ARTIKEL-29-DATENSCHUTZGRUPPE

00530/12/DE
WP 191

Stellungnahme 01/2012 zu den Reformvorschlägen im Bereich des Datenschutzes

Angenommen am 23. März 2012

Inhaltsverzeichnis

Einleitung

Die Artikel-29-Datenschutzgruppe (Datenschutzgruppe oder WP29) begrüßt die von der Europäischen Kommission angenommenen Vorschläge, die darauf gerichtet sind, die Position der betroffenen Person zu stärken, den für die Verarbeitung Verantwortlichen stärker in die Verantwortung zu nehmen und die Stellung der Aufsichtsbehörden auf nationaler und internationaler Ebene zu verbessern. Bei weiterer Verbesserung können die vorgeschlagenen Vorschriften einen deutlichen Abbau der bestehenden rechtlichen Fragmentierung bewirken und den Datenschutz europaweit stärken.

Die Datenschutzgruppe begrüßt insbesondere die Aufnahme von Bestimmungen, die dem für die Verarbeitung Verantwortlichen Anreize bieten, von Beginn an in vernünftigen Datenschutz zu investieren (Datenschutz-Folgenabschätzungen, Datenschutz durch Technik und datenschutzfreundliche Voreinstellungen). Die Vorschläge weisen den mit der Verarbeitung personenbezogener Daten Befassten während des gesamten Lebenszyklus der Daten eine klare Verantwortung und Rechenschaftspflicht zu.

Die Datenschutzgruppe unterstreicht die Bedeutung der Bestimmungen, mit denen – insbesondere durch die Präzisierung des Begriffs „Einwilligung“, die Einführung eines allgemeinen Transparenzgrundsatzes und verbesserte Rechtsschutzmechanismen – die Rechte der betroffenen Person klargestellt und gestärkt werden sollen. Darüber hinaus wird die Einführung einer Meldepflicht für Verletzungen des Schutzes personenbezogener Daten und die damit einhergehende Vereinheitlichung in allen Bereichen sehr positiv eingeschätzt.

Die Datenschutzgruppe begrüßt ferner, dass die Vorschläge die Befugnisse und Zuständigkeiten der Aufsichtsbehörden harmonisieren, damit diese sowohl allein als auch gemeinsam die Einhaltung der Vorschriften wirksamer gewährleisten und nötigenfalls durchsetzen können, etwa durch Verhängung hoher Geldbußen.

Trotz ihrer grundsätzlich positiven Haltung gegenüber der vorgeschlagenen Verordnung ist die Datenschutzgruppe der Ansicht, dass der Vorschlag in Teilen präzisierungs- und verbesserungsbedürftig ist. Im Hinblick auf die Richtlinie für den Datenschutz im Bereich der Polizei und Justiz ist die Datenschutzgruppe von dem mangelnden Ehrgeiz der Kommission enttäuscht und fordert nachdrücklich strengere Vorschriften.

Die Datenschutzgruppe hat beide Vorschläge sorgfältig analysiert und legt mit dieser Stellungnahme ihre erste allgemeine Reaktion darauf vor. In der Stellungnahme werden Problembereiche hervorgehoben und gegebenenfalls Verbesserungen vorgeschlagen. Die Datenschutzgruppe wird künftig möglicherweise noch weitere Stellungnahmen zu bestimmten Vorschriften oder Aspekten der Vorschläge vorlegen.

Die Datenschutzgruppe fordert den Rat und die Mitglieder des Europäischen Parlaments auf, die Gelegenheit zu nutzen, um beide Vorschläge zu verbessern und den Schutz personenbezogener Daten in der Europäischen Union zu stärken.

Allgemeine Bemerkungen

Die Verordnung erfüllt den Anspruch, der zunehmenden Bedeutung des Datenschutzes in der Rechtsordnung der EU Rechnung zu tragen (Artikel 16 des Vertrags, Artikel 8 der Charta).

Sie bewahrt und stärkt die Grundprinzipien des Datenschutzes, erlegt den für die Verarbeitung Verantwortlichen und Auftragsverarbeitern klare und einheitliche Verpflichtungen auf, erleichtert den freien Verkehr personenbezogener Daten und stärkt den Rechtsrahmen für eine einheitliche Anwendung der Rechtsvorschriften durch die Datenschutzbehörden, deren Befugnisse erweitert worden sind.

Die Datenschutzgruppe ist enttäuscht, dass ihre Ansichten zu einem umfassenden Rechtsrahmen nicht zur Vorlage eines einheitlichen Rechtsinstruments geführt haben. Die Datenschutzgruppe nimmt zur Kenntnis, dass sich die Kommission aufgrund politischer Zwänge entschlossen hat, einen getrennten Vorschlag für eine Richtlinie für den Bereich der Polizei und Strafjustiz vorzulegen. Umso nötiger ist daher ein hohes Maß an einheitlichen Datenschutzstandards, die auch auf diesen Bereich anwendbar sind. In jedem Fall muss klar sein, dass die neue Richtlinie nicht dazu führen darf, dass Mitgliedstaaten ihre gegenwärtigen Datenschutzstandards für die Polizei und die Strafjustiz lockern. Zudem muss der neue Rechtsrahmen in Einklang mit anderen internationalen Abkommen wie dem Übereinkommen Nr. 108 des Europarates zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten und seinem Zusatzprotokoll stehen. Die Datenschutzgruppe schlägt vor, in den Erwägungsgründen der Verordnung und der Richtlinie eindeutig auf das Übereinkommen Nr. 108 und sein Zusatzprotokoll Bezug zu nehmen.

In früheren Stellungnahmen hat die Datenschutzgruppe die Notwendigkeit eines umfassenden Rechtsrahmens betont. Von diesem Standpunkt aus betrachtet, ist der geringere Anspruch der Richtlinie im Vergleich zur Verordnung enttäuschend. Dass zwei Rechtsinstrumente vorgelegt worden sind, bedeutet nicht notwendigerweise, dass ein umfassender Rechtsrahmen nicht mehr möglich ist, solange das Ziel – ein hohes Datenschutzniveau für die europäischen Bürger auf breiter Front zu erreichen – dasselbe bleibt und die Rechtsinstrumente einen gemeinsamen Ansatz verfolgen, etwa im Hinblick auf die Grundsätze des Datenschutzes, die Rechte der betroffenen Person und die Pflichten des für die Verarbeitung Verantwortlichen und des Auftragsverarbeiters.

Vonseiten des europäischen Gesetzgebers sind während des Gesetzgebungsverfahrens ernsthafte Anstrengungen erforderlich, um die materiellrechtlichen Bestimmungen der Richtlinie denen der Verordnung anzunähern und beide Wortlaute in Einklang zu bringen.

Darüber hinaus sollten für die Organe der EU dieselben Vorschriften wie für die der Mitgliedstaaten gelten. Um eine wirklich umfassende Reform zu erreichen, muss deshalb der gegenwärtig in der Verordnung (EG) Nr. 45/2001 verankerte Datenschutzrechtsrahmen für die Organe der Europäischen Union zum Zeitpunkt des Inkrafttretens der Verordnung an diese angeglichen werden.

Dasselbe gilt auch für die derzeitigen spezifischen Datenverarbeitungsvorschriften in der ehemaligen dritten Säule der EU, etwa in Bezug auf EU-Einrichtungen wie Europol und Eurojust. Die Datenschutzgruppe nimmt zur Kenntnis, dass es möglicherweise schwierig ist, einen Vorschlag für eine vollständige Überarbeitung des derzeitigen Besitzstands zu unterbreiten, und ist gleichzeitig davon überzeugt, dass für die gesamte Datenverarbeitung in diesem Bereich, darunter auch in den EU-Einrichtungen, letztendlich dasselbe hohe Datenschutzniveau gelten muss.

In Anbetracht dessen nimmt die Datenschutzgruppe die Zusage der Kommission zur Kenntnis, weitere Rechtsinstrumente zu überarbeiten, um innerhalb von drei Jahren

festzustellen, wo Angleichungsbedarf besteht. Die Datenschutzgruppe empfiehlt dem Gesetzgeber, eine wesentlich kürzere Frist zu setzen, und fordert die Kommission auf, solche Vorschläge tatsächlich zu unterbreiten. Gleichzeitig erkennt die Datenschutzgruppe an, dass die geltenden Datenschutzregelungen bei einigen bestehenden Instrumenten und Einrichtungen weitreichender als die vorgeschlagene Richtlinie sind. Wie bereits im Hinblick auf die Mitgliedstaaten, die sich in einer vergleichbaren Lage befinden, hervorgehoben wurde, darf die Anpassung der geltenden Vorschriften an die Richtlinie auf keinen Fall zu einer Lockerung geltender Datenschutzstandards führen.

Darüber hinaus bedauert die Datenschutzgruppe, dass weder die Verordnung noch die Richtlinie die Erfassung und Weitergabe von für die Strafverfolgung bestimmten Daten durch nicht-öffentliche Stellen oder andere Behörden als Strafverfolgungsbehörden sowie die anschließende Nutzung dieser Daten durch die Strafverfolgungsbehörden aufgreift. In den vergangenen zehn Jahren hat sich mehrfach gezeigt (etwa bei PNR-Daten oder der Vorratsspeicherung von Telekommunikationsdaten), dass strenge Vorgaben nötig sind, vor allem, wenn die Verarbeitung routinemäßig erfolgt. Umgekehrt gilt genau dasselbe: Regeln zur Gewährleistung des Datenschutzes sind ebenso notwendig, wenn Informationen von Strafverfolgungsbehörden oder anderen „zuständigen“ Behörden an den privaten Sektor oder andere öffentliche Stellen weitergegeben werden.

Schließlich nimmt die Datenschutzgruppe im Hinblick auf beide vorgeschlagene Instrumente mit Besorgnis zur Kenntnis, in welchem Maße die Kommission befugt ist, delegierte Rechtsakte und Durchführungsrechtsakte zu erlassen. Die Datenschutzgruppe erkennt zwar an, dass es möglich sein muss, bestimmte Fragen zu einem späteren Zeitpunkt ausführlicher zu behandeln, ist jedoch der Auffassung, dass dies beispielsweise bei Vorschriften zur Meldung von Verletzungen des Schutzes personenbezogener Daten nicht der Fall ist. Um Rechtssicherheit zu gewährleisten, sind, wie in Artikel 290 AEUV vorgesehen, wesentliche Elemente in die Verordnung selbst einzufügen.

Bewertung der Verordnung

Positive Aspekte

- Insgesamt bietet die Verordnung durch präzisere Begriffsbestimmungen und Vorschriften, die auf eine einheitlichere Anwendung der Rechtsvorschriften abzielen und somit den freien Verkehr von Daten erleichtern, mehr Klarheit.

- Die Verordnung stärkt die Rechte natürlicher Personen. Beispiele hierfür sind mehr Transparenz, bessere Kontrolle der Verarbeitung, Datenminimierung, besondere Vorschriften für die Verarbeitung personenbezogener Daten von Kindern, Stärkung des Rechts auf Auskunft über Daten, Stärkung des Widerspruchsrechts, Recht auf Datenportabilität, Stärkung des Rechts auf Löschung von Daten („Recht auf Vergessenwerden“) und Stärkung des Rechts auf Rechtsschutz durch die Datenschutzbehörden als auch auf gerichtlichen Rechtsschutz.

- Für die für die Verarbeitung Verantwortlichen bringt die Verordnung Vereinfachung und mehr Kohärenz, eine stärkere Fokussierung auf ihre Rechenschaftspflicht für verarbeitete Daten und die Pflicht, dies anhand von Datenschutz durch Technik und

datenschutzfreundliche Voreinstellungen, Datenschutz-Folgenabschätzungen, durch die Benennung eines Datenschutzbeauftragten, die Einhaltung der Meldepflichten für Verletzungen des Schutzes personenbezogener Daten und ein vorbeugendes Herangehen an grenzüberschreitende Datenübermittlungen nachzuweisen. Darüber hinaus werden verbindliche unternehmensinterne Vorschriften ausdrücklich als Instrument zur Handhabung grenzüberschreitender Datenübertragungen anerkannt.

- Es wird eine Rechtsgrundlage für die für Auftragsverarbeiter geltenden Datensicherheitsvorschriften geschaffen. Außerdem werden Auftragsverarbeiter verpflichtet, für bestimmte Verarbeitungsvorgänge die Pflichten des für die Verarbeitung Verantwortlichen zu übernehmen, wenn der Auftragsverarbeiter dabei über die Anweisungen des für die Verarbeitung Verantwortlichen hinausgeht (relevant für Cloud-Anbieter).

- Die Verordnung stärkt die Unabhängigkeit und die Befugnisse von Datenschutzbehörden. Beispiele dafür sind die Befugnis zur Verhängung von Geldbußen, die Pflicht zur Zurateziehung bei legislativen Maßnahmen sowie Bestimmungen zur Gewährleistung einer einheitlichen Anwendung und nötigenfalls Durchsetzung der Rechtsvorschriften, insbesondere durch das Kohärenzverfahren.

Die Rolle der Kommission

Die Datenschutzgruppe hat ernsthafte Vorbehalte im Hinblick auf den Umfang der Befugnisse der Kommission, delegierte Rechtsakte und Durchführungsrechtsakte zu erlassen. Dies ist von besonderer Bedeutung, weil es um ein Grundrecht geht. Selbstverständlich kann es erforderlich sein, bestimmte Fragen in delegierten Rechtsakten oder Durchführungsrechtsakten zu regeln. Allerdings sind nicht alle in den Artikeln 86 und 87 aufgeführten Punkte Detailfragen. Einige Bestimmungen der Verordnung (etwa die zur Meldung von Verletzungen des Schutzes personenbezogener Daten, zur Amtshilfe, zur Kohärenz und zu Beschränkungen des Rechts auf Unterrichtung und Auskunft im Zusammenhang mit der Datenverarbeitung zu historischen oder statistischen Zwecken sowie zum Zwecke der wissenschaftlichen Forschung) sind nicht ohne delegierte Rechtsakte oder Durchführungsrechtsakte anwendbar. Darüber hinaus betreffen andere delegierte Rechtsakte den sachlichen Anwendungsbereich der Verordnung, etwa Artikel 6 Absatz 1 Buchstabe f in Verbindung mit Artikel 6 Absatz 5, wonach die Kommission befugt ist, die „berechtigten Interessen“ des für die Verarbeitung Verantwortlichen für verschiedene Verarbeitungssituationen und Bereiche zu definieren. Zur Gewährleistung von Rechtssicherheit sind, wie in Artikel 290 AEUV vorgesehen, wesentliche Elemente in die Verordnung selbst aufzunehmen.

In der Praxis kann sich der Erlass von delegierten Rechtsakten oder Durchführungsrechtsakten für eine Vielzahl von Artikeln über mehrere Jahre hinziehen. Dies könnte wiederum Rechtsunsicherheit für Auftragsverarbeiter und für die Verarbeitung Verantwortliche bedeuten, die eine rasche Umsetzung und konkrete Leitlinien erwarten. Die Datenschutzgruppe fordert die Kommission auf, zumindest darzulegen, welche delegierten Rechtsakte und Durchführungsrechtsakte sie kurz-, mittel- und langfristig zu erlassen beabsichtigt.

Ungeachtet der Rolle der Kommission als Hüterin der Verträge hat die Datenschutzgruppe auch starke Vorbehalte im Hinblick auf die der Kommission in Einzelfällen, die im Rahmen des Kohärenzverfahrens behandelt wurden, zugedachte Funktion, weil diese einen Eingriff in die unabhängige Stellung der Datenschutzbehörden bedeutet. Wenn eine Sache vom Europäischen Datenschutzausschuss im Rahmen des Kohärenzverfahrens behandelt wird oder wurde, sollte die Kommission Gelegenheit zur rechtlichen Beurteilung haben, prinzipiell jedoch nicht eingreifen. Es könnte ein Verfahren in Betracht gezogen werden, wonach die Kommission und der Europäische Datenschutzausschuss den Europäischen Gerichtshof um eine Stellungnahme zur Auslegung der Verordnung ersuchen können.

