Bundesrat **Drucksache** **51/1/12**

19.03.12

Empfehlungen
der Ausschüsse

EU - In - R

zu **Punkt ...** der 895. Sitzung des Bundesrates am 30. März 2012

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) 10 final; Ratsdok. 5833/12

A

Der federführende Ausschuss für Fragen der Europäischen Union (EU),

der Ausschuss für Innere Angelegenheiten (In) und

der Rechtsausschuss (R)

empfehlen dem Bundesrat, zu der Vorlage gemäß Artikel 12 Buchstabe b EUV wie folgt Stellung zu nehmen:

EU
R

1. Der Bundesrat begrüßt die Zielsetzung des Richtlinienvorschlags, die polizeiliche und justizielle Zusammenarbeit in Strafsachen unter Achtung des Grundrechts auf Schutz personenbezogener Daten zu erleichtern.

EU
R

2. Die Subsidiaritätsrüge gemäß Artikel 12 Buchstabe b EUV erfasst auch die Frage der Zuständigkeit der EU - siehe die Stellungnahmen des Bundesrates vom 9. November 2007, BR-Drucksache 390/07 (Beschluss), Ziffer 5, und vom

...

Vertrieb: Bundesanzeiger Verlagsgesellschaft mbH, Postfach 10 05 34, 50445 Köln
Telefon (02 21) 97 66 83 40, Fax (02 21) 97 66 83 44, www.betrifft-gesetze.de
ISSN 0720-2946

26. März 2010, BR-Drucksache 43/10 (Beschluss), Ziffer 2 sowie vom 16. Dezember 2011, BR-Drucksache 646/11 (Beschluss). Der Grundsatz der Subsidiarität ist ein Kompetenzausübungsprinzip. Gegen das Subsidiaritätsprinzip wird auch dann verstoßen, wenn keine Kompetenz der Union besteht. Daher muss im Rahmen der Subsidiaritätsprüfung zunächst die Frage der Rechtsgrundlage geprüft werden.

EU R

3. Der vorgelegte Vorschlag für eine Richtlinie zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten zum Zwecke der Verhütung, Untersuchung, Aufdeckung und Verfolgung von Straftaten lässt sich nicht auf Artikel 16 Absatz 2 AEUV stützen, soweit sich der Anwendungsbereich der Richtlinie auch auf die Datenverarbeitung in innerstaatlichen Verfahren erstreckt.

EU In

4. Mithin ist der Vorschlag der Kommission, soweit er den rein innerstaatlichen Informationsverkehr der Polizeibehörden einbezieht, nicht von der angegebenen Rechtsgrundlage des Artikels 16 Absatz 2 AEUV gedeckt.

EU R

5. Nach dem in Artikel 5 Absatz 2 EUV normierten Grundsatz der begrenzten Einzelermächtigung darf die EU nur innerhalb der Grenzen der Zuständigkeiten tätig werden, die die Mitgliedstaaten ihr in den Verträgen zur Verwirklichung der darin niedergelegten Ziele übertragen haben.

EU In R

6. Artikel 16 Absatz 2 AEUV gestattet nur, Vorschriften über den Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die Mitgliedstaaten im Rahmen der Ausübung von Tätigkeiten, die in den Anwendungsbereich des Unionsrechts fallen, zu erlassen.

EU R

7. Das innerstaatliche Strafverfahren fällt jedoch nur innerhalb enger Grenzen in den Anwendungsbereich des Unionsrechts. Die eingeschränkten Kompetenzen der EU zum Erlass von Richtlinien für das Strafverfahren (Artikel 82 Absatz 2 AEUV) begrenzen daher auch die datenschutzrechtliche Kompetenz der EU für diesen Sachbereich. Dies steht einer Harmonisierung der rein innerstaatlichen Datenverarbeitung im Strafverfahren entgegen. Die Verarbeitung personenbezogener Daten ist ein maßgeblicher Bestandteil des Strafverfahrens. Der Richtlinienvorschlag führt daher zu weitreichenden Eingriffen in das Strafverfahrensrecht, die zur Erleichterung der gegenseitigen Anerkennung von Ent-

scheidungen und der Zusammenarbeit in Strafsachen mit grenzüberschreitender Dimension nicht erforderlich sind. So enthält der Vorschlag Regelungen, die den Mitgliedstaaten umfangreiche Vorgaben für die Führung der Verfahrensakten (Artikel 5 und 6), für Ermittlungsmaßnahmen unter Verwendung besonderer Kategorien von personenbezogenen Daten (Artikel 8) sowie für die Akteneinsicht und Auskunftserteilung (Artikel 11 bis 14) machen.

In der Begründung des Richtlinienvorschlags wird zur Einbeziehung der innerstaatlichen Datenverarbeitung ausgeführt, die zuständigen Behörden könnten nicht ohne weiteres zwischen der innerstaatlichen Datenverarbeitung und dem grenzüberschreitenden Austausch von personenbezogenen Daten unterscheiden oder vorhersehen, ob es zu bestimmten personenbezogenen Daten später einen grenzüberschreitenden Austausch geben wird. Dies vermag die Erforderlichkeit des weiten Anwendungsbereichs der Richtlinie jedoch nicht zu begründen. Die zuständigen Behörden können die grenzüberschreitende Übermittlung von Daten, die zuvor nach den Vorschriften des innerstaatlichen Strafverfahrensrechts erhoben wurden, ohne weiteres nach den dafür geltenden Regeln beurteilen. Sollten rechtliche Defizite bei der Datenübermittlung im Rahmen der justiziellen und polizeilichen Zusammenarbeit bestehen, könnten diese bereichsspezifischen Regelungen überarbeitet werden. Die von der Kommission angenommenen praktischen Schwierigkeiten bei einer rechtlichen Unterscheidung zwischen der innerstaatlichen Datenverarbeitung und dem grenzüberschreitenden Austausch von personenbezogenen Daten können dagegen keine Erweiterung der bestehenden Kompetenzen begründen. Diese Ausführungen gelten entsprechend für die Verarbeitung personenbezogener Daten im Bereich des Polizeirechts.

EU
In

8. Der Kompetenzrahmen des Artikels 16 Absatz 2 AEUV ("Anwendungsbereich des Unionsrecht") wird gemäß Artikel 2 Absatz 6 AEUV im polizeilichen Bereich durch Artikel 87 AEUV konkretisiert. Danach ist nur die Zusammenarbeit zwischen den mitgliedstaatlichen Polizei- und Strafverfolgungsbehörden erfasst. Artikel 87 Absatz 1 AEUV vermittelt insofern keine Kompetenz zur Regelung von Sachverhalten, die ausschließlich die Tätigkeit dieser Behörden innerhalb eines Mitgliedstaats und damit keine Form der Zusammenarbeit zwischen den Mitgliedstaaten betreffen. Die Regelungsbefugnis bezüglich des polizeilichen Informationsaustauschs, die in Artikel 87 Absatz 2 Buchstabe a AEUV niedergelegt ist, korrespondiert in ihrer Reichweite durch die Ver-

weisung auf die Zwecke des Artikels 87 Absatz 1 mit der dortigen Festlegung des Kompetenzbereiches auf die Zusammenarbeit der mitgliedstaatlichen Behörden. Daraus folgt, dass auch in datenschutzrechtlicher Hinsicht der polizeiliche Informationsverkehr ausschließlich in Bezug auf die Zusammenarbeit zwischen den mitgliedstaatlichen Strafverfolgungsbehörden einer EU-Regelungskompetenz unterworfen ist.

