

**19.03.12****Empfehlungen  
der Ausschüsse**EU - AV - In - R - Wizu **Punkt ...** der 895. Sitzung des Bundesrates am 30. März 2012

---

Vorschlag für eine Verordnung des Europäischen Parlaments und des Rates zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr (Datenschutz-Grundverordnung)

COM(2012) 11 final; Ratsdok. 5853/12

**A**

Der federführende Ausschuss für Fragen der Europäischen Union,  
der Ausschuss für Innere Angelegenheiten und  
der Rechtsausschuss

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

1. Der Bundesrat ist der Auffassung, dass der Vorschlag mit dem Subsidiaritätsprinzip nicht im Einklang steht. Denn nach Artikel 5 Absatz 3 EUV darf die EU in den Bereichen, die nicht in ihre ausschließliche Zuständigkeit fallen, nur tätig werden, sofern und soweit die Ziele der in Betracht gezogenen Maßnahmen von den Mitgliedstaaten weder auf zentraler noch auf regionaler oder lokaler Ebene ausreichend verwirklicht werden können, sondern vielmehr wegen ihres Umfangs oder ihrer Wirkungen auf Unionsebene besser zu verwirklichen sind.

Der Bundesrat bedauert, dass die Kommission die schon in seiner Stellungnahme vom 11. Februar 2011 zur Mitteilung der Kommission über ihr Gesamtkonzept für den Datenschutz in der EU (BR-Drucksache 707/10 (Beschluss)) aufgezeigten Vorbehalte zur Abgrenzung der Rechtsetzungskompetenzen und

zur Wahrung des Subsidiaritätsprinzips nicht berücksichtigt hat. Die jetzt vorliegenden Vorschläge für eine umfassende Modernisierung des Schutzes personenbezogener Daten durch eine Richtlinie zur Regelung des Datenschutzrechts für den Bereich von Polizei und Justiz (vgl. BR-Drucksache 51/12) und eine Überleitung der bestehenden Datenschutzrichtlinie in eine Datenschutz-Grundverordnung bei gleichzeitiger Anpassung datenschutzrechtlicher Regelungen der Richtlinie über die elektronische Kommunikation (RL 2002/58/EG) bestätigen diese Vorbehalte. Der Bundesrat ist daher der Ansicht, dass nach wie vor eine Gesamtkonzeption erforderlich ist, die den Prinzipien der Subsidiarität und Verhältnismäßigkeit besser gerecht wird, als das vorgeschlagene Regelungsmodell.

Die Anforderungen des Artikels 5 Absatz 3 EUV erfüllt die vorgeschlagene Datenschutz-Grundverordnung aus folgenden Gründen nicht:

2. Der Verordnungsvorschlag legt nicht ausreichend dar, dass eine verbindliche Vollregelung des Datenschutzes durch Verordnung im öffentlichen und im nichtöffentlichen Bereich auf europäischer Ebene erforderlich ist. Anders als die bestehende, schon auf eine Vollharmonisierung nationaler Datenschutzgewährleistungen zielende Richtlinie führt eine Verordnungsregelung mit umfassendem verbindlichen Geltungsanspruch zur nahezu vollständigen Verdrängung mitgliedstaatlicher Datenschutzregelungen. Gerade im öffentlichen Bereich, aber auch in weiten Teilen des nichtöffentlichen Datenschutzrechts bestehen in Deutschland wie auch in anderen Mitgliedstaaten differenziertere und damit mehr Vollzugstauglichkeit und Rechtssicherheit vermittelnde Datenschutzgewährleistungen als die durch hohes Abstraktionsniveau geprägten Einzelbestimmungen des Verordnungsvorschlags. Der Anwendungsvorrang der Datenschutz-Grundverordnung stellt den Fortbestand bisher auch unter Gesichtspunkten des Binnenmarktes unstrittiger Kernbereiche deutschen Datenschutzrechts in Frage. Beispielhaft gilt dies etwa für den Sozialdatenschutz oder die vom Wesentlichkeitsvorbehalt geforderten bundes- und landesgesetzlichen Regelungen der Videoüberwachung.
3. Soweit auch im Rahmen europäischer Verordnungsregelungen zumindest mitgliedstaatliche Konkretisierungsbefugnisse anerkannt sind, fehlen entsprechende ausdrückliche Ermächtigungen zu Gunsten der nationalen Gesetzgeber. Vielmehr belegen die in sehr großer Zahl vorgesehenen Ermächti-

gungen zum Erlass delegierter Rechtsakte die weit über die Kompetenzzuweisung des Artikels 16 Absatz 2 AEUV hinausgehende Zielsetzung zu einer umfassenden, ausschließlich durch den europäischen Gesetzgeber bestimmten verbindlichen Vollregelung des gesamten europäischen Datenschutzrechts. Ein unionsweit einheitliches Datenschutzniveau kann dagegen auch weiterhin durch eine Fortentwicklung der bislang geltenden Datenschutzrichtlinie erreicht werden. Auch diese zielt auf eine Vollharmonisierung des Datenschutzrechts ab, belässt den Mitgliedstaaten jedoch die Möglichkeit, auslegungsfähige Tatbestandsmerkmale, wie sie auch die vorgeschlagene Verordnung durchgehend nutzt, im Rahmen der mitgliedstaatlichen Gesetzgebung zu konkretisieren.

4. Die von der Kommission vorgeschlagene verbindliche Vollregelung des Datenschutzrechts im öffentlichen und nichtöffentlichen Bereich geht weit über das Ziel der Gewährleistung eines hohen Datenschutzniveaus in diesen Bereichen und gleicher Wettbewerbsbedingungen hinaus. Auf Grund ihres offen und unbestimmt gefassten sachlichen Anwendungsbereichs wird die vorgeschlagene Verordnung als unmittelbar geltende Regelung mit Ausnahme der in den Artikeln 80 ff. des Vorschlags erfassten Materien des Medien-, Gesundheits- und Beschäftigtendatenschutzes nahezu alle Bereiche des geltenden nationalen Datenschutzrechts verdrängen. Sie erfasst damit auch rein lokale Bereiche wie z. B. die Tätigkeit der örtlichen Gefahrenabwehrbehörden, da der Anwendungsbereich nur den "Bereich nationaler Sicherheit" ausnimmt, für Fragen der "öffentlichen Sicherheit" aber lediglich Abweichungsbefugnisse nach Maßgabe des Artikels 21 einräumt. Mit der Erstreckung der vorgeschlagenen Verordnung auf sämtliche Tätigkeiten im Geltungsbereich des Unionsrechts (Artikel 2 Absatz 2 Buchstabe a des Vorschlags) beansprucht die Kommission außerdem datenschutzrechtliche Regelungskompetenzen zu einer verbindlichen Regelung von Sachbereichen, wie z. B. dem Bildungssystem, in denen eine Kompetenz zur Harmonisierung von Rechts- und Verwaltungsvorschriften sogar ausdrücklich ausgeschlossen ist (z. B. Artikel 165 Absatz 4 AEUV). Gleiches gilt auch für den Bereich des nicht straftatenbezogenen Gefahrenabwehrrechts, dessen Regelungskompetenz weiterhin ausschließlich den Mitgliedstaaten zufällt (vgl. Artikel 72, 87, 276 AEUV).
5. Der Bundesrat ist ferner der Ansicht, dass die Verarbeitung personenbezogener Daten durch die öffentlichen Verwaltungen der Mitgliedstaaten grundsätzlich nicht in die Rechtsetzungskompetenz der EU fällt und daher zur Vermeidung

eines Subsidiaritätsverstoßes vom sachlichen Anwendungsbereich der Verordnung auszunehmen ist. Für diesen Bereich und für die Verarbeitung zur Wahrnehmung von Aufgaben, die im öffentlichen Interesse liegen, enthält zwar Artikel 6 Absatz 3 Satz 1 Buchstabe b in Verbindung mit Absatz 1 Buchstabe e des Verordnungsvorschlags die Befugnis zum Erlass mitgliedstaatlicher Regelungen. Deren Reichweite wird aber durch spezifische unionsrechtliche Anforderungen begrenzt (Artikel 6 Absatz 3 Satz 2 des Verordnungsvorschlags), so dass im Ergebnis keine eigenständigen Regelungsbefugnisse der Mitgliedstaaten im Bereich der Datenverarbeitung öffentlicher Verwaltungen verbleiben.

6. Ein weiterer Widerspruch zu den Prinzipien der Subsidiarität und Verhältnismäßigkeit ergibt sich insbesondere im Bereich der Datenverarbeitung öffentlicher Verwaltungen schließlich noch aus der in Artikel 1 Absatz 3 des Verordnungsvorschlags vorgesehenen Regelung, die zur Gewährleistung des freien Datenverkehrs auch jegliche über die Verordnung hinausgehende nationale Datenschutzgewährleistung untersagt: Gerade bei der Datenverarbeitung im Bereich der öffentlichen Verwaltungen wie z. B. im Sozialdatenschutzrecht mit seinen restriktiven Verfahrensregelungen (etwa in Gestalt des Gebots organisationsrechtlicher Trennungen der Datenverarbeitung) sind höhere nationale Datenschutzstandards denkbar, ohne dass dadurch Belange des Binnenmarkts beeinträchtigt werden.
7. Die vorgeschlagene Datenschutz-Grundverordnung ist ungeeignet, eine für nahezu alle Bereiche geltende umfassende Regelung des Datenschutzes zu gewährleisten und verletzt daher auch insoweit die Prinzipien der Subsidiarität und Verhältnismäßigkeit. Wegen ihres hohen Abstraktionsniveaus, das Anforderungen generalisiert und die differenzierten Schutzrechte des allgemeinen und fachrechtlichen Datenschutzes der Mitgliedstaaten nivelliert, verweist die vorgeschlagene Verordnung bei vielen für den Schutz des Persönlichkeitsrechts und der sonstigen Grundrechtsausübung der Bürgerinnen und Bürger wesentlichen Fragen auf delegierte Rechtsakte der Kommission, um weiterhin dem Ziel der Vollharmonisierung gerecht werden zu können. Jedenfalls bis zum Erlass detaillierterer Regelungen durch delegierte europäische Rechtsakte wird dadurch der praktische Vollzug des Datenschutzrechts mit vielfältigen Rechtsunsicherheiten belastet, da die geltenden innerstaatlichen Regelungen nach nur zweijähriger Übergangszeit nicht mehr anwendbar sein sollen. Das

von der Kommission betonte Ziel, durch den Erlass der vorgeschlagenen Verordnung die Rechtssicherheit für Wirtschaft und Staat bei der Verarbeitung personenbezogener Daten zu erhöhen, wird damit verfehlt. Demgegenüber würde die Aufnahme der vorgeschlagenen Verordnungs-Regelungen in die Fortführung der bestehenden Datenschutzrichtlinie für das nationale Datenschutzrecht lediglich Anpassungspflichten begründen, aber im Interesse von Rechtssicherheit und Vollzugstauglichkeit den Fortbestand nationaler Regelungen erlauben.

