KOMMISSION DER EUROPÄISCHEN GEMEINSCHAFTEN

Brüssel, den 4.10.2005
KOM(2005) 475 endgültig

2005/0202 (CNS)

Vorschlag für einen

RAHMENBESCHLUSS DES RATES

über den Schutz personenbezogener Daten, die im Rahmen der polizeilichen und justiziellen Zusammenarbeit in Strafsachen verarbeitet werden

{SEC(2005) 1241}

(von der Kommission vorgelegt)

BEGRÜNDUNG

1) HINTERGRUND DES VORSCHLAGS

- **Gründe und Ziele**

Am 4. November 2004 hat der Europäische Rat das Haager Programm zur Stärkung von Freiheit, Sicherheit und Recht in der Europäischen Union[1] angenommen. Darin wird die Kommission ersucht, bis spätestens Ende 2005 Vorschläge zur Verwirklichung des Verfügbarkeitsgrundsatzes vorzulegen, damit der grenzüberschreitende Austausch von strafverfolgungsrelevanten Informationen zwischen den Mitgliedstaaten verbessert werden kann. Gemäß dem Haager Programm sind bei den Vorschlägen bestimmte Hauptbedingungen in Bezug auf den Datenschutz streng einzuhalten.

Im Juni 2005 haben der Rat und die Kommission einen Aktionsplan zur Umsetzung des Haager Programms[2] angenommen. Dieser gründet sich auf die Mitteilung der Kommission an den Rat und das Europäische Parlament „Das Haager Programm: Zehn Prioritäten für die nächsten fünf Jahre - Die Partnerschaft zur Erneuerung Europas im Bereich der Freiheit, der Sicherheit und des Rechts“[3]. Der Aktionsplan sieht unter anderem vor, dass die Kommission im Jahr 2005 Vorschläge *(1) zur Einführung des Verfügbarkeitsgrundsatzes in Bezug auf strafverfolgungsrelevante Informationen und (2) für angemessene Schutzmaßnahmen und einen wirksamen Rechtsschutz in Bezug auf den Transfer personenbezogener Daten für Zwecke der polizeilichen und justiziellen Zusammenarbeit* vorlegt. Der Rat „Justiz und Inneres“ hat die Kommission in seiner Erklärung der EU zu den Londoner Bombenanschlägen[4] vom 13. Juli 2005 aufgefordert, diese Vorschläge bis spätestens Oktober 2005 vorzulegen.

Dieser Rahmenbeschluss stellt auf den Schutz der personenbezogenen Daten ab, die im Rahmen der polizeilichen und justiziellen Zusammenarbeit zwischen den Mitgliedstaaten der Europäischen in Strafsachen (Titel VI EU-Vertrag) verarbeitet werden. Diese Zusammenarbeit – insbesondere bei der Terrorismusverhütung und -bekämpfung – soll unter strikter Einhaltung der wesentlichen Datenschutzvorschriften verbessert werden. Durch den Rahmenbeschluss soll zudem sichergestellt werden, dass insbesondere im Hinblick auf die Verwirklichung des Verfügbarkeitsgrundsatzes die Grundrechte und vor allem das Recht auf den Schutz der Privatsphäre und der Schutz personenbezogener Daten in der gesamten Europäischen Union gewahrt bleiben. Außerdem soll dafür Sorge getragen werden, dass der Austausch sachdienlicher Informationen zwischen den Mitgliedstaaten nicht durch Unterschiede beim Datenschutz behindert wird.

---

1 ABl. C 53 vom 3.3.2005, S. 1.
2 ABl. C 198 vom 12.8.2005, S. 1.
3 KOM(2005) 184 endg. vom 10.5.2005.
4 Arbeitsdokument des Rates 11158/05 REV 1 JAI 255.

- **Allgemeiner Hintergrund**

Auf Initiative Italiens[5] wurde der Schutz personenbezogener Daten im Rahmen des dritten Pfeilers bereits im Jahre 1998 erörtert. Der Rat „Justiz und Inneres" nahm seinerzeit den so genannten Wiener Aktionsplan[6] an. Dieser sah vor, dass in Bezug auf die horizontalen Fragen der polizeilichen und justiziellen Zusammenarbeit in Strafsachen innerhalb von zwei Jahren nach Inkrafttreten des Vertrags die Frage geprüft werden sollte, ob die Datenschutzvorschriften harmonisiert werden könnten. Im Jahre 2001 jedoch scheiterte die Annahme einer Entschließung über die Aufnahme von entsprechenden Datenschutzbestimmungen in Rechtsakte des dritten Pfeilers[7]. Im Juni 2003 schlug der griechische Ratsvorsitz gemeinsame Regeln für den Schutz personenbezogener Daten im Rahmen des dritten Pfeilers[8] vor, die sich auf die Datenschutzrichtlinie 95/46/EG und die Charta der Menschenrechte der Europäischen Union gründeten. Im Jahr 2005 haben die Datenschutzstellen der Mitgliedstaaten der Europäischen Union und der Europäische Datenschutzbeauftragte ein neues Rechtsinstrument für den Schutz personenbezogener Daten im Rahmen des dritten Pfeilers[9] gefordert. Zudem hat sich das Europäische Parlament dafür ausgesprochen, die im Rahmen der Rechtsvorschriften des dritten Pfeilers geltenden Bestimmungen über den Schutz personenbezogener Daten zu einem Rechtsakt zusammenfassen, durch den derselbe Schutz gewährleistet wird, wie ihn die einschlägigen Vorschriften des ersten Pfeilers vorsehen[10].

Das Haager Programm macht die Verwirklichung des Verfügbarkeitsgrundsatzes von einer Reihe von Hauptbedingungen auf dem Gebiet des Datenschutzes abhängig. Der Europäische Rat hat eingeräumt, dass die auf europäischer Ebene geltenden Datenschutzbestimmungen in ihrer jetzigen Form nicht für die Verwirklichung des Verfügbarkeitsgrundsatzes ausreichen, welche ja gegebenenfalls Modalitäten wie den gegenseitigen Zugriff auf nationale Datenbanken oder deren Interoperabilität, oder den direkten (Online-)Zugang zu den bestehenden zentralen Datenbanken der EU erfordern würde.

Das Ziel eines ausreichenden Datenschutzes steht auch im Mittelpunkt des Kooperationsabkommens, das sieben Mitgliedstaaten der EU (Deutschland, Österreich, Belgien, Niederlande, Luxemburg, Frankreich und Spanien) am 27. Mai 2005 in Prüm abgeschlossen haben und das diese Länder generell als Vorbild für den Informationsaustausch zwischen den Mitgliedstaaten empfehlen. Das Abkommen sieht vor, das die Strafverfolgungsbehörden eines beteiligten Landes unter bestimmten Bedingungen einen automatischen direkten Zugriff auf die von einem anderen beteiligten Land gespeicherten personenbezogenen Daten erhalten. Diese Form der Zusammenarbeit tritt in Kraft, sobald die Datenschutzbestimmungen des Abkommens in den beteiligten Ländern in nationales Recht umgesetzt worden sind.

---

5 Arbeitsdokument des Rates 8321/98 JAI 15.

6 ABl. C 19 vom 23.1.1999, S. 1.

7 Arbeitsdokument des Rates 6316/2/01 REV 2 JAI 15

8 2514. Tagung des Rates „Justiz und Inneres" am 5.-6. Juni 2003 in Luxemburg, Ratsdokument 9845/03 (Presse 150), S. 32.

9 Siehe die auf der Frühjahreskonferenz der europäischen Datenschutzstellen vom 25.-26. April 2005 in Krakau angenommene Erklärung und Stellungnahme über die Strafverfolgung und den Informationsaustausch in der EU.

10 Siehe Empfehlung 1 der am 7. Juni 2005 vom Europäischen Parlament angenommenen Empfehlungen für den Europäischen Rat und den Rat zum Informationsaustausch und zur Zusammenarbeit bei der Bekämpfung terroristischer Handlungen (2005/2046(INI).

- **Bestehende einschlägige Rechtsvorschriften**

Die Charta der Grundrechte der Europäischen Union[11] erkennt das Recht auf Privatsphäre (Artikel 7) und das Recht auf den Schutz personenbezogener Daten (Artikel 8) ausdrücklich an. Personenbezogene Daten dürfen nur nach Treu und Glauben für festgelegte Zwecke und mit Einwilligung der betroffenen Person oder auf einer sonstigen gesetzlich geregelten legitimen Grundlage verarbeitet werden. Jede Person hat das Recht, Auskunft über die sie betreffenden erhobenen Daten zu erhalten und die Berichtigung der Daten zu erwirken. Die Einhaltung dieser Vorschriften wird von einer unabhängigen Stelle überwacht.

Die Richtlinie 95/46/EG des Europäischen Parlaments und des Rates vom 24. Oktober 1995 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr[12] enthält grundlegende Bestimmungen über die Rechtmäßigkeit der Verarbeitung personenbezogener Daten und über die Rechte der betroffenen Person. Sie schließt zudem Bestimmungen über Rechtsbehelfe, Haftung, Sanktionen, die Übermittlung personenbezogener Daten an Drittstaaten, Verhaltensregeln, Kontrollstellen, eine Datenschutzgruppe und schließlich gemeinschaftliche Durchführungsmaßnahmen ein. Die Richtlinie gilt jedoch nicht für Tätigkeiten, die nicht in den Bereich des Gemeinschaftsrechts fallen, also beispielsweise die unter Titel VI EU-Vertrag fallenden Tätigkeiten. Dementsprechend können die Mitgliedstaaten selbst über geeignete Vorschriften für die Datenverarbeitung und den Datenschutz entscheiden. Im Rahmen von Titel VI EU-Vertrag ist der Schutz personenbezogener Daten durch unterschiedliche Rechtsakte geregelt, so insbesondere durch die Rechtsakte zur Einführung der gemeinsamen Informationssysteme auf europäischer Ebene (z.B. das Übereinkommen zur Durchführung des Übereinkommens von Schengen mit spezifischen Datenschutzbestimmungen für das Schengener Informationssystem[13], das Europol-Übereinkommen von 1995[14] sowie u.a. die Bestimmungen über die Übermittlung von personenbezogenen Daten durch Europol an Drittstaaten und Drittstellen[15], der Beschluss über die Errichtung von Eurojust aus dem Jahr 2002[16] und die Bestimmungen der Geschäftsordnung betreffend die Verarbeitung und den Schutz personenbezogener Daten bei Eurojust[17], das Übereinkommen über den Einsatz der Informationstechnologie im Zollbereich aus dem Jahre 1995 mit spezifischen Datenschutzbestimmungen für das Zollinformationssystem[18] und das Übereinkommen über die Rechtshilfe in Strafsachen zwischen den Mitgliedstaaten der Europäischen Union aus dem Jahre 2000, insbesondere Artikel 23[19]). In Bezug auf das Schengener Informationssystem ist vor allem die Frage der Einrichtung, des Betriebs und der Nutzung des Schengener Informationssystems der zweiten Generation (SIS II) von Belang, die bereits Gegenstand von

---

11 ABl. C 364 vom 18.12.2000, S. 1, 10.
12 ABl. L 281 vom 23.11.1995, S. 31.
13 ABl. L 239 vom 22.2.2000, S. 19.
14 ABl. C 316 vom 27.11.1995, S. 2.
15 ABl. C 88 vom 30.3.1999, S. 1.
16 ABl. L 63 vom 6.3.2002, S. 1.
17 ABl. C 68 vom 19.3.2005, S. 1.
18 ABl. C 316 vom 27.11.1995, S. 34.
19 ABl. C 197 vom 12.7.2000, S. 1, 15.

Vorschlägen der Kommission für einen entsprechenden Ratsbeschluss[20] und zwei Verordnungen[21] gewesen ist.

Zu beachten gilt es ferner Artikel 8 der Europäischen Konvention zum Schutze der Menschenrechte und Grundfreiheiten sowie das Übereinkommen Nr. 108 des Europarats zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten aus dem Jahre 1981, das diesbezügliche Zusatzprotokoll über Kontrollstellen und grenzüberschreitenden Datenverkehr aus dem Jahr 2001 sowie die Empfehlung R (87) 15 von 1987 über die Nutzung personenbezogener Daten im Polizeibereich. Das Übereinkommen ist von allen Mitgliedstaaten ratifiziert worden, das Zusatzprotokoll hingegen nicht.