Auch gemäß Artikel 51 der Charta der Grundrechte der EU erfasst Artikel 8 der Charta nur mitgliedstaatliche Tätigkeiten, soweit sie Unionsrecht durchführen; eine Kompetenzerweiterung durch die Anwendung der Charta ist nach Artikel 51 Absatz 2 der Charta ebenfalls ausgeschlossen. Durch die Interpretation des Artikels 8 der Charta und des Artikels 16 Absatz 2 AEUV unter Außerachtlassung der Besonderheiten der Bestimmungen über den Raum der Freiheit, Sicherheit und des Rechts wird durch den Richtlinienvorschlag das Primärrecht derart erweiternd ausgelegt, dass eine im Urteil des Bundesverfassungsgerichts vom 30. Juni 2009 (Az.: 2 BvE 2/08 u. a.) beschriebene verfassungsrechtlich bedeutsame Spannungslage zum Prinzip der begrenzten Einzelermächtigung und zur verfassungsrechtlichen Integrationsverantwortung des einzelnen Mitgliedstaats mit Auswirkungen auf die tatsächliche Gewährleistung von Sicherheit und Ordnung entsteht. Die nur formelhafte Formulierung des Artikels 2 Absatz 3 Buchstabe a des Richtlinienvorschlags ist nicht geeignet, die in besonderem Maße zu Lasten der Polizeihoheit der Länder gehende sachliche Kompetenzausweitung zu vermeiden.

EU In

9. Der Bundesrat sieht ebenfalls keine Kompetenz der EU für die Regelung des nicht straftatbezogenen Gefahrenabwehrrechts. Auch hier besteht die begründete Gefahr, dass die EU ohne entsprechende klarstellende Ausnahme die datenschutzrechtliche Zuständigkeit nach Artikel 16 AEUV zu Lasten der mitgliedstaatlichen Kompetenz für die nicht straftatbezogene Gefahrenabwehr im Sinne des Bundesverfassungsgerichtsurteils vom 30. Juni 2009 (Az.: 2 BvE 2/08 u. a.) erweiternd abrundet und sachlich ausdehnt. Hier ist die formelhafte Formulierung des Artikels 2 Absatz 3 Buchstabe a des Richtlinienvorschlags ebenfalls nicht geeignet, diesen in den einzelnen Bestimmungen angelegten Kompetenztransfer zu vermeiden.

EU R

10. Der Richtlinienvorschlag verstößt auch gegen das in Artikel 5 Absatz 3 EUV verankerte Subsidiaritätsprinzip im engeren Sinne, soweit der Vorschlag

Regelungen für die rein innerstaatliche Datenerhebung und -verarbeitung enthält. Insofern ist ein Mehrwert der vorgesehenen europaweit einheitlichen Regelungen nicht erkennbar. Im Gegenteil können die Mitgliedstaaten die rein innerstaatliche Datenverarbeitung (Erhebung, Speicherung und Übermittlung) ausreichend selbst regeln bzw. ist dieser Bereich im deutschen Recht durch die geltenden Datenschutzgesetze bereits ausreichend geregelt.

EU
In

11. Auch die Begründung bezüglich der Einbeziehung des rein innerstaatlichen polizeilichen Informationsverkehrs und dessen Vereinbarkeit mit dem Subsidiaritätsprinzip verstößt gegen die von der Kommission zu beachtenden Vorgaben des Artikels 5 des Protokolls Nr. 2 zum Lissabon-Vertrag, an die die Kommission gemäß Artikel 51 EUV gebunden ist. Die Ausführungen in der Begründung unter Nummer 3.2 des Richtlinienvorschlags behaupten die Konformität mit dem Subsidiaritätsprinzip lediglich, ohne die nach Artikel 5 des Protokolls erforderlichen quantitativen und qualitativen Angaben darzulegen. Das Begleitdokument SEK (2012) 73 weist auf Seite 3 insoweit nur auf eine spekulativ angenommene Behinderung des mitgliedstaatlichen Informationsaustausches zwischen den zuständigen Behörden hin. Dieser Annahme liegt nach Darlegung im Folgenabschätzungsdokument SEK (2012) 72 auf Seite 34 unter Buchstabe d jedoch lediglich die Einschätzung einer nicht-öffentlichen Studie eines migrationspolitischen Beratungsinstituts zugrunde. Die Grundlagen der Studie des bereichsfernen Instituts sind somit weder überprüfbar noch nachvollziehbar dargelegt und daher ungeeignet. Andere nachvollziehbare Angaben fehlen.

EU
In

12. Die Regelung berührt zudem den Schutzgehalt des Artikels 72 AEUV. Der Artikel 72 AEUV ergänzt für den polizeilichen Bereich Artikel 5 Absatz 3 EUV. Die aus Artikel 72 AEUV folgende besonders intensive Erforderlichkeitsprüfung für entsprechende Eingriffe ist weder im Richtlinienvorschlag selbst noch in den Begleitdokumenten enthalten. Die vorgeschlagenen Einschränkungen des rein innerstaatlichen Informationsverkehrs der Polizeien sowie die Möglichkeiten nach Artikel 27 des Richtlinienvorschlags, die Anforderungen an und damit die datenschutzrechtliche Zulässigkeit der Verwendung von innerstaatlichen informationstechnologischen Verfahren und Systemen verbindlich zu reglementieren, berühren insoweit die durch Artikel 72 AEUV garantierte Wahrnehmungverantwortlichkeit und -fähigkeit der Polizei, für die rein innerstaatliche Gewährleistung von Sicherheit und Ordnung zu sorgen. Sollten

bestimmte Verfahren und Systeme für datenschutzrechtlich unzulässig erklärt werden, dürften diese nicht mehr eingesetzt werden, wodurch die konkrete Aufgabenwahrnehmung der Polizei im einzelnen Einsatzfall massiv eingeschränkt werden würde.

EU In

13. Der Zwang zur Abänderung bestehender bi- oder multilateraler Polizeiabkommen in Artikel 60 des Richtlinienvorschlags berührt die Regelungen der Wiener Vertragsrechtskonvention sowie die außenpolitische Kompetenz der Mitgliedstaaten. Artikel 351 AEUV sieht nur vor, dass die Mitgliedstaaten alle geeigneten Mittel anwenden, um eventuelle Unvereinbarkeiten geschlossener Übereinkünfte mit den EU-Verträgen zu beheben. Die rigide Formulierung des Artikels 60 des Richtlinienvorschlags wird insofern kritisch betrachtet. Eine Ausgestaltung als "sunset-clause" wäre zu prüfen.

EU In

14. Es ist nicht ersichtlich, dass die Mitgliedstaaten nicht die Fähigkeit besitzen, den innerbehördlichen Datenschutz durch Aufgaben- und Tätigkeitsbeschreibungen für behördliche Datenschutzbeauftragte ausreichend verwirklichen zu können. Zudem ergibt sich aus dem Richtlinienvorschlag kein Nachweis, dass durch die in Artikel 30 ff. des Richtlinienvorschlags enthaltene Regelungsdichte der behördliche Datenschutz besser als durch zum Teil schon bestehende nationale Regelungen verwirklicht wird, wodurch ebenfalls das Subsidiaritätsprinzip verletzt wird.