8. Der Verordnungsvorschlag widerspricht den Prinzipien der Subsidiarität und Verhältnismäßigkeit, da die Regelungen zu den Einwirkungsrechten der Kommission im Rahmen des sogenannten Kohärenzverfahrens (Artikel 57 ff., insbesondere Artikel 60 f. des Verordnungsvorschlags) nicht mit der durch Artikel 16 Absatz 2 Satz 2 AEUV gewährleisteten Unabhängigkeit der Datenschutzbehörden zu vereinbaren sind. Das Erfordernis der völligen Unabhängigkeit der Datenschutzkontrollstellen erfordert es nach der Rechtsprechung des Europäischen Gerichtshofs bereits, die bloße Gefahr einer politischen Einflussnahme auf die Entscheidungen der Kontrollstellen auszuschließen. Die in der vorgeschlagenen Verordnung eröffneten Befugnisse zur Aussetzung datenschutzaufsichtlicher Verfahren eröffnen aber unmittelbare Möglichkeiten der Einflussnahme, bei denen nicht auszuschließen ist, dass diese durch die umfassenden Exekutivaufgaben außerhalb des Datenschutzrechts beeinflusst werden, die der Kommission ungeachtet ihrer formalen Unabhängigkeit obliegen.
9. Durch die Entscheidung für eine Regelung europäischer Datenschutzstandards im Wege einer Rechtsverordnung schafft die Kommission Rechtsunsicherheiten über die im Bereich elektronischer Kommunikationsdienste nach der Richtlinie 2002/58/EG geltenden Datenschutzregelungen. Die nach dieser Richtlinie bestehenden mitgliedstaatlichen Umsetzungspflichten zur Regelung des Datenschutzes bei elektronischen Kommunikationsdiensten werden durch Artikel 88 Absatz 2 des Verordnungsvorschlags abgeändert, der die Verweisungen der Richtlinie über elektronische Kommunikationsdienste auf die Datenschutzrichtlinie als Verweisungen auf die vorgeschlagene Datenschutz-Grundverordnung modifizieren soll. Die Mitgliedstaaten werden damit vor die Aufgabe gestellt, neue spezifische nationale Datenschutzstandards für elektronische Kommunikationsdienste zu formulieren, während ihnen im Bereich des allge-

meinen Datenschutzrechts durch den Anwendungsvorrang der vorgeschlagenen Verordnung keine Rechtsetzungskompetenzen verbleiben. Der gerade in der Informationsgesellschaft zentrale Bereich des Datenschutzes bei elektronischen Kommunikationsdiensten wird daher durch die Entscheidung für den Erlass einer Datenschutz-Grundverordnung an Stelle der Fortentwicklung der Datenschutzrichtlinie mit erheblichen Rechtsunsicherheiten belastet, die durch keine anderweitigen Vorteile zur Verwirklichung der Schutzaufträge des Artikels 16 Absatz 1 AEUV ausgeglichen werden.

10. Die Entscheidung für eine Datenschutz-Grundverordnung bei gleichzeitiger Regelung des Datenschutzes im Bereich von Polizei und Justiz durch eine Richtlinie schafft Abgrenzungsschwierigkeiten, die weitere Belege für die Verletzung der Prinzipien von Subsidiarität und Verhältnismäßigkeit begründen. Der Bundesrat stellt fest, dass die bisherige Konzeption zur Neuordnung des EU-Datenschutzrechts dazu führen würde, dass Polizei und Ordnungsbehörden im Rahmen ihrer Aufgabenwahrnehmung hinsichtlich der Verarbeitung personenbezogener Daten unterschiedliche Rechtsvorschriften zu beachten haben. Ziel der Richtlinie für den Datenschutz bei Polizei und Justiz (siehe Artikel 1 Absatz 1 und die Begründung Ziffer 3.4.1, BR-Drucksache 51/12) ist es, Bestimmungen für die Verarbeitung personenbezogener Daten zum Zwecke der Verhütung, Aufdeckung, Untersuchung oder Verfolgung von Straftaten festzulegen. Die vorgeschlagene Datenschutz-Grundverordnung findet auf diesen Bereich keine Anwendung (Artikel 2 Absatz 2 Buchstabe e des Vorschlags). Die Polizeien der Länder sind aber sowohl für den Bereich der Verhütung von Straftaten als auch für den Bereich der allgemeinen Gefahrenabwehr zuständig, der vorbehaltlich begrenzter Ausnahmen nach Maßgabe des Artikels 21 des Vorschlags von den verbindlichen Anforderungen der vorgeschlagenen Datenschutz-Grundverordnung erfasst wird. Diese Zersplitterungen zeigen, dass ein besserer Schutz personenbezogener Daten im Rahmen der Rechtsetzungskompetenzen der EU durch eine Fortentwicklung der Datenschutzrichtlinie zu verwirklichen wäre, nicht aber durch drei Rechtsakte unterschiedlicher Bindungswirkung für die Mitgliedstaaten - die beabsichtigte Datenschutzgrundverordnung und die vorgeschlagene Richtlinie zum Datenschutz bei Polizei und Justiz sowie die bestehende Richtlinie 2002/58/EG.

**B**

Der Ausschuss für Fragen der Europäischen Union (EU),

der Ausschuss für Agrarpolitik und Verbraucherschutz (AV),

der Ausschuss für Innere Angelegenheiten (In),

der Rechtsausschuss (R) und

der Wirtschaftsausschuss (Wi)

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

Zur Vorlage allgemein

EU  
R

11. Der Bundesrat begrüßt die Zielsetzung des Verordnungsvorschlags, einen kohärenten und durchsetzbaren Rechtsrahmen im Bereich des Datenschutzes in der Union zu schaffen, um das in Artikel 8 der Grundrechtecharta und Artikel 16 Absatz 1 AEUV verankerte Recht auf Schutz personenbezogener Daten unionsweit einheitlich zu gewährleisten, Sicherheit und Klarheit für die Online-Wirtschaft zu schaffen und deren Kontrolle rechtlich und praktisch zu verbessern, um so das Vertrauen der Verbraucher in die Sicherheit des Datenverkehrs zu erhöhen.

EU  
In  
Wi

12. Der Bundesrat begrüßt daher die Initiative der Kommission, das europäische Datenschutzrecht angesichts grundlegender Herausforderungen durch Globalisierung und technologische Entwicklung zu modernisieren, um die Rechte des Einzelnen zu stärken, den Verwaltungsaufwand für die Unternehmen zu verringern und ein einheitlich hohes Schutzniveau in und außerhalb der EU zu gewährleisten.

EU  
AV

13. Der Bundesrat begrüßt für Datenverarbeitungen durch nichtöffentliche Stellen die Reform der aus dem Jahr 1995 stammenden EU-Datenschutzvorschriften und vor allem die damit verbundene Absicht der Kommission, insbesondere Online-Rechte des Einzelnen auf Wahrung der Privatsphäre und das Vertrauen in elektronische Medien zu stärken.

- EU  
R
14. Der Vorschlag für eine Datenschutz-Grundverordnung soll sowohl für den öffentlichen Bereich als auch den nichtöffentlichen Bereich gelten. Die tatsächlichen Gegebenheiten und Zielsetzungen beim Datenschutz im Verhältnis des Bürgers zu staatlichen Stellen einerseits und im Verhältnis des Einzelnen zu Unternehmen andererseits unterscheiden sich aber grundlegend. Es scheint daher sehr zweifelhaft, ob es möglich ist, mit ein- und demselben Rechtsetzungsvorschlag den unterschiedlichen Ausgangslagen hinreichend Rechnung zu tragen.
- EU  
R
15. Der Verordnungsvorschlag enthält neben einzelnen Öffnungsklauseln zugunsten der Mitgliedstaaten (vgl. Artikel 6 Absatz 3, Artikel 21, Artikel 80, Artikel 82, Artikel 84) in praktisch allen Regelungsbereichen Ermächtigungen der Kommission zum Erlass delegierter Rechtsakte (vgl. Artikel 86). Dem Gebot, die wesentlichen Fragen im Zusammenhang mit der Abwägung der berührten grundrechtlich geschützten Interessen selbst zu beantworten, wird der Verordnungsvorschlag damit nicht gerecht. Auch vor diesem Hintergrund sollte erwogen werden, ob - sofern überhaupt eine Neuregelung des Schutzes personenbezogener Daten in der EU für erforderlich gehalten wird - nicht eine Richtlinie eher als eine Verordnung geeignet wäre, die beabsichtigten Leitlinien vorzugeben.
- EU  
In
16. Der Bundesrat erinnert an seine Entschließung zum Entwurf eines Gesetzes zur Änderung des Bundesdatenschutzgesetzes vom 9. Juli 2010 (BR-Drucksache 259/10 (Beschluss)), in der die vordringlichen Handlungsfelder einer Modernisierung des Datenschutzrechts aufgezeigt werden, um den Schutz der informationellen Selbstbestimmung auch unter den Bedingungen der Informationsgesellschaft zu gewährleisten. Der Bundesrat unterstützt daher insbesondere die Zielsetzung, auch für Informationsdienstleistungen globaler Anbieter die Beachtung europäischer Datenschutzstandards durchzusetzen. Die zeitgleich von der Regierung der Vereinigten Staaten von Amerika vorgestellte Initiative für einen Rechtsrahmen für den Schutz der Privatsphäre in der globalen IT-Wirtschaft bietet die Chance, in zentralen Bereichen des internationalen Datenverkehrs Reformansätze zu gemeinsamen Schutzstandards zusammenzuführen. Der Bundesrat bittet die Bundesregierung, die bereits eingeleiteten völker-



rechtlichen Verhandlungen zwischen der EU und den Vereinigten Staaten von Amerika im Interesse der Rechtssicherheit für Betroffene und Unternehmen zu unterstützen und den Bundesrat über die Fortentwicklung der Verhandlungen zu unterrichten.

EU  
AV

17. Insbesondere begrüßt der Bundesrat die in dem Verordnungsvorschlag vorgesehenen Regelungen über die Information der betroffenen Personen, auch im Fall des Datenverlusts, sowie die Erhöhung der Strafen für Datenschutzverstöße. Zu begrüßen ist ferner, dass der Verordnungsvorschlag vorsieht, dass sich auch Unternehmen, die keinen Sitz in der EU haben, nach der Verordnung richten müssen, wenn sie sich mit Diensten oder Produkten an EU-Verbraucherinnen und EU-Verbraucher wenden oder die Datenverarbeitung der Beobachtung des Verhaltens der Verbraucherinnen und Verbraucher dient. Diese Unternehmen müssen einen Vertreter in der EU benennen, wenn sie mehr als 250 Mitarbeiter haben. In diesem Zusammenhang weist der Bundesrat aber darauf hin, dass für Ermittlungs- und Rechtsdurchsetzungsbefugnisse im EU-Ausland zwischenstaatliche Verträge geschaffen werden müssten, die bislang nicht bestehen. Er bittet deshalb die Bundesregierung, sich zum einen bei der Kommission dafür einzusetzen, dass derartige Verträge abgeschlossen werden, und zum anderen die genannten Beschränkungen für die Bürgerinnen und Bürger transparent zu machen, damit nicht unerfüllbare Erwartungen geweckt werden.

EU  
In

18. Ungeachtet der Beachtung der Prinzipien von Subsidiarität und Verhältnismäßigkeit bittet der Bundesrat, im weiteren Rechtsetzungsverfahren außerdem folgende Gesichtspunkte zu berücksichtigen:

Zu Artikel 2 - Begrenzung und Klarstellung des sachlichen Anwendungsbereichs

EU  
R

19. Der Bundesrat geht davon aus, dass das innerstaatliche Verfahrensrecht für die Tätigkeit der Gerichte nicht in den Geltungsbereich des Unionsrechts fällt, so dass die Verordnung nach Artikel 2 Absatz 2 Buchstabe a auf die Verarbeitung personenbezogener Daten durch die Gerichte im Rahmen der gerichtlichen Tätigkeit keine Anwendung findet.

- EU  
R
20. Der Bundesrat hält es aber - nicht zuletzt im Hinblick auf die Einführung elektronischer Gerichtsakten - für erforderlich, dies in Artikel 2 der Verordnung ausdrücklich klarzustellen.

#### Zur internationalen Rechtshilfe in gerichtlichen Verfahren

- EU  
R
21. Der Bundesrat bittet, im weiteren Rechtsetzungsverfahren zu prüfen, ob darauf hingewirkt werden soll, dass der im Zusammenhang mit der internationalen Rechtshilfe in gerichtlichen Verfahren notwendige, grenzüberschreitende Austausch von personenbezogenen Daten vom Anwendungsbereich der Verordnung ausgenommen wird.