- **Übereinstimmung mit anderen Politikbereichen und Zielen der Europäischen Union**

Es ist den Besonderheiten der Vorschriften über die Datenverarbeitung und den Datenschutz im Rahmen von Titel VI EU-Vertrag Rechnung zu tragen. Diese müssen zum einen mit der allgemeinen Politik der Union auf dem Gebiet des Schutzes der Privatsphäre und des Datenschutzes auf der Grundlage der Charta der Grundrechte der Europäischen Union und der Richtlinie 95/46/EG übereinstimmen. Die Grundprinzipien des Datenschutzes gelten zudem für den Datenschutz sowohl im Rahmen des ersten als auch im Rahmen des dritten Pfeilers. Auch muss die Übereinstimmung mit anderen Rechtsakten gewährleistet sein, die spezifische Pflichten in Bezug auf Informationen vorsehen, die von Belang für die Kriminalitätsvorbeugung und –bekämpfung sein können. Zu beachten ist zudem die Entwicklung in Bezug auf die Frage der Archivierung von Daten, die im Zusammenhang mit der Erbringung öffentlich zugänglicher elektronischer Kommunikationsdienstleistungen verarbeitet und gespeichert werden, oder von Daten, die über öffentliche Kommunikationsnetze übertragen werden, zur Verhütung, Aufdeckung, Untersuchung und Verfolgung von Straftaten und strafbaren Handlungen, einschließlich terroristischer Straftaten. Besonders hinzuweisen ist auf den engen Zusammenhang zwischen dem vorgeschlagenen Rahmenbeschluss und dem Vorschlag der Kommission für eine Richtlinie des Europäischen Parlaments und des Rates über die Vorratsspeicherung von Daten, die bei der Bereitstellung öffentlicher elektronischer Kommunikationsdienste verarbeitet werden, und zur Änderung der Richtlinie 2002/58/EG[22].

2) KONSULTATION BETROFFENER UND FOLGENABSCHÄTZUNG

- **Konsultation Betroffener**

Konsultationsmethoden, Hauptadressaten und allgemeines Profil der Antwortenden

Am 22. November 2004 und am 21. Juni konsultierte die Kommission Regierungssachverständige aus den Mitgliedstaaten, Island, Norwegen und der Schweiz, und am 11. Januar 2005 konsultierte sie Sachverständige der Datenschutzstellen dieser Länder. Der Europäische Datenschutzbeauftragte, Europol, Eurojust und das Sekretariat der Gemeinsamen Kontrollstellen waren dabei ebenfalls vertreten. Durch die Konsultationen

[20] KOM(2005) 230 endg.
[21] KOM(2005) 236 endg. und KOM(2005) 237 endg.
[22] KOM (2005) 438 endg. vom 21.9.2005.

sollte vor allem ermittelt werden, ob ein Rechtsakt über die Verarbeitung und den Schutz personenbezogener Daten im Rahmen des dritten Pfeilers benötigt wird und welchen Inhalts dieser gegebenenfalls sein müsste. Die Konsultation erfolgte unter anderem anhand eines Fragebogens und eines Arbeitsdokuments der Kommission über den in einem etwaigen Rechtsakt zu verfolgenden allgemeinen Ansatz und den Bezug zu den geltenden Rechtsvorschriften, die Rechtsgrundlage, den Anwendungsbereich, die Grundsätze bezüglich der Datenqualität, die Kriterien für eine rechtmäßige Datenverarbeitung durch Polizei- und Justizbehörden, die Behandlung personenbezogener Daten nicht verdächtigter Personen, die Anforderungen für die Übermittlung personenbezogener Daten an die zuständigen Behörden in anderen Mitgliedstaaten oder in Drittländern, die Rechte der Betroffenen, Kontrollbehörden und ein etwaiges Beratungsgremium für den Datenschutz im Rahmen des dritten Pfeilers.

Die Datenschutzgruppe nach Artikel 29 der Richtlinie 95/46/EG wurde regelmäßig über die aktuellen Entwicklungen unterrichtet. Vertreter der Kommission wohnten den Sitzungen der polizeilichen Arbeitsgruppe auf der Konferenz der Europäischen Datenschutzstellen vom 12. April und 21. Juni 2005 bei. Am 31. Januar 2005 nahmen Vertreter der Kommission an einem öffentlichen Seminar mit dem Titel „Datenschutz und Sicherheit der Bürger: Welche Grundsätze für die Europäische Union?“ teil, das vom Ausschuss für bürgerliche Freiheiten, Justiz und Inneres veranstaltet wurde. Die Kommission hat zudem den Ergebnissen der Frühjahrskonferenz der Europäischen Datenschutzstellen (Krakow, 25.-26. April 2005) Rechnung getragen und auch den Standpunkt des Europäischen Parlaments berücksichtigt, der unter anderem in der Empfehlung des Parlaments an den Europäischen Rat und den Rat über den Informationsaustausch und die Zusammenarbeit betreffend terroristische Straftaten (2005/2046(INI) vom 7. Juni 2005) zum Ausdruck gekommen ist.

Zusammenfassung und Berücksichtigung der Antworten

Sowohl das Europäische Parlament als auch die Datenschutzstellen in der Europäischen Union haben sich sehr für einen Rechtsakt über den Schutz personenbezogener Daten im Rahmen des dritten Pfeilers ausgesprochen. Die Regierungsvertreter aus den Mitgliedstaaten, Island, Norwegen und der Schweiz sowie die Sachverständigen von Europol und Eurojust konnten sich diesbezüglich auf keinen gemeinsamen Standpunkt einigen. Gleichwohl könnte die Kommission hieraus den Schluss ziehen, dass im Prinzip keine Einwände gegen einen solchen Rechtsakt bestehen. Es schien Einigkeit darüber zu bestehen, dass die Verwirklichung des Verfügbarkeitsgrundsatzes mit dem Erlass geeigneter Datenschutzbestimmungen einhergehen muss. Einige Mitgliedstaaten haben sich dafür ausgesprochen, zunächst festzulegen, wie der Informationsaustausch künftig erfolgen soll, und dann entsprechende Bestimmungen zum Schutz personenbezogener Daten zu erlassen. Andere Mitgliedstaaten würden es vorziehen, einschlägige Datenschutzbestimmungen gleich in den Rechtsakt über den Verfügbarkeitsgrundsatz aufzunehmen.

Die Kommission vertritt nach Abwiegen der unterschiedlichen Auffassungen den Standpunkt, dass die Verwirklichung des Verfügbarkeitsgrundsatzes weiter voranschreiten und die Art und Intensität des Informationsaustausches zwischen den Mitgliedstaaten grundlegend verändern wird. Diese Entwicklung wird beträchtliche Auswirkungen auf die personenbezogenen Daten und das Recht auf Datenschutz mit sich bringen, zu denen ein entsprechendes Gegengewicht zu schaffen sein wird. In jedem Fall bringen die jüngsten Maßnahmen für einen automatischen direkten Datenzugriff, der mehr oder weniger gezielt erfolgt, die Gefahr mit sich, dass nicht zulässige, sachlich nicht richtige oder nicht mehr aktuelle Daten ausgetauscht werden. Bei diesen Initiativen ist es dem für die Datenverarbeitung Verantwortlichen nämlich nicht *in jedem einzelnen Fall* möglich, die Rechtmäßigkeit der Datenübermittlung und die

sachliche Richtigkeit der betreffenden Daten zu überprüfen. Folglich müssen diese Initiativen mit strikten Bestimmungen über die permanente Gewährleistung und Überprüfung der Qualität der Daten, auf die ein automatischer direkter Zugriff möglich sein soll, einhergehen.

Da den Auswirkungen, die die Verwirklichung des Verfügbarkeitsgrundsatzes mit sich bringen wird, besondere Aufmerksamkeit entgegengebracht wird, wird es nicht ausreichen, lediglich Bestimmungen über einzelne Aspekte des Datenschutzes zu erlassen. Ein Rechtsakt über den Datenschutz im Rahmen des dritten Pfeilers kann grundsätzlich zur Förderung der polizeilichen und justiziellen Zusammenarbeit in Strafsachen beitragen, weil er deren Effizienz und Rechtmäßigkeit sowie die Wahrung der Grundrechte und insbesondere des Rechts auf den Schutz personenbezogener Daten fördert.

Ein solcher Rechtsakt ist vor allem im Hinblick auf die Verwirklichung des Verfügbarkeitsgrundsatzes nötig und sollte mit ihr Schritt halten. Der Rahmenbeschluss sollte sich weitestgehend an den Geist und den Aufbau der Richtlinie 95/46/EG anlehnen und zugleich den besonderen Anforderungen der polizeilichen und justiziellen Zusammenarbeit in Strafsachen nach Maßgabe des Proportionalitätsgrundsatzes Rechnung tragen. Die Grundsätze der Empfehlung R (87) 15 des Europarates von 1987 über die Nutzung personenbezogener Daten im Polizeibereich sind mit Blick auf den Erlass rechtsverbindlicher europäischer Bestimmungen berücksichtigt worden. Es gilt klare Regeln für den Schutz von personenbezogenen Daten, die den zuständigen Behörden anderer Mitgliedstaaten zur Verfügung gestellt wurden oder werden, aufzustellen. So muss u.a. eine Regelung eingeführt werden, die die Qualität der Datenverarbeitung sichert. Sie muss Bestimmungen einschließen, die die Rechte der Betroffenen und die Befugnisse der Kontrollstellen regeln, denn die Qualität der betreffenden Daten wird voraussichtlich auch davon abhängen, wie von diesen Rechten und Befugnissen Gebrauch gemacht wird.

- **Folgenabschätzung**

Es wurden folgende Möglichkeiten in Erwägung gezogen: Anwendbarkeit der Richtlinie 95/46/EG; kein oder zu einem späteren Zeitpunkt folgender Vorschlag für Vorschriften zum Schutz personenbezogener Daten im Rahmen des dritten Pfeilers; spezifische einschlägige Bestimmungen in einem Rechtsakt über den Informationsaustausch nach dem Verfügbarkeitsgrundsatz; Rahmenbeschluss über den Schutz personenbezogener Daten im Rahmen des dritten Pfeilers. Bezüglich des Rahmenbeschlusses wurde geprüft, inwieweit dieser auch für den Informationsaustausch über Informationssysteme und Gremien der EU gelten sollte.

Wie in Artikel 3 Absatz 2 der Richtlinie 95/46/EG festgelegt ist, finden die grundlegenden und umfassenden Bestimmungen dieser Richtlinie keine Anwendung auf die Verarbeitung personenbezogener Daten, die für die Ausübung von Tätigkeiten erfolgt, die nicht in den Anwendungsbereich des Gemeinschaftsrechts fallen. Eine Anwendbarkeit der Richtlinie auf die polizeiliche und justizielle Zusammenarbeit in Strafsachen wäre selbst durch die Streichung dieses Artikels nicht automatisch gewährleistet, denn zum einen werden nicht alle Eigenheiten dieser Zusammenarbeit in der Richtlinie erfasst, so dass einige Präzisierungen erforderlich wären, und zum anderen müssen die legislativen Anforderungen von Titel VI EU-Vertrag, der ja auf die Förderung der polizeilichen und justiziellen Zusammenarbeit in Strafsachen abstellt, eingehalten werden. Die Möglichkeit, überhaupt keinen oder erst zu einem späteren Zeitpunkt einen Vorschlag für Vorschriften über die Verarbeitung und den

Schutz personenbezogener Daten im Rahmen des dritten Pfeilers vorzulegen, muss ausgeschlossen werden, da dies wahrscheinlich dazu führen würde, dass neue Formen des Informationsaustauschs nach dem Verfügbarkeitsgrundsatz eingeführt würden, ohne dass die strikte Einhaltung der wesentlichen Datenschutzbedingungen gewährleistet wäre. Auch die Aufnahme spezifischer Datenschutzbestimmungen in einen Rechtsakt über den Informationsaustausch nach dem Verfügbarkeitsgrundsatz wäre wegen der zu erwartenden Auswirkungen eines solchen Rechtsaktes nicht ausreichend. Die einzige zufrieden stellende Lösung ist folglich ein Rahmenbeschluss über den Schutz personenbezogener Daten, die im Rahmen der polizeilichen und justiziellen Zusammenarbeit in Strafsachen verarbeitet werden. Sie würde, wenn überhaupt, voraussichtlich keine großen Verwaltungskosten für die Mitgliedstaaten mit sich bringen.