Die Rolle der europäischen Datenschutzbehörden in der Politikgestaltung

Die Datenschutzgruppe ist der Auffassung, dass die wichtige Rolle, die sie bislang bei der Politikgestaltung gespielt hat und die der Europäische Datenschutzausschuss künftig übernehmen kann (etwa durch die Herausgabe von Leitlinien oder Empfehlungen), in den Vorschlägen zum Ausdruck kommen sollte.

In Artikel 66 heißt es, dass der Europäische Datenschutzausschuss von sich aus oder auf Ersuchen der Kommission in allen Fragen, die im Zusammenhang mit dem Schutz personenbezogener Daten stehen, berät und die Anwendung der Verordnung betreffende Fragen prüft. Nach dem Verständnis der Datenschutzgruppe schließt dies auch andere Rechtsvorschriften ein. Sie schlägt daher vor, Artikel 66 Absatz 1 Buchstabe a um folgenden Wortlaut zu erweitern: *„… sowie zu jeglichen weiteren oder besonderen Maßnahmen zum Schutz der Rechte und Freiheiten natürlicher Personen bei der Verarbeitung personenbezogener Daten und zu jeglichen anderen vorgeschlagenen Maßnahmen der Union, die diese Rechte und Freiheiten berühren.“*

Darüber hinaus schlägt die Datenschutzgruppe vor, nicht nur der Europäischen Kommission, sondern auch dem Europäischen Parlament die Möglichkeit einzuräumen, den Europäischen Datenschutzausschuss um Stellungnahme zu ersuchen, indem in Artikel 66 Absatz 1 Buchstabe b *„und des Europäischen Parlaments“* eingefügt wird.

Darüber hinaus empfiehlt die Datenschutzgruppe nachdrücklich, eine Bestimmung aufzunehmen, wonach die Kommission in jedem Fall verpflichtet ist, bei Angemessenheitsbeschlüssen (Artikel 41) und im Zusammenhang mit Standarddatenschutzklauseln (Artikel 42) den Europäischen Datenschutzausschuss zurate zu ziehen und zu Verhaltensregeln auf europäischer Ebene (Artikel 38) den Rat und die Zustimmung des Europäischen Datenschutzausschusses einzuholen. In jedem Fall sollte in die Artikel 86 und 87 eine Verpflichtung der Kommission, den Europäischen Datenausschuss zu allen delegierten Rechtsakten und Durchführungsrechtsakten zurate zu ziehen, aufgenommen werden.

Die nationalen Behörden sollten weiterhin Leitlinien und Empfehlungen erarbeiten können, die bei erheblichen Auswirkungen auf andere Mitgliedstaaten im Rahmen des Kohärenzverfahrens zu behandeln wären. Sie sollten außerdem in der Lage sein, die Entwicklung von Zertifizierungssiegeln und -zeichen, die dem Schutz natürlicher Personen dienen, zu überwachen.

Schwellenwerte für KMU

Die Datenschutzgruppe nimmt zur Kenntnis, dass in den Vorschlag für eine Verordnung Ausnahmen und Schwellenwerte aufgenommen wurden, um den Verwaltungsaufwand für Kleinst-, Klein- und mittlere Unternehmen (KKMU) zu begrenzen und die Auswirkungen auf diese Unternehmen zu lindern. Schwellenwerte enthalten die Bestimmungen zur Benennung eines Vertreters in der EU (Artikel 25), Dokumentation (Artikel 28 Absatz 4), Benennung von Datenschutzbeauftragten (Artikel 35 Absatz 1) und Verhängung von Geldbußen (Artikel 79 Absatz 3). Darüber hinaus sieht der Vorschlag delegierte Rechtsakte und Durchführungsrechtsakte vor, die es der Kommission ermöglichen, weitere Maßnahmen für KKMU zu ergreifen, so etwa in Artikel 12 Absatz 6 zu Verfahren und Vorkehrungen, damit die betroffene Person ihre Rechte ausüben kann, Artikel 14 Absatz 7 zur Information der betroffenen Person, Artikel 22 Absatz 4 zur Rechenschaftspflicht und Artikel 33 Absatz 6 zur Durchführung von Datenschutz-Folgenabschätzungen.

Die Datenschutzgruppe ist der Ansicht, dass betroffene Personen unabhängig davon, ob ihre Daten von einem KKMU oder einem Großunternehmen verarbeitet werden, denselben Schutz genießen sollten. Sie sieht jedoch ein, dass einige der vorgeschlagenen Verpflichtungen KKMU belasten könnten. Deshalb erkennt die Datenschutzgruppe die Gründe für die Einführung dieser Schwellenwerte zwar prinzipiell an, befürchtet allerdings, dass die Ausnahmen sowohl in der Praxis als auch im Hinblick auf den Schutz personenbezogener Daten zu widersprüchlichen und unerwünschten Ergebnissen führen. Sie hält Schwellenwerte, die Art und Umfang der Datenverarbeitung berücksichtigen für besser geeignet.

Auswirkungen auf den Haushalt und die Mittel

Die Datenschutzgruppe ist darüber erfreut, dass die Vorschläge den wichtigen Beitrag der Datenschutzbehörden zur Gewährleistung der Einhaltung der Vorschriften durch Erweiterung der Aufgaben der Datenschutzbehörden und des Europäischen Datenschutzausschusses anerkennen. Sie bezweifelt jedoch stark, dass die erheblichen Auswirkungen dieser erweiterten Aufgaben auf den Haushalt hinreichend erkannt worden sind. Um die Datenschutzbehörden und den Europäischen Datenschutzausschuss in die Lage zu versetzen, ihre Aufgaben einschließlich der Amtshilfe und der Zusammenarbeit im Rahmen des Kohärenzverfahrens wirksam zu erfüllen, müssen die Mitgliedstaaten dazu verpflichtet werden, die notwendigen finanziellen, personellen und technischen Ressourcen bereitzustellen.

Deshalb empfiehlt die Datenschutzgruppe nachdrücklich eine unabhängige umfassende Abschätzung des Kostenanstiegs, der aufgrund der gegenwärtigen Vorschläge auf die Datenschutzbehörden und den Europäischen Datenschutzbeauftragten (als Sekretariat des Europäischen Datenschutzausschusses) zukommt. Im Anschluss an diese Abschätzung sollte klargestellt werden, was unter „angemessenen personellen, technischen und finanziellen Ressourcen, Räumlichkeiten und […] der erforderlichen Infrastruktur“ der Datenschutzbehörden im Sinne von Artikel 47 Absatz 5 zu verstehen ist.

Die Datenschutzgruppe beabsichtigt, die Kommission in einem eigenen Schreiben auf den Zweck und die Rahmenbedingungen dieser Folgenabschätzung anzusprechen.

Allgemeine Bestimmungen

Anwendungsbereich

Gemäß Artikel 3 Absatz 2 findet die Verordnung auch Anwendung auf die Verarbeitung personenbezogener Daten von in der Union ansässigen betroffenen Personen durch einen nicht in der Union niedergelassenen für die Verarbeitung Verantwortlichen, wenn die Datenverarbeitung dazu dient, diesen Personen in der Union Waren oder Dienstleistungen anzubieten, oder der Beobachtung ihres Verhaltens dient.

Wenngleich in den Erwägungsgründen zu definieren versucht wird, was mit dem „Angebot von Waren und Dienstleistungen" und der „Beobachtung ihres Verhaltens" gemeint ist, erachtet die Datenschutzgruppe eine weitere Präzisierung dieser Begriffe für hilfreich.

Es sollte klargestellt werden, dass das „Angebot von Waren und Dienstleistungen" auch kostenlose Dienstleistungen umfasst (bei denen die betreffenden Personen die Dienstleistungen faktisch durch die Preisgabe personenbezogener Daten bezahlen). Die Datenschutzgruppe schlägt daher vor, in etwa folgenden Wortlaut einzufügen: *„einschließlich Dienstleistungen, die ohne finanzielle Kosten für diese Personen erbracht werden"*.

Darüber hinaus erweckt Erwägungsgrund 21 den Eindruck, als sei die „Beobachtung des Verhaltens" lediglich mit der Nachvollziehung von Internetaktivitäten und dem Anlegen von Profilen verbunden. Die Datenschutzgruppe empfiehlt, den Wortlaut so abzuändern, dass auch Verarbeitungsvorgänge, bei denen der für die Verarbeitung Verantwortliche an sich keine Profile anlegt, unter Umständen eine „Beobachtung des Verhaltens" darstellen können, wenn sie zu Entscheidungen über eine betroffene Person führen oder die Analyse oder Vorhersage ihrer persönlichen Vorlieben, Verhaltensweisen und Einstellungen beinhalten.

Betroffene Person und personenbezogene Daten

Die Datenschutzgruppe begrüßt die Definition des Begriffs „betroffene Person" in Artikel 4 Absatz 1 der vorgeschlagenen Verordnung, wonach eine *„betroffene Person eine bestimmte natürliche Person oder eine natürliche Person, die […] bestimmt werden kann"*, ist. Eine natürliche Person kann bestimmt werden, wenn sie in einer Personengruppe von allen anderen Mitgliedern der Gruppe unterschieden und somit anders behandelt werden kann Dies wurde bereits in der Stellungnahme der Datenschutzgruppe zum Begriff „personenbezogene Daten" (WP136) dargelegt. In Erwägungsgrund 23 sollte daher klargestellt werden, dass der Begriff der Bestimmbarkeit auch eine derartige Aussonderung umfasst.

Erwägungsgrund 24 sieht in Bezug auf die Definition personenbezogener Daten vor, dass Kennnummern, Standortdaten, Online-Kennungen oder sonstige Elemente nicht zwangsläufig und unter allen Umständen als personenbezogene Daten zu betrachten sind. In der jetzigen Fassung könnte der letzte Satz zu einer zu engen Auslegung des Begriffs personenbezogener Daten etwa in Bezug auf IP-Adressen oder Cookie-IDs führen. Die Datenschutzgruppe erinnert daran, dass personenbezogene Daten solche Daten sind, die sich auf eine bestimmbare Person beziehen. *„Daten beziehen sich auf eine Person, wenn sie die Identität, die Merkmale oder das Verhalten dieser Person betreffen oder wenn sie verwendet werden, um die Art festzulegen oder zu beeinflussen, in der die Person behandelt oder beurteilt*

wird.“[1] Die Datenschutzgruppe hat bereits in ihrer Stellungnahme WP136 verschiedene Szenarien entwickelt, die aufzeigen, warum IP-Adressen als Daten einzustufen sind, die sich auf eine bestimmbare Personen beziehen, *„vor allem in Fällen, in denen der Zweck der Verarbeitung von IP-Adressen in der Identifizierung der Computernutzer besteht (beispielsweise durch Inhaber von Urheberrechten zur strafrechtlichen Verfolgung von Computernutzern wegen Verletzung von Rechten an geistigem Eigentum) […].“* In diesem Fall wie auch im Fall von Cookies geht der für die Verarbeitung Verantwortliche vom Vorhandensein der Mittel aus, die zur Identifizierung und besonderen Behandlung der betreffenden Personen „vernünftigerweise eingesetzt werden könnten“.[2] Die Datenschutzgruppe schlägt daher vor, Erwägungsgrund 24 entsprechend abzuändern.

Biometrische Daten

Die Datenschutzgruppe begrüßt die Einführung einer Definition für biometrische Daten in Artikel 4 Absatz 11 der Verordnung. Sie sieht den gegenwärtigen Wortlaut, der die Möglichkeit der eindeutigen Identifizierung eines Menschen in den Mittelpunkt stellt, jedoch skeptisch. Biometrische Daten werden nicht nur zur Identifizierung, sondern auch zur Authentifizierung (Bestätigung der Identität ohne tatsächliche Identifizierung der betreffenden Person) verwendet. Anstatt in den Mittelpunkt zu stellen, was biometrische Daten ermöglichen, sollte sich die Definition darauf konzentrieren, welche Arten von Daten als biometrische Daten einzustufen sind. Die Datenschutzgruppe schlägt daher vor, in Artikel 4 Absatz 11 die Formulierung *„… die dessen eindeutige Identifizierung ermöglichen, …“* durch *„… die für jede Person einzigartig sind, …“* zu ersetzen.

Hauptniederlassung

Die Art und Weise, wie bestimmt wird, wo ein multinationales EU- oder Nicht-EU-Unternehmen seine Hauptniederlassung im Sinne von Artikel 4 Absatz 13 und Erwägungsgrund 27 hat, bedarf einer weiteren Präzisierung, auch für Fälle, in denen einzelne Firmen des Unternehmens in unterschiedlichen Branchen tätig sind. So könnte etwa der „beherrschende Einfluss“ einer Niederlassung auf Verarbeitungsvorgänge im Hinblick auf die Umsetzung der Vorschriften zum Schutz personenbezogener Daten einfließen.

Die Datenschutzgruppe nimmt zur Kenntnis, dass Artikel 4 des Entwurfs der Verordnung unterschiedliche Definitionen für Firmen enthält, die nicht eindeutig voneinander abgegrenzt sind. Einerseits beziehen sich die Begriffe „für die Verarbeitung Verantwortlicher“ und „Hauptniederlassung“ darauf, wo relevante Entscheidungen über die Datenverarbeitung getroffen werden, während es andererseits bei den Definitionen für „Unternehmen“ und „Unternehmensgruppe“ um wirtschaftliche Tätigkeit und die Unternehmensstruktur geht.

Ein weiterer Begriff wird für Auftragsverarbeiter eingeführt, bei denen als Hauptniederlassung der Ort der „Hauptverwaltung“ gelten soll. Ferner ist nach Kapitel VIII über Rechtsbehelfe, Haftung und Sanktionen für Klagen gegen einen für die Verarbeitung Verantwortlichen oder einen Auftragsverarbeiter ein Gericht am Ort einer beliebigen Niederlassung zuständig, unabhängig davon, ob die Niederlassung überhaupt etwas mit der betreffenden Verarbeitung zu tun hat (sie könnte von anderen EU-Niederlassungen des betreffenden für die Verarbeitung Verantwortlichen bzw. Auftragsverarbeiters sogar rechtlich völlig unabhängig sein).

---

1 WP136, S. 11.
2 WP136, S. 19.

Nach Ansicht der Datenschutzgruppe überschneiden sich diese Definitionen und sollten daher präzisiert werden. In jedem Fall sollte der Zusammenhang zwischen der Hauptniederlassung und den Aufgaben des für die Verarbeitung Verantwortlichen klargestellt werden.

Die Definition der Hauptniederlassung scheint in erster Linie dazu gedacht zu sein, die für einen konkreten Fall oder ein konkretes Unternehmen federführende nationale Datenschutzbehörde zu bestimmen. Ein klares Verständnis des Begriffs „Hauptniederlassung“ ist von wesentlicher Bedeutung, da es sich entscheidend auf die Bestimmung der zuständigen Behörde im Sinne von Artikel 51 Absatz 2 auswirkt, sofern die Verarbeitung personenbezogener Daten im Rahmen der Tätigkeiten der Niederlassung eines für die Verarbeitung Verantwortlichen oder Auftragsverarbeiters in der Union stattfindet und der für die Verarbeitung Verantwortliche oder Auftragsverarbeiter Niederlassungen in mehr als einem Mitgliedstaat hat (siehe weiter unten auf Seite 28).

Pseudonymisierung

Nach Auffassung der Datenschutzgruppe sollte das Konzept der Pseudonymisierung in dem Instrument deutlicher dargelegt werden (beispielsweise durch eine Definition des Begriffs „pseudonymisierte Daten“ in Einklang mit der Definition von personenbezogenen Daten), weil es zur Verbesserung des Datenschutzes, etwa bei Datenschutz durch Technik und datenschutzfreundliche Voreinstellungen, beitragen kann. Die Datenschutzgruppe schlägt daher die Einführung einer grundsätzlichen Pflicht zur Anonymisierung oder Pseudonymisierung personenbezogener Daten vor, sofern dies entsprechend dem Zweck der Verarbeitung möglich und angemessen ist. Ein solcher Grundsatz könnte in Artikel 5 sowie im Rahmen des Datenschutzes durch Technik und datenschutzfreundliche Voreinstellungen in Artikel 23 verankert werden.