Anders als das Strafverfahren sind andere gerichtliche Verfahren vom Anwendungsbereich der vorgeschlagenen Verordnung nicht ausdrücklich ausgenommen. Dies hat zur Folge, dass die vorgeschlagene Verordnung auch auf den im Rahmen der internationalen Rechtshilfe in gerichtlichen Verfahren mit Ausnahme des Strafverfahrens erfolgenden Datenverkehr angewandt werden könnte, obwohl der Rechtshilfeverkehr selbst in - nationalen und zwischenstaatlichen - Sondervorschriften geregelt ist. Dies könnte insbesondere mit Blick auf den Rechtshilfeverkehr mit Drittstaaten problematisch sein. So könnte etwa ein ansonsten erfolgversprechendes Rechtshilfeersuchen eines Mitgliedstaates an ein Drittland, bezüglich dessen die Kommission gemäß Artikel 41 Absatz 5 des Verordnungsvorschlags festgestellt hat, dass es keinen "angemessenen Schutz" bietet, allein an dem aus Artikel 41 Absatz 6 des Verordnungsvorschlags fließenden Datenübermittlungsverbot scheitern. Umgekehrt könnte die Versagung von - ansonsten möglicher - Rechtshilfe gegenüber einem solchen Drittland dazu führen, dass das Drittland dem Grundsatz der Gegenseitigkeit folgend künftig seinerseits den Mitgliedstaaten der Europäischen Union keine Rechtshilfe mehr leistet. Diese Folgen sind nach Auffassung des Bundesrates zu vermeiden, eine Abwägung im konkreten Fall wird doch häufig dazu führen, dass das - auch öffentliche - Interesse an der Führbarkeit des jeweiligen gerichtlichen Verfahrens und an einem funktionierenden Rechtshilfeverkehr mit dem betroffenen Drittland überhaupt das Interesse des Betroffenen am Unterbleiben der konkreten Datenübermittlung deutlich überwiegt. Ob die Vorschriften der Artikel 42 ff. des Verordnungsvorschlags diese Problematik

befriedigend zu lösen vermögen, erscheint jedenfalls fraglich.

Weitere Ergänzungen zum innerstaatlichen Verfahrensrecht der Gerichte

EU  
R

22. Sollte entgegen der Ansicht des Bundesrates die Datenverarbeitung durch die Gerichte vom Anwendungsbereich der Verordnung erfasst sein, erscheinen dem Bundesrat folgende Anmerkungen veranlasst:

- Der Verordnungsvorschlag trägt den Besonderheiten rechtsprechender Tätigkeit, die wesentlich durch das Gebot der Gewährung rechtlichen Gehörs gekennzeichnet ist, nicht hinreichend Rechnung.

Das Gebot der Gewährung rechtlichen Gehörs verpflichtet das Gericht, den Sachvortrag der Parteien umfassend zur Kenntnis zu nehmen, und verhindert auf diese Weise, dass das Gericht Art und Umfang der von ihm zu verarbeitenden personenbezogenen Daten selbst steuern kann. Umgekehrt hat das Gericht sicherzustellen, dass der gesamte Akteninhalt zumindest für die Dauer des Verfahrens als Entscheidungsgrundlage zur Verfügung steht, und ist in weitem Umfang zur Offenlegung ihm bekannt gewordener Tatsachen verpflichtet. Vor diesem Hintergrund sind die in den Kapiteln III und IV des Verordnungsvorschlags geregelten Benachrichtigungs-, Informations- und Dokumentationspflichten für ein Zivilgericht nicht erfüllbar. Eine klare Regelung, die Akten, Aktensammlungen und ihre Deckblätter vom Anwendungsbereich der Verordnung ausnimmt, fehlt. Insbesondere bestehen Zweifel, ob Gerichtsakten, die regelmäßig durch die Vergabe von Aktenzeichen systematisiert und ihrem Inhalt nach chronologisch geordnet werden, durch die in Erwägungsgrund 13 Satz 3 angesprochene Bereichsausnahme erfasst würden. Sachgerechte Ergebnisse ließen sich für den Bereich der Zivilgerichtsbarkeit letztlich ebenso wie für andere Bereiche nur durch Schaffung umfangreicher Ausnahmenvorschriften erzielen. Ein Nutzen aus der Einbeziehung der rechtsprechenden Tätigkeit der Gerichte in den Anwendungsbereich der Verordnung wäre damit nicht mehr gegeben.

- Die in Artikel 9 gewählte Anknüpfung an eine Unterscheidung verschiedener Kategorien personenbezogener Daten begegnet Bedenken. Neben den praktischen Schwierigkeiten bei der Zuordnung ist insoweit zu berücksichtigen, dass eine pauschale Kategorisierung nicht geeignet ist, den Umständen des jeweiligen Einzelfalls hinreichend Rechnung zu tragen.

Überdies gibt die vorgesehene Regelung Anlass zu Zweifeln, ob die Vorschriften über die Verarbeitung besonders geschützter personenbezogener Daten hinreichend Raum lassen, um wichtige öffentliche Aufgaben, wie sie beispielsweise den Gerichten in Betreuungs- und Abstammungsverfahren übertragen sind, zu erfüllen. In diesem Zusammenhang ist insbesondere zu berücksichtigen, dass vielfach ein unabdingbares praktisches Bedürfnis danach besteht, Gerichte und Behörden zu berechnen und zu verpflichten, auch besonders geschützte personenbezogene Daten zu Erfüllung öffentlicher Aufgaben an andere Stellen weiterzuleiten. Die entsprechenden Befugnisse und Verpflichtungen drohen indes durch die Bestimmungen des Verordnungsvorschlags zumindest für den Bereich besonders geschützter personenbezogener Daten unangemessen beschränkt zu werden.

- Ebenfalls als zu restriktiv gefasst erscheint die in dem Verordnungsvorschlag vorgesehene Regelungsstruktur für den Bereich der gerichtlich beziehungsweise amtlich geführten Register. Diese tragen regelmäßig einem besonderen Informationsbedürfnis Rechnung, das es - beispielsweise im Bereich des Grundstücksverkehrs - rechtfertigen kann, bestimmte personenbezogene Daten auch unbefristet zu verarbeiten. Insbesondere erscheint eine Beschränkung des Einsichtsrechts auf einzelne Teile eines Registerblatts in zahlreichen Fällen praktisch nicht durchführbar. So lässt sich vielfach im Voraus nicht zuverlässig beurteilen, auf welche Teile eines Registerblatts sich ein berechtigtes Interesse an der Einsichtnahme genau bezieht. Hier sollte im Interesse eines angemessenen Ausgleichs der berührten Interessen sowie zur Erhaltung eines effektiven Registerverkehrs daran festgehalten werden, dass - sofern überhaupt Einsicht gewährt wird - diese das gesamte Registerblatt beziehungsweise auch die gesamten diesbezüglich geführten Registerakten umfasst.
- Der Bundesrat ist der Auffassung, dass auch bei Gewährleistung eines hohen Datenschutzniveaus eine effektive Durchsetzung privater Rechte gewährleistet bleiben muss. Eine solche Rechtsdurchsetzung ist indes ohne Verarbeitung personenbezogener Daten nicht möglich. Diesem Umstand trägt der Verordnungsvorschlag in seiner bisherigen Form nicht hinreichend Rechnung. Um die Interessen privater Gläubiger angemessen zu schützen, sollte der mit der Erfüllung der in den Kapiteln III und IV des Verordnungsvorschlags geregelten Benachrichtigungs-, Informations- und Doku-

mentationspflichten verbundene bürokratische Aufwand begrenzt werden. Darüber hinaus sollte im Zusammenhang mit der Frage nach der Rechtmäßigkeit der Datenverarbeitung erwogen werden, die in Artikel 6 Absatz 1 Buchstabe a bis e enthaltene Aufzählung in zweierlei Hinsicht zu ergänzen. Zum einen könnte vorgesehen werden, dass die Verarbeitung personenbezogener Daten unabhängig vom Ergebnis einer einzelfallbezogenen Abwägung rechtmäßig ist, wenn sie zum Zwecke der Durchsetzung eines vollstreckbaren Titels erfolgt. In diesem Fall nämlich ist die Verarbeitung personenbezogener Daten lediglich Begleiterscheinung des mit einer Vollstreckung verbundenen weitergehenden Eingriffs in die Rechte des Schuldners. Zum anderen könnte geprüft werden, ob die Verarbeitung personenbezogener Daten auch dann, wenn noch kein vollstreckbarer Titel besteht, vorbehaltlich des notwendigen Schutzes besonders sensibler Daten im Sinne von Artikel 9 regelmäßig als rechtmäßig anzusehen ist, wenn sie der Durchsetzung eigener oder der Abwehr fremder Ansprüche dient. Die Anordnung eines entsprechenden Regel-Ausnahme-Verhältnisses böte gegenüber der in Artikel 6 Absatz 1 Buchstabe f vorgesehenen ergebnisoffenen Abwägung den Vorteil größerer Rechtssicherheit, ließe aber zugleich Raum, berechtigten Belangen des Datenschutzes im Einzelfall Geltung zu verschaffen.

#### Ausnahme des Justizvollzugs vom Anwendungsbereich

EU  
R

23. Im Hinblick auf den Justizvollzug ist der Bundesrat der Auffassung, dass hinsichtlich der Regelungen in Artikel 2 Absatz 2 Buchstabe a und Artikel 2 Absatz 3 Buchstabe a des Vorschlags 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, klargestellt werden sollte, dass die Verordnung und die Richtlinie keine Anwendung auf die Verarbeitung personenbezogener Daten im Bereich des Justizvollzugs finden sollen.

Der Bundesrat hat bereits in seiner Stellungnahme vom 23. September 2011, BR-Drucksache 366/11 (Beschluss) zum Grünbuch der Kommission: Stärkung des gegenseitigen Vertrauens im europäischen Rechtsraum - Grünbuch zur

Anwendung der EU-Strafrechtsvorschriften im Bereich des Freiheitsentzugs, COM(2011) 327 final, darauf hingewiesen, dass die Zuständigkeit zum Erlass von Regelungen über den Vollzug freiheitsentziehender Maßnahmen in Justizvollzugsanstalten und damit über die Haftbedingungen ebenso wie die Aufsicht über den Vollzug freiheitsentziehender Maßnahmen den Mitgliedstaaten und nicht der EU obliegt. Dies gilt auch und insbesondere für die Regelungen des Datenschutzes im Justizvollzug, die in Deutschland durchgehend ein hohes Datenschutzniveau garantieren. Die beabsichtigte Schaffung eines weitgehend einheitlichen Datenschutzrahmens in der EU darf nicht dazu führen, dass eine im Vertrag über die Arbeitsweise der EU nicht angelegte Zuständigkeit der EU für den Justizvollzug geschaffen wird.

- EU  
AV
24. Der Bundesrat sieht Korrekturbedarf beim personalen Anwendungsbereich. Durch Artikel 2 Absatz 2 Buchstabe d wird der personale Anwendungsbereich des Datenschutzrechts gegenüber dem geltenden Recht erweitert, da Datenverarbeitungen im Rahmen persönlicher oder familiärer Tätigkeiten nur unter der zusätzlichen Voraussetzung ausgenommen werden sollen, dass keinerlei Gewinnerzielungsabsicht besteht. Beispielsweise könnten damit auch Kundendateien natürlicher Personen für Privatverkäufe (eBay, Wohnungsverkauf) unter den Anwendungsbereich fallen. Für eine derartige Erweiterung wird keine Notwendigkeit gesehen. Nicht die Gewinnerzielungsabsicht, sondern die Gewerbsmäßigkeit sollte den Anwendungsbereich eröffnen.

#### Zu den einzelnen Vorschriften

- EU  
AV
25. Der Bundesrat befürchtet, dass Datenverarbeitungen, die von einer verantwortlichen Stelle ohne Niederlassung in der EU, aber mit Eingriffen in Rechte von EU-Bürgerinnen und EU-Bürger betrieben werden, nicht vollständig vom räumlichen Geltungsbereich der Verordnung erfasst werden. So erscheint beispielsweise unklar, ob die Verordnung bei der Erstellung und Veröffentlichung von Bildaufnahmen von Straßen und Gebäuden im Rahmen eines Geodatendienstes ohne Sitz in der EU zur Anwendung gelangt. Denn weder sind die in Artikel 3 Absatz 2 genannten Zwecke erfüllt, noch passt die für extraterritoriale Stellen wie Botschaften konzipierte Sondervorschrift in Artikel 3 Absatz 3. Insofern wird angeregt, jegliche Verarbeitung personenbezogener Daten unabhängig vom Sitz der verantwortlichen Stelle dem Geltungsbereich der Datenschutzverordnung zu unterwerfen, wenn sie an einem

Ort erfolgt, der dem Recht eines Mitgliedstaates unterliegt. Dabei sollte mit Blick auf Datenverknüpfungen die Verwirklichung eines einzigen datenschutzrechtlichen Tatbestands im Geltungsbereich der Verordnung genügen, um die gesamte Vorgangsreihe der Verarbeitung dem europäischen Datenschutzrecht zu unterwerfen.