Die Kommission hat die in ihrem Arbeitsprogramm vorgesehene Folgenabschätzung durchgeführt. Der Bericht ist abrufbar unter der Adresse http://europa.eu.int/comm/dgs/justice_home/evaluation/dg_coordination_evaluation_annexe_en.htm.

3) RECHTLICHE ELEMENTE DES VORSCHLAGS

- **Zusammenfassung der vorgeschlagenen Maßnahmen**

Der vorgeschlagene Rahmenbeschluss enthält allgemeine Bestimmungen über die Rechtmäßigkeit der Verarbeitung personenbezogener Daten sowie Bestimmungen über spezifische Formen der Datenverarbeitung (Übermittlung personenbezogener Daten an die zuständigen Behörden anderer Mitgliedstaaten, Weiterverarbeitung – insbesondere Weitergabe – der von den zuständigen Behörden anderer Mitgliedstaaten übersandten bzw. zur Verfügung gestellten Daten), die Rechte der Betroffenen, die Vertraulichkeit und Sicherheit der Verarbeitung, Rechtsbehelfe, Haftung, Sanktionen, Kontrollstellen und die Einsetzung einer Gruppe für den Schutz von Personen bei der Verarbeitung personenbezogener Daten zum Zwecke der Verhütung, Aufdeckung, Untersuchung und Verfolgung von Straftaten. Besonders zu berücksichtigen ist dabei der Grundsatz, dass personenbezogene Daten nur solchen Drittländern und internationalen Stellen übermittelt werden dürfen, die einen gleichwertigen Schutz gewährleisten. Der Rahmenbeschluss sieht einen Mechanismus für die EU-weite Einhaltung dieses Grundsatzes vor.

- **Rechtsgrundlage**

Dieser Rahmenbeschluss gründet sich auf die Artikel 30, 31 und 34 Absatz 2 Buchstabe b des Vertrags über die Europäische Union. Vor allem im Hinblick auf die Verwirklichung des Verfügbarkeitsgrundsatzes sind geeignete Vorschriften über die Verarbeitung und den Schutz personenbezogener Daten einschließlich einheitlicher Bestimmungen über die Übermittlung personenbezogener Daten an Drittländer und internationale Stellen von wesentlicher Bedeutung für die Verbesserung der polizeilichen und justiziellen Zusammenarbeit in Strafsachen und insbesondere bei der Bekämpfung von Terrorismus und sonstigen Schwerverbrechen. Zudem werden die Mitgliedstaaten einander nur in vollem Umfang vertrauen, wenn es klare und einheitliche Bestimmungen über die mögliche Weiterleitung der übermittelten Daten an weitere Beteiligte (insbesondere Drittländer) gibt. Die vorgeschlagenen Bestimmungen gewährleisten, dass der Informationsaustausch zwischen den

zuständigen Behörden nicht durch Unterschiede beim Datenschutz in den Mitgliedstaaten beeinträchtigt wird.

- **Subsidiarität und Verhältnismäßigkeit**

Dieser Rahmenbeschluss regelt eine Reihe von Aspekten mit besonderer Bedeutung für die polizeiliche und justizielle Zusammenarbeit zwischen den Mitgliedstaaten in Strafsachen und insbesondere den Informationsaustausch. Auf diese Weise soll ein wirksames und rechtmäßiges Vorgehen bei der Verhütung und Bekämpfung von Straftaten und insbesondere Schwerverbrechen und terroristischen Handlungen in *allen* Mitgliedstaaten gefördert und gewährleistet werden. Nationale, bilaterale oder multilaterale Lösungen könnten zwar einzelnen Mitgliedstaaten dienlich sein, würden aber nicht der Notwendigkeit Rechnung tragen, dass es die innere Sicherheit in der gesamten Union zu gewährleisten gilt. Der Informationsbedarf der Strafverfolgungsbehörden hängt weitgehend von der Integration zwischen den Ländern ab. Der zu Strafverfolgungszwecken dienende Informationsaustausch zwischen den Mitgliedstaaten wird voraussichtlich zunehmen und muss daher von einheitlichen Vorschriften über die Datenverarbeitung und den Datenschutz flankiert werden. Dieser Rahmenbeschluss wird dem in Artikel 2 EU-Vertrag und Artikel 5 EG-Vertrag festgelegten Subsidiaritätsgrundsatz insofern gerecht, als er auf eine Angleichung der Rechts- und Verwaltungsvorschriften der Mitgliedstaaten abzielt, die durch unilaterale Maßnahmen der Mitgliedstaaten nicht in geeigneter Form erreicht werden kann und daher ein konzertiertes Vorgehen auf EU-Ebene erfordert. Entsprechend dem in demselben Artikel festgeschriebenen Verhältnismäßigkeitsprinzip geht dieser Beschluss nicht über das für die Erreichung dieses Ziels erforderliche Maß hinaus. Er bezieht sich insbesondere ausschließlich auf die für die polizeiliche und justizielle Zusammenarbeit in Strafsachen relevante Verarbeitung personenbezogener Daten.

- **Gewähltes Mittel**

Vorgeschlagener Rechtsakt: Rahmenbeschluss. Letzterer stellt auf eine Angleichung der Rechtsvorschriften der Mitgliedstaaten über den Schutz personenbezogener Daten, die zum Zwecke der Kriminalitätsverhütung und –bekämpfung verarbeitet werden, ab.

4) AUSWIRKUNGEN AUF DEN HAUSHALT

Die Umsetzung dieses Vorschlags für einen Rahmenbeschluss würde nur zu geringen zusätzlichen Verwaltungsausgaben zu Lasten des Gemeinschaftshaushalts führen (Sitzungen und Sekretariat des Ausschusses nach Artikel 16 und des Beratergremiums nach Artikel 31).

2005/0202 (CNS)

Vorschlag für einen

RAHMENBESCHLUSS DES RATES

über den Schutz personenbezogener Daten, die im Rahmen der polizeilichen und justiziellen Zusammenarbeit in Strafsachen verarbeitet werden

DER RAT DER EUROPÄISCHEN UNION -

gestützt auf den Vertrag über die Europäische Union, insbesondere auf Artikel 30, Artikel 31 und Artikel 34 Absatz 2 Buchstabe b,

auf Vorschlag der Kommission[23],

nach Stellungnahme des Europäischen Parlaments[24],

in Erwägung nachstehender Gründe:

(1) Die Europäische Union hat sich das Ziel gesetzt, die Union als einen Raum der Freiheit, der Sicherheit und des Rechts zu erhalten und weiterzuentwickeln; durch ein gemeinsames Vorgehen der Mitgliedstaaten bei der polizeilichen und justiziellen Zusammenarbeit in Strafsachen soll ein hohes Maß an Sicherheit gewährleistet werden.

(2) Das gemeinsame Vorgehen im Bereich der polizeilichen Zusammenarbeit gemäß Artikel 30 Absatz 1 Buchstabe b des Vertrags über die Europäische Union und das gemeinsame Vorgehen im Bereich der justiziellen Zusammenarbeit in Strafsachen gemäß Artikel 31 Absatz 1 Buchstabe a des Vertrags über die Europäische Union bringen die Notwendigkeit der Verarbeitung der betreffenden Informationen mit sich, die nach Maßgabe geeigneter Bestimmungen über den Schutz personenbezogener Daten erfolgen sollte.

(3) Die im Rahmen von Titel VI des Vertrags über die Europäische Union erlassenen Rechtsvorschriften sollen zur Verbesserung der polizeilichen und justiziellen Zusammenarbeit in Strafsachen beitragen, indem sie ihre Effizienz, ihre Rechtmäßigkeit und die Achtung der Grundrechte und insbesondere des Rechts auf den Schutz der Privatsphäre und den Schutz personenbezogener Daten fördern. Einheitliche Vorschriften über die Verarbeitung und den Schutz personenbezogener Daten, die zum Zwecke der Kriminalitätsverhütung und –bekämpfung verarbeitet werden, können zur Erreichung dieser Ziele beitragen.

---

23 …

24 …

(4) Im Haager Programm zur Stärkung von Freiheit, Sicherheit und Recht in der Europäischen Union, das der Europäische Rat am 4. November 2004 angenommen hat, wurde die Notwendigkeit eines innovativen Konzepts für den grenzüberschreitenden Austausch von strafverfolgungsrelevanten Informationen unter strenger Einhaltung bestimmter Hauptbedingungen für den Datenschutz hervorgehoben und die Kommission ersucht, bis spätestens Ende 2005 entsprechende Vorschläge vorzulegen. Dieser Aufforderung wurde in Form des Aktionsplans des Rates und der Kommission zur Umsetzung des Haager Programms zur Stärkung von Freiheit, Sicherheit und Recht in der Europäischen Union[25] entsprochen.

(5) Der Austausch personenbezogener Daten im Rahmen der polizeilichen und justiziellen Zusammenarbeit in Strafsachen, insbesondere nach dem im Haager Programm festgelegten Grundsatz der Verfügbarkeit von Informationen, sollte durch klare und rechtsverbindliche Bestimmungen unterstützt werden, die das gegenseitige Vertrauen zwischen den zuständigen Behörden fördern und sicherstellen, dass die betreffenden Informationen so geschützt werden, dass eine Behinderung dieser Zusammenarbeit zwischen den Mitgliedstaaten ausgeschlossen ist und gleichzeitig die Grundrechte der betroffenen Personen in vollem Umfang gewahrt bleiben. Die geltenden Rechtsvorschriften auf europäischer Ebene reichen hierfür nicht aus. Die Richtlinie 95/46/EG des Europäischen Parlaments und des Rates vom 24. Oktober 1995 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr[26] findet keine Anwendung auf die Verarbeitung personenbezogener Daten, die für die Ausübung von Tätigkeiten erfolgt, die nicht in den Anwendungsbereich des Gemeinschaftsrechts fallen, beispielsweise Tätigkeiten gemäß Titel VI des Vertrags über die Europäische Union, und auf keinen Fall auf Verarbeitungen betreffend die öffentliche Sicherheit, die Landesverteidigung, die Sicherheit des Staates und die Tätigkeiten des Staates im strafrechtlichen Bereich.

(6) Eine Rechtsvorschrift mit einheitlichen Bestimmungen über den Schutz personenbezogener Daten, die zum Zwecke der Kriminalitätsverhütung und -bekämpfung verarbeitet werden, sollte im Einklang mit der allgemeinen Datenschutzpolitik der Union stehen. Sie sollte zudem der Notwendigkeit, dass es die Effizienz der rechtmäßigen Maßnahmen der Polizei-, Zoll-, Justiz- und sonstigen zuständigen Behörden zu verbessern gilt, so weit wie möglich Rechnung tragen und daher die geltenden und bewährten Grundsätze und Begriffsbestimmungen übernehmen, die insbesondere in der Richtlinie 95/46/EG des Europäischen Parlaments und des Rates festgelegt oder für den Informationsaustausch durch Europol bzw. Eurojust oder die Verarbeitung im Rahmen des Zollinformationssystems und vergleichbaren Instrumenten vorgesehen sind.

(7) Die Angleichung der Rechtsvorschriften der Mitgliedstaaten sollte nicht zu einer Lockerung des Datenschutzes in diesen Ländern führen, sondern vielmehr auf ein hohes Maß an Schutz in der gesamten Union abstellen.

(8) Es ist erforderlich, die Ziele des Datenschutzes im Rahmen der polizeilichen und justiziellen Tätigkeiten sowie Bestimmungen über die Rechtmäßigkeit der Verarbeitung personenbezogener Daten festzulegen, um dafür Sorge zu tragen, dass

---

[25] ABl. C 198 vom 12.8.2005, S. 1.

[26] ABl. L 281 vom 23.11.1995, S. 31.

etwaige ausgetauschte Informationen zuvor rechtmäßig und in Übereinstimmung mit den geltenden Grundsätzen in Bezug auf die Datenqualität verarbeitet werden. Gleichzeitig dürfen die rechtmäßigen Tätigkeiten der Polizei-, Zoll-, Justiz- und sonstigen zuständigen Behörden in keiner Weise behindert werden.