Datenschutz durch Technik und datenschutzfreundliche Voreinstellungen

Die Datenschutzgruppe begrüßt die Einführung des Datenschutzes durch Technik und datenschutzfreundliche Voreinstellungen in Artikel 23, rät jedoch zu einer weiteren Klarstellung seiner Bedeutung in einem Erwägungsgrund, etwa durch die Angabe, dass datenschutzfreundliche Merkmale von Produkten und Dienstleistungen automatisch aktiviert und entsprechende Verfahren während der Planung der Datenverarbeitung oder der Entwicklung eines Produktes angewandt werden müssen. Natürlich obliegt dem für die Verarbeitung Verantwortlichen der Nachweis, dass er bei seiner Verarbeitungstätigkeit die Konzepte des Datenschutzes durch Technik und datenschutzfreundliche Voreinstellungen, die geeignete Maßnahmen im Sinne von Artikel 22 Absatz 1 darstellen, berücksichtigt.

Die Datenschutzgruppe nimmt zur Kenntnis, dass die Kommission befugt ist, einschlägige technische Standards festzulegen. Die Datenschutzgruppe ist der festen Überzeugung, dass die Kommission den Europäischen Datenschutzausschuss und internationale Normungsorganisationen bei der Erarbeitung dieser technischen Standards einbeziehen und gegebenenfalls zurate ziehen sollte.

<u>Grundsatz des Zugangs der Öffentlichkeit zu Informationen</u>

Gemäß Erwägungsgrund 18 ermöglicht es die Verordnung, dass bei der Anwendung ihrer Vorschriften der Grundsatz des Zugangs der Öffentlichkeit zu amtlichen Dokumenten

berücksichtigt wird. Der Grundsatz des Zugangs der Öffentlichkeit zu amtlichen Dokumenten ist seit langem ein wichtiges Grundrecht und sollte deshalb nicht nur in einem Erwägungsgrund erwähnt, sondern auch in einem Artikel der Verordnung zum Ausdruck gebracht werden.

Weiterverarbeitung zu unvereinbaren Zwecken

Gemäß Artikel 6 Absatz 4 können Daten zu nicht mit dem ursprünglichen Zweck vereinbaren Zwecken weiterverarbeitet werden, wenn sich eine andere Rechtsgrundlage (ausgenommen das berechtigte Interesse des für die Verarbeitung Verantwortlichen) findet. Wenngleich die Datenschutzgruppe nicht in Frage stellt, dass eine Weiterverarbeitung von Daten zu anderen Zwecken möglich bleiben muss, eröffnet der gegenwärtige Wortlaut der vorgeschlagenen Bestimmung Möglichkeiten zur Weiterverarbeitung von Daten zu unvereinbaren Zwecken, die sowohl im öffentlichen als auch im privaten Sektor zu höchst unerwünschten Ergebnissen führen können, insbesondere wenn sie auf Buchstabe b (Erfüllung eines Vertrags) oder Buchstabe e (öffentliches Interesse) beruhen. Nach Ansicht der Datenschutzgruppe steht diese Bestimmung im Widerspruch zum allgemeinen Grundsatz der Zweckbindung, einem Schlüsselkonzept des Datenschutzes in Europa. Sie empfiehlt daher nachdrücklich, Artikel 6 Absatz 4 entweder zu streichen oder unter Bezugnahme auf Artikel 21 zu präzisieren. In diesem Zusammenhang macht die Datenschutzgruppe außerdem darauf aufmerksam, dass sie sich im Laufe des Jahres 2012, wie in ihrem Arbeitsprogramm 2012–2013 angekündigt, eingehender mit dem Thema „Vereinbarkeit der Nutzung“ befassen wird.

Ausnahmen für Behörden

Einer der Gründe für die Überarbeitung des Rechtsrahmens für den Datenschutz ist die Schaffung eines umfassenden Instrumentariums. Der Rechtsrahmen soll durch einheitliche Regeln für den öffentlichen wie den privaten Sektor die Rechtssicherheit der in den verschiedenen Bereichen angebotenen Datenschutzgarantien insbesondere für natürliche Personen verbessern.

Die Datenschutzgruppe hat bereits ihre Enttäuschung über den mangelnden Ehrgeiz im Bereich der Polizei und Justiz zum Ausdruck gebracht. Doch auch in der Verordnung selbst wird dem öffentlichen Sektor eine Sonderstellung eingeräumt. Die Datenschutzgruppe ist darüber besorgt, dass die Verordnung Behörden aus Gründen des öffentlichen Interesses mehrfach weitreichende Ausnahmen gewährt. Sie ist der Ansicht, dass weitreichende und nicht näher bestimmte Ausnahmen, die außerdem keine ausreichenden Garantien für den Schutz von natürlichen Personen bieten, nicht gerechtfertigt sind, und schlägt deshalb vor, in der Verordnung so weit wie möglich die besonderen öffentlichen Interessen zu benennen. Dies würde auch zu einer Harmonisierung innerhalb der EU beitragen.

Wie bereits ausgeführt, gewährt Artikel 6 Absatz 4 auch Behörden sehr weitreichende Möglichkeiten, den ursprünglichen Verarbeitungszweck durch einen unvereinbaren Zweck zu ersetzen. Darüber hinaus erlaubt Artikel 9 Absatz 2 Buchstabe g die Verarbeitung sensibler Daten für *„im öffentlichen Interesse“* liegende Aufgaben. Dasselbe gilt für die Ausnahmen nach Artikel 17 Absatz 5, insbesondere im Hinblick auf das öffentliche Interesse und die Interessen Dritter. Die Datenschutzgruppe empfiehlt, diese Ausnahme auf *„wesentliches öffentliches Interesse“* zu beschränken.

Ferner bietet Artikel 21 die Möglichkeit, Grundsätze des Datenschutzes und die Rechte der betroffenen Personen zu beschränken, und erweitert somit im Vergleich zur derzeitigen Situation die Beschränkungsmöglichkeiten, ohne ausreichende Garantien vorzusehen, die bei Inanspruchnahme des Artikels einzuhalten sind. Darüber hinaus kann Artikel 21 Absatz 1 Buchstabe c zum Schutz einer unbegrenzten Kategorie *„sonstiger öffentlicher Interessen"* in Anspruch genommen werden. Die Datenschutzgruppe hält dies für zu weit gefasst und rät daher dringend, in Artikel 21, Absatz 1 Buchstabe c die Formulierung *„sonstiger öffentlicher Interessen der Union oder eines Mitgliedstaats …"* zu streichen und die Bestimmung mit *„zum Schutz eines wichtigen wirtschaftlichen oder finanziellen Interesses …"* zu beginnen.

Nach Artikel 33 Absatz 5 sind Behörden von der Pflicht zur Durchführung von Datenschutz-Folgenabschätzungen ausgenommen, wenn die Verarbeitung aufgrund einer rechtlichen Verpflichtung erfolgt. Nach Ansicht der Datenschutzgruppe besteht die einzige in diesem Zusammenhang gerechtfertigte Ausnahme darin, dass eine Datenschutz-Folgenabschätzung im Gesetzgebungsverfahren bereits durchgeführt wurde.

Die Datenschutzgruppe ist der festen Überzeugung, dass grundsätzliche Ausnahmen für den öffentlichen Sektor nicht gerechtfertigt sind und den umfassenden Rechtsrahmen beeinträchtigen. Sie rät deshalb nachdrücklich dazu, den öffentlichen und den privaten Sektor nach Möglichkeit gleich zu behandeln und zur Einhaltung derselben Grundregeln zu verpflichten. Allerdings muss auch verhindert werden, dass der neue Rechtsrahmen dazu führt, dass das in den Mitgliedstaaten in verschiedenen Bereichen bereits erreichte Datenschutzniveau sinkt. Vor allem im öffentlichen Sektor bestehen aufgrund konstitutioneller und rechtlicher Traditionen und Entwicklungen Unterschiede im Datenschutzniveau. Der neue Rechtsrahmen sollte daher zu einheitlich hohen Standards in diesem Bereich führen und gleichzeitig den Mitgliedstaaten weitere Regelungen (wie bereits in Kapitel IX vorgesehen) ermöglichen, solange diese der Verordnung nicht zuwiderlaufen. Sie könnten also die Verordnung auch ergänzen.

Minderjährige

Die Datenschutzgruppe erkennt die Bedeutung des Grundsatzes des „Kindeswohls" und des Konzepts des progressiven Schutzes nach Reifegrad an.[3] Wenngleich die Verordnung die Vorschriften zur Gültigkeit, zum Zustandekommen oder zu den Rechtsfolgen eines Vertrags mit einem Kind nach dem allgemeinen Vertragsrecht der Mitgliedstaaten unberührt lässt, begrüßt die Datenschutzgruppe, dass nach Artikel 8 Absatz 1 die Verarbeitung personenbezogener Daten eines Kindes, dem Dienste der Informationsgesellschaft angeboten werden, bis zum vollendeten dreizehnten Lebensjahr nur dann rechtmäßig ist, wenn und insoweit die Einwilligung hierzu durch die Eltern oder den Vormund des Kindes oder mit deren Zustimmung erteilt wird.

Die Datenschutzgruppe ist sich der mit der Harmonisierung der Altersgrenzen in einem solchen Instrument verbundenen Schwierigkeiten bewusst und sieht ein, dass in rein nationalen Fällen das innerstaatliche Recht der Mitgliedstaaten gelten soll. Die Datenschutzgruppe schlägt jedoch vor, die in der Verordnung eingeführte Mindestregelung für die Behandlung Minderjähriger auszuweiten, da es neben Dienstangeboten der Informationsgesellschaft weitere Situationen gibt, für die Sonderregelungen denkbar sind.

[3] Siehe Stellungnahme 2/2009 zum Schutz der personenbezogenen Daten von Kindern (WP 160) und Arbeitspapier 1/2008 zum Schutz der personenbezogenen Daten von Kindern (WP 147).

Grundsätzlich fehlen in der Verordnung Bestimmungen, die regeln, wie Rechte vertretungsweise ausgeübt werden können, und zwar nicht nur bei Minderjährigen, sondern auch bei nicht geschäftsfähigen Personen oder durch anwaltliche Vertretung.

Recht auf Vergessenwerden

Die Datenschutzgruppe begrüßt die Aufnahme des Rechtes auf Vergessenwerden und auf Löschung als Mittel zur Verbesserung des Einflusses betroffener Personen auf den Umgang mit ihren personenbezogenen Daten. Allerdings wird die Wirksamkeit dieser Rechte durch ihre Ausgestaltung in der Verordnung und die Funktionsweise des Internets in der Praxis erheblich eingeschränkt.

Der für die Verarbeitung Verantwortliche ist nicht nur für die Löschung der Daten verantwortlich, sondern auch dafür, Dritte, die die Daten unter Verwendung von Querverweisen, Kopien oder Replikationen verarbeiten, über den Wunsch der betroffenen Person zu informieren. Diese Verpflichtung allein dem für die Verarbeitung Verantwortlichen aufzuerlegen, führt zu Einschränkungen, weil Fälle denkbar sind, in denen der für die Verarbeitung Verantwortliche alle vertretbaren Schritte unternommen hat, um Dritte zu informieren, ihm aber nicht alle bestehenden Kopien oder Replikationen bekannt sind, oder in denen neue Kopien oder Replikationen auftauchen, nachdem der für die Verarbeitung Verantwortliche alle bekannten Dritten informiert hat. Noch schwerer wiegt, dass offenbar keine Bestimmung der Verordnung Dritte verpflichtet, dem Wunsch der betroffenen Person nachzukommen, es sei denn, sie sind ebenfalls für die Verarbeitung Verantwortliche.

Die Verordnung enthält keinerlei Anleitung, wie betroffene Personen ihre Rechte ausüben können, wenn der für die Verarbeitung Verantwortliche nicht mehr existiert, untergetaucht, nicht identifizierbar oder nicht kontaktierbar ist. Deshalb sollte die Stellung von Dritten, die Daten verarbeiten, unter Festlegung der Bedingungen und der Funktion, in der sie dem Wunsch der betroffenen Person nachkommen müssen, sowie der Folgen, falls sie dies nicht tun, präzisiert werden.

Ebenso könnte in Betracht gezogen werden, die Rechte der betroffenen Person so auszuweiten, dass sie die Löschung von Daten direkt von Dritten fordern kann, wenn dies über den für die Verarbeitung Verantwortlichen nicht möglich ist.

Schließlich gibt es kein Verfahren für die Löschung von Querverweisen auf Daten bzw. die Vernichtung von Kopien oder Replikationen solcher Daten, die gemäß Artikel 17 Absatz 3 nicht gelöscht werden, obwohl die in diesem Artikel aufgeführten Gründe auf sie selbst nicht zutreffen. Derartige Querverweise, Kopien oder Replikationen können jedoch den Zugriff auf den ursprünglichen Inhalt erleichtern, auch wenn dies nach dem Artikel nicht unbedingt gerechtfertigt ist. Die Datenschutzgruppe ist sich natürlich der Notwendigkeit bewusst, ein ausgewogenes Verhältnis zwischen den Schutz der Privatsphäre betreffenden Rechten und dem Recht auf freie Meinungsäußerung zu finden. Das Verhältnis zwischen Artikel 17 Absatz 3 und der Verpflichtung nach Artikel 17 Absatz 2 sollte in der Verordnung klargestellt werden.

Direktwerbung

Die Datenschutzgruppe weist darauf hin, dass ungeachtet Artikel 19 Absatz 2 der Verordnung, der ein Widerspruchsrecht gegen Datenverarbeitung zum Zwecke der Direktwerbung vorsieht, die Bestimmungen der Richtlinie 2002/58/EG – wie auch in Artikel 89 der Verordnung vorgesehen – in vollem Umfang anwendbar bleiben. Dies gilt insbesondere im Zusammenhang mit verhaltensbezogener Internetwerbung und E-Mail-Marketing, wo eine Einwilligung erforderlich ist.

Profiling

Die Datenschutzgruppe befürwortet die in der Verordnung enthaltene Bestimmung zum Profiling. Sie bezweifelt jedoch, dass der gewählte Ansatz den mit der Erstellung und Verwendung von Profilen, insbesondere im Internet, verbundenen Problemen gerecht wird. Darüber hinaus weist die Datenschutzgruppe darauf hin, dass die Formulierung „in maßgeblicher Weise beeinträchtigt“ in Artikel 20 Absatz 1 ungenau ist. Es sollte klargestellt werden, dass die Bestimmung beispielsweise auch die Verwendung von Web-Analyse-Tools, Tracking zur Bewertung des Nutzerverhaltens, das Anlegen von Bewegungsprofilen durch mobile Anwendungen oder die Erstellung von persönlichen Profilen durch soziale Netzwerke betrifft.

Außerdem sollte die Bestimmung nicht auf eine rein automatisierte Verarbeitung beschränkt werden, sondern auch teilautomatisierte Verarbeitungsverfahren umfassen. Nach Ansicht der Datenschutzgruppe sollte ein Ansatz gewählt werden, bei dem die Zwecke, zu denen Profile erstellt und genutzt werden dürfen, eindeutig definiert sind und die für die Verarbeitung Verantwortlichen konkret verpflichtet werden, die betroffene Person insbesondere über ihr Recht zu unterrichten, der Erstellung und Nutzung von Profilen zu widersprechen.

Vertreter

Die Datenschutzgruppe ist der Auffassung, dass die Funktion und die Aufgaben des Vertreters nach Artikel 25 einer weiteren Präzisierung bedürfen. Vor allem in Anbetracht dessen, dass Artikel 79 Absatz 6 Buchstabe f bei Nichtbenennung eines Vertreters die höchstmögliche Geldbuße vorsieht, sollte klargestellt werden, welche Funktion der Vertreter gegenüber betroffenen Personen, Gerichten und Datenschutzbehörden hat. Der Auftrag des Vertreters sollte genau festgelegt werden, um den Umfang seiner Aufgaben, seiner Funktion und seiner Haftung eindeutig zu bestimmen.