EU  
AV

26. Die Neufassung des Begriffs der "personenbezogenen Daten" kann nach Einschätzung des Bundesrates zu einer Einengung des Anwendungsbereichs des Datenschutzrechts und damit zu Schutzlücken führen. Wenn Artikel 4 Absatz 1 in Verbindung mit Absatz 2 für die Personenbezogenheit eines Datums (in der zweiten Alternative) die voraussichtliche Zuordnung der betroffenen Person zu einer Kennung, zu einem Standort oder einem besonderen Merkmal verlangt, erscheint fraglich, ob beispielsweise Einrichtungen zur Videoüberwachung unter die Verordnung fallen. Zumindest bei zufällig aufgenommenen Personen dürfte es an der Betroffenheit im Sinne von Artikel 4 Absatz 1 fehlen, solange keine systematische Auswertung vorgenommen wird. Dies wäre allerdings nicht konsistent mit der Regelung der Datenschutzfolgenabschätzung in Artikel 33 Absatz 2 Buchstabe c, die offenbar davon ausgeht, dass die weiträumige Videoüberwachung von der Verordnung erfasst ist. Die Verknüpfung des Tatbestandsmerkmals der Bestimmbarkeit mit der voraussichtlichen Bestimmung der Person bzw. der Zuordnung einzelner Merkmale zu der Person erscheint in sich nicht ganz widerspruchsfrei und birgt ein hohes Maß an Rechtsunsicherheit. Gerade um einer unkontrollierten Sammlung von Nutzerdaten im Internet datenschutzrechtlich wirksam begegnen zu können, sollte wie bisher nach Artikel 2 Buchstabe a der Richtlinie 95/46/EG die Bestimmbarkeit der Person genügen, um den Anwendungsbereich zu eröffnen.

EU  
In

27. Der Bundesrat hält es für erforderlich, die in der vorgeschlagenen Verordnung den Mitgliedstaaten übertragenen Befugnisse zum Erlass nationaler Rechtsvorschriften sowohl für den öffentlichen als auch für den nichtöffentlichen Bereich zu präzisieren. Die in der Rechtsprechung des Europäischen Gerichtshofs anerkannten Möglichkeiten zur ausdrücklichen Ermächtigung der Mitgliedstaaten zur Ergänzung von Verordnungen werden bislang nicht hinreichend genutzt. Erforderlich sind hierzu umfassende, den Regelungen über delegierte Rechtsakte gleichgestellte und hinreichend bestimmte Ermächtigungen, die für das bestehende ausdifferenzierte Datenschutzrecht Bestandsschutz und die Möglichkeit zur Fortentwicklung im Rahmen der von der vorgeschlagenen

Verordnung abstrakt definierten Grundprinzipien gewährleisten. Die bisher lediglich in Artikel 6 Absatz 3 Buchstabe b des Entwurfs vorgesehene Schnittstelle zum Erlass einzelstaatlicher Regelungen, die eine öffentliche Aufgabe begründen können, zu deren Erfüllung die Verarbeitung personenbezogener Daten erforderlich ist, eröffnet selbst im öffentlichen Bereich bislang keine hinreichenden Spielräume. So ist beispielsweise offen, ob der Erlass nationaler Rechtsakte zur Begründung einer Datenverarbeitung entsprechend der Begriffsbestimmung in Artikel 4 Absatz 3 des Entwurfs für jede der dort genannten Phasen der Datenverarbeitung zulässig sein soll oder ob die Mitgliedstaaten auf die Regelung des "Ob" der Datenerhebung beschränkt bleiben. Für den Bereich des nichtöffentlichen Datenschutzes ergibt sich aus dem Verordnungsentwurf bisher nur für die Kommission im Rahmen delegierter Rechtsakte nach Artikel 6 Absatz 5 des Entwurfs die Möglichkeit, die unbestimmten Rechtsbegriffe im Rahmen des Tatbestands der Datenverarbeitung "zur Wahrnehmung berechtigter Interessen" (Artikel 6 Absatz 1 Buchstabe f des Entwurfs) zu konkretisieren, nicht aber für die Mitgliedstaaten. Nationale Konkretisierungen wie sie z. B. zur Gewährleistung der Rechtssicherheit und einheitlicher Vollzugsstandards in den §§ 28 ff. BDSG z. B. für Auskunfteien aufgenommen wurden, bleiben damit ausgeschlossen.

- EU  
AV
28. Der Bundesrat hält es für notwendig, die Generalklausel in Artikel 6 Absatz 1 Buchstabe f, wonach jede Datenverarbeitung zulässig ist, die zur Wahrung berechtigter Interessen der verantwortlichen Stelle erforderlich ist und der keine überwiegenden schutzwürdigen Interessen oder Grundrechte der betroffenen Person entgegenstehen, für bestimmte Datenübermittlungen an Dritte einzuschränken. Der Bundesrat ist insoweit der Auffassung, dass Datenübermittlungen an Dritte zu Werbezwecken grundsätzlich nur mit Einwilligung der betroffenen Person zulässig sein sollen. Außerdem sollen Schuldnerdaten nur in engen Grenzen übermittelt werden dürfen, die nicht hinter dem bestehenden Datenschutzniveau des § 28a BDSG zurückbleiben sollen.
- EU  
In
29. Der Bundesrat ist der Auffassung, dass sich der Begriff der Einwilligung in die Datenverarbeitung und die damit im Zusammenhang stehenden Regelungen der vorgeschlagenen Datenschutzgrundverordnung an der Freiwilligkeit der Datenverfügung und damit an dem Grundrecht auf informationelle Selbstbestimmung des Betroffenen orientieren sollten. Dieses Grundrecht ist durch Artikel 4 Absatz 8 und die Regelungen des Artikel 7 Absatz 1 bis 3 des Vorschlags



hinreichend geschützt, denn unter den die Freiwilligkeit einer Einwilligung ausschließenden Zwang fallen auch diejenigen erheblichen Ungleichverhältnisse, in denen die betroffene Person Schutz benötigt, weil die (nach außen als freiwillig abgegeben erscheinende) Einwilligungserklärung aufgrund der konkreten Konstellation nicht mehr als freiwillig abgegebene Willenserklärung einzuordnen ist.

EU  
AV

30. Der Bundesrat begrüßt, dass in Artikel 4 Absatz 8 eine konkludente Einwilligung ausdrücklich ausgeschlossen wird. Andererseits greift das Hervorhebungsgebot nach Artikel 7 Absatz 2 bei einer gemeinsam mit anderen Erklärungen erteilten Einwilligung (z.B. im Rahmen von AGB) zu kurz, wenn es nur für "schriftliche" Einwilligungen gelten soll und damit Schriftform im Sinne von § 126 BGB gemeint sein sollte.

EU  
In

31. Dagegen kann auch bei Bestehen eines erheblichen Ungleichgewichts die Einwilligung in die Datenverarbeitung auf einer freien Willensentscheidung des Betroffenen beruhen, beispielsweise um eine ausschließlich vorteilhafte Rechtsfolge herbeizuführen. Es wäre z. B. im Hinblick auf solche Konstellationen im Rahmen von Arbeitsverhältnissen schwer vermittelbar, in diesen Situationen eine Datenverarbeitung ausnahmslos zu untersagen.

EU  
Wi

32. Der Bundesrat ist der Auffassung, dass im Rahmen von Arbeitsverhältnissen eine freiwillige Einwilligung der betroffenen Person auch zukünftig als Grundlage für eine rechtmäßige Datenverarbeitung herangezogen werden können soll. Die Möglichkeit einer Einwilligung ist für den Beschäftigten insbesondere bei freiwilligen Zusatzleistungen des Arbeitgebers von Vorteil (z. B. unternehmensinterne Personaldatenbank, private Nutzung von E-Mails etc.). Da Artikel 7 Nr. 4 dem Wortlaut nach auch auf das Arbeitsverhältnis Anwendung finden könnte, sollte jedenfalls eine Klarstellung erfolgen, dass eine freiwillige Einwilligung zulässige Rechtsgrundlage für die Datenverarbeitung im Arbeitsverhältnis sein kann.

EU  
In

33. Daneben ist sicherzustellen, dass weiterhin mitgliedstaatliche Regelungen möglich sind, die eine Einwilligung als Rechtsgrundlage für Datenerhebungen und -verwendungen auch im Rahmen von Tätigkeiten der öffentlichen Verwaltung vorsehen.

- EU  
In  
(bei  
Annahme  
entfällt  
Ziffer 36)
34. Artikel 7 Absatz 4 sollte daher gestrichen werden.
- EU  
AV
35. Die Wirksamkeit der Einwilligung sollte auch durch allgemeine Rechtsgrundsätze wie dem der guten Sitten, zwingende Verbotsnormen und den unantastbaren Kern des gemeinen Persönlichkeitsrechts begrenzt sein.
- AV
36. Die in Artikel 7 Absatz 4 gesetzte Wirksamkeitsgrenze bei einem erheblichen Ungleichgewicht zwischen der betroffenen Person und der verantwortlichen Stelle erscheint insoweit nicht ausreichend.
- EU  
AV
37. Um das in Artikel 17 nur andeutungsweise geregelte "Recht auf Vergessen" zu stärken, sollte außerdem geprüft werden, die Einwilligung grundsätzlich befristet auszugestalten.
- EU  
AV
38. Der Bundesrat hält den Schutz von Minderjährigen für unzureichend. Die Altersgrenze von 13 Jahren für eine wirksame Einwilligung in Datenverarbeitungen bei einem Angebot über "Dienste der Informationsgesellschaft" sollte, wenn anstelle der Einsichtsfähigkeit überhaupt eine starre Altersgrenze gewählt wird, zumindest bei 14 Jahren liegen. Außerdem sollte der europäische Gesetzgeber die altersbezogene Einwilligungsfähigkeit nicht nur für Dienste der Informationsgesellschaft, sondern für alle von der Verordnung erfassten Sachverhalte regeln oder zumindest klarstellen, dass insoweit nationales Recht gilt. Klarzustellen ist außerdem, dass die Regelung in Artikel 8 Absatz 1 auch für entgeltfreie Dienstleistungen gilt, da der Begriff "Dienste der Informationsgesellschaft" in Artikel 1 der Richtlinie 98/34/EG als entgeltliche Dienstleistung definiert wird. Darüber hinaus ist klarstellungsbedürftig, ob sich Artikel 8 Absatz 1 ausschließlich auf solche Datenverarbeitungen bezieht, bei denen die Rechtmäßigkeit auf die Einwilligung gestützt wird, oder ob bei jeder Datenverarbeitung der Einwilligungsvorbehalt der Eltern bzw. gesetzlichen Vertreter gelten soll.