(9) Die Gewährleistung eines hohen Schutzes der personenbezogenen Daten europäischer Bürger setzt einheitliche Bestimmungen voraus, die die Rechtmäßigkeit und die Qualität der von den zuständigen Behörden in anderen Mitgliedstaaten verarbeiteten Daten regeln.

(10) Es ist angezeigt, auf europäischer Ebene die Bedingungen festzulegen, unter denen die zuständigen Behörden der Mitgliedstaaten personenbezogene Daten öffentlichen und nicht-öffentlichen Stellen in anderen Mitgliedstaaten übersenden und zur Verfügung stellen dürfen.

(11) Die Weiterverarbeitung der von der zuständigen Behörde eines anderen Mitgliedstaats übermittelten oder zur Verfügung gestellten Daten, insbesondere die Weitergabe oder Bereitstellung dieser Daten, sollte durch einheitliche Bestimmungen auf europäischer Ebene geregelt werden.

(12) Personenbezogene Daten, die von einem Mitgliedstaat der Europäischen Union an Drittländer oder internationale Stellen übermittelt werden, sollten grundsätzlich angemessen geschützt werden.

(13) In diesem Rahmenbeschluss sollte das Verfahren für die Annahme der erforderlichen Maßnahmen zur Ermittlung des bestehenden Datenschutzes in einem Drittland oder einer internationalen Einrichtung festgelegt werden.

(14) Um den Schutz personenbezogener Daten ohne Beeinträchtigung des Zweckes strafrechtlicher Untersuchungen zu gewährleisten, ist es erforderlich, die Rechte der betroffenen Personen festzulegen.

(15) Es ist angezeigt, einheitliche Bestimmungen über die Vertraulichkeit und die Sicherheit der Faktenverarbeitung, über die Haftung und über Sanktionen bei unrechtmäßiger Verwendung der Daten durch die zuständigen Behörden sowie die den Betroffenen zur Verfügung stehenden Rechtsbehelfe festzulegen. Außerdem ist es erforderlich, dass die Mitgliedstaaten strafrechtliche Sanktionen für besonders schwere und vorsätzlich begangene Verstöße gegen die Datenschutzbestimmungen vorsehen.

(16) Die Einrichtung unabhängiger Kontrollstellen in den Mitgliedstaaten ist ein wesentliches Element des Schutzes personenbezogener Daten, die im Rahmen der polizeilichen und justiziellen Zusammenarbeit zwischen den Mitgliedstaaten in Strafsachen verarbeitet werden.

(17) Diese Stellen sind mit den notwendigen Mitteln für die Erfüllung dieser Aufgabe auszustatten, d.h. Untersuchungs- und Einwirkungsbefugnisse, insbesondere bei Beschwerden einzelner Personen, sowie Klagerecht. Die Kontrollstellen haben zur Transparenz der Verarbeitungen in den Mitgliedstaaten beizutragen, denen sie unterstehen. Ihre Befugnisse dürfen jedoch weder die Vorschriften für Strafverfahren noch die Unabhängigkeit der Gerichte berühren.

(18) Es ist eine Gruppe für den Schutz der Rechte von Personen bei der Verarbeitung personenbezogener Daten zum Zwecke der Verhütung, Aufdeckung, Untersuchung und Verfolgung von Straftaten einzusetzen, die ihre Aufgaben in völliger Unabhängigkeit wahrzunehmen hat. Sie hat die Kommission und die Mitgliedstaaten zu beraten und insbesondere zur einheitlichen Anwendung der zur Umsetzung dieses Rahmenbeschlusses erlassenen innerstaatlichen Vorschriften beizutragen.

(19) Artikel 47 des Vertrags über die Europäische Union besagt, dass dieser Vertrag die Verträge zur Gründung der Europäischen Gemeinschaften sowie die nachfolgenden Verträge und Akte zu ihrer Änderung oder Ergänzung unberührt lässt. Entsprechend berührt dieser Rahmenbeschluss nicht den Schutz personenbezogener Daten im Rahmen des Gemeinschaftsrechts und insbesondere der Richtlinie 95/46/EG des Europäischen Parlaments und des Rates zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr, der Verordnung (EG) Nr. 45/2001 des Europäischen Parlaments und des Rates vom 18. Dezember 2000 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die Organe und Einrichtungen der Gemeinschaft und zum freien Datenverkehr[27] und der Richtlinie 2002/58/EG des Europäischen Parlaments und des Rates vom 12. Juli 2002 über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre in der elektronischen Kommunikation (Datenschutzrichtlinie für elektronische Kommunikation)[28].

(20) Dieser Rahmenbeschluss berührt nicht die Datenschutzbestimmungen der einschlägigen Rechtsvorschriften über die Verarbeitung und den Schutz personenbezogener Daten durch Europol, Eurojust und das Zollinformationssystem.

(21) Die sich auf den Schutz personenbezogener Daten beziehenden Bestimmungen in Titel IV des Übereinkommens von 1990 zur Durchführung des Übereinkommens von Schengen vom 14. Juni 1985 betreffend den schrittweisen Abbau der Kontrollen an den gemeinsamen Grenzen[29] (nachfolgend „Übereinkommen von Schengen"), die gemäß dem Protokoll im Anhang zum Vertrag über die Europäische Union und zum Vertrag über die Gründung der Europäischen Gemeinschaften in den Rahmen der Europäischen Union integriert wurden, sollten in Bezug auf Angelegenheiten, die in den Anwendungsbereich des Vertrags über die Europäische Union fallen, durch die einschlägigen Bestimmungen dieses Rahmenbeschlusses ersetzt werden.

(22) Es ist angezeigt, dass dieser Rahmenbeschluss auch die personenbezogenen Daten erfasst, die im Rahmen des Schengener Informationssystems der zweiten Generation und des damit verbundenen Austausches von Zusatzinformationen gemäß dem Beschluss JI/2006/… über die Einrichtung, den Betrieb und die Nutzung des Schengener Informationssystems der zweiten Generation verarbeitet werden.

(23) Dieser Rahmenbeschluss lässt die sich auf den rechtswidrigen Datenzugriff beziehenden Bestimmungen des Rahmenbeschlusses 2005/222/JI des Rates vom 24. Februar 2005 über Angriffe auf Informationssysteme[30] unberührt.

---

27 ABl. 8 vom 12.1.2001, S. 1.
28 ABl. L 201 vom 31.7.2002, S. 37.
29 ABl. L 239 vom 22.9.2000, S. 19.
30 ABl. L 69 vom 16.3.2005, S. 67.

(24) Es ist angezeigt, Artikel 23 des Übereinkommens über die Rechtshilfe in Strafsachen zwischen den Mitgliedstaaten der Europäischen Union[31] zu ersetzen.

(25) Jedwede Bezugnahme auf das Übereinkommen des Europarats vom 28. Januar 1981 zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten sollte als Bezugnahme auf diesen Rahmenbeschluss gelesen werden.

(26) Da sich die Ziele der zu treffenden Maßnahme, nämlich die Festlegung einheitlicher Vorschriften über den Schutz personenbezogener Daten, die im Rahmen der polizeilichen und justiziellen Zusammenarbeit in Strafsachen verarbeitet werden, auf Ebene der Mitgliedstaaten nicht ausreichend verwirklichen lassen und daher wegen des Umfangs und der Wirkungen der Maßnahme besser auf Ebene der Europäischen Union zu erreichen sind, kann der Rat im Einklang mit dem in Artikel 5 EG-Vertrag niedergelegten Subsidiaritätsprinzip, auf das in Artikel 2 EU-Vertrag Bezug genommen wird, tätig werden. Entsprechend dem in Artikel 5 EG-Vertrag ebenfalls genannten Grundsatz der Verhältnismäßigkeit geht dieser Rahmenbeschluss nicht über das für die Erreichung dieser Ziele erforderliche Maß hinaus.

(27) Das Vereinigte Königreich beteiligt sich an diesem Rahmenbeschluss im Einklang mit Artikel 5 des Protokolls zur Einbeziehung des Schengen-Besitzstands in den Rahmen der Europäischen Union im Anhang zum EU-Vertrag und zum EG-Vertrag sowie Artikel 8 Absatz 2 des Beschlusses 2000/365/EG des Rates vom 29. Mai 2000 zum Antrag des Vereinigten Königreichs Großbritannien und Nordirland, einzelne Bestimmungen des Schengen-Besitzstands auf sie anzuwenden[32].

(28) Irland beteiligt sich an diesem Rahmenbeschluss im Einklang mit Artikel 5 des Protokolls zur Einbeziehung des Schengen-Besitzstands in den Rahmen der Europäischen Union im Anhang zum EU-Vertrag und zum EG-Vertrag sowie Artikel 6 Absatz 2 des Beschlusses 2002/192/EG des Rates vom 28. Februar 2002 zum Antrag Irlands auf Anwendung einzelner Bestimmungen des Schengen-Besitzstands auf Irland.

(29) Im Hinblick auf Island und Norwegen stellt dieser Rahmenbeschluss eine Weiterentwicklung der Bestimmungen des Schengen-Besitzstands im Sinne des Übereinkommens zwischen dem Rat der Europäischen Union sowie der Republik Island und dem Königreich Norwegen über die Assoziierung dieser beiden Staaten bei der Umsetzung, Anwendung und Entwicklung des Schengen-Besitzstands dar, die zu dem Bereich nach Artikel 1 Buchstabe h des Beschlusses 1999/437/EG des Rates vom 17. Mai 1999 zum Erlass bestimmter Durchführungsvorschriften zu dem Übereinkommen[33] gehören.

(30) Im Fall der Schweiz bedeutet dieser Rahmenbeschluss eine Weiterentwicklung der Bestimmungen des Schengen-Besitzstands im Sinne des Abkommens zwischen der Europäischen Union, der Europäischen Gemeinschaft und der Schweizerischen Eidgenossenschaft über die Assoziierung der Schweizerischen Eidgenossenschaft bei der Umsetzung, Anwendung und Entwicklung des Schengen-Besitzstands. Die Bestimmungen fallen in den in Artikel 1 Buchstabe h des Beschlusses 1999/437/EG

---

31 ABl. C 197 vom 12.7.2000, S. 3.
32 ABl. L 131 vom 1.6.2000, S. 43.
33 ABl. L 176 vom 10.7.1999, S. 31.

des Rates vom 17. Mai 1999 genannten Bereich; dieser Artikel ist in Verbindung mit Artikel 4 Absatz 1 des Ratsbeschlusses 2004/849/EG über die Unterzeichnung des Abkommens im Namen der Europäischen Union und die vorläufige Anwendung einiger Bestimmungen dieses Abkommens[34] zu lesen.

(31) Bei diesem Rahmenbeschluss handelt es sich um einen Rechtsakt, der auf dem Schengen-Besitzstand aufbaut oder im Sinne von Artikel 3 Absatz 1 der Beitrittsakte von 2003 anderweitig mit ihm zusammenhängt.

(32) Dieser Rahmenbeschluss steht im Einklang mit den Grundrechten und Grundsätzen, die mit der Charta der Grundrechte der Europäischen Union anerkannt wurden. Er stellt auf die vollständige Wahrung des Rechts auf Schutz der Privatsphäre und des Rechts auf Schutz personenbezogener Daten gemäß Artikel 7 bzw. Artikel 8 der Charta der Grundrechte der Europäischen Union ab -

HAT FOLGENDEN RAHMENBESCHLUSS ANGENOMMEN:

KAPITEL I
GEGENSTAND, BEGRIFFSBESTIMMUNGEN UND ANWENDUNGSBEREICH

Artikel 1
Gegenstand

1. In diesem Rahmenbeschluss werden einheitliche Bestimmungen zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten im Rahmen der polizeilichen und justiziellen Zusammenarbeit in Strafsachen gemäß Titel VI des Vertrags über die Europäische Union festgelegt.

2. Die Mitgliedstaaten stellen sicher, dass die Offenlegung personenbezogener Daten gegenüber den zuständigen Behörden anderer Mitgliedstaaten nicht aus Gründen, die mit dem Schutz personenbezogener Daten gemäß diesem Rahmenbeschluss zusammenhängen, eingeschränkt oder untersagt wird.