Begründung (nur gegenüber dem Plenum):

Der Richtlinienvorschlag verläßt durch die Einbeziehung des rein innerstaatlichen Informationsaustauschs der Polizei den der EU durch die Mitgliedstaaten vertraglich zugewiesenen Kompetenzbereich und verstößt daher gegen das Subsidiaritätsprinzip. Die angeführten Begründungen, gerade auch mit Blick auf den nach Artikel 72 AEUV besonders geschützten Zuständigkeitsbereich der Mitgliedstaaten, sind behauptender und zum Teil spekulativer Natur und erfüllen nicht ansatzweise die aus dem Protokoll Nr. 2 zum Lissabonner Vertrag folgenden obligatorischen Begründungspflichten. Dies ist um so weniger hinzunehmen, als der Vorschlag ohne vertragliche Grundlage erheblich in die polizeiliche Länderkompetenz eingreift. Die zwingende Anweisung zur Revision bestehender bi- oder multilateraler Polizeiabkommen ist ebenfalls kritisch zu würdigen. Zudem enthält der Richtlinienvorschlag, auch wenn er als Richtlinie ausgestaltet ist, im Hinblick auf die Ausgestaltung der Aufgaben der behördlichen Datenschutzbeauftragten eine Regelungsdichte, die einer Verordnung vergleichbar ist. Eine entsprechende Darlegung, welche Defizite im Bereich des behördlichen Datenschutzes überhaupt bestehen sollen und warum - sofern ein Defizit überhaupt anzunehmen wäre - dieses nicht

genauso gut oder gar besser durch mitgliedstaatliche Maßnahmen erreicht werden kann, fehlt in Gänze.

EU R 15. Der Bundesrat verweist ergänzend auf seine Stellungnahme zur Mitteilung der Kommission an das Europäische Parlament, den Rat, den Europäischen Wirtschafts- und Sozialausschuss und den Ausschuss der Regionen: Gesamtkonzept für den Datenschutz in der Europäischen Union, COM(2010) 609 final; BR-Drucksache 707/10 (Beschluss), Ziffer 8.

B

Der federführende Ausschuss für Fragen der Europäischen Union (EU),

der Ausschuss für Innere Angelegenheiten (In) und

der Rechtsausschuss (R)

empfehlen dem Bundesrat zu der Vorlage gemäß den §§ 3 und 5 EUZBLG wie folgt Stellung zu nehmen:

Zur Vorlage allgemein

EU In R [EU In] {EU R} 16. Der Bundesrat begrüßt die Zielsetzung des Richtlinienvorschlags, [die polizeiliche Zusammenarbeit] sowie die {polizeiliche} und justizielle Zusammenarbeit in Strafsachen unter Achtung des Grundrechts auf Schutz personenbezogener Daten zu erleichtern.

EU In R [EU R] {EU In} 17. Dem weitreichenden Vorschlag zur Änderung der Datenschutzvorschriften [in den Bereichen der polizeilichen und justiziellen Zusammenarbeit in Strafsachen] steht der Bundesrat jedoch in {einigen, auch} wesentlichen Punkten kritisch gegenüber.

EU In 18. Der Bundesrat hält die vorgeschlagenen Regelungen zum jetzigen Zeitpunkt mit Blick auf den Rahmenbeschluss Datenschutz für nicht erforderlich.

EU
In

19. Nach dem Richtlinienvorschlag soll die Richtlinie an die Stelle des Rahmenbeschlusses 2008/977/JI des Rates vom 27. November 2008 über den Schutz personenbezogener Daten, die im Rahmen der polizeilichen und justiziellen Zusammenarbeit in Strafsachen verarbeitet werden (Rahmenbeschluss Datenschutz), treten. Der Rahmenbeschluss Datenschutz enthält weitreichende Regelungen für eine Vereinheitlichung des Datenschutzes im Bereich der ehemaligen "Dritten Säule" und verfolgt damit das gleiche Ziel wie der Richtlinienvorschlag. Eine vollständige Implementation der Vorgaben des Rahmenbeschlusses Datenschutz in das innerstaatliche Recht der Mitgliedstaaten ist noch nicht erfolgt und eine Evaluation des Rahmenbeschlusses und seiner Umsetzung wird frühestens im Jahr 2014 stattfinden. Es erscheint daher derzeit nicht sachgerecht, im Wege eines neuen Rechtsaktes einen neuen Rechtsrahmen für den Datenschutz im Bereich der justiziellen Zusammenarbeit in Strafsachen und der polizeilichen Zusammenarbeit zu schaffen. Das gilt umso mehr, als der Rahmenbeschluss Regelungen enthält, die im Richtlinienvorschlag nicht (mehr) aufgegriffen oder abweichend geregelt werden. Angesichts des Umfangs der Kompetenzausweitung sowie des erheblichen Änderungsbedarfs bei den einzelnen Bestimmungen des Richtlinienvorschlags sollte überprüft werden, ob eine gegebenenfalls geboten erscheinende Modifizierung des bestehenden Rahmenbeschlusses 2008/977/JI dem Erlass der Richtlinie vorzuziehen wäre.

EU
In

20. Soweit der Richtlinienvorschlag auch die rein innerstaatliche polizeiliche Datenverarbeitung in den Anwendungsbereich einbezieht, lehnt der Bundesrat den Vorschlag ab, da er von den vertraglichen Grundlagen nicht gedeckt ist. Der Kompetenzrahmen des Artikels 16 Absatz 2 AEUV wird im polizeilichen Bereich durch Artikel 87 AEUV konkretisiert. Danach ist nur die Zusammenarbeit zwischen den mitgliedstaatlichen Polizei- und Strafverfolgungsbehörden erfasst. Artikel 87 Absatz 1 AEUV vermittelt insofern keine Kompetenz zur Regelung von Sachverhalten, die ausschließlich die Tätigkeit dieser Behörden innerhalb eines Mitgliedstaats und damit keine Form der Zusammenarbeit zwischen den Mitgliedstaaten betreffen. Die nur formelhafte Formulierung des Artikels 2 Absatz 3 Buchstabe a des Richtlinienvorschlags ist nicht geeignet, die in besonderem Maße zu Lasten der Polizeihoheit der Länder gehende sachliche Kompetenzausweitung zu vermeiden. Die Bundesregierung wird

daher gebeten, sich in Artikel 1 des Richtlinienvorschlags für eine klarstellende Begrenzung des Anwendungsbereichs auf die mitgliedstaatliche Zusammenarbeit der Strafverfolgungsbehörden einzusetzen, da ansonsten eine im Urteil des Bundesverfassungsgerichts vom 30. Juni 2009 (Az.: 2 BvE 2/08 u. a.) beschriebene verfassungsrechtlich bedeutsame Spannungslage zum Prinzip der begrenzten Einzelermächtigung und zur verfassungsrechtlichen Integrationsverantwortung entstehen könnte.