- EU  
AV
39. Der Bundesrat sieht es als problematisch an, dass im Gegensatz zur geltenden Rechtslage nach Artikel 9 Absatz 2 Buchstabe f besonders sensible Daten künftig auch zur außergerichtlichen Geltendmachung von Rechtsansprüchen ohne Einwilligung des Betroffenen verarbeitet werden dürften. Damit könnten beispielsweise Patientendaten, aber auch andere sensible Daten ohne Einwilligung des Betroffenen an Inkassounternehmen zu Abrechnungszwecken weitergegeben werden. Auf Grund der Missbrauchsgefahren, aber auch wegen der Kollision mit strafbewehrten Geheimhaltungspflichten unter anderem von Ärzten (§ 203 StGB) erscheint es vorzugswürdig, die Übermittlung besonders sensibler Daten an Dritte wie bisher nur zum Zweck der gerichtlichen Geltendmachung von Rechtsansprüchen einwilligungsfrei zuzulassen.
- EU  
AV
40. Die Pflicht zur Mitteilung von Berichtigungen und Löschungen nach Artikel 13 sollte sich auch auf Widersprüche erstrecken. Insoweit besteht ein besonderes Bedürfnis für eine Information der Datenempfänger, um eine weitere Datennutzung gemäß Artikel 19 Absatz 3 effektiv zu verhindern. Außerdem ist nicht verständlich, weshalb die Information des Betroffenen über sein Widerspruchsrecht in Artikel 14 Absatz 1 Buchstabe d sowie in Artikel 15 Absatz 1 Buchstabe e durch die gewählte Verknüpfung "beziehungsweise" als Alternative zur Information über das Recht auf Löschung oder Berichtigung genannt wird.
- EU  
AV
41. Falls personenbezogene Daten nicht bei den betroffenen Personen erhoben werden, haben die für die Verarbeitung Verantwortlichen nach Artikel 14 Absatz 4 Buchstabe b die Betroffenen zum Zeitpunkt der Erfassung der Daten zu informieren oder innerhalb einer angemessenen Frist nach ihrer Erhebung, die den besonderen Umständen Rechnung trägt. Der Bundesrat regt an, zu prüfen, ob "innerhalb einer angemessenen Frist" durch "unverzüglich" ersetzt werden sollte.
- EU  
R
42. Die datenschutzrechtlichen Belange der an einem gerichtlichen Verfahren Beteiligten werden durch die in den nationalen Verfahrensordnungen enthaltenen bereichsspezifischen Datenverarbeitungs- und Datenschutzregelungen gewahrt. Diese Regelungen sind integraler Bestandteil der jeweiligen Verfahrensart; eine Überlagerung durch die in Kapitel III der Verordnung statuierten Rechte der Betroffenen, insbesondere die in Artikel 14 geregelten Informationspflichten

der für die Verarbeitung Verantwortlichen, das in Artikel 15 normierte Auskunftsrecht und die in Artikel 16 bis 18 gewährten Ansprüche auf Berichtigung, Löschung und Datenübertragbarkeit würden zu einer Veränderung der in der nationalen Verfahrensordnung vorgesehenen Verfahrensgestaltung führen.

- EU  
AV
43. Der Bundesrat unterstützt das vorgesehene "Recht, vergessen zu werden", d. h. das Recht, die Löschung der personenbezogenen Daten zu verlangen, wenn sie nicht mehr benötigt werden oder wenn die Betroffenen ihre Einwilligung zurückziehen. Wurden die Daten bereits veröffentlicht, müssen alle vertretbaren Schritte, auch technischer Art, unternommen werden, um Dritte, die die Daten verarbeiten, über das Löschungsverlangen zu informieren.
- EU  
AV
44. Der Bundesrat begrüßt das vorgesehene Recht auf Datenportabilität, auf Grund dessen Verbraucherinnen und Verbraucher eine elektronische Kopie ihrer personenbezogenen Daten verlangen können und sie ihre einmal auf einer Plattform gespeicherten Daten unbehindert auf eine andere Plattform überführen dürfen. Dadurch wird die Kontrolle der Verbraucherinnen und Verbraucher über ihre Onlinedaten gestärkt. Das Recht auf Datenportabilität sollte wegen der damit verbundenen Missbrauchsgefahr allerdings nicht - wie es Artikel 18 Absatz 1 vorsieht - davon abhängen, ob die verantwortliche Stelle ihre Verarbeitungen in einem "gängigen" Format tätigt.
- EU  
AV
45. Der Weitergabe und Nutzung von personenbezogenen Daten zum Zwecke des Direktmarketings können Betroffene nach Artikel 19 Absatz 2 "unentgeltlich" widersprechen. Auf dieses Recht müssen sie hingewiesen werden. Die Erwähnung der Unentgeltlichkeit sollte gestrichen werden, da sich diese schon aus Artikel 12 Absatz 4 Satz 1 für alle nicht missbräuchlichen Anträge und Maßnahmen des Kapitels III ergibt.
- EU  
In
46. Der Bundesrat begrüßt die Fortentwicklung bestehender datenschutzrechtlicher Schutzprinzipien zu einem eigenständigen Zulassungserfordernis für Verfahren zur Profilbildung (Artikel 20 des Verordnungsvorschlags), wie sie u. a. in der Entschließung vom 10. Juli 2010 (BR-Drucksache 259/10 (Beschluss)) gefordert wurde, das durch die Verpflichtung zur Datenschutzfolgen-Abschätzung zusätzlich verfahrensrechtlich abgesichert wird (Artikel 33 Absatz 2 Buchstabe a des Verordnungsvorschlags).

- EU  
AV 47. Der Bundesrat begrüßt grundsätzlich die vorgesehenen Vorschriften über die Datenverarbeitung zur Profilbildung. Die Beschränkung in Artikel 20 Absatz 1, nach der diese Vorschrift nur auf die "rein" automatische Verarbeitung beschränkt ist, sollte gestrichen werden, so dass sie auf jede - auch nur teilweise automatisierte - systematische Verarbeitung zur Profilbildung Anwendung findet.
- EU  
In 48. Wegen des besonderen Schutzbedürfnisses sollten auch weitergehende Anforderungen an die Profilbildung auf der Grundlage personenbezogener Daten von Kindern aufgenommen werden, die mindestens den Anforderungen an die Profilbildung auf der Grundlage sensitiver Daten nach Artikel 20 Absatz 3 und Artikel 9 des Verordnungsvorschlags gleichzustellen sind. Darüber hinaus ist sicherzustellen, dass die Mitgliedstaaten befugt bleiben, bewährte spezifische Regelungen wie etwa zum Datenschutz bei Auskunfteien beizubehalten.
- EU  
AV 49. Die Vorschriften, mit denen die geeigneten Maßnahmen zur Wahrung der berechtigten Interessen der Betroffenen festgelegt werden sollen, sollen nach Auffassung des Bundesrates entweder in der Verordnung selbst geregelt werden oder den Mitgliedstaaten überlassen bleiben. Eine Gemengelage von Regelungskompetenzen der Mitgliedstaaten und der Kommission wird wegen der erheblichen Bedeutung von Bewertungsverfahren insoweit als nicht sachgerecht angesehen.
- EU  
AV 50. Der Regelungen zu den datenschutzfreundlichen Voreinstellungen werden grundsätzlich begrüßt.
- EU  
In 51. Der Bundesrat unterstützt die Zielsetzung, verstärkt technische Schutzkonzepte als Beitrag zur Gewährleistung der informationellen Selbstbestimmung in das bestehende System formaler sowie materiell-rechtlicher Anforderungen an die Zulässigkeit der Datenverarbeitung aufzunehmen. Allerdings beschränken sich diese Ansätze bislang auf Einzelaspekte wie den allgemeinen Grundsatz datenschutzfreundlicher Voreinstellungen, den der Bundesrat bereits in seinem Gesetzentwurf vom 17. Juni 2011 (BR-Drucksache 156/11 (Beschluss)) zur Stärkung des Datenschutzes in Sozialen Netzwerken in konkreterer Form

entwickelt hatte. Im nationalen Recht in Gestalt organisatorischer und technischer Maßnahmen (§ 9 BDSG) bereits etablierte datenschutztechnische Grundprinzipien oder in der Diskussion stehende Fortentwicklungen wie die Schaffung technologieneutraler Schutzziele als Leitbild künftiger datenschutzgerechter IT-Verfahren fehlen allerdings.

- EU  
AV  
In
52. Der Bundesrat fordert daher, jedenfalls die in Artikel 23 Absatz 2 enthaltenen Anforderungen zu präzisieren und um Kriterien und Anforderungen hinsichtlich der zu treffenden Maßnahmen und Verfahren zu ergänzen.
- EU  
In
53. Hierbei sind insbesondere Anonymisierung und Pseudonymisierung nach dem Stand der Technik zu fordern. Außerdem ist klarzustellen, dass Datenschutz durch Technik auch die Auswahl und Gestaltung von Datenverarbeitungssystemen betrifft.
- EU  
AV
54. Der Bundesrat spricht sich in diesem Zusammenhang dafür aus, vor allem Anbieter von Telemediendiensten, insbesondere von sozialen Netzwerken, dazu zu verpflichten, die Sicherheitseinstellungen auf der höchsten Sicherheitsstufe gemäß dem Stand der Technik voreinzustellen.
- EU  
In
55. Angesichts der für die Neuregelung der Auftragsdatenverarbeitung im Bundesdatenschutzgesetz maßgeblichen Gründe und der positiven Erfahrungen mit dieser Vorschrift hält es der Bundesrat für geboten, diese in weitergehendem Umfang in die Verordnung zu übernehmen, als dies bislang vorgesehen ist. Sichergestellt werden muss insbesondere, dass sämtliche Festlegungen schriftlich und konkret getroffen werden und eine wirksame Kontrolle der Auftragsdatenverarbeitung durch die verantwortliche Stelle erfolgen kann.
- EU  
AV
56. Der in Artikel 26 Absatz 2 geregelte Mindestinhalt einer Vereinbarung zwischen Auftragsverarbeitern und den für die Verarbeitung Verantwortlichen sollte um die Angabe von Gegenstand und Dauer des Auftrags sowie Umfang, Art und Zweck der vorgesehenen Verarbeitung, der Art der Daten und des Kreises der Betroffenen ergänzt werden. Eine wirksame Kontrolle der Auftragsdatenverarbeitung durch die verantwortliche Stelle kann umfassend nur erfolgen, wenn in Artikel 26 Absatz 2 der verantwortlichen Stelle auch ein Kontrollrecht vor Ort eingeräumt wird und den Auftragsverarbeiter entsprechende Mitwirkungspflichten treffen. In Artikel 24 sollte klargestellt werden, dass die Be-

troffenen sich sowohl an die verantwortliche Stelle als auch an den Auftragsdatenverarbeiter wenden können.

- EU  
In
57. Der Bundesrat weist darauf hin, dass Artikel 30 Absatz 3 der Kommission die Möglichkeit eröffnet, eigene Standards der Informationssicherheit zu erlassen, die nicht mit nationalen Standards übereinstimmen müssen. Hier besteht die potenzielle Gefahr, dass umfangreiche Investitionen im Bereich der Informationssicherheit ganz oder teilweise erneut nach den dann gültigen Regeln zu tätigen sind. Es muss daher sichergestellt werden, dass die Standardsetzung durch die Kommission eng mit den national etablierten Standards harmoniert. Der Bundesrat fordert daher, bei beabsichtigten Standardsetzungen die nationalen Akteure eng einzubeziehen und nationale Standardsetzungen im Bereich der Informationssicherheit zu berücksichtigen.
- EU  
Wi
58. Der Bundesrat unterstützt die Kommission in ihrem Bemühen, die Stellung der betroffenen Person zu stärken und die Datensicherheit durch Vorgabe von geeigneten und zumutbaren technischen und organisatorischen Maßnahmen zu erhöhen, die die für die Verarbeitung Verantwortlichen zu treffen haben. Die in Artikel 31 und 32 des Vorschlags vorgesehenen Melde- und Benachrichtigungspflichten für die Unternehmen sind allerdings sehr weitgehend. Diese Pflichten kämen ihrem Wortlaut nach schon bei geringfügigen Verstößen zur Anwendung - unabhängig davon, ob schwerwiegende Beeinträchtigungen für die Rechte oder schutzwürdigen Interessen der Betroffenen drohen. Nach Auffassung des Bundesrates ist das in Deutschland nach aktueller Rechtslage in § 42 a BDSG gewährte Schutzniveau ausreichend.
- EU  
In
59. Der Bundesrat hält die Verpflichtung zur Meldung von Datenpannen für zu weitgehend. Bei der vorgeschlagenen Regelung kommt es weder darauf an, ob die Daten ihrer Art nach besonders schutzwürdig sind noch auf die Schwere und Tragweite des Vorfalls für die Betroffenen. Ein so weitgehender Anwendungsbereich dürfte zu einer Meldeflut bei den Aufsichtsbehörden und zur Benachrichtigung von Betroffenen selbst in Fällen führen, in denen dies für die bessere Wahrnehmung von Schutzrechten nicht erforderlich ist.
- EU  
AV
60. Der Bundesrat sieht die Datenschutzfolgenabschätzung in ihrer Wirksamkeit geschmälert, wenn die Sachverhalte, die die Pflicht zur Datenschutzfolgenabschätzung begründen sollen, in der Verordnung nicht näher konkretisiert wer-

den. Auch spricht sich der Bundesrat dafür aus, die inhaltlichen Anforderungen an die Datenschutzfolgenabschätzung bereits im Verordnungstext näher zu regeln. Ein konkretes Risiko für die Rechte und Freiheiten betroffener Personen wird außerdem bei der Verarbeitung personenbezogener Daten aus allen Dateien gesehen, die Daten über Kinder, genetische Daten oder biometrische Daten enthalten - unabhängig vom Umfang der Datei. Das Wort "umfangreichen" in Artikel 33 Absatz 2 Buchstabe d sollte deshalb gestrichen werden.