Artikel 2
Begriffsbestimmungen

Im Sinne dieses Rahmenbeschlusses bezeichnet der Ausdruck

(a) „personenbezogene Daten“ alle Informationen über eine bestimmte oder bestimmbare natürliche Person („betroffene Person“); als bestimmbar wird eine Person angesehen, die direkt oder indirekt identifiziert werden kann, insbesondere durch Zuordnung zu einer Kennummer oder zu einem oder mehreren spezifischen Elementen, die Ausdruck ihrer physischen, physiologischen, psychischen, wirtschaftlichen, kulturellen oder sozialen Identität sind;

[34] ABl. L 368 vom 15.12.2004, S. 26.

(b) „Verarbeitung personenbezogener Daten“ („Verarbeitung“) jeden mit oder ohne Hilfe automatisierter Verfahren ausgeführten Vorgang oder jede Vorgangsreihe im Zusammenhang mit personenbezogenen Daten wie das Erheben, das Speichern, die Organisation, die Aufbewahrung, die Anpassung oder Veränderung, das Auslesen, das Abfragen, die Benutzung, die Weitergabe durch Übermittlung, Verbreitung oder jede andere Form der Bereitstellung, die Kombination oder die Verknüpfung sowie das Sperren, Löschen oder Vernichten;

(c) „Datei mit personenbezogenen Daten“ („Datei“) jede strukturierte Sammlung personenbezogener Daten, die nach bestimmten Kriterien zugänglich sind, gleichgültig, ob diese Sammlung zentral, dezentralisiert oder nach funktionalen oder geographischen Gesichtspunkten aufgeteilt geführt wird;

(d) „für die Verarbeitung Verantwortlicher“ die natürliche oder juristische Person, Behörde, Einrichtung oder jede andere Stelle, die allein oder gemeinsam mit anderen über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheidet, wobei die Zwecke und Mittel der Verarbeitung durch innerstaatliche oder im Rahmen von Titel VI des Vertrags über die Europäische Union erlassene Rechtsvorschriften festgelegt sind und auch der für die Verarbeitung Verantwortliche oder die Kriterien für seine Ernennung durch innerstaatliche oder im Rahmen von Titel VI des Vertrags über die Europäische Union erlassene Rechtsvorschriften festgelegt werden können;

(e) „Auftragsverarbeiter“ die natürliche oder juristische Person, Behörde, Einrichtung oder jede andere Stelle, die personenbezogene Daten im Auftrag des für die Verarbeitung Verantwortlichen verarbeitet;

(f) „Dritter“ die natürliche oder juristische Person, Behörde, Einrichtung oder jede andere Stelle, außer der betroffenen Person, dem für die Verarbeitung Verantwortlichen, dem Auftragsverarbeiter und den Personen, die unter der unmittelbaren Verantwortung des für die Verarbeitung Verantwortlichen oder des Auftragsverarbeiters befugt sind, die Daten zu verarbeiten;

(g) „Empfänger“ die natürliche oder juristische Person, Behörde, Einrichtung oder jede andere Stelle, die Daten erhält, gleichgültig, ob es sich bei ihr um einen Dritten handelt oder nicht;

(h) „Einwilligung der betroffenen Person“ jede Willensbekundung, die ohne Zwang, für den konkreten Fall und in Kenntnis der Sachlage erfolgt und mit der die betroffene Person akzeptiert, dass die sie betreffenden personenbezogenen Daten verarbeitet werden;

(i) „internationale Einrichtungen“ Einrichtungen oder Organisationen, die durch internationale Abkommen geschaffen wurden;

(j) „zuständige Behörden“ Polizei-, Zoll-, Justiz- oder sonstige zuständige Behörden der Mitgliedstaaten im Sinne von Artikel 29 des Vertrags über die Europäische Union.

Artikel 3
Anwendungsbereich

1. Dieser Rahmenbeschluss gilt für die ganz oder teilweise automatisierte Verarbeitung personenbezogener Daten sowie für die nicht automatisierte Verarbeitung personenbezogener Daten, die in einer Datei gespeichert sind oder gespeichert werden sollen, durch eine zuständige Behörde zum Zwecke der Verhütung, Aufdeckung, Untersuchung und Verfolgung von Straftaten.

2. Dieser Rahmenbeschluss gilt nicht für die Verarbeitung personenbezogener Daten durch

   – das Europäische Polizeiamt (Europol),

   – die Europäische Einheit für justizielle Zusammenarbeit (Eurojust),

   – das durch das Übereinkommen aufgrund von Artikel K.3 des Vertrags über die Europäische Union über den Einsatz der Informationstechnologie im Zollbereich und diesbezügliche Änderungen geschaffene Zollinformationssystem.

KAPITEL II
ALLGEMEINE BESTIMMUNGEN ÜBER DIE RECHTMÄSSIGKEIT DER VERARBEITUNG PERSONENBEZOGENER DATEN

Artikel 4
Grundsätze in Bezug auf die Qualität der Daten

1. Die Mitgliedstaaten sehen vor, dass personenbezogene Daten

   (a) nach Treu und Glauben und auf rechtmäßige Weise verarbeitet werden;

   (b) für festgelegte eindeutige und rechtmäßige Zwecke erhoben und nicht in einer mit diesen Zweckbestimmungen nicht zu vereinbarenden Weise weiterverarbeitet werden. Die Weiterverarbeitung von Daten zu historischen, statistischen oder wissenschaftlichen Zwecken ist im Allgemeinen nicht als unvereinbar mit den Zwecken der vorausgegangenen Datenerhebung anzusehen, sofern die Mitgliedstaaten geeignete Garantien vorsehen;

   (c) den Zwecken entsprechen, für die sie erhoben und/oder weiterverarbeitet werden, dafür erheblich sind und nicht darüber hinausgehen;

   (d) sachlich richtig und, wenn nötig, auf den neuesten Stand gebracht sind; es sind alle angemessenen Maßnahmen zu treffen, damit im Hinblick auf die Zwecke, für die sie erhoben oder weiterverarbeitet werden, nichtzutreffende oder unvollständige Daten gelöscht oder berichtigt werden. Die Mitgliedstaaten können vorsehen, dass Daten mit unterschiedlicher sachlicher Richtigkeit und Zuverlässigkeit verarbeitet werden dürfen, müssen in diesem Fall jedoch vorsehen, dass diese Daten nach sachlicher Richtigkeit und Zuverlässigkeit

unterschieden werden und insbesondere faktische Daten von sich auf Meinungen oder persönlichen Ansichten gründenden Daten unterschieden werden;

(e) nicht länger, als es für die Realisierung der Zwecke, für die sie erhoben oder weiterverarbeitet werden, erforderlich ist, in einer Form aufbewahrt werden, die die Identifizierung der betroffenen Personen ermöglicht. Die Mitgliedstaaten sehen geeignete Garantien für personenbezogene Daten vor, die über die vorgenannte Dauer hinaus für historische, statistische oder wissenschaftliche Zwecke aufbewahrt werden.

2. Der für die Verarbeitung Verantwortliche sorgt für die Einhaltung von Absatz 1.

3. Die Mitgliedstaaten sorgen für eine klare Unterscheidung zwischen den personenbezogenen Daten von

– Personen, die im Verdacht stehen, eine Straftat begangen zu haben oder an einer Straftat beteiligt gewesen zu sein,

– Personen, die wegen einer Straftat verurteilt worden sind,

– Personen, bei denen ernst zu nehmende Hinweise dafür bestehen, dass sie eine Straftat begehen werden,

– Personen, die möglicherweise im Rahmen einer strafrechtlichen Untersuchung oder eines anschließenden Strafverfahrens als Zeugen vorgeladen werden könnten,

– Personen, die Opfer einer Straftat geworden sind, oder bei denen bestimmte Fakten darauf hindeuten,

– Personen, die Hinweise zu Straftaten geben können,

– Personen, die mit den oben genannten Personen im Kontakt oder in Verbindung stehen, und

– Personen, die in keine der obigen Kategorien fallen.

4. Die Mitgliedstaaten sehen vor, dass eine Verarbeitung personenbezogener Daten nur notwendig ist, falls

– aufgrund der vorliegenden Fakten berechtigter Grund zu der Annahme besteht, dass die betreffenden personenbezogenen Daten die Verhütung, Aufdeckung, Untersuchung und Verfolgung einer Straftat ermöglichen, erleichtern oder beschleunigen würden und

– es kein anderes, die Rechte der betroffenen Personen weniger berührendes Mittel gibt und

– die Datenverarbeitung angesichts des betreffenden Delikts unverhältnismäßig wäre.

Artikel 5
Kriterien für eine rechtmäßige Datenverarbeitung

Die Mitgliedstaaten sehen vor, dass personenbezogene Daten von den zuständigen Behörden nur verarbeitet werden dürfen, wenn es eine entsprechende Rechtsvorschrift gibt, in der festgelegt ist, dass diese Verarbeitung zur Erfüllung der rechtmäßigen Aufgaben der betreffenden Behörden sowie zur Verhütung, Aufdeckung, Untersuchung und Verfolgung von Straftaten notwendig ist.

Artikel 6
Verarbeitung besonderer Kategorien personenbezogener Daten

1. Die Mitgliedstaaten untersagen die Verarbeitung personenbezogener Daten, aus denen die rassische und ethnische Herkunft, politische Meinungen, religiöse oder philosophische Überzeugungen oder die Gewerkschaftszugehörigkeit hervorgehen, sowie von Daten über Gesundheit oder Sexualleben.

2. Absatz 1 findet keine Anwendung,

   – wenn die Verarbeitung gesetzlich vorgeschrieben und unabdingbar für die Erfüllung der rechtmäßigen Aufgaben der betreffenden Behörde im Hinblick auf die Verhütung, Aufdeckung, Untersuchung und Verfolgung von Straftaten ist oder die betroffene Person ausdrücklich ihre Einwilligung zu der Datenverarbeitung erteilt hat, und

   – wenn die Mitgliedstaaten für spezifische Fälle geeignete Garantien vorsehen, beispielsweise eine Beschränkung des Datenzugriffs auf das für die rechtmäßige, die Datenverarbeitung rechtfertigende Verarbeitung zuständige Personal.

Artikel 7
Fristen für die Speicherung personenbezogener Daten

1. Die Mitgliedstaaten sehen vor, dass, sofern nicht durch innerstaatliche Rechtsvorschriften etwas anderes bestimmt wird, personenbezogene Daten nicht länger gespeichert werden dürfen, als es für die Erfüllung des Zwecks, zu dem sie gesammelt wurden, nötig ist. Personenbezogene Daten der in Artikel 4 Absatz 3 letzter Gedankenstrich genannten Personen dürfen nur so lange gespeichert werden, wie es für die Erfüllung des Zwecks, zu dem sie gesammelt wurden, unbedingt erforderlich ist.

2. Die Mitgliedstaaten sehen verfahrensrechtliche und technische Maßnahmen vor, die sicherstellen, dass die Fristen für die Speicherung personenbezogener Daten eingehalten werden. Die Einhaltung der Fristen wird regelmäßig überprüft.

KAPITEL III – Formen der Datenverarbeitung

ABSCHNITT I – ÜBERMITTLUNG UND BEREITSTELLUNG PERSONENBEZOGENER DATEN AN DIE ZUSTÄNDIGEN BEHÖRDEN ANDERER MITGLIEDSTAATEN

Artikel 8
Übermittlung und Bereitstellung personenbezogener Daten an die zuständigen Behörden anderer Mitgliedstaaten

Die Mitgliedstaaten sehen vor, dass personenbezogene Daten den zuständigen Behörden anderer Mitgliedstaaten nur übermittelt oder zur Verfügung gestellt werden dürfen, wenn dies zur Erfüllung einer der rechtmäßigen Aufgaben der die Daten übermittelnden oder empfangenden Behörde sowie zur Verhütung, Aufdeckung, Untersuchung und Verfolgung von Straftaten erforderlich ist.