EU
In

21. Der Bundesrat sieht ebenfalls keine Kompetenz der EU für die Regelung des nicht straftatbezogenen Gefahrenabwehrrechts. Auch hier besteht die begründete Gefahr, dass die EU ohne entsprechend klarstellende Ausnahme die datenschutzrechtliche Zuständigkeit nach Artikel 16 AEUV zu Lasten der mitgliedstaatlichen Kompetenz für die nicht straftatbezogene Gefahrenabwehr im Sinne des Bundesverfassungsgerichtsurteils vom 30. Juni 2009 (Az.: 2 BvE 2/08 u. a.) erweiternd abrundet und sachlich ausdehnt. Die formelhafte Formulierung des Artikels 2 Absatz 3 Buchstabe a des Richtlinienvorschlags ist nicht geeignet, diesen in den einzelnen Bestimmungen angelegten Kompetenztransfer zu vermeiden. Die Bundesregierung wird gebeten, sowohl im Anwendungsbereich der Richtlinie als auch bei der parallelen Datenschutz-Grundverordnung (COM (2012)11) eindeutig klarzustellen, dass mangels einer der EU übertragenen Kompetenz die Informationsverarbeitung im Bereich der nicht straftatbezogenen Gefahrenabwehr den beiden Rechtsakten nicht unterfällt. Darüber hinaus bestünde ansonsten die Gefahr eines sachlich nicht angemessenen, zweispurigen Regelungssystems im Gefahrenabwehrrecht. Nachdem der Richtlinienvorschlag nur die Verhütung von Straftaten, nicht aber die sonstigen Bereiche der polizeilichen Gefahrenabwehr erfasst, stellte sich für letztere die Frage, ob diesbezüglich die insoweit wenig passenden Regelungen der geplanten Verordnung zur Anwendung kämen. Es dürfen aus Sicht des Bundesrats mit Blick auf die nationalen Regelungen und die Interessenlage jedenfalls keine grundsätzlich unterschiedlichen Regelungen gelten, je nachdem, ob es um die Verhütung von Straftaten oder die Abwehr sonstiger Gefahren geht. Es muss daher vermieden werden, dass für die Tätigkeiten der Polizeibehörden sowohl die Datenschutz-Grundverordnung als auch die Richtlinie anwendbar wären.

EU In

22. Der Bundesrat ist der Auffassung, dass zahlreiche Vorschriften des Richtlinienvorschlags jedenfalls in ihrer derzeit geplanten Ausgestaltung nicht geboten sind, sie insbesondere die berechtigten Belange einer effektiven Strafverfolgung und Gefahrenabwehr nicht hinreichend berücksichtigen und gleichzeitig den Mitgliedstaaten wesentliche Gestaltungsspielräume für die Beibehaltung und Weiterentwicklung des Datenschutzniveaus nehmen. Zudem lassen die Vorschriften bisweilen erhebliche Schwierigkeiten im praktischen Vollzug befürchten.

Zu Artikel 4

EU In

23. Der in Artikel 4 Buchstabe a des Richtlinienvorschlags niedergelegte Grundsatz von Treu und Glauben ist dem Bereich der Eingriffsverwaltung fremd. Gleiches gilt für die Verwendung des Grundsatzes in Artikel 11 Absatz 1 Buchstabe g des Richtlinienvorschlags. Die Strafverfolgungsbehörden als Teil der vollziehenden Gewalt sind an Gesetz und Recht gebunden. Polizeiliches und justizielles Handeln hat daher stets rechtmäßig zu sein, so dass der Artikel 4 Buchstabe a insgesamt entfallen kann.

Zu Artikel 5

EU In R

[EU In]

{EU R}

24. Der Richtlinienvorschlag sieht in Artikel 5 vor, dass "soweit wie möglich" zwischen den personenbezogenen Daten fünf verschiedener Kategorien von Personen zu unterscheiden ist. Eine solche [weitgehende] Differenzierung ist aus Sicht des Bundesrates weder der Sache nach geboten noch wird sie praktischen Erfordernissen gerecht. Sie erscheint auch deshalb zweifelhaft, weil andere Bestimmungen des Richtlinienvorschlags nicht an diese Klassifizierung anknüpfen und somit {besondere} Auswirkungen nicht erkennbar sind.

EU R

25. Für das Gebot, dass das mitgliedstaatliche Recht den jeweiligen Umständen Rechnung trägt, bedarf es einer solchen Kategorienbildung nicht. Der Hinweis, dass ähnliche Bestimmungen bereits im Europol- und Eurojust-Beschluss enthalten sind, kann die mangelnde Praktikabilität nicht in Frage stellen. Die Polizei- und Justizbehörden haben es allein in Deutschland jährlich mit einer

siebenstelligen Zahl von Ermittlungsverfahren zu tun; dies übertrifft jedenfalls die Fallbelastung von Eurojust um ein Vielfaches.

Zu Artikel 6

EU In R

26. Nach Artikel 6 des Richtlinienvorschlags soll außerdem "soweit wie möglich" nach sachlicher Richtigkeit und Zuverlässigkeit der Daten sowie danach differenziert werden, ob die Daten auf Fakten oder auf persönlichen Einschätzungen beruhen.

EU R

27. Der Bundesrat weist darauf hin, dass eine solche Bewertung und Unterscheidung zu einem unzumutbaren Verfahrensaufwand für die Polizei- und Justizbehörden führen würde, ohne dass diese Differenzierung innerhalb der Verfahrensakten eine rechtliche Bedeutung hätte. Auch der Richtlinienvorschlag sieht keine Rechtsfolgen für die Einordnung in diese Kategorien vor. Zudem wird eine solche Unterscheidung bei der ersten Erfassung der Daten vielfach noch nicht möglich sein. Das Ermittlungsverfahren ist vielmehr darauf angelegt, die erfassten Daten ständig auf ihre sachliche Richtigkeit und Zuverlässigkeit zu überprüfen und abschließend zu einer sicheren Unterscheidung zwischen diesen Kategorien zu gelangen. Ein Erfordernis für die Regelung in Artikel 6 des Richtlinienvorschlags ist daher nicht ersichtlich.

EU In

28. Da im Weiteren keine besonderen Auswirkungen an die jeweiligen Klassifizierungen geknüpft werden, erscheint dieser Passus entbehrlich.

Zu Artikel 7

EU In R

29. Artikel 7 des Richtlinienvorschlags erlaubt die Datenverarbeitung - einschließlich der Datenübermittlung - nur aufgrund bestimmter Zulässigkeitsgründe. Diese Gründe sind jedoch zu eng gefasst, um den legitimen Interessen Privater und der Öffentlichkeit, die eine Datenübermittlung erforderlich machen können, gerecht zu werden.

EU R

30. Die Polizei- und Justizbehörden müssen in zahlreichen Fällen Informationen, die sie im Zuge ihrer Ermittlungen erhalten, an andere Behörden weitergeben, damit diese von relevanten Umständen erfahren und selbst notwendige Maßnahmen ergreifen können. Dies gilt beispielsweise im Kinder- und Jugend-

schutz oder bei der Gewerbeaufsicht. Diese Übermittlung dient nicht der Erfüllung einer Aufgabe der übermittelnden Behörde, so dass Artikel 7 Buchstabe a des Richtlinienvorschlags nicht erfüllt sein dürfte, der nur von den gesetzlichen Aufgaben der "zuständigen" Behörde spricht. Die Gründe für solche Zuverlässigkeitsprüfungen erreichen aber regelmäßig auch noch nicht das Stadium einer unmittelbaren Gefahr für die öffentliche Sicherheit, so dass auch der Zulässigkeitsgrund des Artikels 7 Buchstabe d nicht eröffnet wäre. Das öffentliche Interesse an dieser Datenübermittlung gebietet es jedoch, eine Datenverarbeitung nach Artikel 7 des Richtlinienvorschlags auch dann zuzulassen, wenn das mitgliedstaatliche Recht dies in der konkreten Situation gestattet und die Datenübermittlung erforderlich ist, damit die empfangende Behörde ihre Aufgaben erfüllen kann.

