artikel 63 Inkrafttreten, Anwendung und Artikel 64 Adressaten

Es handelt sich um notwendige rechtsförmliche Regelungen **ohne unmittelbaren Umsetzungsbedarf** und **ohne unmittelbare Auswirkungen auf die Polizeiarbeit**.