Artikel 9
Überprüfung der Qualität der übermittelten oder zur Verfügung gestellten Daten

1. Die Mitgliedstaaten sehen vor, dass die Qualität personenbezogener Daten spätestens vor ihrer Übermittlung oder Bereitstellung überprüft wird. Bei allen Datenübermittlungen ist nach Möglichkeit auf ergangene Gerichtsentscheidungen und erfolgte Verfahrenseinstellungen hinzuweisen; in Bezug auf Daten, die sich auf Stellungnahmen oder persönliche Meinungen gründen, ist vor der Übermittlung eine Überprüfung an der Quelle durchzuführen und die sachliche Richtigkeit und Zuverlässigkeit der Daten anzugeben.

2. Die Mitgliedstaaten sehen vor, dass die Qualität von personenbezogenen Daten, die den zuständigen Behörden anderer Mitgliedstaaten im Wege eines automatischen direkten Zugriffs verfügbar gemacht werden, regelmäßig überprüft wird, damit sichergestellt ist, dass die Daten sachlich richtig und auf dem neuesten Stand sind.

3. Die Mitgliedstaaten sehen vor, dass personenbezogene Daten, die sachlich nicht mehr richtig oder nicht mehr aktuell sind, nicht übermittelt oder zur Verfügung gestellt werden.

4. Die Mitgliedstaaten sehen vor, dass eine zuständige Behörde, die einer zuständigen Behörde eines anderen Mitgliedstaats personenbezogene Daten übermittelt oder zur Verfügung gestellt hat, letztere unverzüglich in Kenntnis setzt, falls sie von sich aus oder auf Antrag der betroffenen Person feststellt, dass die betreffenden Daten nicht hätten übermittelt bzw. zur Verfügung gestellt werden dürfen oder dass sachlich nicht richtige oder nicht mehr aktuelle Daten übermittelt bzw. zur Verfügung gestellt wurden.

5. Die Mitgliedstaaten sehen vor, dass eine zuständige Behörde, die gemäß Absatz 4 in Kenntnis gesetzt wurde, die betreffenden Daten löscht oder berichtigt. Ebenso hat diese Behörde die Daten zu berichtigen, wenn sie feststellt, dass diese sachlich nicht richtig sind. Falls die Behörde berechtigten Grund zu der Vermutung hat, dass die ihr

übersandten personenbezogenen Daten sachlich nicht richtig sind oder gelöscht werden sollten, unterrichtet sie unverzüglich die zuständige Behörde, die ihr die betreffenden Daten übermittelt bzw. zur Verfügung gestellt hat.

6. Die Mitgliedstaaten sehen unbeschadet der innerstaatlichen Vorschriften für Strafverfahren vor, dass personenbezogene Daten auf Antrag der betroffenen Person gekennzeichnet werden, falls ihre sachliche Richtigkeit von der betroffenen Person in Abrede gestellt wird und nicht ermittelt werden kann. Diese Kennzeichnung darf nur mit Einwilligung der betroffenen Person oder auf Beschluss des zuständigen Gerichts oder der zuständigen Kontrollstelle wieder gelöscht werden.

7. Die Mitgliedstaaten sehen vor, dass personenbezogene Daten, die von einer Behörde eines anderen Mitgliedstaats übersandt wurden, gelöscht werden,

   – falls die Daten nicht hätten übermittelt, zur Verfügung gestellt oder entgegengenommen werden dürfen,

   – falls eine nach dem innerstaatlichen Recht des anderen Mitgliedstaats vorgesehene diesbezügliche Frist abgelaufen ist und die Behörde, die die betreffenden Daten übermittelt oder zur Verfügung gestellt hat, die empfangende Behörde bei der Übermittlung oder Bereitstellung über diese Frist in Kenntnis gesetzt hat, und die personenbezogenen Daten nicht mehr für Gerichtsverfahren benötigt werden,

   – falls die Daten nicht mehr für den Zweck, zu dem sie übermittelt oder zur Verfügung gestellt wurden, benötigt werden.

8. Falls personenbezogene Daten ohne vorherigen Antrag übermittelt wurden, überprüft die empfangende Behörde unverzüglich, ob die Daten für den Zweck, für den sie übermittelt wurden, benötigt werden.

9. Falls berechtigter Grund zu der Vermutung besteht, dass eine Datenlöschung schützenswerten Interessen der betroffenen Person schaden würde, dürfen personenbezogene Daten nicht gelöscht, sondern lediglich nach innerstaatlichem Recht gesperrt werden. Gesperrte Daten dürfen nur zu dem Zweck verwendet oder übermittelt werden, zu dem sie nicht gelöscht wurden.

Artikel 10
Protokollierung und Dokumentierung

1. Die Mitgliedstaaten sehen vor, dass jede automatische Übermittlung und jeder automatische Erhalt personenbezogener Daten, insbesondere im Wege eines direkten automatischen Zugriffs, protokolliert wird, um die anschließende Überprüfung der Gründe für die Übermittlung, der übermittelten Daten, des Zeitpunkts der Übermittlung, der beteiligten Behörden und der Personen in der empfangenden Behörde, die die Daten entgegengenommen und die Übermittlung veranlasst haben, zu ermöglichen.

2. Die Mitgliedstaaten sehen vor, dass jede nicht automatische Übermittlung und jeder nicht automatische Erhalt personenbezogener Daten dokumentiert wird, um die anschließende Überprüfung der Gründe für die Übermittlung, der übermittelten Daten, des Zeitpunkts der Übermittlung, der beteiligten Behörden und der Personen

in der empfangenden Behörde, die die Daten entgegengenommen und die Übermittlung veranlasst haben, zu ermöglichen.

3. Die Behörde, die diese Informationen protokollarisch oder dokumentarisch erfasst hat, übermittelt diese der zuständigen Kontrollstelle auf Anforderung so rasch wie möglich. Die Informationen dürfen nur zur Datenschutzkontrolle und zur Sicherstellung der ordnungsgemäßen Verarbeitung sowie der Integrität und Sicherheit der Daten verwendet werden.

ABSCHNITT II – WEITERVERARBEITUNG, INSBESONDERE WEITERGABE UND ÜBERTRAGUNG, VON DATEN, DIE VON DEN ZUSTÄNDIGEN BEHÖRDEN ANDERER MITGLIEDSTAATEN ÜBERSANDT ODER ZUR VERFÜGUNG GESTELLT WURDEN

Artikel 11
Weiterverarbeitung von personenbezogenen Daten, die von der zuständigen Behörde eines anderen Mitgliedstaats übersandt oder zur Verfügung gestellt wurden

1. Die Mitgliedstaaten sehen vor, dass personenbezogene Daten, die von der zuständigen Behörde eines anderen Mitgliedstaats übersandt oder zur Verfügung gestellt wurden, nach Maßgabe dieses Rahmenbeschlusses, insbesondere der Artikel 4, 5 und 6, nur zu folgenden Zwecken weiterverarbeitet werden dürfen:

   (a) zur Erfüllung des Zwecks, zu dem die Daten übermittelt oder zur Verfügung gestellt wurden, oder

   (b) erforderlichenfalls zur Verhütung, Aufdeckung, Untersuchung und Verfolgung von Straftaten oder zur Abwehr einer Bedrohung der öffentlichen Sicherheit oder einer Person, sofern nicht die Interessen oder die Grundrechte der betroffenen Person überwiegen.

2. Zu den in Absatz 1 Buchstabe b genannten Zwecken dürfen die personenbezogenen Daten nur mit Einwilligung der Behörde, die sie übermittelt oder zur Verfügung gestellt hat, weiterverarbeitet werden.

3. Absatz 1 Buchstabe b gilt nicht für personenbezogene Daten, die von der zuständigen Behörde eines anderen Mitgliedstaats übersandt oder zur Verfügung gestellt wurden, und für die im Rahmen von Titel VI des Vertrags über die Europäische Union erlassene Rechtsvorschriften ausdrücklich vorsehen, dass sie ausschließlich zur Erfüllung des Zwecks verarbeitet werden dürfen, zu dem sie übermittelt oder zur Verfügung gestellt wurden.

Artikel 12
Übermittlung an andere zuständige Behörden

Die Mitgliedstaaten sehen vor, dass personenbezogene Daten, die von der zuständigen Behörde eines anderen Mitgliedstaats übersandt oder zur Verfügung gestellt wurden, nur dann an andere zuständige Behörden in einem Mitgliedstaat weitergegeben oder diesen zur Verfügung gestellt werden dürfen, wenn folgende Anforderungen erfüllt sind:

(a) Die Weitergabe oder Bereitstellung der Daten ist durch eine Gesetzesvorschrift geregelt, die eindeutig eine Pflicht zur Weitergabe der Daten begründet oder diese erlaubt.

(b) Die Weitergabe oder Bereitstellung ist zur Erfüllung der rechtmäßigen Aufgaben der Behörde, die die betreffenden Daten erhalten hat, oder der Behörde, an die die Daten weitergeleitet werden sollen, notwendig.

(c) Die Weitergabe oder Bereitstellung ist zur Erfüllung des Zwecks, zu dem die Daten übermittelt wurden, oder zur Verhütung, Aufdeckung, Untersuchung und Verfolgung von Straftaten oder zur Abwehr einer Bedrohung der öffentlichen Sicherheit oder einer Person erforderlich, und es überwiegen keine Interessen oder Grundrechte der betroffenen Person.

(d) Die zuständige Behörde des Mitgliedstaats, die die Daten der anderen zuständigen Behörde, die diese weitergeben oder zur Verfügung stellen will, übermittelt oder zur Verfügung gestellt hat, hat ihre vorherige Einwilligung zu der Weitergabe oder Bereitstellung der Daten erteilt.

Artikel 13
Übermittlung an andere als die zuständigen Behörden

Die Mitgliedstaaten sorgen dafür, dass personenbezogene Daten, die von der zuständigen Behörde eines anderen Mitgliedstaats übersandt oder zur Verfügung gestellt wurden, im Ausnahmefall an andere als die zuständigen Behörden in einem Mitgliedstaat weitergegeben werden dürfen, wenn folgende Anforderungen erfüllt sind:

(a) Die Weitergabe der Daten ist durch eine Gesetzesvorschrift geregelt, die eindeutig eine Pflicht zur Weitergabe der Daten begründet oder diese erlaubt.

(b) Die Weitergabe ist

zur Erfüllung des Zwecks, zu dem die Daten übermittelt wurden, zur Verhütung, Aufdeckung, Untersuchung und Verfolgung von Straftaten oder zur Abwehr einer Bedrohung der öffentlichen Sicherheit oder einer Person erforderlich, und es überwiegen keine Interessen oder Grundrechte der betroffenen Person,

oder

sie ist unabdingbar für die Erfüllung der rechtmäßigen Aufgaben der Behörde, an die die Daten weitergeleitet werden sollen, und der Zweck, zu dem die Daten von dieser Behörde gesammelt oder verarbeitet werden sollen, ist sowohl mit der ursprünglichen Bearbeitung der Daten als auch mit den rechtlichen Pflichten der zuständigen Behörde, die die Daten weitergeben will, vereinbar,

oder

sie liegt zweifelsfrei im Interesse der betroffenen Person, und diese hat ihre Einwilligung zu der Weitergabe erteilt oder die Umstände lassen eindeutig eine solche Einwilligung vermuten.

(c) Die zuständige Behörde eines anderen Mitgliedstaats, die der zuständigen Behörde die Daten, die diese weitergeben will, übermittelt oder zur Verfügung gestellt hat, hat ihre vorherige Einwilligung zu der Weitergabe der Daten erteilt.

Artikel 14
Übermittlung an nicht-öffentliche Stellen

Die Mitgliedstaaten sehen vor, dass unbeschadet innerstaatlicher Strafverfahrensvorschriften personenbezogene Daten, die von der zuständigen Behörde eines anderen Mitgliedstaat übersandt oder zur Verfügung gestellt wurden, nur in Sonderfällen an nicht-öffentliche Stellen in einem Mitgliedstaat übermittelt werden dürfen, wenn sämtliche folgende Anforderungen erfüllt sind:

a) Die Übermittlung der Daten ist durch eine Gesetzesvorschrift geregelt, die eindeutig zur Übermittlung der Daten verpflichtet bzw. diese erlaubt,

b) die Übermittlung ist zu dem Zweck, zu dem die fraglichen Daten übermittelt oder zur Verfügung gestellt wurden, oder zur Verhütung, Aufdeckung, Untersuchung oder Verfolgung von Straftaten oder zur Abwehr einer Bedrohung der öffentlichen Sicherheit oder einer Person notwendig, sofern nicht die Interessen oder die Grundrechte der betroffenen Person überwiegen, und

c) die zuständige Behörde des Mitgliedstaats, der die Daten derjenigen zuständigen Behörde übermittelt oder zur Verfügung gestellt hat, die diese weiterübermitteln will, hat zuvor ihre Einwilligung zu deren Übermittlung an nicht-öffentliche Stellen gegeben.