EU In R [EU R]

31. [Zudem setzt Artikel 7 des Richtlinienvorschlags einer Datenübermittlung an Private zu enge Grenzen], da sie nur auf Artikel 7 Buchstabe c gestützt werden könnte, der jedoch die Notwendigkeit der Datenverarbeitung zur Wahrung lebenswichtiger Interessen einer anderen Person voraussetzt. Auch unterhalb dieser Schwelle können Private jedoch ein berechtigtes Interesse an einer Datenübermittlung haben, z.B. um eigene Rechtsansprüche durchzusetzen. Der Richtlinienvorschlag sollte daher eine Datenübermittlung an Private unter Abwägung der berechtigten Interessen des Privaten und des schutzwürdigen Interesses des Betroffenen an einer Versagung der Übermittlung zulassen.

EU In

32. Auch Artikel 7 Buchstabe d erscheint im Hinblick auf die polizeilich erforderliche Verarbeitung personenbezogener Daten außerhalb eines konkreten Strafverfahrens als zu eng gefasst.

EU R

33. Auch die Datenübermittlung zu Forschungszwecken würde durch den Richtlinienvorschlag in seiner derzeitigen Fassung ausgeschlossen. Das öffentliche Interesse an wissenschaftlicher Forschung gebietet jedoch die rechtliche Möglichkeit der Datenübermittlung in den Fällen, in denen dieses Interesse das schutzwürdige Interesse des Betroffenen an einem Ausschluss der Übermittlung überwiegt und eine Verarbeitung nichtanonymisierter Daten erforderlich ist.

Zu Artikel 8

EU In (bei Annahme entfällt Ziffer 35)

34. Artikel 8 des Richtlinienvorschlags regelt ein grundsätzliches Verbot der Verarbeitung besonderer Kategorien personenbezogener Daten. Eine Ausnahme gilt vor allem, wenn die Verarbeitung durch eine Vorschrift gestattet ist, die - in ihrem Inhalt unklare - "geeignete Garantien" vorsieht. Die Vorschrift ist nach Auffassung des Bundesrates jedenfalls in der gewählten Fassung abzulehnen. Im Bereich der Strafverfolgung und der straftatbezogenen Gefahrenabwehr ist eine entsprechende Sonderbehandlung solcher Daten bereits deswegen nicht sachgerecht, weil Polizei- und Ermittlungsbehörden oftmals darauf angewiesen sind, auch solche Umstände in Erfahrung zu bringen und zu speichern, um die Ermittlungen erfolgreich führen zu können (z.B. ethnische Herkunft bei der Fahndung nach einer Person) oder um sich selbst oder andere schützen zu können (z. B. Hinweise auf Infektionsgefahr; Gefahrenpotenzial aufgrund psychischer Prädispositionen). Zumindest ist die Vorschrift dahingehend abzuändern, dass die Daten der genannten Art nur verarbeitet werden dürfen, wenn dies auch unter Berücksichtigung von deren besonderer Sensibilität zur Erfüllung der Aufgaben der jeweiligen Stellen notwendig ist.

R

35. Artikel 8 des Richtlinienvorschlags enthält ein grundsätzliches Verbot der Verarbeitung von Daten besonderer Kategorien (z. B. genetische Daten). Die Polizei- und Justizbehörden müssen die Daten der genannten Kategorien jedoch vielfach verwenden, um die Ermittlungen zu führen (z. B. ethnische Herkunft bei der Fahndung nach dem Täter, genetische Daten zum Nachweis der Täterschaft). Auch um sich selbst oder andere zu schützen, sind die Behörden in vielen Fällen darauf angewiesen, beispielsweise Daten über ansteckende Krankheiten oder psychische Störungen eines Beschuldigten zu speichern und weiterzuleiten. Artikel 8 Absatz 2 Buchstabe a erlaubt zwar, im mitgliedstaatlichen Recht Ausnahmeregelungen zu schaffen, die "geeignete Garantien" enthalten müssen. Solche Ausnahmeregelungen wären aber in erheblichem Umfang erforderlich, um die Vielfalt der denkbaren Fälle zu erfassen und im Einzelnen zu regeln. Daher wäre es sachgerechter, statt des grundsätzlichen Verbots mit der Möglichkeit von Ausnahmeregelungen in der Richtlinie die Verarbeitung von Daten der genannten Art zuzulassen, wenn dies auch unter Berücksichtigung der besonderen Sensibilität der Daten zur Erfüllung der Aufgaben der jeweiligen Stellen notwendig ist.

Zu Artikel 8 und 9

EU In

36. Der in Artikel 9 des Richtlinienvorschlags niedergelegte absolute Nutzungsausschluss von Daten der Kategorien des Artikels 8 des Richtlinienvorschlags erscheint mit Blick auf spezielle polizeiliche Analysedateien wie zum Beispiel von Sexualstraftaten zu eng und schränkt die Ermittlungsarbeit der Polizei nicht nur bei der Aufklärung von Sexualstraftaten unangemessen ein. Die Einschränkung ist allgemeinen Datenschutzgesetzen entnommen, die meistens eine Bereichsausnahme für die Strafverfolgung bzw. die öffentliche Sicherheit und Ordnung enthalten. Innerhalb eines speziellen Rechtsakts für den Strafverfolgungsbereich erscheint dieser Ausnahmetatbestand systemwidrig; auch die Strafprozessordnung enthält keine entsprechende einschränkende Regelung. Die Übernahme der vergleichbaren Regelung in Artikel 9 der vorgeschlagenen Datenschutz-Grundverordnung verkennt insoweit die Besonderheiten des Raumes der Sicherheit, der Freiheit und des Rechts nach Titel V des AEUV.

Zu Artikel 11 bis 14

EU R

37. Der Richtlinienvorschlag sieht in Artikel 11 bis 14 umfassende Rechte der betroffenen Person auf Information und Auskunft über die Verarbeitung ihrer personenbezogenen Daten vor. Die strafverfahrensrechtlichen Vorschriften der Mitgliedstaaten enthalten jedoch bereits eigene, differenzierte Regelungen dazu, unter welchen Umständen den Verfahrensbeteiligten Akteneinsicht zu gewähren oder Auskunft zu erteilen und damit auch Kenntnis von der Verarbeitung ihrer personenbezogenen Daten zu verschaffen ist. Ein daneben bestehendes Recht auf frühzeitige Information aller betroffenen Personen über die Erfassung personenbezogener Daten, wie es Artikel 11 des Richtlinienvorschlags vorsieht, wird dagegen einen erheblichen Verwaltungsaufwand auslösen, ohne dass eine solche Unterrichtung erforderlich wäre: Die Beschuldigten oder Zeugen wissen entweder aufgrund ihres Kontakts mit der Ermittlungsbehörde, dass ihre Daten erfasst wurden, oder dieser Umstand wird den Beschuldigten oder ihren Kontaktpersonen berechtigterweise nicht offenbart, um den Ermittlungszweck nicht zu gefährden.