Nach Artikel 78 Absatz 2 wirken, falls der für die Verarbeitung Verantwortliche einen Vertreter benannt hat, Sanktionen gegen den Vertreter. Ebenso klar sollten die Vorschriften für den Fall von verwaltungsrechtlichen Sanktionen nach Artikel 79 formuliert sein. Aus der sowohl in Erwägungsgrund 63 als auch in Artikel 4 Absatz 14 verwendeten Formulierung *„gegenüber den Aufsichtsbehörden […] als Ansprechpartner“* geht nicht eindeutig hervor, dass gegen einen Vertreter auch verwaltungsrechtliche Sanktion im Sinne des Artikels 79 verhängt werden können.

Ferner sollte klar sein, dass die Niederlassung eines Vertreters in der EU nach Artikel 25 Absatz 3 *(„muss in einem der Mitgliedstaaten niedergelassen sein“)* **nicht** die Hauptniederlassung gemäß Artikel 4 Absatz 13 begründet und somit bei der Bestimmung der federführenden Datenschutzbehörde nach Artikel 51 Absatz 2 **keine entscheidende** Rolle spielt.

Was die Ausnahmen von der Pflicht zur Benennung eines Vertreters anbelangt, sieht die Datenschutzgruppe keinen gewichtigen Grund, einen für die Verarbeitung Verantwortlichen aus einem Drittland, das einen angemessenen Schutz bietet, von der Pflicht zu befreien. Dass ein Drittland einen angemessenes Datenschutzniveau aufweist, ändert nichts an der Notwendigkeit einer Anlaufstelle in der Europäischen Union. Die Datenschutzgruppe schlägt daher vor, Artikel 25 Absatz 2 Buchstabe a zu streichen.

Wenn Ausnahmen von der Pflicht zur Benennung eines Vertreters gewährt werden sollen, dann sollten sie sich an Art und Umfang der Verarbeitung personenbezogener Daten sowie der (potenziellen) Zahl der betroffenen Personen in der EU orientieren. Die jetzige Schwellenwert für die Beschäftigtenzahl des für die Verarbeitung Verantwortlichen birgt die Gefahr, dass kleine Unternehmen, deren Datenverarbeitungsvorgänge die betroffenen Personen Risiken aussetzen, von der Pflicht ausgenommen werden. Außerdem ist die Formulierung *„betroffenen Personen **nur gelegentlich** Waren oder Dienstleistungen anbieten“* trotz der Erläuterung in Erwägungsgrund 64 zu vage und könnte in der Praxis zu häufig zu Fehlinterpretationen führen.

Rechenschaftspflicht

Die Datenschutzgruppe begrüßt die Einführung des Grundsatzes der Rechenschaftspflicht in der Verordnung, insbesondere in Artikel 22, sehr und stimmt dem Ziel, wirksame Verfahren und Mechanismen einzurichten, die sich vorrangig mit jenen Verarbeitungsvorgängen befassen, die konkrete Risiken für die Rechte und Freiheiten betroffener Personen bergen können, voll und ganz zu. Dennoch hegt die Datenschutzgruppe gewisse Zweifel im Hinblick auf diejenigen Artikel, die den allgemeinen Grundsatz zu konkretisieren versuchen.

Zunächst muss die Skalierbarkeit gewährleistet sein. Bei der Anwendung des Grundsatzes der Rechenschaftspflicht muss es möglich sein, die Größe des für die Verarbeitung Verantwortlichen und die Art der Verarbeitungsvorgänge einzubeziehen. Darüber hinaus sollten die Aufsichtsbehörden in der Lage sein, bei der Verhängung von Sanktionen und Geldbußen die bestehenden Rechenschaftsverfahren zu berücksichtigen.

Darüber hinaus verpflichtet Artikel 28 den für die Verarbeitung Verantwortlichen, die seiner Zuständigkeit unterliegenden Verarbeitungsvorgänge zu dokumentieren. Artikel 28 Absatz 2 schreibt vor, was genau zu dokumentieren ist. Diese Verpflichtung steht im Zusammenhang mit den allgemeinen Rechenschaftspflichten gemäß Artikel 22, wonach der für die Verarbeitung Verantwortliche *den Nachweis dafür erbringen* können muss, welche Strategien und Maßnahmen die Einhaltung der Verordnung gewährleisten. Im Prinzip sollte jeder für die Verarbeitung Verantwortliche, Auftragsverarbeiter und gegebenenfalls Vertreter eines für die Verarbeitung Verantwortlichen verpflichtet werden, bestimmte grundlegende Unterlagen über seine Datenverarbeitungsvorgänge zu führen.

Die Datenschutzgruppe begrüßt die in Artikel 33 vorgesehene Verpflichtung zur Durchführung einer Datenschutz-Folgenabschätzung, ist jedoch der Ansicht, dass eine Folgenabschätzung selbstverständlich auch dann durchgeführt werden sollte, wenn nicht klar ist, ob die Verarbeitungsvorgänge konkrete Risiken für die Rechte und Freiheiten betroffener Personen bergen. Deshalb rät die Datenschutzgruppe, Artikel 33 Absatz 1 in Einklang mit Erwägungsgrund 70 zu bringen, und schlägt vor, im ersten Satz das Wort *„können“* wie folgt einzufügen: *„Bei Verarbeitungsvorgängen, die aufgrund ihres Wesens, ihres Umfangs oder*

ihrer Zwecke konkrete Risiken für die Rechte und Freiheiten betroffener Personen bergen ***können*** *…“.*

Nach Ansicht der Datenschutzgruppe können die Ausnahmeregelungen nach Artikel 28 Absatz 4 Buchstabe b für die Dokumentation und Artikel 35 Absatz 1 Buchstabe b für die Benennung des Datenschutzbeauftragten unbeabsichtigte Folgen haben, vor allem dann, wenn ein Kleinunternehmen mit weniger 250 Mitarbeitern viele personenbezogene Daten verarbeitet oder die Verarbeitung an sich risikobehaftet ist. Außerdem werden große Unternehmen, die nur in begrenztem Umfang personenbezogene Daten verarbeiten, durch den derzeitigen Wortlaut unverhältnismäßig stark belastet. Die Datenschutzgruppe ist der Ansicht, dass es sinnvoller wäre, statt der Gesamtzahl der Mitarbeiter eines Unternehmens Art und Umfang der Verarbeitung personenbezogener Daten sowie die Zahl der unmittelbar mit dieser Verarbeitung befassten Mitarbeiter und/oder die Zahl der betroffenen Personen zugrunde zu legen.

Nach Auffassung der Datenschutzgruppe sollte für die Verarbeitung der in Artikel 9 aufgeführten Kategorien sensibler Daten grundsätzlich eine Datenschutz-Folgenabschätzung durchgeführt werden. Deshalb sollten in Artikel 33 Absatz 2 Buchstabe b alle Kategorien sensibler Daten aufgenommen werden.

Zudem sollten die in Artikel 33 Absatz 2 (Buchstaben b, c und d) enthaltenen Beschränkungen für Verarbeitungsvorgänge (*„in großem Umfang“*, *„weiträumige“* bzw. *„umfangreichen“*) gestrichen werden, weil die Datenschutzgruppe bei diesen Verarbeitungsvorgängen selbst im kleinen Maßstab eine Datenschutz-Folgenabschätzung für erforderlich hält.

Dies gilt insbesondere für die Verarbeitung von biometrischen Daten, die nach Ansicht der Datenschutzgruppe unter bestimmten Umständen als risikobehaftet einzustufen sind, weshalb ungeachtet jeglicher in Artikel 33 vorgesehener Schwellenwerte eine Datenschutz-Folgenabschätzung durchgeführt werden sollte. Außerdem ist, wie bereits erwähnt, ist die in Artikel 33 Absatz 5 vorgesehene Befreiung von Behörden von der Durchführung einer Folgenabschätzung ungerechtfertigt, es sei denn, eine solche Folgenabschätzung wurde bereits während des Gesetzgebungsverfahrens durchgeführt.

<u>Meldung von Verletzungen des Schutzes personenbezogener Daten</u>

Die Datenschutzgruppe begrüßt die Einführung einer Meldepflicht für Verletzungen des Schutzes personenbezogener Daten und die damit einhergehende Vereinheitlichung in allen Bereichen. Die Datenschutzgruppe bezweifelt dennoch, dass die Meldepflicht in ihrer derzeit vorgesehenen Form zu zufriedenstellenden Ergebnissen führen wird. Vor allem der Umfang der Pflicht zur Meldung an die Aufsichtsbehörde sollte gezielter ausgerichtet und begrenzt werden. Es sollte vermieden werden, dass Aufsichtsbehörden durch die Bearbeitung von Meldungen geringfügiger Verletzungen, die sich wahrscheinlich nicht nachteilig auf die Rechte von betroffenen Personen auswirken, abgelenkt und überlastet werden. Darüber hinaus sind die Rolle und die Aufgaben der Datenschutzbehörden im Falle einer Meldung (und danach) zu präzisieren.

Die Datenschutzgruppe ist sich darüber im Klaren, dass ein Meldefrist von 24 Stunden unter gewissen Umständen nicht eingehalten werden kann. In Artikel 31 Absatz 1 wurde dem durch die Möglichkeit Rechnung getragen, eine Verletzung später als 24 Stunden nach ihrer

Feststellung zu melden. Nichtsdestotrotz ist eine frühzeitige Meldung wichtig. Die Datenschutzgruppe schlägt daher ein aus zwei Schritten bestehendes Verfahren vor, wonach der für die Verarbeitung Verantwortliche die Verletzung grundsätzlich innerhalb von 24 Stunden nach ihrer Feststellung melden muss. Können innerhalb der Frist von 24 Stunden nicht alle Informationen vorgelegt werden, hat der für die Verarbeitung Verantwortliche die Möglichkeit, die Meldung in einem zweiten Schritt zu vervollständigen.

Die Kriterien für eine Verletzung des Schutzes personenbezogener Daten sowie die Umstände, unter denen einen solche Verletzung der Aufsichtsbehörde und den betroffenen Personen zu melden ist (etwa wenn konkrete Gefahren oder Schäden für die betroffenen Personen zu befürchten sind), müssen noch näher bestimmt werden. Nach Ansicht der Datenschutzgruppe sollte der Europäische Datenschutzausschuss in jedem Fall an der Festlegung dieser Kriterien und Umstände mitwirken.

Das Meldeformblatt sollte entsprechend den Empfehlungen der Datenschutzgruppe und von ENISA eine auf objektiven Kriterien beruhende Bewertung der Schwere der Verletzung des Schutzes personenbezogener Daten enthalten.

Rolle und Funktionsweise der Datenschutzbehörden

Unabhängigkeit

Dem derzeitigen Wortlaut zufolge können Mitglieder der Datenschutzbehörden ausschließlich vom Parlament oder der Regierung ernannt werden. Die Datenschutzgruppe würde es jedoch begrüßen, wenn die Mitgliedstaaten auch anderen unabhängigen Einrichtungen, etwa dem Justizrat, die Nominierung und/oder Ernennung von Mitgliedern der Datenschutzbehörden gestatten dürfen.

Befugnisse

Neben der Befugnis zur Durchführung von Untersuchungen sollten die Datenschutzbehörden auch ausdrücklich befugt sein, Prüfungen durchzuführen.

Mittelausstattung

Damit die Datenschutzbehörden ihre durch die Verordnung erweiterten Aufgaben und Befugnisse, auch im Rahmen der Amtshilfe, Zusammenarbeit und Mitwirkung im Europäischen Datenschutzausschuss, effektiv wahrnehmen können, sieht die Verordnung vor, dass die Mitgliedstaaten sicherstellen, dass die Aufsichtsbehörden mit angemessenen personellen, technischen und finanziellen Ressourcen, Räumlichkeiten und mit der erforderlichen Infrastruktur ausgestattet werden. Wie bereits ausgeführt, rät die Datenschutzgruppe nachdrücklich dazu, nach einer unabhängigen umfassenden Abschätzung des Kostenanstiegs, der aufgrund der gegenwärtigen Vorschläge auf die Datenschutzbehörden zukommt, konkret festzulegen, was unter einem angemessenen Haushalt zu verstehen ist.

Ein angemessener Haushalt könnte sich aus einem Festbetrag für die grundlegenden Funktionen aller Datenschutzbehörden und einem ergänzenden Betrag zusammensetzen, der nach einer an der Bevölkerungszahl eines Mitgliedstaats und seinem BIP orientierten Formel errechnet wird. Einfließen könnte auch die Zahl der multinationalen Unternehmen, die ihren Sitz in diesem Mitgliedstaat haben. In einem Erwägungsgrund sollten die Mitgliedstaaten

ausdrücklich ermuntert werden, verschiedene Möglichkeiten zur Finanzierung der Datenschutzbehörden in Betracht zu ziehen, um eine angemessene Ausstattung der Behörde zu gewährleisten.

Ermessensspielraum

Um effektiv zu sein, sollten die Datenschutzbehörden wählen können und unbeschadet ihrer Verpflichtungen zur Zusammenarbeit, Amtshilfe und Kohärenz nach Kapitel VII in der Lage sein, eigene Prioritäten festzulegen und von sich aus Maßnahmen zu ergreifen. Die Datenschutzbehörden sollten ihre Ressourcen entsprechend dem strategischen Charakter und die Komplexität der anstehenden Probleme zuteilen können, etwa unter Berücksichtigung des tatsächlichen oder möglichen Schadens für den Datenschutz, der Zahl der betroffenen Personen und der angewandten Technologie. Datenschutzbehörden, die ihre eigenen Prioritäten festlegen dürfen, können auch besser mit finanziellen und budgetären Zwängen umgehen.

Die in Artikel 52 Absätze 2 und 3 vorgesehenen Aufgaben (die Aufsichtsbehörde *„fördert“* und *„berät auf Antrag jede betroffene Person“*) scheinen den für eine effektive Tätigkeit der Datenschutzbehörden notwendigen Ermessensspielraum zu verringern. Außerdem schlägt die Datenschutzgruppe zur Gewährleistung des Ermessensspielraums der Datenschutzbehörden vor, in Artikel 34 Absatz 3 das Wort *„kann“* einzufügen und folgendermaßen zu formulieren: *„und **kann** geeignete Vorschläge zur Beseitigung dieser Mängel unterbreiten“*.

Zuständigkeit der Datenschutzbehörden (zentrale Kontaktstelle)

Artikel 51 Absatz 1 regelt die Zuständigkeit einer Datenschutzbehörde im Hoheitsgebiet ihre Mitgliedstaats. Diese allgemeine Regel wird durch Artikel 51 Absatz 2 ergänzt, wonach die Datenschutzbehörde des Mitgliedstaats, in dem sich die Hauptniederlassung eines für die Verarbeitung Verantwortlichen befindet, für die Aufsicht über dessen Verarbeitungstätigkeit in allen Mitgliedstaaten zuständig ist.

Die Artikel-29-Datenschutzgruppe befürwortet das Konzept einer federführenden Behörde und eine klare Verpflichtung der Datenschutzbehörden zur Zusammenarbeit und zur Anwendung des Kohärenzverfahrens, wenn Personen in mehreren Mitgliedstaaten voraussichtlich von Verarbeitungsvorgängen betroffen sind, weil dies zu einer einheitlichen Auslegung und Anwendung des EU-Rechtsrahmens führt und damit Rechtssicherheit schafft. Wie bereits erwähnt, müssen jedoch, damit das Verfahren funktionieren kann, die Definition der Hauptniederlassung und die Auswirkungen auf die Zuständigkeiten der anderen Datenschutzbehörden präzisiert werden. Auch die Art des vorgeschlagenen Kohärenzverfahrens wirft Fragen auf.

In jedem Fall sollte klar sein, dass eine federführende Datenschutzbehörde nicht ausschließlich zuständig ist. Die Zuständigkeit der federführenden Datenschutzbehörde gilt vorbehaltlich der Pflicht zur Zusammenarbeit, zur Gewährung und Annahme von Amtshilfe und zur Anwendung des Kohärenzverfahrens, wie in Kapitel VII über Zusammenarbeit und Kohärenz festgelegt, sowie unter der Voraussetzung, dass sie ihr Handeln mit anderen beteiligten Datenschutzbehörden abstimmt.