Artikel 15
Übertragung an die zuständigen Behörden in Drittländern oder an internationale Einrichtungen

1. Die Mitgliedstaaten stellen sicher, dass die personenbezogenen Daten, die von der zuständigen Behörde eines anderen Mitgliedstaats übersandt oder zur Verfügung gestellt wurden, nicht an zuständige Behörden von Drittländern oder internationale Einrichtungen weiterübertragen werden, es sei denn, diese Weiterübertragung ist mit diesem Rahmenbeschluss vereinbar und sämtliche folgende Anforderungen sind erfüllt:

a) Die Übertragung der Daten ist durch eine Rechtsvorschrift geregelt, die eindeutig zur Übertragung der Daten verpflichtet oder dies erlaubt,

b) die Übertragung ist zu dem Zweck, zu dem die fraglichen Daten übertragen oder zur Verfügung gestellt wurden, oder zur Verhütung, Aufdeckung, Untersuchung oder Verfolgung von Straftaten oder zur Abwehr einer Bedrohung der öffentlichen Sicherheit oder einer Person notwendig, sofern nicht die Interessen oder die Grundrechte der betroffenen Person überwiegen,

c) die zuständige Behörde eines anderen Mitgliedstaats, die derjenigen zuständigen Behörde die Daten übermittelt oder zur Verfügung gestellt hat, die

diese weiterübertragen will, hat zuvor ihre Einwilligung zur Weiterübertragung der Daten gegeben,

d) in diesem Drittland oder dieser internationalen Einrichtung, an das bzw. die die Daten übertragen werden sollen, ist ein angemessener Datenschutz gewährleistet.

2. Die Mitgliedstaaten stellen sicher, dass die Angemessenheit des Datenschutzes, den ein Drittland oder eine internationale Einrichtung gewährleistet, unter Berücksichtigung aller Umstände beurteilt wird, die bei einer Datenübertragung oder einer Datenübertragungskategorie eine Rolle spielen. Bei der Beurteilung sind insbesondere folgende Aspekte zu berücksichtigen: Art der Daten, Zweck und Dauer der Verarbeitung, derentwegen die Daten übertragen werden, Herkunfts- und das Endbestimmungsland, die in dem betreffenden Drittland oder der betreffenden Einrichtung geltenden allgemeinen oder sektoriellen Rechtsnormen, die dort geltenden Standesregeln und Sicherheitsmaßnahmen sowie geeignete Garantien seitens des Datenempfängers.

3. Die Mitgliedstaaten und die Kommission unterrichten einander über die Fälle, in denen ihres Erachtens ein Drittland oder eine internationale Einrichtung keinen angemessenen Schutz im Sinne des Absatzes 2 gewährleistet.

4. Wird nach dem Verfahren des Artikels 16 festgestellt, dass ein Drittland oder eine internationale Einrichtung keinen angemessenen Schutz im Sinne des Absatzes 2 gewährleistet, ergreifen die Mitgliedstaaten die erforderlichen Maßnahmen, um die Übertragung der personenbezogenen Daten an das fragliche Drittland bzw. die internationale Einrichtung zu verhindern.

5. Nach dem Verfahren des Artikels 16 kann festgestellt werden, dass ein Drittland oder eine internationale Einrichtung aufgrund seiner innerstaatlichen Rechtsvorschriften bzw. internationaler Verpflichtungen hinsichtlich des Schutzes der Privatsphäre sowie der Freiheiten und Grundrechte von Personen ein angemessenes Schutzniveau im Sinne des Absatzes 2 gewährleistet.

6. Personenbezogene Daten, die von der zuständigen Behörde eines anderen Mitgliedstaats übersandt wurden, dürfen ausnahmsweise an zuständige Behörden eines Drittlandes oder internationale Einrichtungen, in dem bzw. denen ein angemessener Datenschutz nicht gewährleistet ist, weiterübertragen werden, wenn dies zum Schutz der grundlegenden Interessen eines Mitgliedstaats oder zur Abwehr einer drohenden ernsthaften Gefahr für die öffentliche Sicherheit oder für eine oder mehrere Personen unbedingt notwendig ist.

Artikel 16

Ausschuss

1. Wird auf diesen Artikel Bezug genommen, so wird die Kommission von einem Ausschuss unterstützt, der sich aus Vertretern der Mitgliedstaaten zusammensetzt und in dem der Vertreter der Kommission den Vorsitz führt.

2. Der Ausschuss gibt sich auf Vorschlag seines Vorsitzenden eine Geschäftsordnung auf der Grundlage der Standardgeschäftsordnung, die im Amtsblatt der Europäischen Union veröffentlicht wurde.

3. Der Vertreter der Kommission unterbreitet dem Ausschuss einen Entwurf der zu treffenden Maßnahmen. Der Ausschuss gibt seine Stellungnahme zu diesem Entwurf innerhalb einer Frist ab, die der Vorsitzende unter Berücksichtigung der Dringlichkeit der betreffenden Frage festsetzen kann. Die Stellungnahme wird mit der Mehrheit abgegeben, die in Artikel 205 Absatz 2 des Vertrags zur Gründung der Europäischen Gemeinschaft für die Annahme der vom Rat auf Vorschlag der Kommission zu fassenden Beschlüsse vorgesehen ist. Bei der Abstimmung im Ausschuss werden die Stimmen der Vertreter der Mitgliedstaaten gemäß dem vorgenannten Artikel gewogen. Der Vorsitzende nimmt an der Abstimmung nicht teil.

4. Die Kommission erlässt die beabsichtigten Maßnahmen, wenn sie mit der Stellungnahme des Ausschusses übereinstimmen. Stehen die geplanten Maßnahmen mit der Stellungnahme des Ausschusses nicht in Einklang oder liegt keine Stellungnahme vor, so unterbreitet die Kommission dem Rat unverzüglich einen Vorschlag für die zu treffenden Maßnahmen und unterrichtet das Europäische Parlament.

5. Der Rat kann innerhalb von zwei Monaten ab seiner Befassung mit qualifizierter Mehrheit über den Vorschlag befinden.

   Hat sich der Rat innerhalb dieser Frist mit qualifizierter Mehrheit gegen den Vorschlag ausgesprochen, so überprüft die Kommission den Vorschlag. Die Kommission kann dem Rat einen geänderten Vorschlag vorlegen, ihren Vorschlag erneut vorlegen oder einen Vorschlag für einen Rechtsakt vorlegen. Hat der Rat nach Ablauf dieser Frist weder den vorgeschlagenen Durchführungsrechtsakt erlassen noch sich gegen den Vorschlag für die Durchführungsmaßnahmen ausgesprochen, so wird der vorgeschlagene Durchführungsrechtsakt von der Kommission erlassen.

Artikel 17
Ausnahmen von den Artikeln 12, 13, 14 und 15

Die Artikel 12, 13, 14 und 15 kommen nicht zur Anwendung, wenn in nach Titel VI des Vertrags über die Europäische Union verabschiedeten speziellen Vorschriften ausdrücklich festgelegt ist, dass personenbezogene Daten, die von der zuständigen Behörde eines anderen Mitgliedstaats übersandt oder zur Verfügung gestellt wurden, nicht weiterübermittelt oder nur unter ganz besonderen Bedingungen weiterübermittelt werden dürfen.

Artikel 18
Unterrichtung auf Antrag der zuständigen Behörde

Die Mitgliedstaaten sehen vor, dass die zuständige Behörde, die die personenbezogenen Daten übersandt oder zur Verfügung gestellt hat, auf deren Antrag über die weitere Verarbeitung und deren Ergebnisse unterrichtet werden muss.

KAPITEL IV
RECHTE DER BETROFFENEN PERSON

Artikel 19
Informationsrecht bei der Erhebung von Daten von Personen mit deren Wissen

1. Die Mitgliedstaaten sehen vor, dass die Person, bei der die sie betreffenden Daten mit ihrem Wissen erhoben werden, vom für die Verarbeitung Verantwortlichen oder seinem Vertreter zumindest die nachstehenden Informationen kostenlos erhält, sofern diese ihr noch nicht vorliegen:

   a) Identität des für die Verarbeitung Verantwortlichen und gegebenenfalls seines Vertreters,

   b) Zwecke der Verarbeitung, für die die Daten bestimmt sind,

   c) weitere Informationen, beispielsweise

   – die Rechtsgrundlage der Verarbeitung,

   – die Empfänger oder Kategorien der Empfänger der Daten,

   – ob die Beantwortung von Fragen oder andere Formen der Zusammenarbeit obligatorisch oder freiwillig ist bzw. sind, sowie mögliche Folgen einer Antwortverweigerung oder Verweigerung der Zusammenarbeit,

   – das Recht auf Auskunft über die sie betreffenden Daten und auf Berichtigung dieser Daten,

   sofern sie unter Berücksichtigung der spezifischen Umstände, unter denen die Daten erhoben werden, notwendig sind, um gegenüber der betroffenen Person eine Verarbeitung nach Treu und Glauben zu gewährleisten.

2. Die in Absatz 1 genannten Informationen werden nur dann verweigert oder nur eingeschränkt erteilt, wenn dies aus folgenden Gründen notwendig ist:

   a) um dem für die Verarbeitung Verantwortlichen die ordnungsgemäße Erfüllung seiner Aufgaben zu ermöglichen,

   b) um nicht laufende Ermittlungen, Untersuchungen oder Verfahren oder die zuständigen Behörden bei der ordnungsgemäßen Erfüllung ihrer Aufgaben zu behindern,

   c) um die öffentliche Sicherheit und Ordnung in einem Mitgliedstaat zu schützen,

   d) um die Rechte und Freiheiten Dritter zu schützen,

   sofern nicht die Interessen oder die Grundrechte der betroffenen Person überwiegen.

3. Werden die in Absatz 1 genannten Informationen verweigert oder nur beschränkt erteilt, teilt der für die Datenverarbeitung Verantwortliche der betreffenden Person mit, dass sie unbeschadet der Einlegung eines Rechtsmittels bei Gericht und unbeschadet eines innerstaatlichen Strafverfahrens bei der zuständigen Kontrollstelle Einspruch einlegen kann.

4. Die Gründe für die vollständige oder teilweise Verweigerung der Informationen in Absatz 2 werden nicht genannt, wenn dies dem Zweck der Verweigerung entgegensteht. In diesem Fall teilt der für die Datenverarbeitung Verantwortliche der betreffenden Person mit, dass sie unbeschadet der Einlegung eines Rechtsmittels bei Gericht und unbeschadet eines innerstaatlichen Strafverfahrens bei der zuständigen Kontrollstelle Einspruch einlegen kann. Legt die von der Verarbeitung ihrer Daten betroffene Person bei einer Kontrollstelle Beschwerde ein, prüft diese Stelle die Beschwerde. Bei der Prüfung der Beschwerde setzt die Kontrollbehörde die betroffene Person nur darüber in Kenntnis, ob die Daten ordnungsgemäß verarbeitet wurden und, sollte dies nicht der Fall gewesen sein, ob die erforderliche Berichtigung erfolgt ist.