EU In

38. In Artikel 11 des Richtlinienvorschlags ist geregelt, dass die datenerhebende Stelle den Betroffenen - sofort oder jedenfalls zeitnah nach Erhebung - in zumindest sieben Punkten zu informieren hat. Derartig ausufernde Informationspflichten, die im nationalen Recht keine Grundlage finden, sind durch rechtsstaatliche Grundsätze, insbesondere die berührten Grundfreiheiten und Grundrechte, nicht geboten und führen zu einer sachlich nicht mehr gerechtfertigen "Bürokratisierung" der Arbeit der Polizei- und Justizbehörden.

EU R

39. Auch das weitreichende Auskunftsrecht in Artikel 12 des Richtlinienvorschlags ist insbesondere unter Berücksichtigung der Ermittlungszwecke im Strafverfahren nicht erforderlich. Dieses Auskunftsrecht gerät in Konflikt mit bestehenden Rechten auf Akteneinsicht nach innerstaatlichem Recht. § 147 Absatz 7 Satz 1 StPO räumt dem sich selbst verteidigenden Beschuldigten lediglich einen Anspruch auf Überlassung von Auskünften und Abschriften aus den Akten ein, wenn er sich ansonsten nicht angemessen verteidigen könnte. Weitere Voraussetzungen sind, dass der Untersuchungszweck - auch in einem anderen Strafverfahren - nicht gefährdet werden darf und keine schutzwürdigen Interessen Dritter entgegenstehen. Artikel 12 Absatz 1 des Richtlinienvorschlags geht darüber hinaus, indem ein grundsätzlich ohne weitere Voraussetzungen bestehendes Auskunftsrecht begründet wird.

EU In

40. Das in Artikel 12 des Richtlinienvorschlags geregelte Auskunftsrecht geht in seinem Umfang auch zumeist deutlich über die in den Polizeigesetzen der Länder bestehenden Regelungen sowie auch die bisherigen, durch die EU gesetzten Bestimmungen im Bereich der ehemaligen "Dritten Säule" (vgl. Artikel 17 des Rahmenbeschlusses Datenschutz, Artikel 31 Absatz 1 des Ratsbeschlusses Prüm) hinaus. Eine solche einseitig die Interessen des Betroffenen berücksichtigende Regelung bedeutete einen erheblich erhöhten administrativen Aufwand und ist in diesem Ausmaß rechtsstaatlich nicht gefordert. Zudem bestehen Bedenken gegen die in Artikel 12 Absatz 2 vorgeschlagene Regelung, wonach die betroffene Person das Recht hat, von dem für die Verarbeitung Verantwortlichen eine Kopie der verarbeiteten personenbezogenen Daten zu verlangen. Insoweit besteht die Gefahr, dass die betroffene Person Daten erlangt, die nicht vom Auskunftsrecht umfasst sind oder an deren Zurück-

haltung ein berechtigtes Interesse besteht. Darüber hinaus gebieten rechtsstaatliche Grundsätze die Erteilung einer Auskunft durch Überlassung einer Kopie der verarbeiteten personenbezogenen Daten nicht.

EU R 41. Die Mitgliedstaaten können zwar nach Artikel 13 Absatz 1 des Richtlinienvorschlags durch Rechtsvorschrift das Auskunftsrecht einschränken, u. a. um zu gewährleisten, dass behördliche Ermittlungen nicht behindert werden, oder um die Rechte anderer zu schützen. Eine widerspruchsfreie Regelung, welche die Besonderheiten des Strafverfahrensrechts in den Mitgliedstaaten berücksichtigt, sollte jedoch das Auskunftsrecht von vornherein für die Fälle ausschließen, in denen die Akteneinsicht nach Maßgabe der mitgliedstaatlichen Bestimmung verweigert werden könnte.

Soweit Artikel 13 Absatz 1 des Richtlinienvorschlags eine Einschränkung des Auskunftsrechts zulässt, sieht Artikel 13 Absatz 3 zudem die schriftliche Unterrichtung des Betroffenen über die Auskunftsverweigerung vor, die ausnahmsweise auch ohne Angabe von Gründen erfolgen darf. Der Bundesrat gibt jedoch zu bedenken, dass allein die Mitteilung, die Behörde verweigere die Auskunft über die Verarbeitung der personenbezogenen Daten der betroffenen Person, bereits die Zwecke des Ermittlungsverfahrens gefährden könnte. Ein Beschuldigter kann daraus den Rückschluss ziehen, dass die Ermittlungsbehörden Erkenntnisse über ihn sammeln, und sich auf weitere Ermittlungsmaßnahmen vorbereiten. Daher sollte die Richtlinie auch eine Regelung wie in § 491 Absatz 1 Satz 6 StPO zulassen, nach der die Behörden bei Verweigerung der Auskunftserteilung dem Betroffenen gegenüber offen lassen, ob seine Daten überhaupt verarbeitet wurden oder lediglich die Auskunft verweigert wird.

EU R 42. Artikel 14 Absatz 1 des Richtlinienvorschlags sieht vor, dass die betroffenen Personen jederzeit eine Überprüfung des Handelns der datenverarbeitenden Stellen, insbesondere einer Verweigerung der Auskunft, durch die Aufsichtsbehörde verlangen können. Eine datenschutzrechtliche Überprüfung während eines noch laufenden Ermittlungsverfahrens könnte jedoch entgegen der berechtigten Interessen des Beschuldigten (insbesondere in Haftsachen) oder des mutmaßlichen Opfers das Verfahren erheblich verzögern. Daher wäre es sachgerecht, in Artikel 14 die Überprüfung durch die Aufsichtsbehörde bis zum Abschluss des Strafverfahrens auszuschließen.

Zu Artikel 17

EU R

43. Die in Artikel 17 vorgesehene Möglichkeit, das einzelstaatliche Strafprozessrecht zur Anwendung kommen zu lassen, ist im Grundsatz zu begrüßen. Allerdings überzeugt die Beschränkung auf personenbezogene Daten "in einem Gerichtsbeschluss oder einem Gerichtsdokument" nicht. Diese Formulierung erfasst möglicherweise nicht personenbezogene Daten, die aufgrund eines gerichtlichen Beschlusses erhoben werden, und ist daher zu präzisieren.

Zudem empfiehlt es sich, die Regelung auf personenbezogene Daten, die aufgrund einer Entscheidung der Staatsanwaltschaft erhoben werden, die von den Strafgerichten überprüft werden kann, auszuweiten. Nur so kann sichergestellt werden, dass für die Datenerhebung und -verarbeitung als wesentliche Aufgabe des strafrechtlichen Ermittlungsverfahrens eine einheitliche gerichtliche Überprüfung durch die Strafgerichte sichergestellt ist.

Zu Artikel 24

EU R

44. Die in Artikel 24 Absatz 1 des Richtlinienvorschlags enthaltene Protokollierungs- und Dokumentationspflicht erscheint als zu weitgehend und führt jedenfalls bei nicht automatisierter Datenverarbeitung zu einem unverhältnismäßig hohen Verwaltungsaufwand, der durch einen geringen bis nicht ersichtlichen Mehrwert, der sich aus dieser Dokumentationspflicht ergibt, nicht gerechtfertigt ist.