Darüber hinaus betont die Datenschutzgruppe, dass das in Artikel 51 Absatz 2 verankerte Prinzip der zentralen Kontaktstelle nur dann greift, wenn der für die Verarbeitung

Verantwortliche oder der Auftragsverarbeiter mehr als eine Niederlassung in der EU hat, nicht jedoch wenn keine Niederlassung in der EU besteht und die Datenverarbeitung dazu dient, Personen in der Union Waren oder Dienstleistungen anzubieten, oder der Beobachtung ihres Verhaltens dient (Artikel 3 Absatz 2). Folglich ist in diesem Fall nach Artikel 51 Absatz 1 jede Datenschutzbehörde zuständig, deren Mitgliedstaat von Verarbeitungsvorgängen betroffen ist, wobei jedoch die Verordnung nicht regelt, welche Behörde dann federführend ist. Nach Ansicht der Datenschutzgruppe kommt gerade in diesen Fällen der Zusammenarbeit und Kohärenz besondere Bedeutung zu.

Da die derzeit zur Definition des Begriffs Hauptniederlassung in Artikel 4 Absatz 13 verwendeten Elemente, wie bereits erläutert, nicht ausreichen und somit unklar ist, wie in grenzüberschreitenden Fällen die federführende zuständige Datenschutzbehörde zu bestimmen ist, schlägt die Datenschutzgruppe vor,

1. die nicht ausschließliche Zuständigkeit der federführenden Datenschutzbehörde vorbehaltlich der Pflicht zur Zusammenarbeit, zur Gewährung und Annahme von Amtshilfe und zur Anwendung des Kohärenzverfahrens, wie in Kapitel VII über Zusammenarbeit und Kohärenz festgelegt, zu akzeptieren und
2. für Fälle, in denen keine Niederlassung in der EU besteht (oder unklar ist, wo sich die Hauptniederlassung befindet) Kriterien zur Bestimmung der federführenden Datenschutzbehörde zu erwägen, beispielsweise
   - den Mitgliedstaat, in dem die betreffenden Verarbeitungstätigkeiten hauptsächlich stattfinden,
   - den Mitgliedstaat, in dem Personen betroffen sind,
   - den Mitgliedstaat, in dem Personen gemäß Artikel 73 Absatz 1 bei der Datenschutzbehörde Beschwerden erhoben oder Bedenken angemeldet haben.

Es leuchtet ein, dass für jedes der genannten Kriterien mehrere Mitgliedstaaten infrage kommen können. Jedoch sollten sich die betreffenden Datenschutzbehörden anhand dieser Kriterien darüber abstimmen, wer die Federführung übernimmt. In Fällen, wo dies nicht offensichtlich ist oder keine Einigung erzielt wird, sollte der Europäische Datenschutzausschuss anhand derselben Kriterien über die Federführung entscheiden.

Amtshilfe

Die Datenschutzgruppe schlägt ein umfassendes Konzept vor, das auf Federführung und Zusammenarbeit zwischen Datenschutzbehörden beruht. Immer wenn gemäß Artikel 56 *„voraussichtlich Personen in mehreren Mitgliedstaaten von Verarbeitungsvorgängen betroffen sind“*, sollten die betreffenden Datenschutzbehörden grundsätzlich zur Zusammenarbeit verpflichtet sein, weil eben Bürger ihrer Mitgliedstaaten betroffen sind. Diese Zusammenarbeit sollte die rechtliche Beurteilung sowie konkrete aufsichtsrechtliche Maßnahmen umfassen.

Die Datenschutzgruppe ist der Ansicht, dass die Datenschutzbehörden einander auch dann zweckdienliche Informationen gemäß Artikel 55 Absatz 1 übermitteln sollten, wenn noch keine in Artikel 58 Absatz 1 genannte Maßnahme erlassen wurde (etwa im Falle einer Verletzung des Schutzes personenbezogener Daten). Darüber hinaus sollten die Datenschutzbehörden einander positive Entscheidungen zu Datenschutz-Folgenabschätzungen mitteilen.

Die Datenschutzgruppe schlägt vor, in den Artikeln 55 und 56 klarzustellen, dass im Falle einer anstehenden Entscheidung, an der sowohl die federführende Datenschutzbehörde nach

Artikel 51 Absatz 2 als auch eine andere zuständige Datenschutzbehörde nach Artikel 51 Absatz 1 beteiligt ist, die federführende und die „vor Ort“ befindliche Behörde im Hinblick auf die Beurteilung des Falls und die zu treffenden Maßnahmen *einvernehmlich* vorgehen. Erzielen die betreffenden Datenschutzbehörden bei der Beurteilung des Falls und/oder den bi- oder multilateral zu treffenden Maßnahmen kein Einvernehmen, ist die Angelegenheit im Rahmen des Kohärenzverfahrens nach Artikel 57 zu behandeln.

Die Datenschutzgruppe begrüßt die vorgeschlagenen Maßnahmen, mit denen die Zusammenarbeit zwischen den Datenschutzbehörden gewährleistet werden soll, und weist darauf hin, dass die federführende Datenschutzbehörde, wie bereits ausgeführt, nicht ausschließlich zuständig ist. Sie betont jedoch, dass mehr getan werden muss, um die Amtshilfe abzusichern, und zwar sowohl in Bezug auf die Mittelausstattung der Datenschutzbehörden (siehe oben) als auch bei wichtigen Einzelheiten der praktischen Durchführung der Amtshilfe. Die Sprachwahl, Fristen, Umfang und Art der angeforderten Informationen sowie technische Mittel, Formate und Verfahren für den Informationsaustausch sind Aspekte, die für eine wirksame Zusammenarbeit zwischen den Datenschutzbehörden in der Praxis und somit auch für das Prinzip der zentralen Kontaktstelle von entscheidender Bedeutung sind.

Kohärenz

Die Datenschutzgruppe stellt mit Befriedigung fest, dass ihr Vorschlag für einen der kohärenten Anwendung der Datenschutzvorschriften dienenden Mechanismus der Zusammenarbeit und Koordination in den Artikeln 57 und 58 des Vorschlags aufgegriffen wurde.

Sie ist jedoch der Ansicht, dass ein solcher Mechanismus nur dann für Kohärenz sorgen sollte, wenn dies notwendig ist, und nicht in die Unabhängigkeit der nationalen Aufsichtsbehörden und die Aufgaben der verschiedenen Beteiligten eingreifen darf.

In Anbetracht der breiten Anwendungsbereichs von Artikel 58 Absatz 2 Buchstabe a, der die Datenverarbeitung im Zusammenhang mit jeglicher Art eines grenzüberschreitenden Angebots von Waren oder Dienstleistungen innerhalb der EU betrifft, schlägt die Datenschutzgruppe vor, nur solche Angelegenheiten im Rahmen des Kohärenzverfahrens innerhalb des Europäischen Datenschutzausschusses zu behandeln, in denen die nach Artikel 51 zuständigen Datenschutzbehörden bei der Beurteilung des Falls und/oder den bi- oder multilateral zu treffenden Maßnahmen kein Einvernehmen erzielen. In jedem Fall sollte der Europäische Datenschutzausschuss über Angelegenheiten von grundlegender Bedeutung für den Datenschutz oder den freien Verkehr personenbezogener Daten innerhalb der EU unterrichtet werden.

Um zu vermeiden, dass es aufgrund des breiten Anwendungsbereichs des Verfahrens zu einer Vielzahl von Fällen kommt (da nach Artikel 58 Absatz 3 **jede** Behörde beantragen kann, dass eine Angelegenheit im Rahmen des Kohärenzverfahrens behandelt wird), schlägt die Datenschutzgruppe vor, Anträge nach Artikel 58 Absatz 3 dem Europäischen Datenschutzausschuss zur Abstimmung vorzulegen.

Ungeachtet der Rolle der Kommission als Hüterin der Verträge hat die Datenschutzgruppe starke Vorbehalte im Hinblick auf die der Kommission in Einzelfällen, die im Rahmen des Kohärenzverfahrens behandelt wurden, zugedachte Funktion, weil diese einen Eingriff in die unabhängige Stellung der Datenschutzbehörden und des Europäischen

Datenschutzausschusses bedeutet. Wenn eine Sache vom Europäischen Datenschutzausschuss im Rahmen des Kohärenzverfahrens behandelt wird oder wurde, sollte die Kommission Gelegenheit zur rechtlichen Beurteilung haben, prinzipiell jedoch nicht eingreifen. Dies gilt insbesondere im Falle der in Artikel 60 Absatz 1, Artikel 62 Absatz 1 Buchstabe a und Artikel 62 Absatz 2 vorgesehenen Aussetzung einer Maßnahme. Zudem reichen *ernsthafte Zweifel* nicht für ein Eingreifen der Kommission aus.

Die Datenschutzgruppe betont, dass es dem Europäischen Datenschutzausschuss selbst obliegt, dafür zu sorgen, dass seine Stellungnahmen von allen beteiligten Datenschutzbehörden befolgt und einheitlich angewandt werden.

Um den Stellungnahmen des Europäischen Datenschutzausschusses mehr Wirkung zu verleihen, könnte für Fälle, in denen eine oder mehrere Datenschutzbehörden von einer nach Artikel 58 Absatz 7 abgegebenen Stellungnahme des Europäischen Datenschutzausschusses abzuweichen gedenken, ein Bestätigungsverfahren eingeführt werden. Der Europäische Datenschutzausschuss sollte in diesen Fällen die Möglichkeit haben, seine Stellungnahme mit qualifizierter Mehrheit zu bestätigen und so die Bedeutung eines einheitlichen Vorgehens in Fällen von grundsätzlicher Bedeutung für den Datenschutz innerhalb der EU zu unterstreichen. Als weitere Möglichkeit könnte den Datenschutzbehörden gestattet werden, abweichende Standpunkte zum Ausdruck zu bringen. Diese Standpunkte sollten begründet sein und veröffentlicht werden.

Darüber hinaus sollte ein Verfahren vorgesehen werden, nach dem der Europäische Datenschutzausschuss und die Kommission den Europäischen Gerichtshof um Stellungnahme zur Auslegung der Verordnung ersuchen können, falls eine Datenschutzbehörde beabsichtigt, eine Stellungnahme, die der Europäische Datenschutzausschuss mit qualifizierter Mehrheit bestätigt hat, nicht zu befolgen.

Anwendung von einzelstaatlichem Recht (Kapitel IX)

Wenn die Mitgliedstaaten eigene Regelungen nach den Artikeln 80 bis 83 erlassen, werden diese mit den Regeln über die Zuständigkeit der Datenschutzbehörden und die Federführung unter den Datenschutzbehörden kollidieren.

In der jetzigen Fassung der Verordnung bleibt unklar, wie in Fällen zu verfahren ist, die sich aus angrenzendem einzelstaatlichem Recht ergeben, etwa der Zuständigkeitsbereich der für die Hauptniederlassung des für die Verarbeitung Verantwortlichen zuständigen Datenschutzbehörde im Beschäftigungskontext. Fraglich ist, ob beispielsweise die deutsche Datenschutzbehörde in einer Angelegenheit, die einen Mitarbeiter einer spanischen Tochtergesellschaft eines Unternehmens mit Hauptniederlassung in Deutschland betrifft, spanisches Arbeitsrecht auslegen und anwenden müsste. Es sollte daher klargestellt werden, dass in Fällen, in denen nach Kapitel IX der Verordnung einzelstaatliches Recht anzuwenden ist, abweichend von Artikel 51 Absatz 2 stets die jeweilige einzelstaatliche Datenschutzbehörde (natürlich in Zusammenarbeit mit der federführenden Datenschutzbehörde) für die Anwendung des in dem konkreten Fall angrenzenden nationalen Rechts zuständig ist (im obigen Beispiel wäre die spanische Datenschutzbehörde für die Anwendung des spanischen Datenschutzrechts im Beschäftigungskontext zuständig).

Die Datenschutzgruppe betont, dass der Anwendungsbereich der nach Kapitel IX erlassenen einzelstaatlichen Rechtsvorschriften grundsätzlich präzisierungsbedürftig ist.

Fristen

Die Datenschutzgruppe stimmt zu, dass es darauf ankommt, dass der Europäische Datenschutzausschuss im Rahmen des Kohärenzverfahrens angeforderte Stellungnahmen möglichst rasch abgibt. Die Fristen dafür sollten jedoch so gewählt werden, dass die Beratungsqualität gewährleistet ist. Um eine wirkliche Annahme und Unterstützung vor Ort sicherzustellen und zu gewährleisten, dass die Stellungnahme auch einer möglichen gerichtlichen Überprüfung standhält, müssen die vorgeschlagenen engen Fristen in jedem Fall verlängert werden.

Zentrale Kontaktstelle für betroffene Personen

Betroffene Personen im Zuständigkeitsbereich der EU-Datenschutzbehörden sollten ebenso wie die für die Verarbeitung Verantwortlichen eine zentrale Kontaktstelle haben. Nach der Verordnung haben betroffene Personen mehrere Möglichkeiten, ihre Rechte wahrzunehmen und Rechtsbehelfe in Anspruch zu nehmen. Betroffenen Personen können in allen Mitgliedstaaten Beschwerde bei einer Datenschutzbehörde (ihrer nationalen Datenschutzbehörde, der Datenschutzbehörde des Mitgliedstaats, in dem der für die Verarbeitung Verantwortliche seine Hauptniederlassung hat, oder jeder anderen Datenschutzbehörde in der Union) erheben. Außerdem können betroffene Personen vor den Gerichten ihres Mitgliedstaats oder des Mitgliedstaats, in dem der für die Verarbeitung Verantwortliche eine Niederlassung hat, klagen.

Wenngleich diese Möglichkeiten die Rechte der betroffenen Personen scheinbar erweitern, können sie auch zu Verwirrung und Unsicherheit darüber führen, wer letztlich der betroffenen Person Rede und Antwort stehen muss.

Die Datenschutzgruppe schlägt vor zu präzisieren, dass sich betroffene Personen unbeschadet des Rechts auf gerichtlichen Rechtsbehelf grundsätzlich an die für ihren Wohnsitz oder eine Niederlassung des für die Verarbeitung Verantwortlichen bzw. des Auftragsverarbeiters zuständige Datenschutzbehörde wenden sollten. Um in der Lage zu sein, der betroffenen Person zu antworten, müsste die betreffende Datenschutzbehörde in diesem Mitgliedstaat mit der für die Hauptniederlassung des für die Verarbeitung Verantwortlichen zuständigen Datenschutzbehörde (der federführenden Behörde) zusammenarbeiten und die erforderlichen Untersuchungs- und gegebenenfalls Durchsetzungsmaßnahmen abstimmen. Dabei bleibt die ursprünglich angesprochene Datenschutzbehörde jedoch unter allen Umständen für den Kontakt zur betroffenen Person zuständig.

Institutionelle Struktur des Europäischen Datenschutzausschusses

Die Datenschutzgruppe nimmt zur Kenntnis, dass sie durch den mit Artikel 64 eingerichteten Europäischen Datenschutzausschuss ersetzt wird.

Die Datenschutzgruppe ist der Auffassung, dass der Ausschuss seinen Vorsitzenden und die stellvertretenden Vorsitzenden demokratisch wählen können sollte. Nach Ansicht der Datenschutzgruppe wurden keine überzeugenden Gründe genannt, die einen ständigen Stellvertreterposten für den Europäischen Datenschutzbeauftragten rechtfertigen.

Darüber hinaus wäre ein völlig unabhängiges Sekretariat wünschenswert. Die Datenschutzgruppe nimmt jedoch zur Kenntnis, dass das Sekretariat des Datenschutzausschusses vom Europäischen Datenschutzbeauftragten gestellt werden soll. Zu prüfen wären die dafür erforderlichen praktischen Vorkehrungen und einzurichtenden Berichtswege sowie insbesondere, wie die Unabhängigkeit der Mitglieder des Sekretariats gewährleistet werden kann und welche rechtlichen und institutionellen Folgen die Übernahme des Sekretariats des Europäischen Datenschutzausschusses durch eines seiner Mitglieder hätte.