- EU  
AV
61. Der Bundesrat begrüßt die Einführung eines betrieblichen Datenschutzbeauftragten, hält jedoch die in Artikel 35 Absatz 1 aufgestellten Schwellen und Kriterien für nicht angemessen. So sollte die Bestellung eines betrieblichen Datenschutzbeauftragten grundsätzlich bei jeder verantwortlichen Stelle sichergestellt sein, deren Kerntätigkeit in der Verarbeitung oder Nutzung personenbezogener Daten besteht (z. B. Auskunfteien, Detekteien, Callcenter, Lettershops u. ä.). Darüber hinaus sollte in die Verordnung eine Verschwiegenheitsverpflichtung der Datenschutzbeauftragten aufgenommen werden sowie deren Recht auf Fort- und Weiterbildung und die Übernahme der dafür entstehenden Kosten.
- EU  
In
62. Der Bundesrat stellt fest, dass die in Artikel 35 entwickelten Anforderungen an die Bestellung betrieblicher oder behördlicher Datenschutzbeauftragter den positiven Erfahrungen deutscher Unternehmen mit dem Modell innerbetrieblicher Eigenkontrolle des Datenschutzes nur begrenzt Rechnung tragen. Angesichts der sonstigen Ansätze zur Stärkung unternehmerischer Verantwortung und Haftung für die Rechtmäßigkeit der Datenverarbeitung setzt der Schwellenwert für die obligatorische Bestellung betrieblicher Datenschutzbeauftragter für Unternehmen erst ab 250 Beschäftigten falsche Signale zum Abbau bewährter betrieblicher Datenschutzkonzepte. Bei besonders datenschutzkritischen Kerntätigkeiten (z. B. bei Auskunfteien, Detekteien, Call-Centern) sollte eine Pflicht zur Bestellung eines betrieblichen Datenschutzbeauftragten unabhängig von der Mitarbeiterzahl bestehen.
- EU  
Wi
63. Der Bundesrat ist der Auffassung, dass bei der unbestreitbar notwendigen Fortentwicklung und Verbesserung der Regelungen über den Datenschutz zusätzlicher bürokratischer Aufwand für die Unternehmen soweit wie möglich vermieden werden sollte. Vor diesem Hintergrund hält es der Bundesrat für wünschenswert, dass für die unternehmens- bzw. konzerninterne Datenüber-



mittlung in oder aus Drittstaaten Erleichterungen eingeräumt werden können, sofern der Schutz der personenbezogenen Daten durch adäquate unternehmens- und konzerninterne Maßnahmen auf hohem Niveau sichergestellt bleibt. Für international aufgestellte Unternehmen sollten angesichts der vielfältigen wirtschaftlichen Verflechtungen keine unnötig hohen Hürden für den internen Datenaustausch aufgebaut werden. Der Bundesrat verweist insoweit auch auf seine Stellungnahme zur Mitteilung der Kommission zum Gesamtkonzept für den Datenschutz in der EU (BR-Drucksache 707/10 (Beschluss)).

EU  
AV

64. Der Verordnungsvorschlag bietet nach Ansicht des Bundesrates allerdings keinen hinreichenden Schutz vor Datenübermittlungen in Drittstaaten mit unzureichenden Datenschutzstandards. Das Genehmigungserfordernis nach Artikel 42 droht wegen der weit gefassten Ausnahmeregelung in Artikel 44 leerzulaufen. Die Ausnahmegesetzgebung des Artikels 44 bedarf daher einer deutlichen Einschränkung. Zum anderen erscheint selbst im Falle einer Genehmigungspflicht fragwürdig, dass der Verordnungsvorschlag von der Genehmigungsfähigkeit einer Datenübermittlung in Drittstaaten ausgeht, obwohl das dortige Recht keinen angemessenen Datenschutz im Sinne von Artikel 41 bietet. Insbesondere die in Artikel 42 Absatz 2 Buchstabe d angesprochenen vertraglichen Vereinbarungen zwischen den an der Datenverarbeitung beteiligten Stellen sind gesetzlichen Datenschutzstandards nicht gleichwertig, zumal sie grundsätzlich nur zwischen den Parteien gelten und damit den Betroffenen keine subjektiven Rechte gewähren. Insoweit wären mindestens die Anforderungen an unternehmensinterne Vorschriften gemäß Artikel 43 zugrunde zu legen, zu denen unter anderem die Übertragung individuell durchsetzbarer Rechte der Betroffenen zählt.

EU  
In

65. Der Bundesrat stellt fest, dass die Vorschläge der Kommission zur näheren Ausgestaltung der völligen Unabhängigkeit der Datenschutzaufsichtsbehörden weit über die Anforderungen hinausgehen, die der bisherigen Datenschutzrichtlinie und den weiteren sekundärrechtlichen Regelungen zur Stellung des Europäischen Datenschutzbeauftragten zu entnehmen waren und die auch vom Europäischen Gerichtshof als tauglicher Auslegungsmaßstab herangezogen wurden. Insbesondere die statusrechtlichen Regelungen erzeugen abermals Konflikte mit der Organisations-, Budget- und Personalhoheit der Mitgliedstaaten, die durch das Erfordernis einer Gewährleistung unabhängiger Datenschutzkontrolle nicht zu rechtfertigen sind. Der Bundesrat bittet deshalb,

im weiteren Rechtsetzungsverfahren zu prüfen, ob die Anforderungen nicht auf die bereits in der Verordnung (EU) Nr. 45/2001 enthaltenen und von den Mitgliedstaaten nach der Entscheidung des Europäischen Gerichtshofs vom 9. März 2010 den nationalen Gesetzgebungsverfahren zu Grunde gelegten Detailanforderungen an die völlige Unabhängigkeit beschränkt werden können. Der Bundesrat bittet im Übrigen sicherzustellen, dass bei der nach Artikel 48 Absatz 1 des Vorschlags vorgesehenen Ernennung der Mitglieder der (unabhängigen) Aufsichtsbehörde durch Parlament oder Regierung auch in Fortführung bestehender Rechtslage und Rechtspraxis die Ernennung durch einen Wahlakt des zuständigen Parlamentes erfolgen kann. Angesichts unterschiedlicher Formulierungen in Artikel 48 Absatz 1 und Artikel 47 Absatz 6 des Vorschlags bittet der Bundesrat außerdem klarzustellen, dass eine Aufsichtsbehörde auch alleine durch eine Person geleitet werden kann, wie es dem Staatsaufbau in Deutschland gerecht würde. Soweit sich Artikel 48 Absatz 1 des Vorschlags auf das weitere Personal der Aufsichtsbehörde bezieht, sollte klargestellt werden, dass das Ernennungsrecht für dieses Personal auch dem jeweiligen Leiter der Behörde zustehen kann. Mit Rücksicht auf verfassungsrechtlich legitimierte Frage- und Informationsrechte der Parlamente ist zudem klarzustellen, dass diese bei Wahrung der völligen Unabhängigkeit auch in Zukunft zulässig und notwendig sind.

- EU  
AV
66. Nach Artikel 51 Absatz 2 soll, wenn ein Unternehmen Niederlassungen in mehreren Mitgliedstaaten hat, die Aufsichtsbehörde des Mitgliedstaats, in dem sich die Hauptniederlassung dieses Unternehmens befindet, zuständig sein - und zwar für die Aufsicht über die Verarbeitung in allen Mitgliedstaaten ("One-Stop-Shop"). Der Bundesrat spricht sich dafür aus, dass diese Zuständigkeit keine ausschließliche ist, sondern eine federführende. Die Regelung sollte generell nicht gelten, wenn Unternehmen zwar über Niederlassungen in mehreren Mitgliedstaaten verfügen, es aber um rein nationale Sachverhalte geht. In diesen Fällen sollte es aus Gründen der Verfahrensökonomie bei der allgemeinen Zuständigkeitsregelung des Artikels 51 Absatz 1 bleiben. Außerdem fällt auf, dass Artikel 51 keine Zuständigkeitsregelung für Datenverarbeitungen durch nicht in der EU niedergelassene Stellen trifft.

EU  
R

67. Zu Artikel 51 - Hilferwägungen zur Kontrollbefugnis der Aufsichtsbehörden im Hinblick auf gerichtliche Tätigkeit

Für den Fall, dass die Datenverarbeitung durch die Gerichte vom Anwendungsbereich der Verordnung erfasst sein sollte, hält es der Bundesrat für erforderlich, die Reichweite der Kontrollbefugnisse der Aufsichtsbehörden im Hinblick auf gerichtliche Tätigkeiten in Artikel 51 Absatz 3 des Verordnungsvorschlags zu präzisieren. Nach Artikel 51 Absatz 3 soll die Aufsichtsbehörde nicht zuständig sein für die Überwachung der von Gerichten im Rahmen ihrer gerichtlichen Tätigkeit vorgenommenen Verarbeitungen. Ausweislich des Erwägungsgrundes 99 soll die Regelung die Unabhängigkeit der Richter bei der Ausübung ihrer richterlichen Tätigkeit garantieren. Diesem Zweck wird nach dem Wortlaut des Artikels 51 Absatz 3 jedoch nicht umfassend Rechnung getragen. Nach diesem Wortlaut wäre die Aufsichtsbehörde auch dann zuständig, wenn ein Gericht etwa aufgrund eines Richtervorbehalts eine Datenverarbeitung durch eine Behörde angeordnet oder gestattet hat oder durch Urteil oder Beschluss eine Datenverarbeitung für rechtmäßig erklärt hat. Denn in solchen Fällen erklärt das Gericht zwar eine beabsichtigte Datenverarbeitung für zulässig, nimmt die Datenverarbeitung aber gerade nicht selbst vor. Die Aufsichtsbehörde wäre folglich nicht gehindert, gegen eine richterlich angeordnete oder bestätigte, aber in Verantwortung einer anderen Stelle durchgeführte Datenerhebung vorzugehen.

Ein solches Ergebnis wäre jedoch nicht mit der - verfassungsrechtlich gewährleisteten - richterlichen Unabhängigkeit in Einklang zu bringen. Die richterliche Unabhängigkeit steht einer Überprüfung rechtsprechender Tätigkeiten durch andere staatliche Gewalten entgegen. Der Richter muss bei der Rechtsfindung frei von Einwirkungen anderer staatlicher Organe sein. Dies gilt auch für Maßnahmen informeller Art wie etwa Empfehlungen oder fallbezogene Vorhaltungen. Nicht nur in laufenden Verfahren ist jede Einflussnahme auf die richterliche Entscheidung - also die Einwirkung auf den zur Entscheidung berufenen Richter in anderer als prozessual zulässiger Weise - verfassungsrechtlich untersagt. Auch nach ihrem Abschluss sind gerichtliche Verfahren kontrollresistent. Um klarzustellen, dass eine Beeinträchtigung der richterlichen Unabhängigkeit in jeder Form ausgeschlossen sein muss, sollte Artikel 51

Absatz 3 des Verordnungsvorschlags dahin ergänzt werden, dass die Aufsichtsbehörde auch nicht zuständig ist, soweit Datenverarbeitungen gerichtlich angeordnet, bestätigt oder für zulässig erklärt wurden.