Im nationalen Recht ist für automatisierte Verfahren durch die Vorschrift des § 10 Absatz 2 BDSG festgelegt, dass die beteiligten Stellen zu gewährleisten haben, dass die Zulässigkeit des Abrufverfahrens kontrolliert werden kann. Hierzu haben sie Anlass und Zweck des Abrufverfahrens, Dritte, an die übermittelt wird, Art der zu übermittelnden Daten und nach § 9 BDSG erforderliche technische und organisatorische Maßnahmen schriftlich festzulegen. Im öffentlichen Bereich können die erforderlichen Festlegungen auch durch die Fachaufsichtsbehörden getroffen werden.

Für die nicht automatisierte Datenverarbeitung und -übermittlung ist eine über die eigentliche Verarbeitungs- und Übermittlungstätigkeit, welche aufgrund entsprechender Verfügungen oder Ähnlichem veranlasst wird, hinausgehende Dokumentationspflicht ein zusätzlicher Aufwand, der deshalb nicht sinnvoll ist, weil weitergehende Informationen, die der Überprüfung der Rechtmäßigkeit der

Datenverarbeitung dienlich sein könnten, in entsprechenden Dokumentationen nicht enthalten sein werden.

Mit dem BDSG und den darin enthaltenen weitreichenden Möglichkeiten (Gleiches gilt für die Landesdatenschutzgesetze, sofern deren Anwendungsbereich eröffnet ist), die Beachtung der Vorschriften einerseits überprüfen und andererseits Verstöße ahnden zu können, steht bereits ein umfassendes Kontrollinstrumentarium zur Verfügung, das als ausreichend erachtet wird.

Zu Artikel 26 bis 28

EU R

45. Nach Artikel 26 des Richtlinienvorschlags sind die Aufsichtsbehörden im Wege einer Vorabkontrolle zu Rate zu ziehen, wenn personenbezogene Daten der besonderen Kategorien im Sinne von Artikel 8 in neu anzulegenden Dateien verarbeitet werden sollen oder sonst spezifische Risiken für die Grundrechte und Grundfreiheiten bestehen. Da nicht ausgeschlossen werden kann, dass eilbedürftige Ermittlungsmaßnahmen wie beispielsweise Formen der Rasterfahndung von dieser Bestimmung erfasst werden, sollte anstelle der Vorabkontrolle zumindest bei Gefahr im Verzug eine nachträgliche Unterrichtung der Aufsichtsbehörde genügen.

EU In

46. Die Delegationsregelung für den Erlass von Durchführungsbestimmungen in Artikel 27 Absatz 3 des Richtlinienvorschlags enthält unbestimmte Rechtsbegriffe ("erforderlichenfalls", "situationsabhängige Konkretisierung"), die das Ausmaß der auf die Kommission zu übertragenden Rechtsetzungsgewalt kaum bestimmbar machen und daher abzulehnen sind.

EU In

47. Die in Artikel 28 des Richtlinienvorschlags geregelte Meldung einer Verletzung des Schutzes personenbezogener Daten an die Aufsichtsbehörde erscheint insbesondere mit Blick auf die Abkopplung von berechtigten Schutzinteressen der betroffenen Person nicht sachgerecht. Darüber hinaus ist die (viel zu) weitgehende Delegation der Rechtssetzungsbefugnis an die Kommission in Artikel 28 Absatz 5 des Richtlinienvorschlags abzulehnen.

Zu Artikel 37

EU In

48. Der Bundesrat ist der Auffassung, dass die Verpflichtung zur Einhaltung von Verfügungsbeschränkungen dem Empfänger der Daten aufzuerlegen ist. Die Regelung des Artikels 37 des Richtlinienvorschlags ist weder effektiv noch verlässlich und selbst bei außerordentlich hohem Verwaltungs- und damit Zeit- und Kostenaufwand praktisch kaum umsetzbar.

Zu Artikel 44

EU R

49. Der Bundesrat erachtet es für erforderlich, die Reichweite der Kontrollbefugnisse der Aufsichtsbehörden im Hinblick auf gerichtliche Tätigkeiten in Artikel 44 Absatz 2 des Richtlinienvorschlags zu präzisieren. Gemäß Artikel 44 Absatz 2 soll die Aufsichtsbehörde nicht für die Überwachung der von Gerichten im Rahmen ihrer gerichtlichen Tätigkeit vorgenommenen Verarbeitungen zuständig sein. Ausweislich des Erwägungsgrunds 55 soll die Regelung die Unabhängigkeit der Richter bei der Ausübung ihrer richterlichen Tätigkeit garantieren. Diesem Zweck wird nach dem Wortlaut des Artikels 44 Absatz 2 jedoch nicht umfassend Rechnung getragen. Jedenfalls erscheint es nach dem Richtlinienvorschlag möglich, dass die Datenschutzbeauftragten insoweit im richterlichen Bereich Kontrollkompetenzen beanspruchen, als die richterliche Zuständigkeit national ausschließlich durch einfaches Recht eröffnet ist, wie etwa in Teilbereichen ermittlungsrichterlicher Funktion und bei den Aufgaben des Vollstreckungsleiters. Mit dem deutschen Verfassungsverständnis wäre es unvereinbar, Aufsichtsbehörden Kontrollkompetenzen im richterlichen Bereich zu eröffnen, unabhängig davon, ob Datenverarbeitungen richterlich angeordnet, bestätigt oder für zulässig erklärt wurden. Entsprechendes gilt auch für Maßnahmen informeller Art, wie etwa Empfehlungen oder fallbezogene Vorhaltungen sowohl in laufenden Verfahren als auch nach deren Abschluss.

Es ist daher geboten, dass in Übereinstimmung mit dem das Grundgesetz prägenden Gewaltenteilungsprinzip Artikel 44 Absatz 2 des Richtlinienvorschlags dahingehend ergänzt wird, dass die Aufsichtsbehörde nicht zuständig ist, wenn Datenverarbeitungen gerichtlich angeordnet, bestätigt oder für zulässig erklärt wurden.

Zu Artikel 46 und 53

EU R

50. Artikel 46 des Richtlinienvorschlags sieht vor, dass die Mitgliedstaaten die Aufsichtsbehörden mit weitreichenden Kompetenzen ausstatten. Zu diesen sollen nicht nur Untersuchungsbefugnisse gehören, sondern auch wirksame Einwirkungsbefugnisse. Diese sollen insbesondere eine Befugnis der Aufsichtsbehörden umfassen, die Beschränkung, Löschung oder Vernichtung von Daten anzuordnen. Derart weitreichender Einwirkungsbefugnisse bedarf es nicht, weil die Strafverfolgungsbehörden an Gesetz und Recht gebunden und gerichtlicher Kontrolle unterworfen sind. Sie wären zudem geeignet, die Arbeit der Strafverfolgungsbehörden erheblich zu beeinträchtigen.

Die Befugnisse der in Kapitel VI des Richtlinienvorschlags vorgesehenen Aufsichtsbehörde sollten auf allgemeine Überprüfungen der Datenverarbeitungssysteme der Staatsanwaltschaften beschränkt und Einzelfallprüfungen ausgeschlossen werden.