Datenübermittlungen ins Ausland

Die Verordnung betont zu Recht die Rechenschaftspflicht der für die Verarbeitung Verantwortlichen, um zu gewährleisten, dass personenbezogene Daten bei Übermittlung in Länder außerhalb des Europäischen Wirtschaftsraums (EWR) geschützt bleiben. Sie bietet den für die Verarbeitung Verantwortlichen verschiedene Erleichterungen in Form von Angemessenheitsbeschlüssen, eines straffen Systems verbindlicher unternehmensinterner Vorschriften, genehmigter Vertragsklauseln und Einzelgenehmigungen durch die Datenschutzbehörde. Darüber hinaus sieht sie in Artikel 44 diverse Ausnahmeregelungen vor.

Die Ausnahmeregelungen, insbesondere Artikel 44 Absatz 1 Buchstabe h, sind jedoch nach wie vor sehr weitreichend und tendenziell in vielen Situationen anwendbar. Wie die Datenschutzgruppe in einer früheren Stellungnahme (WP 114) ausgeführt hat, sollten solche Ausnahmeregelungen nur insoweit angewandt werden, als die Verarbeitung nicht massenhaft, wiederholt oder routinemäßig erfolgt.

Darüber hinaus können nach Artikel 42 zur Regelung von Übermittlungen ins Ausland auch unverbindliche Instrumente verwendet werden, die der Genehmigung durch eine Datenschutzbehörde bedürfen. Dennoch galt Verbindlichkeit bei bestehenden Instrumenten (z. B. CCT, verbindliche unternehmensinterne Vorschriften, SH, angemessenes Datenschutzniveau von Drittländern) bislang stets als wichtige Voraussetzung für die Regelung von Übermittlungen ins Ausland. Deshalb wird vorgeschlagen, Artikel 42 Absatz 5 bis auf den letzten Satz zu streichen und den Verweis auf Artikel 34 entsprechend anzupassen.

Für Artikel 41 Absatz 6 sollte klargestellt werden, ob *„unbeschadet der Bestimmungen der Artikel 42 bis 44“* bedeutet, dass im Falle eines negativen Angemessenheitsbeschlusses der Kommission die Übermittlung von Daten an das betreffende Drittland dennoch aufgrund dieser Artikel möglich ist.
Schließlich sollte, wenn die Kommission durch Beschluss festgestellt hat, dass ein Drittland beziehungsweise ein Gebiet oder ein Verarbeitungssektor eines Drittlands oder eine internationale Organisation einen angemessenen Schutz bietet (Artikel 41), eine solche Übermittlung keiner weiteren Genehmigung bedürfen. Wie jedoch bereits erwähnt, empfiehlt die Datenschutzgruppe nachdrücklich, die Kommission zu verpflichten, den Europäischen Datenschutzausschuss bei Angemessenheitsbeschlüssen zurate zu ziehen.

Nach EU-Recht nicht zulässige Weitergabe von Daten

Die Datenschutzgruppe betont, dass in der Verordnung für Fälle von nach EU-Recht oder dem Recht von Mitgliedstaaten nicht zulässiger Weitergabe von Daten unbedingt die Anwendung von Rechtshilfeabkommen vorgesehen werden sollte. Nach Ansicht der Datenschutzgruppe

wird ohne die obligatorische Anwendung bestehender Rechtshilfeabkommen die breite Übermittlung personenbezogener Daten im Rahmen der großen und unbegrenzten Kategorie von *„wichtigen Gründen des öffentlichen Interesses“* nach Artikel 44 Absatz 1 Buchstabe d ermöglicht, selbst wenn die Übermittlung massenhaft, häufig und routinemäßig erfolgt. Wenn eine Entscheidung eines Gerichts oder einer Verwaltungsbehörde eines Drittlands vorsieht, dass ein für die Verarbeitung Verantwortlicher oder Auftragsverarbeiter Daten aus der EU in das Drittland übermittelt und zwischen dem ersuchenden Drittland und der EU oder einem oder mehreren Mitgliedstaaten kein Rechtshilfeabkommen oder anderes internationales Abkommen besteht, sollte die Übermittlung dieser Daten untersagt werden. Die Datenschutzgruppe betont, dass in Fällen, in denen ein Rechtshilfeabkommen besteht, die nach dem Rechtshilfeabkommen (oder vergleichbaren internationalen Abkommen) zuständige Behörde den Antrag bearbeiten und nötigenfalls die Datenschutzbehörde zurate ziehen sollte.

Recht auf Haftung und Schadenersatz

Die Datenschutzgruppe begrüßt die in Artikel 77 Absatz 1 enthaltenen Bestimmungen, wonach jede Person, der wegen einer rechtswidrigen Verarbeitung oder einer anderen mit dieser Verordnung nicht zu vereinbarenden Handlung ein Schaden entstanden ist, Anspruch auf Schadenersatz gegen den für die Verarbeitung Verantwortlichen oder gegen den Auftragsverarbeiter hat. Die Datenschutzgruppe begrüßt ferner, dass Artikel 77 Absatz 2 gewährleistet, dass es in Fällen, in denen mehr als ein für die Verarbeitung Verantwortlicher oder mehr als ein Auftragsverarbeiter an der Verarbeitung beteiligt ist, nicht der betroffenen Person obliegt, sich an denjenigen für die Verarbeitung Verantwortlichen zu wenden, der die Gesamtverantwortung trägt. Nach Ansicht der Datenschutzgruppe muss jedoch (in einem Erwägungsgrund) klargestellt werden, dass mit „Schaden“ nicht nur materielle Schäden, sondern auch Notlagen (immaterielle Schäden) gemeint sind.

Im Falle einer Entscheidung einer anderen Datenschutzbehörde (etwa der für die Hauptniederlassung zuständigen Behörde), die eine betroffene Person beeinträchtigt oder schädigt, sollte die betroffene Person vor den Verwaltungsgerichten ihres Wohnsitzlandes gegen die Entscheidung klagen können.

Die von der Europäischen Kommission vorgeschlagene Lösung, wonach entweder die betroffene Person oder die Datenschutzbehörde gegen die andere Datenschutzbehörde in dem anderen Mitgliedstaat Klage erheben kann, ist alles andere als zufriedenstellend. Die Datenschutzgruppe fordert eine Regelung, die es betroffenen Personen ermöglicht, gegen Verwaltungsentscheidungen vor den Verwaltungsgerichten ihres Wohnsitzlandes zu klagen.

Geldbußen

Die Datenschutzgruppe begrüßt die Einführung empfindlicher Geldbußen, weil diese die Datenschutzbehörden in die Lage versetzen, ihrer Rolle als Verfolgungsbehörden gerecht zu werden, und – durch Abschreckung – dazu beitragen können, dass die für die Verarbeitung Verantwortlichen die Vorschriften genauer befolgen.

Nach Artikel 79 Absatz 1 ist jede Aufsichtsbehörde *„befugt“*, verwaltungsrechtliche Sanktionen zu verhängen. Dies wird durch Erwägungsgrund 120 untermauert, wonach jede Aufsichtsbehörde *„befugt sein“* sollte, verwaltungsrechtliche Vergehen zu ahnden. Artikel 79 Absätze 4 – 6 besagen jedoch, dass die Aufsichtsbehörde in den jeweiligen Situationen eine

Geldbuße *„verhängt“*. Die Datenschutzgruppe ist der Meinung, dass den Datenschutzbehörden für die Entscheidung, wann eine Geldbuße zu verhängen ist, ein gewisser Ermessensspielraum zugestanden werden sollte, da viele Faktoren die Art der Zuwiderhandlung beeinflussen und bei der Entscheidung über die Verhängung einer Geldbuße berücksichtigt werden sollten. Sie schlägt daher vor, den Wortlaut in Artikel 79 Absätze 4 – 6 entsprechend zu ändern.

Die Datenschutzgruppe begrüßt die durch Artikel 79 erreichte Harmonisierung in der Regelung, welche Zuwiderhandlung welche maximale Geldbuße nach sich zieht, da dies zu einer einheitlicheren Verhängung von Geldbußen in der Europäischen Union führen wird. Dennoch schlägt die Datenschutzgruppe vor, in Artikel 58 Absatz 2 ausdrücklich die Möglichkeit vorzusehen, Abweichungen bei der Anwendung verwaltungsrechtlicher Sanktionen im Kohärenzverfahren nach Abschnitt 2 Kapitel VII zu behandeln, so wie dies auch in Erwägungsgrund 120 vorgesehen ist.

Die Datenschutzgruppe versteht ferner den Wortlaut von Artikel 79 so, dass bei Zuständigkeit mehrerer Datenschutzbehörden jede von ihnen befugt ist, eine Geldbuße zu verhängen, was wiederum Fragen im Hinblick auf das Verbot der Doppelbestrafung (ne bis in idem) aufwirft.

Darüber hinaus ist die Datenschutzgruppe der Ansicht, dass der für die mildere Ahndung von ersten und unabsichtlichen Verstößen vorgesehene Schwellenwert in der Praxis von zu wenigen für die Verarbeitung Verantwortlichen erfüllt würde und deshalb gestrichen werden sollte. Falls ein Schwellenwert eingeführt werden soll, wäre es auf jeden Fall sinnvoller, dabei statt der Mitarbeiterzahl des für die Verarbeitung Verantwortlichen die Zahl der beeinträchtigten betroffenen Personen zugrunde zu legen.

<u>Rechtsbehelfe</u>

Die Datenschutzgruppe begrüßt die Einführung eines umfassenden Regelwerks zu Rechtsbehelfen für betroffene Personen, wonach auch Organisationen und Verbände die Rechte betroffener Personen gegenüber für die Verarbeitung Verantwortlichen und Auftragsverarbeitern ausüben können. Sie hält jedoch verschiedene Aspekte in Bezug auf Kapitel VIII für präzisierungsbedürftig.

In Anbetracht des breiten Anwendungsbereichs von Artikel 73 Absatz 1, wonach jede betroffene Person das Recht auf Beschwerde bei **einer beliebigen** mitgliedstaatlichen Datenschutzbehörde hat, ist die Datenschutzgruppe der Auffassung, dass sich die betroffene Person, wie auch schon in Bezug auf die zentrale Kontaktstelle für betroffene Personen ausgeführt, grundsätzlich an die für ihren Wohnsitz oder die für den Sitz des für die Verarbeitung Verantwortlichen bzw. Auftragsverarbeiters zuständige Datenschutzbehörde wenden sollte.

Wenn zudem die Datenschutzbehörde, bei der die Beschwerde eingeht, sachlich nicht zuständig ist, müsste diese Behörde nach Ansicht der Datenschutzgruppe verpflichtet sein, mit der als zentrale Kontaktstelle für die betroffene Person fungierenden Datenschutzbehörde und der für die Niederlassung des für die Verarbeitung Verantwortlichen zuständigen Datenschutzbehörde zusammenzuarbeiten. In diesem Fall sollte die Behörde, an die die Beschwerde gerichtet wurde, unabhängig von ihrer sachlichen Zuständigkeit verpflichtet sein, die betroffene Person über den Fortgang des Falls zu unterrichten. Dies ergibt sich aus der Notwendigkeit einer zentralen Kontaktstelle für betroffene Personen (siehe oben).

In Artikel 74 Absatz 2 sollte nach Ansicht der Datenschutzgruppe klargestellt werden, welche Datenschutzbehörde dafür zuständig ist, *„im Fall einer Beschwerde tätig zu werden, wenn keine zum Schutz ihrer Rechte notwendige Entscheidung ergangen ist“*. Im Falle der federführenden Datenschutzbehörde nach Artikel 51 Absatz 2 wäre dies die Datenschutzbehörde des Mitgliedstaats, in dem der Auftragsverarbeiter bzw. für die Verarbeitung Verantwortliche seine Hauptniederlassung hat, und in jedem anderen Fall die zuständige Behörde nach Artikel 51 Absatz 1. Daher sollte in Artikel 74 Absatz 2 präzisiert werden, dass die Verpflichtung zum Tätigwerden die zuständige Aufsichtsbehörde *„… im Sinne von Artikel 51 Absatz 1 oder 2“* betrifft.

Darüber hinaus sieht Artikel 74 Absatz 4 vor, dass eine betroffene Person, die von einer Entscheidung einer Datenschutzbehörde betroffen ist, die ihren Sitz in einem anderen Mitgliedstaat hat als dem, in dem die betroffene Person ihren gewöhnlichen Aufenthalt hat, die Datenschutzbehörde in dem Mitgliedstaat ihres gewöhnlichen Aufenthalts ersuchen kann, in ihrem Namen gegen die zuständige Datenschutzbehörde in dem anderen Mitgliedstaat Klage zu erheben. Wenngleich die Datenschutzgruppe anerkennt, dass diese Bestimmung aufgenommen wurde, um zu gewährleisten, dass betroffene Personen ihre Rechte gegenüber Datenschutzbehörden in anderen Mitgliedstaaten ausüben können, ist sie dennoch der Ansicht, dass die Bestimmung im Widerspruch zur grundsätzlichen Pflicht der Datenschutzbehörden zur Zusammenarbeit und Amtshilfe in grenzüberschreitenden Fällen nach den Artikeln 55 und 56 und auch zu der Bestimmung steht, nach der eine Angelegenheit bei Meinungsverschiedenheiten zwischen den Datenschutzbehörden vor den Europäischen Datenschutzausschuss gebracht werden soll. Daher weist die Datenschutzgruppe nachdrücklich darauf hin, dass andere, mit den Grundsätzen der Verordnung vereinbare Möglichkeiten, wie betroffene Personen gegen sie betreffende Entscheidungen von Datenschutzbehörden gerichtlich vorgehen können, sorgfältig geprüft werden müssen.

Artikel 75 Absatz 2 sieht vor, dass betroffene Personen gegen einen für die Verarbeitung Verantwortlichen oder gegen einen Auftragsverarbeiter vor den Gerichten des Mitgliedstaats, in dem der für die Verarbeitung Verantwortliche oder der Auftragsverarbeiter eine Niederlassung hat, oder wahlweise auch vor den Gerichten des Mitgliedstaats, in dem die betroffene Person ihren gewöhnlichen Aufenthalt hat, klagen können. Die Datenschutzgruppe hält die Möglichkeit der Klageerhebung in **einem beliebigen** Mitgliedstaat, in dem der für die Verarbeitung Verantwortliche oder der Auftragsverarbeiter eine Niederlassung hat, sei es die Hauptniederlassung oder die Niederlassung, in der relevante Entscheidungen über die Datenverarbeitung getroffen werden, für problematisch.

Obwohl Artikel 75 Absatz 4 vorsieht, dass die Mitgliedstaaten endgültige Entscheidungen anderer Gerichte vollstrecken, ist es fraglich, ob eine Entscheidung eines Gerichts in einem Mitgliedstaat, in dem der für die Verarbeitung Verantwortliche oder der Auftragsverarbeiter nicht seine Hauptniederlassung hat, wirklich vollstreckbar ist. Dies muss klargestellt werden.

Darüber hinaus begrüßt die Datenschutzgruppe zwar die in Artikel 75 Absatz 2 vorgesehene Möglichkeit, gegen einen für die Verarbeitung Verantwortlichen vor den Gerichten des Mitgliedstaats, in dem die betroffene Person ihren gewöhnlichen Aufenthalt hat, Klage zu erheben – ein Konzept, das dem des Verbraucherschutzes nach der Brüssel-I-Verordnung ähnelt und die Stellung der betroffenen Personen stärken soll –, kann jedoch nicht erkennen, wie die Entscheidung eines Gerichts des Mitgliedstaats, in dem die betroffene Person ihren gewöhnlichen Aufenthalt hat, vollstreckt werden soll, wenn der für die Verarbeitung

Verantwortliche oder der Auftragsverarbeiter seine Niederlassung in einem anderen Mitgliedstaat hat.