- EU  
R 68. Der Bundesrat begrüßt die Bestrebungen, durch Einführung eines Kohärenzverfahrens in Artikel 57 des Verordnungsvorschlags eine unionsweit einheitliche Anwendung der Regelungen sicherzustellen.
- EU  
AV 69. Der Bundesrat sieht jedoch das in Artikel 57 ff. vorgesehene Kohärenzverfahren, insbesondere den in Artikel 59 Absatz 3 angeordneten Aufschub behördlicher Maßnahmen während der Prüfung durch die Kommission, kritisch, da er die Gefahr erheblicher Verzögerungen birgt.
- EU  
R 70. Bedenken begegnet insbesondere die vorgesehene Befugnis der Kommission, geplante Maßnahmen der unabhängigen Aufsichtsbehörden bis zu zwölf Wochen lang auszusetzen und gegebenenfalls sogar selbst einstweilige Maßnahmen anzuordnen. Dies steht in Widerspruch zu der völligen Unabhängigkeit der Aufsichtsbehörden gemäß Artikel 8 Absatz 3 der Grundrechtecharta, Artikel 16 Absatz 2 AEUV sowie Artikel 47 Absatz 1 des Verordnungsvorschlags. Entscheidungen der unabhängigen Aufsichtsbehörden wären danach einer Kontrolle durch die Kommission unterworfen. Die Bedenken werden noch dadurch verstärkt, dass die Befugnisse der Kommission an eingeschränkt nachprüfbar Voraussetzungen gekoppelt werden. So soll etwa für die Aussetzung einer Maßnahme genügen, dass die Kommission "ernsthaft bezweifelt", dass die geplante Maßnahme die "ordnungsgemäße Anwendung" der Verordnung sicherstellt oder dass die Kommission "befürchtet", dass die Maßnahme zu einer uneinheitlichen Anwendung der Verordnung führt.
- EU  
In 71. Unbeschadet grundsätzlicher kompetenzrechtlicher Einwände hält der Bundesrat eine klare Beschränkung des sog. Kohärenzverfahrens auf Sachverhalte für erforderlich, die grenzüberschreitenden Bezug haben, so dass rein nationale Fragen des Vollzugs europäischen Datenschutzrechts, also insbesondere Fragen des Datenschutzes bei öffentlichen Stellen nicht im Europäischen Datenschutzausschuss zu behandeln sind. Verfahrensoptionen wie die Antragsrechte nach Artikel 58 Absatz 3 und 4 des Verordnungsvorschlags, durch die ohne weitere Voraussetzungen jegliche Datenschutzfrage zum Gegenstand des Kohärenzverfahrens gemacht werden kann, sind im Sinne dieser Zielsetzung zu

beschränken. Außerdem ist zu gewährleisten, dass die Strukturen föderal organisierter Mitgliedstaaten auch bei den Entsendungsregelungen des Datenschutzausschusses berücksichtigt werden, um sicherzustellen, dass die im föderalen Verwaltungsaufbau zuständigen Kontrollstellen an den Beratungen von Angelegenheiten beteiligt werden, die in ihre Vollzugsverantwortung fallen. Außerdem sollte der Europäische Datenschutzausschuss spiegelbildlich zur Beteiligung der Datenschutzkontrollstellen in nationalen Rechtsetzungsverfahren stärker in Verfahren zum Erlass delegierter Rechtsakte eingebunden werden, da diese in höherem Maße Fragen des Datenschutzvollzugs als den Aufgabenkreis des bislang zu beteiligenden Europäischen Datenschutzbeauftragten betreffen. Über die genannten Kompetenzen in Artikel 66 des Verordnungsvorschlags hinaus sollte dem Ausschuss daher ein Beteiligungsrecht eingeräumt werden, um die Expertise der Datenschutzbehörden einzubringen und die Transparenz des Delegations- und Komitologieverfahrens zu erhöhen.

EU  
In

72. Die Eingriffsbefugnisse der Aufsichtsbehörde nach Artikel 53 des Verordnungsvorschlags sind nach Auffassung des Bundesrates gegenüber den öffentlichen Stellen zu weit gefasst. Die Aufsichtsbehörde hat jederzeit das Recht und die Möglichkeit, sich bei Datenschutzverstößen der öffentlichen Verwaltung an die Öffentlichkeit oder das jeweilige Parlament zu wenden. Ein Weisungs- oder Untersagungsrecht einschließlich der Befugnis zur Ahndung durch Bußgeldzahlungen ist im Verhältnis der Aufsichtsbehörden zu den öffentlichen Stellen weder erforderlich noch geboten. Die Befugnis zur Verhängung von Bußgeldern steht auch dem Europäischen Datenschutzbeauftragten gegenüber den Organen und Einrichtungen der Union nicht zu. Insoweit sollten die Befugnisse der Aufsichtsbehörden im Verhältnis zu öffentlichen Stellen an den Regelungen zum Europäischen Datenschutzbeauftragten ausgerichtet werden.

EU  
R

73. Hinsichtlich der in den Artikeln 74 bis 76 vorgesehenen gerichtlichen Rechtsbehelfe ist zweifelhaft, ob und inwieweit für die Ausgestaltung der gerichtlichen Verfahren auf das nationale Recht zurückgegriffen werden kann. Der Bundesrat hält es deshalb für erforderlich, in der Verordnung klarzustellen, dass für die Durchführung der in der Verordnung vorgesehenen Rechtsbehelfsverfahren das innerstaatliche Gerichtsverfassungs- und Verfahrensrecht gilt.

EU  
R

74. Der Bundesrat bittet im weiteren Rechtsetzungsverfahren zu prüfen, ob das Verhältnis der verschiedenen in den Artikeln 74 und 75 genannten gerichtlichen Rechtsbehelfe im Falle mehrfacher Klageerhebung näher geregelt werden sollte. Sowohl der Aufsichtsbehörde als auch den von der Datenverarbeitung betroffenen Personen stehen gerichtliche Rechtsbehelfe offen, und zwar sowohl gegen den für die Verarbeitung Verantwortlichen als auch gegen den Auftragsverarbeiter. Ebenso können diese Stellen ihrerseits gegen Entscheidungen der Aufsichtsbehörde klagen. Daneben soll noch das Recht von Verbänden bestehen, im Namen eines oder mehrerer Betroffener zu klagen. Eine Regelung zur möglichen Aussetzung eines Gerichtsverfahrens findet sich bislang nur für den Fall, dass zugleich ein Kohärenzverfahren anhängig ist. Im Falle einer Klageerhebung durch unterschiedliche Beteiligte gegen jeweils andere Personen oder Stellen ist es jedoch auch nicht ausgeschlossen, dass derselbe Datenverarbeitungsvorgang verschiedenen Gerichten innerhalb desselben Mitgliedsstaats zur Entscheidung vorgelegt wird. Hier sollte klargestellt werden, ob und gegebenenfalls welches Verfahren in diesem Fall ausgesetzt werden kann.

EU  
In  
Wi

75. Der Bundesrat steht der Einführung eines Klagerechts für Datenschutzbehörden und Verbände ablehnend gegenüber. [Insoweit verweist er auf seine Stellungnahme zur Mitteilung der Kommission zum Gesamtkonzept für den Datenschutz in der EU (BR-Drucksache 707/10 (Beschluss)).]

[EU  
Wi]

(bei  
Annahme  
entfällt  
Ziffer 77)

EU  
In  
(bei  
Annahme  
entfällt  
Ziffer 77)

76. 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 daten-

schutzrechtlicher 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.

AV  
(entfällt  
bei  
Annahme  
von  
Ziffer 75  
oder  
Ziffer 76)

77. Der Bundesrat sieht die Gefahr, dass durch Artikel 76 Absatz 1 den Verbraucherverbänden derzeit zustehende Klagemöglichkeiten bei Verstößen gegen verbraucherrechtliche Vorschriften abgeschnitten würden. Denn Artikel 76 Absatz 1 vermittelt den Verbänden kein eigenständiges Klagerecht. Dies erscheint gerade mit Blick auf die enge Verknüpfung von datenschutzrelevanten Sachverhalten mit Allgemeinen Geschäftsbedingungen oder Datenverarbeitungen im Zusammenhang mit Vertragsverhandlungen (z. B. Scoring, Profiling) nicht sachgerecht. Ziel sollte es vielmehr sein, die Möglichkeiten der Rechtsdurchsetzung für qualifizierte Einrichtungen im Sinne der Richtlinie 2009/22/EG zu stärken. Daher sollte für qualifizierte Einrichtungen im Sinne des UKlaG bzw. der Richtlinie 2009/22/EG die Möglichkeit der Unterlassungsklage ausdrücklich eingeräumt oder zumindest vorbehalten werden.

EU  
R

78. Der Bundesrat regt an zu prüfen, inwieweit die Haftungsnorm des Artikels 77 in Tatbestand und Rechtsfolge konkretisiert werden kann. Die Vorschrift lässt nach ihrer deutschen Fassung wesentliche Haftungsfragen offen. Ihr lässt sich insbesondere nicht mit hinreichender Klarheit entnehmen,

- was unter einer "mit dieser Verordnung nicht zu vereinbarenden Handlung" zu verstehen sein soll,
- ob die Haftung einen Verstoß gegen Rechtsnormen voraussetzt, die zumindest auch dem Schutz des Einzelnen zu dienen bestimmt sind,
- ob die Haftung ein Verschulden des Verantwortlichen voraussetzt und welcher Art dieses sein soll (Vorhersehbarkeit?),
- ob sich dieses Verschulden nur auf den Haftungsbegründungstatbestand oder - was Artikel 77 Absatz 3 nahelegt - auf haftungsausfüllende Um-

stände (z. B. den Kausalverlauf, Folgeschäden) beziehen muss,

- ob der Entlastungsbeweis zum Haftungsausschluss führt oder ob hier weitere Voraussetzungen zu erfüllen sind ("... kann ... befreit werden, ...").

Zum erforderlichen Grad der Konkretisierung ist zu bemerken, dass eine unmittelbar zwischen Zivilrechtssubjekten geltende Haftungsnorm ein wesentlich höheres Maß an Bestimmtheit verlangt als die Regelungsvorgabe an Mitgliedstaaten, wie sie bisher in Artikel 23 der Richtlinie 95/46/EG des Europäischen Parlaments und des Rates vom 24. Oktober 1995 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr enthalten ist. Art und Umfang des ersatzfähigen Schadens werden mangels einschlägiger Vorgaben nach nationalem Recht zu bestimmen sein.

- EU  
Wi
79. Im Übrigen weist der Bundesrat darauf hin, dass der Verordnungsvorschlag für einige wichtige Bereiche keine Regelungen enthält und insofern zu Rechtsunsicherheit führen kann. So wäre beispielsweise für die Verarbeitung von Gesundheitsdaten in der Versicherungswirtschaft eine ausdrückliche Rechtsgrundlage dringend erforderlich.
- EU  
In
80. Der Bundesrat unterstützt grundsätzlich die Zielsetzung, Verstöße gegen datenschutzrechtliche Anforderungen in höherem Maße als bisher im europäischen und nationalen Recht vorgesehen zu sanktionieren. Von individuellen Schadensersatzforderungen losgelöste Ahndungsmöglichkeiten entfalten eine hohe generalpräventive Wirkung und tragen damit zur Verbesserung des Datenschutzniveaus insgesamt bei.
- EU  
In
81. Soweit die EU Regelungen zur Verhängung verwaltungsrechtlicher Sanktionen trifft, sollte es - unabhängig von der Frage des künftigen Rechtsrahmens (Verordnung oder Richtlinie) - den Mitgliedstaaten mit Rücksicht auf ihre Verfassungsidentität überlassen bleiben, die Befugnis zur Verhängung von Sanktionen, insbesondere gegenüber öffentlichen Stellen anderen als den Aufsichtsbehörden für den Datenschutz vorzubehalten. Nach deutschem Verfassungsverständnis können unabhängige, in die Ministerialhierarchie nicht eingegliederte Aufsichtsbehörden gegenüber anderen öffentlichen Stellen grundsätzlich nicht mit Befugnissen zu hoheitlichen Eingriffen, insbesondere zur



Verhängung von Sanktionen, ausgestattet werden. Hierzu besteht auch keine Notwendigkeit. Erstens kann gegenüber öffentlichen Stellen etwaigen Zuwiderhandlungen beim Umgang mit personenbezogenen Daten mit Mitteln der Dienst-, Rechts- oder Fachaufsicht sowie der parlamentarischen Kontrolle ausreichend begegnet werden. Zweitens könnte, sofern sich ausnahmsweise eine Notwendigkeit zur Verhängung von Sanktionen gegenüber öffentlichen Stellen zeigen sollte, hierzu durch nationales Recht anstelle der unabhängigen Aufsichtsbehörde eine andere - in die Ministerialhierarchie eingeordnete - Behörde befugt werden. In Anlehnung an Artikel 46 Buchstabe b des Vorschlags für eine Richtlinie für den Bereich von Polizei und Justiz (BR-Drucksache 51/12) sollten die Sanktionsregelungen der Verordnung für den Bereich der öffentlichen Verwaltung auf die bereits in Artikel 28 Absatz 3 2. Anstrich der Richtlinie 95/46/EG enthaltenen Einwirkungsbefugnisse beschränkt werden.