Datenschutzverletzungen im Einzelfall können durch gerichtliche Überprüfungen nach Maßgabe der Strafprozessordnung und im Wege der Dienstaufsicht (§ 147 GVG) angemessen aufgegriffen und entschieden werden. Überprüfungen in Einzelfällen durch Aufsichtsbehörden im Sinne des Richtlinienvorschlags stellen dagegen einen systemfremden Eingriff in die Strafverfolgung dar. Es ist eine Grundaufgabe für Staatsanwaltschaften und Gerichte, bei Eingriffen jeglicher Art und Tiefe in die Grundrechte von Betroffenen sachgerechte Abwägungen, die gegebenenfalls durch die Instanzen angefochten werden können, vorzunehmen und diese zu begründen. Eingriffe in diese Entscheidungsprozesse der dem Legalitätsprinzip verpflichteten, an die Strafprozessordnung und die Grundrechte gebundenen und unter der Kontrolle der Gerichte stehenden Staatsanwaltschaften durch unabhängige Aufsichtsbehörden, die keiner Kontrolle unterstehen, stellen einem nicht erkennbaren Gewinn an Datenschutz einen erheblichen Verlust an Rechtssicherheit gegenüber. Eine unabhängige Aufsichtsbehörde zur Durchsetzung eines einzelnen Grundrechts im Ermittlungsverfahren ist ein Fremdkörper. Der Bundesrat spricht sich daher dafür aus, dass die einschränkende Regelung in Artikel 44 Absatz 2 des Richtlinienvorschlags auf die Ermittlungstätigkeit von Staatsanwaltschaften erweitert wird.

EU R 51. Der Bundesrat steht auch dem in Artikel 53 Absatz 2 und Artikel 46 Buchstabe c des Richtlinienvorschlags vorgesehenen Klagerecht der Aufsichtsbehörden ablehnend gegenüber. Die sonstigen Untersuchungs- und Einwirkungsbefugnisse der Aufsichtsbehörde nach Artikel 46 des Richtlinienvorschlags sind zur Durchsetzung der nach Maßgabe dieser Richtlinie erlassenen Rechtsvorschriften - auch unter Berücksichtigung der Ausführungen zu Artikel 26 - ausreichend. Die Datenschutzbeauftragten haben in Deutschland darüber hinaus erheblichen Einfluss durch ihre Tätigkeitsberichte, in denen sie die Ergebnisse ihrer Kontrolltätigkeit festhalten und Verbesserungen des Datenschutzes vorschlagen. Die Anrufung eines Gerichts ist daher nicht erforderlich.

EU In 52. Der Bundesrat steht der Einführung eines Klagerechts für Datenschutzbehörden und Verbände kritisch gegenüber.

EU R 53. Artikel 53 Absatz 1 des Richtlinienvorschlags soll es den Datenschutzverbänden erlauben, im Namen der betroffenen Personen Klage gegen die datenverarbeitende Behörde oder die Aufsichtsbehörde zu erheben. Es ist jedoch nicht ersichtlich, dass eine solche Befugnis erforderlich wäre, um Individualrechte ausreichend zu schützen. Das Verwaltungsprozessrecht sieht die Möglichkeit, sich vor Gericht durch Verbände vertreten zu lassen, nur ausnahmsweise in besonderen Sachgebieten vor (§ 67 Absatz 2 Nummer 6 VwGO). Für das Datenschutzrecht ist allerdings nicht evident, dass die von einer Rechtsverletzung Betroffenen bei einer Klage der Unterstützung durch einen Datenschutzverband bedürften, und nicht stattdessen einen der gesetzlich vorgesehenen Bevollmächtigten, insbesondere einen Rechtsanwalt, beauftragen könnten.

EU In 54. Den für die Kontrolle der Einhaltung der Datenschutzvorschriften zuständigen Behörden sind hoheitliche Befugnisse gesetzlich zugewiesen, die es ihnen ermöglichen, bei Verstößen unmittelbar gegenüber Dritten tätig zu werden (§ 38 Absatz 5 BDSG) und Anordnungen erforderlichenfalls durch Maßnahmen des Verwaltungszwangs durchzusetzen. Die Anrufung eines Gerichts ist daher überflüssig. Die Einführung einer Verbandsklage kommt aus Sicht des

Bundesrates - wenn überhaupt - allenfalls insoweit in engen Grenzen in Betracht, als die Durchsetzung zivilrechtlicher Ansprüche gegen die Verursacher datenschutzrechtlicher Rechtsverletzungen effektiver gestaltet werden soll. Die Einführung einer Verbandsklage im öffentlich-rechtlichen Bereich ist aus grundsätzlichen systematischen Erwägungen abzulehnen, da ein solches Klagerecht dem elementaren Grundsatz des nationalen Verwaltungsprozessrechts widerspricht (§ 42 Absatz 2 VwGO), wonach regelmäßig nur eine Verletzung eigener subjektiver Rechte geltend gemacht werden kann. Für eine solche Regelung besteht auch kein Bedürfnis, da sich jeder Betroffene und auch jeder Verband bei Verdacht eines Verstoßes gegen Datenschutzvorschriften an den zuständigen Datenschutzbeauftragten wenden kann

Zu Artikel 57 und 60

EU In

55. Angesichts des sensiblen Regelungsgegenstandes sollte in Artikel 57 Absatz 2 und 3 des Richtlinienvorschlags jeweils eingefügt werden, dass in Anwendung des Artikels 5 Absatz 4 Buchstabe b der Verordnung (EU) 182/2011 ohne eine Stellungnahme des Ausschusses der vorgesehene Durchführungsrechtsakt von der Kommission nicht erlassen werden darf.

EU In

56. Der Zwang zur Abänderung bestehender bi- oder multilateraler Polizeiabkommen in Artikel 60 des Richtlinienvorschlags berührt die Regelungen der Wiener Vertragsrechtskonvention sowie die außenpolitische Kompetenz der Mitgliedstaaten. Artikel 351 AEUV sieht vor, dass die Mitgliedstaaten alle geeigneten Mittel anwenden, um eventuelle Unvereinbarkeiten geschlossener Übereinkünfte mit den EU-Verträgen zu beheben. Die rigide Formulierung des Artikels 60 des Richtlinienvorschlags wird insofern kritisch betrachtet. Eine Ausgestaltung als "sunset-clause" wäre zu prüfen.

Allgemeines

EU R

57. Der Bundesrat wiederholt seine bereits in seinem Beschluss vom 25. November 2005, BR-Drucksache 764/05 (Beschluss), geäußerte Forderung, dass bei der Ausgestaltung des Richtlinienvorschlags im Einzelnen insgesamt keine zusätzlichen bürokratischen Einrichtungen und Anforderungen geschaffen werden und unnötiger Personal- und Kostenaufwand in den Mitgliedstaaten verhindert wird. Der Bundesrat bittet die Bundesregierung, darauf hinzuwirken,

dass die sich für die Mitgliedstaaten ergebenden Mehrbelastungen auf das unbedingt notwendige Maß beschränkt werden.

Direktzuleitung der Stellungnahme an die Kommission

EU 58. Der Bundesrat übermittelt diese Stellungnahme direkt an die Kommission.