Sowohl Artikel 74 Absatz 5 als auch Artikel 75 Absatz 4 sehen vor, dass die Mitgliedstaaten endgültige Entscheidungen der Gerichte im Sinne dieser Artikel vollstrecken. Diese Bestimmungen sind mit ähnlichen Verpflichtungen in Artikel 111 des Schengener Durchführungsübereinkommens vergleichbar. Wie bereits erwähnt, scheint unklar zu sein, nach welchen Verfahrensregeln und von welchen nationalen Behörden Entscheidungen der Gerichte eines Mitgliedstaats in einem anderen Mitgliedstaat vollstreckt werden sollen. Zudem besteht möglicherweise Bedarf, die Auslegung des Begriffs „endgültige Entscheidung“ weiter zu vereinheitlichen (Schengener Informationssystem – Rechtssache zwischen AU und FR).

Kirchen und religiöse Vereinigungen

Nach dem Verständnis der Datenschutzgruppe verpflichtet Artikel 85 Kirchen und religiöse Vereinigungen, die gegenwärtig eigene Regelungen anwenden, diese in Einklang mit der Verordnung zu bringen. In jedem Fall sollte Kirchen und religiösen Vereinigungen nicht gestattet werden, in denjenigen Mitgliedstaaten, deren verfassungsrechtliche Regelungen dies nicht zulassen, eigene Regelwerke, die mit der Verordnung nicht vereinbar sind, zu erlassen.

Bewertung der Richtlinie

Wahl des Instruments

Die Datenschutzgruppe nimmt zur Kenntnis, dass sich die Europäische Kommission ausdrücklich dafür entschieden hat, den Datenschutz nicht insgesamt in einem einzigen Rechtsinstrument zu regeln, sondern zur Regelung des Datenschutzes im Bereich der Polizei und Strafjustiz auf dem von ihr angestrebten einheitlich hohen Niveau eine Richtlinie vorzulegen. Allerdings weist die Datenschutzgruppe auch darauf hin, dass der Vorschlag in seiner jetzigen Form in mehreren Mitgliedstaaten zu einer Lockerung von Datenschutzstandards führen würde. Die Datenschutzgruppe hält dies für inakzeptabel und fordert deshalb den europäischen Gesetzgeber auf, dafür zu sorgen, dass die derzeitigen höheren Datenschutzgarantien in der Europäischen Union als das absolute Minimum für die vorgeschlagene Richtlinie angesehen werden. Die Richtlinie darf nicht als Rechtfertigung für die Streichung weitergehender Datenschutzgarantien in geltenden Gesetzen der Mitgliedstaaten herhalten.

Kohärenz

Obwohl verschiedene Rechtsinstrumente vorgeschlagen wurden, sollten die Vorschriften im Kern einheitlich sein, insbesondere im Hinblick auf die Grundsätze, Verpflichtungen und Aufgaben, einzelnen Rechte und Befugnisse sowie die den Aufsichtsbehörden zur Verfügung stehenden Instrumente. In Anbetracht dessen, dass sich die Richtlinie mit heiklen Verarbeitungsvorgängen befasst, wären geringere Standards in diesem Bereich inakzeptabel. Natürlich sind Beschränkungen und Ausnahmen notwendig, vor allem bei den Rechten der

betroffenen Personen, aber dennoch muss klar sein, dass es sich dabei um Ausnahmen handelt und die Kernaspekte dieselben sind.

Anwendungsbereich

Die Datenschutzgruppe stellt fest und begrüßt, dass in der Richtlinie die im Rahmenbeschluss 2008/977/JI getroffene Unterscheidung zwischen der Verarbeitung personenbezogener Daten in innerstaatlichen und grenzüberschreitenden Fällen aufgegeben wurde. Diese Beschränkung der Anwendbarkeit europäischer Rechtsvorschriften auf reine grenzüberschreitende Fälle ist in der Vergangenheit von der Datenschutzgruppe kritisiert worden.

Der Anwendungsbereich der Richtlinie sollte so klar wie möglich sein. Allerdings wirft der vorgeschlagene Wortlaut verschiedene Fragen auf, unter anderem folgende.

Die Datenschutzgruppe stellt fest, dass es schwierig ist, den Anwendungsbereich der Richtlinie von dem der Verordnung zu trennen. Die Richtlinie ist anwendbar, wenn zuständige Behörden personenbezogene Daten zum Zwecke der Verhütung, Aufdeckung, Untersuchung oder Verfolgung von Straftaten oder der Strafvollstreckung verarbeiten. In allen anderen Fällen ist die Verordnung als grundlegendes Rechtsinstrument für den Schutz personenbezogener Daten anzuwenden. Allerdings sind die unterschiedlichen Traditionen der Mitgliedstaaten bei der Zuordnung der Tätigkeiten ihrer Behörden zu Strafverfolgungszwecken oder rein verwaltungsrechtlichen Zwecken (etwa in den Bereichen Zoll, Einwanderung oder Umwelt) zu berücksichtigen. Infolgedessen kann für ein und dieselbe Einrichtung sowohl die Richtlinie als auch die Verordnung gelten. Es sind Situationen zu vermeiden, in denen derselbe Datenverarbeitungsvorgang, etwa im Zusammenhang mit der Aufrechterhaltung der öffentlichen Ordnung, in einem Staat unter die Verordnung fällt, während in anderen Mitgliedstaaten die auf der Richtlinie basierenden Gesetze anzuwenden sind. Dies ist vor allem dann hinderlich, wenn beide Instrumente, wie gegenwärtig der Fall, zu uneinheitlich sind. Aus diesem Grund ist es notwendig, beide Instrumente besser miteinander in Einklang zu bringen und den Begriff „zuständige Behörden“ klarer zu definieren. Nach Ansicht der Datenschutzgruppe muss klar sein, auf welche gesetzlich vorgesehenen Tätigkeiten der zuständigen Behörden die Richtlinie anzuwenden ist.

Die Datenschutzgruppe hält eine weitere Präzisierung des Umfangs, in dem die Richtlinie im Bereich des Strafverfahrens anwendbar ist, für erforderlich. Die Datenschutzgruppe nimmt zur Kenntnis, dass die Richtlinie auf die Verarbeitung von Daten zum Zwecke der Verfolgung von Straftaten anwendbar ist (Artikel 1). Zugleich ergibt sich nach dem Verständnis der Datenschutzgruppe aus Artikel 17 (und Erwägungsgrund 82), dass Mitgliedstaaten beschließen können, ihr einzelstaatliches Strafprozessrecht, zumindest soweit es um Gerichtsverfahren geht, nicht in Einklang mit den Rechten nach den Artikeln 11 – 16 zu bringen. Aufgrund der Unterschiede in den einzelstaatlichen Strafverfahren lässt sich jedoch kaum bestimmen, welche Phase der Strafverfolgung gemeint ist, wenn nach Artikel 17 der Richtlinie „das einzelstaatliche Strafprozessrecht zur Anwendung kommt, wenn es um personenbezogene Daten in einem Gerichtsbeschluss oder einem Gerichtsdokument geht, die in strafrechtlichen Ermittlungen und in Strafverfahren verarbeitet werden.“ Die Datenschutzgruppe fordert den europäischen Gesetzgeber auf, dafür zu sorgen, dass die Richtlinie zweifelsfrei auf Strafverfahren und die Verfolgung von Straftaten anwendbar ist, und in Einklang mit dem Übereinkommen 108 des Europarates zu vermeiden, dass kein

Datenschutz mehr gewährleistet ist, sobald ein Staatsanwalt oder Ermittlungsrichter an einer Strafverfolgungs- oder Ermittlungsmaßnahme beteiligt ist.
Darüber hinaus ist nach Ansicht der Datenschutzgruppe eine Klarstellung der Bedeutung und des Zwecks der in Artikel 44 Absatz 2 enthaltenen Formulierung „im Rahmen ihrer gerichtlichen Tätigkeit“ erforderlich. Es muss klar sein, in welchem Verhältnis Datenschutzbehörden und Gerichte zueinander stehen und unter welchen Umständen Aufsichtsaufgaben wahrgenommen werden können.

Datenverarbeitungsgrundsätze

Die Richtlinie lässt in ihren Grundsätzen wichtige Aspekte im Zusammenhang mit der Speicherung von personenbezogenen Daten (einschließlich der Speicherungsfristen), der Transparenz im Umgang mit Personen, der Aktualisierung personenbezogener Daten sowie der Frage vermissen, wie gewährleistet werden soll, dass die Daten angemessen, sachlich relevant und nicht exzessiv sind. Ebenso fehlen Bestimmungen zur Rechenschaftspflicht, wonach der für die Verarbeitung Verantwortliche die Einhaltung der Vorschriften nachweisen muss. Der Wortlaut von Artikel 4 sollte mit dem der Verordnung (Artikel 5) in Einklang gebracht werden.

Die Datenschutzgruppe schlägt außerdem vor, Bestimmungen aufzunehmen, die den Zugriff auf Daten auf dazu ordnungsgemäß ermächtigte Bedienstete der zuständigen Behörden, die sie zur Erfüllung ihrer Aufgaben benötigen, beschränken.

Neben den vorstehenden Ausführungen zur mangelnden Übereinstimmung mit der Verordnung begrüßt die Datenschutzgruppe die vorgeschlagene Unterscheidung verschiedener Kategorien von betroffenen Personen. Sie nimmt insbesondere zur Kenntnis, dass zwischen Daten über Verdächtige, Opfer, Zeugen usw. unterschieden werden soll. Außerdem begrüßt sie die vorgesehene Unterscheidung nach Qualität und sachlicher Richtigkeit der von Strafverfolgungsbehörden verarbeiteten Daten. Die Datenschutzgruppe bedauert jedoch, dass diese Unterscheidungen in den Artikeln 5 und 6 durch die Formulierung „so weit wie möglich“ eingeschränkt wurde, und schlägt vor, diese Formulierung zu streichen. Zudem ist sie über die sehr umfangreiche Kategorie sonstiger betroffener Personen (Artikel 5 Absatz 1 Buchstabe e), deren Daten verarbeitet werden dürfen, besorgt. Die Datenschutzgruppe schlägt vor, diese Kategorie so umzuformulieren, dass Daten über nicht verdächtigte Personen nur über einen sehr begrenzten Zeitraum und unter strengen Auflagen verarbeitet werden dürfen. In der Richtlinie sollte klargestellt werden, dass für die in Artikel 5 Absatz 1 Buchstaben b – e vorgesehenen Datenkategorien strengere Fristen und Prüfvorschriften gelten.

Im Hinblick auf die Rechtmäßigkeit der Verarbeitung (Artikel 7) ist unklar, warum die Bestimmungen der Buchstaben b, c und d aufgenommen wurden. Sie scheinen im Widerspruch zu Artikel 1 Absatz 1, der den Zweck der Richtlinie definiert, zu stehen. Die Datenschutzgruppe ist der Auffassung, dass es keinen Spielraum für die Verarbeitung von Daten gibt, wenn diese nicht in Einklang mit dem allgemeinen Zweck der Richtlinie steht. Daher müssen entweder die Buchstaben b, c und d gestrichen oder Artikel 1 Absatz 1 unter Zulassung dieser Verarbeitungsvorgänge angepasst werden.

Nach Ansicht der Datenschutzgruppe sollten nach dem Vorbild der Verordnung besondere Bestimmungen zur Verarbeitung personenbezogener Daten von Kindern aufgenommen werden. Insbesondere sollten die Mitgliedstaaten verpflichtet werden, Altersgrenzen festzulegen, bis zu deren Erreichen Daten nicht ohne hinreichende Begründung zum Zwecke

der Verhütung, Aufdeckung, Untersuchung oder Verfolgung von Straftaten verarbeitet werden dürfen, vor allem wenn besondere Kategorien von Daten erfasst werden sollen. Darüber hinaus sollten die Mitgliedstaaten bei Kinder betreffenden Daten kürzere Fristen für die Speicherung bzw. Aufbewahrung in Polizei- und Justizakten vorsehen.

Die Bestimmung zu besonderen Kategorien (Artikel 8) ist etwas weiter gefasst als im Rahmenbeschluss (2008/977/JI). Die Datenschutzgruppe fragt sich, welche Auswirkungen dies hat, und insbesondere, ob die Ausnahmen in Absatz 2 dazu führen können, dass einzelstaatliche Rechtsvorschriften erlassen werden, die eine Verarbeitung aller sensiblen Daten grundsätzlich zulassen. In diesem Falle würde das allgemeine Verarbeitungsverbot ins Leere laufen. Darüber hinaus gibt es trotz der Einbeziehung genetischer Daten weder einen gesonderten Erwägungsgrund noch einen Artikel zum Umgang mit dieser Art von Daten. Eine solche Bestimmung wäre jedoch eine wichtige Garantie in Bezug auf die Verwendung genetischer Daten und deren Speicherungsfristen.

Die Ausnahmeregelung nach Artikel 8 Absatz 2 birgt die reale Gefahr, dass für besondere Kategorien von personenbezogenen Daten (sensible Daten) ein jeweils unterschiedliches Schutzniveau zugelassen wird. Die Datenschutzgruppe schlägt daher vor, dass der europäische Gesetzgeber diesen Artikel unter Festlegung der erforderlichen geeigneten Garantien so ändert, dass eine einheitliche Umsetzung gewährleistet ist. Außerdem empfiehlt die Datenschutzgruppe, in Absatz 2 vorzusehen, dass die Ausnahmeregelungen nur in Einklang mit den in Artikel 4 festgelegten Bedingungen in Anspruch genommen werden können.

Rechte der betroffenen Personen

Die Datenschutzgruppe stellt fest und begrüßt, dass zumindest in einigen Mitgliedstaaten den betroffenen Personen aufgrund von Artikel 11 Absatz 1 und Artikel 13 Absatz 1, mehr Informationen mitgeteilt werden könnten. Darüber informiert zu werden, welche Daten aus welchem Grund verarbeitet werden, ist einer der wichtigsten Aspekte des Rechtes auf Datenschutz. Es ist jedoch auch festzustellen, dass die Einschränkungen der Pflicht zur Unterrichtung der betroffenen Person nach Artikel 11 Absatz 5 und des Auskunftsrechts nach Artikel 13 Absatz 2 problematisch sind. Die Datenschutzgruppe hält diese Einschränkungen und Ausnahmen für zu weit gefasst und zu allgemein, gestatten sie doch den Mitgliedstaaten, ganze Kategorien von Daten von der Auskunftspflicht auszunehmen. Dies würde die Rechte der betroffenen Personen (und nicht nur ihre Interessen, wie in Kapitel II dargelegt) schwer beeinträchtigen. In der Richtlinie sollte unmissverständlich festgelegt werden, dass jede Einschränkung der Rechte betroffener Personen in jedem Einzelfall unter Berücksichtigung der besonderen Umstände begründet und jede dieser Einschränkungen (nicht nur Unterlassungen) vollständig dokumentiert werden muss. Die Datenschutzgruppe ist zudem der Auffassung, dass eine Einschränkung des Auskunftsrechts und des Rechtes auf Unterrichtung auch so zu verstehen sein sollte, dass die betroffenen Personen in bestimmten Fällen noch teilweise über die Verarbeitung ihrer Daten unterrichtet werden können.

Im Hinblick auf die Einschränkung von Rechten sollte festgelegt werden, dass der für die Verarbeitung Verantwortliche von Fall zu Fall beurteilt, ob die jeweilige Einschränkung anzuwenden ist, und dass jede Einschränkung in Einklang mit der Charta der Grundrechte der Europäischen Union und der Konvention zum Schutze der Menschenrechte und Grundfreiheiten sowie der Rechtsprechung des Europäischen Gerichtshofs und des

Europäischen Gerichtshofs für Menschenrechte stehen und insbesondere den Wesensgehalt dieser Rechte und Freiheiten respektieren muss. Die Datenschutzgruppe empfiehlt, diese Bestimmung in Artikel 13 aufzunehmen.

Im Hinblick auf das Recht auf Berichtigung, das Recht auf Beschwerde, das Recht auf gerichtlichen Rechtsbehelf gegen die nationale Datenschutzbehörde, den für die Verarbeitung Verantwortlichen und den Auftragsverarbeiter sowie das Recht auf Schadenersatz und Haftung scheint die Richtlinie in Einklang mit der Verordnung zu sein.