- EU  
In
82. Selbst bei der Verhängung von Sanktionen gegenüber nichtöffentlichen Stellen sollte es den nationalen Gesetzgebern überlassen bleiben, ob Sanktionen durch die unabhängige Aufsichtsbehörde oder durch eine andere und damit in ministerielle Weisungsstränge eingeordnete Behörde verhängt werden. Zudem sollte die nähere Ausgestaltung der Sanktionstatbestände den nationalen Gesetzgebern überlassen werden, da z. B. in Deutschland mehrere der angeführten Zuwiderhandlungen im Falle der Bereicherungs- oder Schädigungsabsicht als Straftaten eingestuft sind. Zumindest sollte klargestellt werden, dass nationale Rechtsvorschriften im Sinne des Artikels 78 Absatz 3 anstelle einer verwaltungsrechtlichen Sanktion auch eine strafrechtliche Sanktion vorsehen können.
- EU  
In
83. Der Bundesrat weist außerdem darauf hin, dass einzelne Tatbestände des Artikels 79 Absätze 4 bis 6 des Verordnungsvorschlags (insbesondere Artikel 79 Absatz 4 Buchstabe a und Absatz 5 Buchstabe b) Bedenken hinsichtlich ihrer rechtsstaatlichen Bestimmtheit ausgesetzt sind. Anders als im nationalen Recht fehlt auch eine aus Gründen der Verhältnismäßigkeit gebotene klarere Differenzierung der Einzeltatbestände nach formalen oder materiellen Zuwiderhandlungen.
- EU  
In
84. Die Bestimmungen zu den Datenschutzvorschriften von Kirchen und religiösen Vereinigungen oder Gemeinschaften in Artikel 85 des Verordnungsvorschlags

widersprechen der in Artikel 17 Absatz 1 AEUV festgelegten Kompetenzordnung. Nach Artikel 17 Absatz 1 AEUV achtet die EU den Status, den Kirchen, religiöse Vereinigungen oder Gemeinschaften in den Mitgliedstaaten genießen, und beeinträchtigt ihn nicht. Durch Artikel 85 des Verordnungsvorschlags werden die Kirchen und religiösen Vereinigungen oder Gemeinschaften gezwungen, in ihrem innerkirchlichen Handeln die Vorschriften der Verordnung anzuwenden, soweit sie nicht im Zeitpunkt des Inkrafttretens der Verordnung umfassende eigene Datenschutzregelungen anwenden und diese mit der Verordnung in Einklang bringen. Damit wird die formal weiter geltende kirchliche Regelungsbefugnis vollständig entwertet und ausgehöhlt. Wie auch bisher im deutschen Staatskirchenrecht angenommen, besteht ein Regelungsbedürfnis in Bezug auf die Kirchen allenfalls insoweit, als den Kirchen aufgegeben werden kann, ein gleichwertiges Datenschutzrecht sicherzustellen. Ein "Einklang" im Sinne einer inhaltlichen Übereinstimmung mit der Datenschutzgrundverordnung ist jedoch weder erforderlich noch mit der Verfassungsgarantie des kirchlichen Selbstbestimmungsrechts (Artikel 140 GG in Verbindung mit Artikel 137 Absatz 3 der Weimarer Reichsverfassung) zu vereinbaren.

- EU  
R
85. Kritisch sieht der Bundesrat die Vielzahl der Ermächtigungen der Kommission zum Erlass von Durchführungsrechtsakten. Mit Artikel 86 des Verordnungsvorschlags sollen der Kommission umfangreiche Befugnisse eingeräumt werden, delegierte Rechtsakte zu erlassen. Hier ist zum einen fraglich, ob sich alle Regelungsmöglichkeiten der Kommission auf "nicht wesentliche" Vorschriften im Sinne von Artikel 290 Absatz 1 AEUV beziehen. Zum anderen führt die weitreichende Delegation von Regelungsbefugnissen auf die Kommission dazu, dass die praktische Umsetzung der Verordnung in vielen Bereichen zunächst ein Tätigwerden der Kommission voraussetzt. Bis dahin sind die entsprechenden Regelungen für Bürgerinnen und Bürger, Unternehmen und auch für öffentliche Stellen kaum praktisch und rechtssicher anzuwenden.
- EU  
In
86. Unbeschadet grundsätzlicher Subsidiaritätsvorbehalte zur Grundstruktur des Regelungsvorschlags fordert der Bundesrat daher im Hinblick auf die Anforderungen des Artikel 290 Absatz 1 AEUV und die Erhaltung nationaler Regelungsspielräume grundlegende Abstriche bei den in mehr als 25 Vorschriften vorgesehenen Ermächtigungen zum Erlass delegierter Rechtsakte. Andernfalls bleiben wesentliche Fragen des Schutzes der informationellen

Selbstbestimmung wenig transparenten Verfahren überlassen, die im Wesentlichen von Initiativen der Kommission abhängen. Bei den betroffenen Vorschriften handelt es sich um grundlegende materiell- und verfahrensrechtliche Regelungen des Verordnungsvorschlags, also wesentliche Bestimmungen, die nach Artikel 290 Absatz 1 AEUV in der Verordnung selbst zu regeln wären. Außerdem sind Ermächtigungen für delegierte Rechtsakte dort widersprüchlich, wo die Verordnung den Mitgliedstaaten Befugnisse einräumen soll, eigene Regelungen "in den Grenzen dieser Verordnung" zu treffen.

- EU  
In  
(bei  
Annahme  
entfällt  
Ziffer 90)
87. Die in Artikeln 81 Absatz 3, 82 Absatz 3 und 83 Absatz 3 enthaltenen Ermächtigungen sollten daher entfallen.
- EU  
AV
88. In den Artikeln 81, 82 und 84 wird den Mitgliedstaaten die Befugnis eingeräumt, Regelungen "in den Grenzen" dieser Verordnung zu treffen.
- EU  
AV  
In
- [EU  
AV]
89. Gleichzeitig ist klarzustellen, dass nationale Regelungen nicht nur als Konkretisierungen auf der Ebene des durch die Verordnung geregelten Datenschutzniveaus zulässig sind, sondern dass [im Interesse des Datenschutzes] Regelungen der Mitgliedstaaten auch weitergehende datenschutzrechtliche Anforderungen begründen können.
- AV
90. Die Ermächtigung der Kommission, nach den Artikeln 81 und 82 delegierte Rechtsakte für besondere Datenverarbeitungssituationen zu erlassen, sollte auf die Mitgliedstaaten beschränkt werden, die die betreffenden Bereiche nicht selbst geregelt haben.
- EU  
In
91. Der Bundesrat bedauert, dass der Verordnungsvorschlag wichtige Fragen eines zukunftsfähigen Datenschutzkonzepts ungelöst lässt oder ausklammert.
- EU  
In
92. Für die in der Informationsgesellschaft zunehmend bedeutsamen Zertifizierungsverfahren verbleibt es bei bloßen unverbindlichen Förderungsverpflichtungen, ohne den Rechtsrahmen und die Rechtsfolgen solcher Verfahren einschließlich etwaiger Anreizmechanismen näher zu entwickeln.

- EU  
In
93. Ebenso beschränkt sich der Lösungsvorschlag für die Datenübermittlung entgegen mehrfacher Forderungen des Bundesrates und der Wirtschaft auf bloße Verfahrensregelungen über gemeinsame Verantwortlichkeiten (Artikel 24 des Verordnungsvorschlags), ohne aber die für den Datenverkehr innerhalb verbundener Unternehmen wesentlichen materiellen Verarbeitungsanforderungen zu modifizieren.
- EU  
In
94. Der Verordnungsvorschlag enthält außerdem keine Übergangsregelung, die hinreichenden rechtsstaatlichen Vertrauensschutz gewährleistet. Erwägungsgrund 134 und Artikel 91 Absatz 2 legen vielmehr nahe, dass sämtliche Datenverarbeitungsverfahren, für die keine förmlichen Genehmigungen der Aufsichtsbehörde nach Maßgabe der geltenden Datenschutzrichtlinie vorliegen, zwei Jahre nach dem Inkrafttreten der Verordnung den geänderten formellen und materiellen Anforderungen anzupassen sind. Angesichts der im geltenden Recht auf wenige Ausnahmesituationen beschränkten behördlichen Genehmigungspflichten ist daher von umfassenden und hohe Kosten auslösenden Anpassungserfordernissen für sämtliche öffentlichen und nichtöffentlichen Stellen auszugehen, die auch laufende, vielfach von Aufsichtsbehörden überprüfte oder zumindest mit diesen abgestimmte Datenverarbeitungsverfahren betreffen. Angesichts des schon durch die geltende Datenschutzrichtlinie gewährleisteten Schutzniveaus sollte daher im weiteren Verfahren überprüft werden, ob die Anwendung der Neuregelungen unter Gewährung von Anpassungszeiten auf nach Inkrafttreten der Verordnung begonnene Datenverarbeitungsverfahren beschränkt werden kann.

#### Vorlagenbezogene Vertreterbenennung

- EU  
In
95. Der Bundesrat benennt gemäß § 6 Absatz 1 EUZBLG i. V. m. Abschnitt I der Bund-Länder-Vereinbarung für die Beratungen der Vorlage in den Gremien des Rates

einen Vertreter des Freistaates

Bayern,

Bayerisches Staatsministerium des Innern

(MR Michael Will).

Begründung (nur gegenüber dem Plenum):

Infolge der Zusammenlegung von Arbeitsgruppen des Rates der EU wird in der Arbeitsgruppe "Informationsaustausch und Datenschutz" nicht nur der Vorschlag der Kommission 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 (Datenschutz-Richtlinie) beraten, sondern auch der Vorschlag der Kommission für eine Verordnung des Europäischen Parlaments und des Rates zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr (Datenschutz-Grundverordnung). Folglich beziehen sich die Beratungen nicht nur auf den polizeilichen Bereich, sondern auch auf das allgemeine Datenschutzrecht.

Der Bundesrat hat Herrn LKD Bernd Christ, Ministerium für Inneres und Kommunales des Landes Nordrhein-Westfalen, zum Ländervertreter in dieser Arbeitsgruppe benannt. Nordrhein-Westfalen nimmt daher die Interessen der Länder in den Beratungen zum polizeilichen Datenschutz wahr. Im Hinblick auf den allgemeinen Datenschutz wären die Länderinteressen daher in der Ratsarbeitsgruppe nicht repräsentiert. Es empfiehlt sich daher, dass der Bundesrat begrenzt auf die Beratungen zur vorgeschlagenen Datenschutz-Grundverordnung einen weiteren Bundesratsbeauftragten benennt.

Direktzuleitung der Stellungnahme

EU  
AV  
In  
R

96. Der Bundesrat übermittelt diese Stellungnahme direkt an die Kommission.