Allerdings sieht die Richtlinie nicht das Recht vor, der Verarbeitung personenbezogener Daten zu widersprechen. Es gibt viele Situationen, in denen zum Beispiel betroffene Personen, Opfer oder Zeugen die Möglichkeit haben sollten, ihre Daten markieren zu lassen, um die weitere Verarbeitung am Ende des Gerichtsverfahrens einzuschränken.

Außerdem wird der für die Verarbeitung Verantwortliche in der Richtlinie verpflichtet, auf Anfragen von Personen, die ihr Recht auf Auskunft, Berichtigung oder Löschung wahrnehmen, „ohne unangemessene Verzögerung“ zu reagieren. Es ist unklar, warum die in der Verordnung festgelegten Fristen nicht auch hier gelten können. Zudem sollten die Modalitäten, nach denen Personen Rechte ausüben können, besser mit den in der Verordnung beschriebenen Verfahren in Einklang gebracht werden.

Pflichten des für die Verarbeitung Verantwortlichen

Im Hinblick auf Auftragsverarbeiter, Vereinbarungen zwischen gemeinsam für die Verarbeitung Verantwortlichen, die obligatorische Zusammenarbeit mit den nationalen Datenschutzbehörden und die Aufgaben des Datenschutzbeauftragten stehen die Pflichten der für die Verarbeitung Verantwortlichen in Einklang mit den in der Verordnung vorgesehenen Pflichten. Allerdings ist der für die Verarbeitung Verantwortliche nach der Richtlinie nicht verpflichtet, die betroffene Person zu unterrichten, wenn er beabsichtigt, personenbezogene Daten an ein Drittland zu übermitteln, und es leuchtet nicht ein, warum dies ausgeschlossen wurde, vor allem in Anbetracht dessen, dass die Mitgliedstaaten die Rechte von Personen unter bestimmten Umständen einschränken können.

Darüber hinaus sieht die Datenschutzgruppe keinen Grund dafür, dass die den Datenschutz durch Technik und datenschutzfreundliche Voreinstellung betreffenden Regelungen der Richtlinie nicht in Einklang mit der Verordnung stehen. Ein Aspekt des Datenschutzes durch Technik besteht darin, die mit der Verarbeitung verbundenen Risiken frühzeitig zu bestimmen, um sie mildern zu können. Daher drängt die Datenschutzgruppe dazu, in die Richtlinie Bestimmungen aufzunehmen, die Datenschutz-Folgenabschätzungen, auch während des Gesetzgebungsverfahrens, vorsehen. Diese sind ihrer Ansicht nach bei der Verarbeitung personenbezogener Daten im Bereich der Strafverfolgung von besonderer Bedeutung, weil gerade diese Verarbeitungsvorgänge mit erhöhten Risiken für die betroffenen Personen verbunden sind. Die Dokumentationspflichten sind ebenfalls weniger ausführlich geregelt als in der Verordnung. Die von der Richtlinie erfassten zuständigen Behörden sollten zumindest auch die Kontaktdaten ihrer Datenschutzbeauftragten und die Speicherungsfristen dokumentieren müssen.

Die Datenschutzgruppe stellt fest, dass die Anforderungen an die Datensicherheit nicht sehr ausführlich formuliert und somit im Vergleich zu den aktuellen Standards ziemlich gering sind. So sehen etwa die Datensicherheitspflichten im Gegensatz zur Richtlinie keinen Schutz

gegen unbeabsichtigten Verlust vor. Die Datenschutzgruppe fordert den europäischen Gesetzgeber nachdrücklich auf, diesen Aspekt in die Richtlinie einzubeziehen, zumal er sowohl in der aktuellen Richtlinie (95/46/EG) als auch im Rahmenbeschluss zum Datenschutz (2008/977/JI) verankert ist.

Auch die Bestimmungen zur Meldepflicht bei Verletzungen des Schutzes personenbezogener Daten sollten in beiden Instrumenten einheitlich gefasst sein. Die Datenschutzgruppe erkennt jedoch die Unterschiede bei der Benachrichtigung betroffener Personen im Bereich der Strafverfolgung an. So mag es beispielsweise nicht immer praktikabel sein, Personen innerhalb bestimmter Fristen über eine solche Verletzung zu unterrichten, wenn dies strafrechtliche Ermittlungen oder Strafverfolgungsmaßnahmen beeinträchtigen könnte. Die Datenschutzbehörde könnte ebenfalls die Aufgabe übernehmen, unter Berücksichtigung der Angemessenheit der technischen Schutzmaßnahmen zu beurteilen, ob und wann die betroffene Person zu benachrichtigen ist.
Schließlich stehen die Bestimmungen zum Profiling und zur automatischen Datenverarbeitung (Artikel 9) nicht in Einklang mit der Verordnung, da in der Richtlinie relevante Elemente wie die Verhaltensbeurteilung nicht enthalten sind.

Datenübermittlungen ins Ausland

Allgemeine Grundsätze für die Übermittlung und Weitergabe

Artikel 33 enthält Bestimmungen, die sowohl die ursprüngliche Übermittlung als auch die Weitergabe von personenbezogenen Daten an Drittländer oder internationale Organisationen betreffen. Nach Ansicht der Datenschutzgruppe muss zwischen diesen Fällen klar unterschieden werden, um zusätzliche Beschränkungen für die Weitergabe, etwa eine eindeutige Bindung an den Zweck, zu dem die Daten ursprünglich erhoben wurden, und die vorherige Zustimmung der übermittelnden Behörde, vorsehen zu können. Darüber hinaus muss der Empfänger der Daten eine zuständige Behörde im Sinne der Richtlinie sein.

Negative Angemessenheitsbeschlüsse

Der Datenschutzgruppe ist nicht klar, welchen Zweck negative Angemessenheitsbeschlüsse haben und wie sie in der Praxis funktionieren sollen. Die Formulierung legt nahe, dass ein negativer Angemessenheitsbeschluss sämtliche Übermittlungen an ein bestimmtes Drittland, eine internationale Organisation oder einen Verarbeitungssektor blockiert. Artikel 34 Absatz 6 und Artikel 35 Absatz 1 lassen sich jedoch auch so auslegen, dass Übermittlungen in Drittländer, für die ein negativer Angemessenheitsbeschluss vorliegt, zulässig sind, solange die von dem für die Verarbeitung Verantwortlichen und/oder dem Auftragsverarbeiter selbst durchgeführte Beurteilung der Angemessenheit zu einem positiven Ergebnis führt und geeignete Garantien vereinbart worden sind. Der europäische Gesetzgeber wird daher aufgefordert, die Bestimmungen so abzuändern, dass daraus eindeutig hervorgeht, welche Folgen ein negativer Angemessenheitsbeschluss hat und wie er in der Praxis funktioniert.

Datenübermittlung auf der Grundlage geeigneter Garantien

Die Richtlinie sieht in Artikel 35 die Möglichkeit vor, personenbezogene Daten an Drittländer oder internationale Organisationen zu übermitteln, wenn die Kommission keinen Angemessenheitsbeschluss erlassen hat. Falls solche Übermittlungen auf der Grundlage von Selbstbeurteilungen erfolgen sollen, muss die zuständige Behörde nach Ansicht der

Datenschutzgruppe gewährleisten, dass die geeigneten Garantien in einem rechtlich verbindlichen Instrument festgelegt werden. Darüber hinaus sollten bei der Selbstbeurteilung zumindest die in Artikel 26 Absatz 2 der Richtlinie 95/46/EG dargelegten Elemente berücksichtigt werden. Der zur Selbstbeurteilung führende Prozess muss vollständig dokumentiert sein. Die Dokumentation ist den Datenschutzbehörden auf Anfrage vorzulegen.

Ausnahmen

Die Datenschutzgruppe ist besorgt über die Ausnahmen für die Übermittlung personenbezogener Daten ohne Angemessenheitsbeschluss oder geeignete Garantien (Artikel 36) und insbesondere über die nach den Buchstaben c, d und e vorgesehenen Ausnahmen. Diese Ausnahmen würden Spielraum für eine Vielzahl von Übermittlungen ins Ausland auf Einzelfallbasis lassen, solange sie nur „erforderlich“ sind. Es muss klar sein, dass alle Ausnahmen restriktiv auszulegen sind, dass also auf dieser Grundlage erfolgende Übermittlungen nicht die Regel, sondern die Ausnahme sind. Vermieden werden sollte auch, dass der Wortlaut der Bestimmungen die Auslegung zulässt, die bloße Angabe der Notwendigkeit der betreffenden Übermittlung reiche aus, um diese Ausnahmeregelungen in Anspruch nehmen zu können, und somit umfangreiche Übermittlungen ins Ausland auf Einzelfallbasis ohne Garantien für den Schutz der personenbezogenen Daten der betroffenen Personen ermöglicht. Die Datenschutzgruppe ist daher der Auffassung, dass der Wortlaut von Artikel 36 Buchstaben c, d und e die Möglichkeiten, Daten auf Einzelfallbasis ins Ausland zu übermitteln, einschränken sollte.

Des Weiteren stellt die Datenschutzgruppe fest, dass keinerlei Verpflichtung vorgesehen ist, die Inanspruchnahme von Ausnahmen nach Artikel 36 zu dokumentieren. Dies macht es für die Aufsichtsbehörde schwer, wenn nicht unmöglich, zu überprüfen, ob der für die Verarbeitung Verantwortliche bzw. der Auftragsverarbeiter die für die Ausnahmen festgelegten Bedingungen eingehalten hat. Wir schlagen daher vor, eine solche Verpflichtung durch Einfügen des folgenden Absatzes aufzunehmen: *„2. Die Inanspruchnahme dieser Ausnahmen ist zu dokumentieren und die Dokumentation ist der Aufsichtsbehörde auf Verlangen vorzulegen.“*

Schließlich ist die Datenschutzgruppe grundsätzlich der Auffassung, dass die Mitgliedstaaten in Bezug auf Übermittlungen an Drittländer ohne Vorliegen eines Angemessenheitsbeschlusses entscheiden können sollten, ob und in welchem Umfang Datenschutzbehörden in die Übermittlungen einbezogen werden.

<u>Befugnisse der Datenschutzbehörden und Zusammenarbeit</u>

Die Datenschutzgruppe bedauert, dass die Befugnisse der Datenschutzbehörden weder sehr ausführlich geregelt sind noch in Einklang mit den Bestimmungen der Verordnung stehen. Insbesondere enthält die Richtlinie im Gegensatz zur Verordnung keine Regelungen, die den Zugang zu Geschäftsräumen betreffen. Die Aufsichtsbehörde sollte in allen Bereichen die Möglichkeit haben, nötigenfalls Geschäftsräume des für die Verarbeitung Verantwortlichen zu betreten.

Die Richtlinie sieht zwar Amtshilfe zwischen Datenschutzbehörden vor, nicht jedoch die in der Verordnung festgelegten Fristen. Dies birgt die Gefahr mangelnder Einheitlichkeit, weshalb die in der Verordnung enthaltenen Fristempfehlungen für beide Rechtsinstrumente gelten sollten. Ebenfalls zur Vereinheitlichung beider Instrumente sollte die Richtlinie die

Möglichkeit vorsehen, dass sich Datenschutzbehörden an gemeinsamen Maßnahmen beteiligen.

Was fehlt

Die Datenschutzgruppe bedauert, dass die Richtlinie keine Bestimmungen zu Fristen, Überprüfungen und anderen Garantien (etwa die Beschränkung der Verwendung von Daten auf schwere Straftaten usw.) enthält. Die Datenschutzgruppe nimmt Artikel 37 zur Kenntnis, der vorsieht, dass der für die Verarbeitung Verantwortliche den Empfänger personenbezogener Daten auf Verarbeitungsbeschränkungen hinweist und alle vertretbaren Vorkehrungen trifft, um sicherzustellen, dass diese Beschränkungen eingehalten werden. Allerdings gilt Artikel 37 nur für Übermittlungen an Drittländer. Es wird nicht begründet, warum die Richtlinie keine vergleichbare Regelung für die Übermittlung personenbezogener Daten zwischen Mitgliedstaaten der Union enthält. Die empfangenden Mitgliedstaaten sollten in diesen Fällen ebenfalls verpflichtet sein, etwaige vom übertragenden Mitgliedstaat festgelegte Verarbeitungsbeschränkungen zu befolgen. Die Datenschutzgruppe ist überrascht, dass die Richtlinie in dieser Hinsicht einen Rückschritt gegenüber dem Rahmenbeschluss 2008/977/JI darstellt.

Die Datenschutzgruppe stellt fest, dass zuständige Behörden, die Daten übermittelt haben, nicht verpflichtet sind, den Empfänger zu unterrichten, wenn die übermittelten Daten unrichtig waren oder unrechtmäßig übermittelt wurden. Eine solche Verpflichtung ist bei einem freien Verkehr von Strafverfolgungsinformationen von entscheidender Bedeutung. Die Mitgliedstaaten können nach Artikel 39 Absatz 2 vorsehen, dass für die Überwachung der Anwendung der nach der Richtlinie erlassenen Vorschriften dieselbe Datenschutzbehörde zuständig ist wie für die Verordnung. Unter gebührender Berücksichtigung der Gegebenheiten in den Mitgliedstaaten, insbesondere in Ländern mit subnationalen Datenschutzbehörden, würde die Datenschutzgruppe eine Regelung bevorzugen, nach der eine einzige Datenschutzbehörde für die Überwachung beider Instrumente zuständig wäre, weil dies eine einheitliche Anwendung der Vorschriften gewährleisten würde.

Die Datenschutzgruppe bedauert schließlich auch, dass die Richtlinie keine Vorschriften zur Übermittlung von Daten an private Nutzer oder andere Behörden, die keine zuständigen Behörden im Sinne der Richtlinie sind, enthält. Die Datenschutzgruppe fordert deshalb den europäischen Gesetzgeber nachdrücklich auf, eine Bestimmung aufzunehmen, wonach Übermittlungen von Strafverfolgungsdaten an private Nutzer nur unter gesetzlich genau festgelegten Bedingungen zulässig sind.

Brüssel, den 23. März 2012

Für die Datenschutzgruppe
Der Vorsitzende
Jacob KOHNSTAMM

Die belgische und die rumänische Datenschutzbehörde haben sich nur deshalb der Stimme enthalten, weil sie eine Verordnung nicht für das geeignete Rechtsinstrument halten.

Die tschechische Datenschutzbehörde hat sich ebenfalls der Stimme enthalten.

Die estnische Datenschutzbehörde hat gegen die Stellungnahme gestimmt, weil sie bezweifelt, dass das vorgeschlagene Reformpaket im Einklang mit den erklärten Zwecken steht. Nach Ansicht der estnischen Datenschutzbehörde sind zu viele wesentliche Aspekte in dem Paket unbefriedigend geregelt, z. B.:

1) Fehlen einer echten Folgenabschätzung (ablehnende Stellungnahme des Ausschusses für Folgenabschätzung),
2) Form der unmittelbar anwendbaren Verordnung für einen Rechtsrahmen,
3) höherer Verwaltungsaufwand,
4) Umfang der delegierten Rechtsakte,
5) Schwächung der einzelstaatlichen Datenschutzbehörden, Schutz dringend schutzbedürftiger Datenschutzrechte verzögert sich weiter, Verlängerung von Schutzmaßnahmen,
6) Zuständigkeitsproblem beim Entwurf der Datenschutzrichtlinie für Polizei und Strafjustiz,
7) Verstoß gegen den Subsidiaritätsgrundsatz.

Die estnische Datenschutzbehörde kann daher den wichtigsten Schlussfolgerungen nicht zustimmen:

1) Der Entwurf der Verordnung ist zu schwach, um dazu eine „grundsätzlich positive Haltung“ einzunehmen.
2) Wir sind nicht der Auffassung, dass der Entwurf der Richtlinie über den Datenschutz im Bereich Polizei und Justiz zu anspruchslos ist. Wir halten ihn für zu weitreichend, weil die Gesetzgebungskompetenz für innerstaatliches Prozessrecht zu stark eingeschränkt wird.