Artikel 20

Recht auf Information, wenn die Daten nicht von der betroffenen Person oder von der betroffenen Person ohne deren Kenntnis erhoben wurden

1. Wenn die Daten nicht von der betroffenen Person oder von ihr ohne ihre Kenntnis erhoben wurden oder ohne ihr Wissen erhoben wurden, dass Daten über sie erfasst wurden, sehen die Mitgliedstaaten vor, dass der für die Verarbeitung Verantwortliche oder sein Vertreter bei der Speicherung der Daten bzw. im Fall einer beabsichtigten Weitergabe der Daten an Dritte binnen einer angemessenen Frist nach der ersten Weitergabe der Daten zumindest die nachstehenden Informationen kostenlos erteilen muss, sofern diese ihr noch nicht vorliegen, die Information der betroffenen Person nicht unmöglich ist oder keinen unverhältnismäßigen Aufwand erfordert:

   a) Identität des für die Verarbeitung Verantwortlichen und gegebenenfalls seines Vertreters,

   b) Zwecke der Verarbeitung,

   c) weitere Informationen, beispielsweise

   – die Rechtsgrundlage der Verarbeitung,

   – die Datenkategorien, die verarbeitet werden,

   – die Empfänger oder Kategorien der Empfänger der Daten,

   – das Bestehen von Auskunfts- und Berichtigungsrechten bezüglich sie betreffender Daten,

   sofern sie unter Berücksichtigung der spezifischen Umstände, unter denen die Daten erhoben werden, notwendig sind, um gegenüber der betroffenen Person eine Verarbeitung nach Treu und Glauben zu gewährleisten.

2. Die in Absatz 1 aufgeführten Informationen werden nicht vorgelegt, wenn dies zu folgenden Zwecken notwendig ist:

a) um dem für die Verarbeitung Verantwortlichen die ordnungsgemäße Erfüllung seiner Aufgaben zu ermöglichen,

b) um nicht laufende Ermittlungen, Untersuchungen oder Verfahren oder die zuständigen Behörden bei der ordnungsgemäßen Erfüllung ihrer Aufgaben zu behindern,

c) um die öffentliche Sicherheit und Ordnung in einem Mitgliedstaat zu schützen,

d) um die Rechte und Freiheiten Dritter zu schützen,

sofern nicht die Interessen oder die Grundrechte der betroffenen Person überwiegen.

Artikel 21
Recht auf Auskunft, Berichtigung, Löschung oder Sperrung von Daten

1. Die Mitgliedstaaten garantieren jeder betroffenen Person das Recht, vom für die Verarbeitung Verantwortlichen Folgendes zu erhalten:

a) frei und ungehindert in angemessenen Abständen ohne unzumutbare Verzögerung oder übermäßige Kosten

– die Bestätigung, dass sie betreffende Daten verarbeitet werden oder nicht, sowie Informationen zumindest über die Zwecke dieser Verarbeitung, die betroffenen Kategorien der Daten, die Rechtsgrundlage der Verarbeitung und die Empfänger oder Kategorien der Empfänger, an die die Daten weitergegeben wurden,

– eine Mitteilung in verständlicher Form über die Daten, die Gegenstand der Verarbeitung sind, sowie die verfügbaren Informationen über die Herkunft der Daten;

b) je nach Fall die Berichtigung, Löschung oder Sperrung von Daten, deren Verarbeitung nicht den Bestimmungen dieses Rahmenbeschlusses entspricht, insbesondere wenn diese Daten unvollständig oder unrichtig sind,

c) die Gewähr, dass jede Berichtigung, Löschung oder Sperrung, die entsprechend Buchstabe b durchgeführt wurde, den Dritten, an die die Daten weitergegeben wurden, mitgeteilt wird, sofern sich dies nicht als unmöglich erweist oder kein unverhältnismäßiger Aufwand damit verbunden ist.

2. Jede Maßnahme, auf die die betroffene Person gemäß Absatz 1 Anspruch hat, wird verweigert, wenn dies zu folgenden Zwecken notwendig ist:

a) um dem für die Verarbeitung Verantwortlichen die ordnungsgemäße Erfüllung seiner Aufgaben zu ermöglichen,

b) um nicht laufende Ermittlungen, Untersuchungen oder Verfahren oder die zuständigen Behörden bei der ordnungsgemäßen Erfüllung ihrer Aufgaben zu behindern,

c) um die öffentliche Sicherheit und Ordnung in einem Mitgliedstaat zu schützen,

d) um die Rechte und Freiheiten Dritter zu schützen,

sofern nicht die Interessen oder die Grundrechte der betroffenen Person überwiegen.

3. Eine Verweigerung oder Einschränkung der in Absatz 1 genannten Rechte ist schriftlich mitzuteilen. Wird das in Absatz 1 genannte Recht verweigert oder eingeschränkt, so teilt der für die Datenverarbeitung Verantwortliche der betreffenden Person mit, dass sie unbeschadet der Einlegung eines Rechtsmittels bei Gericht und innerstaatlicher Strafverfahren bei der zuständigen Kontrollstelle Einspruch einlegen kann.

4. Die Gründe für die Verweigerung eines Rechts gemäß Absatz 2 werden dem von der Datenverarbeitung Betroffenen nicht genannt, wenn dies dem Zweck der Verweigerung entgegensteht. In diesem Fall teilt der für die Datenverarbeitung Verantwortliche der betreffenden Person mit, dass sie unbeschadet der Einlegung eines Rechtsmittels bei Gericht und unbeschadet innerstaatlicher Strafverfahren bei der zuständigen Kontrollstelle Einspruch einlegen kann. Legt die von der Verarbeitung ihrer Daten betroffene Person bei einer Kontrollstelle Beschwerde ein, prüft diese Stelle die Beschwerde. Bei der Prüfung der Beschwerde setzt die Kontrollbehörde die betroffene Person nur darüber in Kenntnis, ob die Daten ordnungsgemäß verarbeitet wurden und, sollte dies nicht der Fall gewesen sein, ob die erforderliche Berichtigung erfolgt ist.

Artikel 22
Information Dritter über die Berichtigung, Löschung oder Sperrung

Die Mitgliedstaaten sehen vor, dass geeignete technische Maßnahmen getroffen werden müssen, um zu gewährleisten, dass automatisch eine Liste der Datenlieferanten und Empfänger dieser Daten erstellt wird, wenn der für die Verarbeitung Verantwortliche auf Antrag personenbezogene Daten berichtigt, sperrt oder löscht. Der für die Verarbeitung Verantwortliche stellt sicher, dass die auf der Liste aufgeführten Personen über die Änderungen an den personenbezogenen Daten informiert werden.

KAPITEL V
Geheimhaltung und Sicherheit der Verarbeitung

Artikel 23
Geheimhaltung

Personen, die dem für die Verarbeitung Verantwortlichen oder dem Auftragsverarbeiter unterstellt sind und Zugang zu personenbezogenen Daten haben, sowie der Auftragsverarbeiter selbst dürfen personenbezogene Daten nur auf Weisung des für die

Verarbeitung Verantwortlichen verarbeiten, es sei denn, es bestehen gesetzliche Verpflichtungen. Personen, die beauftragt werden, in oder mit einer zuständigen Behörde eines Mitgliedstaats (zusammen) zu arbeiten, unterliegen strengen Geheimhaltungsbestimmungen.

Artikel 24
Sicherheit

1. Die Mitgliedstaaten sehen vor, dass der für die Verarbeitung Verantwortliche die geeigneten technischen und organisatorischen Maßnahmen durchführen muss, die erforderlich sind, um die unbeabsichtigte oder unerlaubte Zerstörung, den unbeabsichtigten Verlust, die unberechtigte Änderung, die unberechtigte Weitergabe oder den unberechtigten Zugang - insbesondere wenn im Rahmen der Verarbeitung Daten in einem Netz übermittelt oder durch einen direkten automatischen Zugang zur Verfügung gestellt werden - und jede andere Form der unerlaubten Verarbeitung personenbezogener Daten zu verhindern. Dabei sind insbesondere die Risiken bei der Verarbeitung und der Art der zu schützenden Daten zu berücksichtigen.

   Diese Maßnahmen müssen unter Berücksichtigung des Standes der Technik und der bei ihrer Durchführung entstehenden Kosten ein Schutzniveau gewährleisten, das den von der Verarbeitung ausgehenden Risiken und der Art der zu schützenden Daten angemessen ist. Als erforderlich gelten Maßnahmen, wenn angesichts des angestrebten Schutzzwecks ihr Aufwand nicht unverhältnismäßig ist.

2. Jeder Mitgliedstaat trifft im Hinblick auf die automatisierte Datenverarbeitung Maßnahmen, die geeignet sind,

   a) Unbefugten den Zugang zu Datenverarbeitungsanlagen, mit denen personenbezogene Daten verarbeitet werden, zu verwehren (Zugangskontrolle),

   b) zu verhindern, dass Datenträger unbefugt gelesen, kopiert, verändert oder entfernt werden können (Datenträgerkontrolle),

   c) die unbefugte Eingabe in den Speicher sowie die unbefugte Kenntnisnahme, Veränderung und Löschung von gespeicherten personenbezogenen Daten zu verhindern (Speicherkontrolle),

   d) zu verhindern, dass automatisierte Datenverarbeitungssysteme mit Hilfe von Einrichtungen zur Datenübertragung von Unbefugten genutzt werden können (Benutzerkontrolle),

   e) zu gewährleisten, dass die zur Benutzung eines automatisierten Datenverarbeitungssystems Berechtigten ausschließlich auf die ihrer Zugriffsberechtigung unterliegenden Daten zugreifen können (Zugriffskontrolle),

   f) zu gewährleisten, dass überprüft und festgestellt werden kann, an welche Stellen personenbezogene Daten mit Hilfe von Einrichtungen zur Datenübertragung übermittelt oder zur Verfügung gestellt wurden oder werden können (Übermittlungskontrolle),

g) zu gewährleisten, dass nachträglich überprüft und festgestellt werden kann, welche personenbezogenen Daten zu welcher Zeit und von wem in automatisierte Datenverarbeitungssysteme eingegeben worden sind (Eingabekontrolle),

h) zu verhindern, dass bei der Übertragung personenbezogener Daten sowie beim Transport von Datenträgern die Daten unbefugt gelesen, kopiert, verändert oder gelöscht werden können (Transportkontrolle),

(i) zu gewährleisten, dass eingesetzte Systeme im Störungsfalle unverzüglich wiederhergestellt werden können (Wiederherstellung) und

(j) zu gewährleisten, dass die Funktionen des Systems fehlerfrei ablaufen, auftretende Fehlfunktionen unverzüglich gemeldet werden (Zuverlässigkeit) und gespeicherte Daten nicht durch Fehlfunktionen des Systems fehlerhaft werden (Datenintegrität).

3. Die Mitgliedstaaten sehen vor, dass der für die Verarbeitung Verantwortliche im Fall einer Verarbeitung in seinem Auftrag einen Auftragsverarbeiter auszuwählen hat, der hinsichtlich der für die Verarbeitung zu treffenden technischen Sicherheitsmaßnahmen und organisatorischen Vorkehrungen ausreichende Gewähr bietet; der für die Verarbeitung Verantwortliche sorgt für die Einhaltung dieser Maßnahmen.

4. Die Durchführung einer Verarbeitung im Auftrag erfolgt auf der Grundlage eines Vertrags oder Rechtsakts, durch den der Auftragsverarbeiter an den für die Verarbeitung Verantwortlichen gebunden ist und in dem insbesondere Folgendes vorgesehen ist:

– Der Auftragsverarbeiter handelt nur auf Weisung des für die Verarbeitung Verantwortlichen.

– Die in den Absätzen 1 und 2 genannten Verpflichtungen gelten auch für den Auftragsverarbeiter, und zwar nach Maßgabe der Rechtsvorschriften des Mitgliedstaats, in dem er niedergelassen ist.

5. Zum Zwecke der Beweissicherung sind die datenschutzrelevanten Elemente des Vertrags oder Rechtsakts und die Anforderungen in Bezug auf die Maßnahmen nach Absatz 1 schriftlich oder in einer anderen, gleichwertigen Form zu dokumentieren.

Artikel 25
Verzeichnis

1. Die Mitgliedstaaten sehen vor, dass jeder für die Verarbeitung Verantwortliche ein Verzeichnis jeder vorgenommenen Verarbeitung oder mehrerer Verarbeitungen zu einem oder mehreren verbundenen Zwecken führen muss. Im Verzeichnis sind folgende Informationen festzuhalten:

a) Name und Anschrift des für die Verarbeitung Verantwortlichen und gegebenenfalls seines Vertreters;

b) die Zweckbestimmung(en) der Verarbeitung;

c) eine Beschreibung der Kategorie(n) der betroffenen Personen und der diesbezüglichen Daten oder Datenkategorien;

d) Rechtsgrundlage der Verarbeitung, für die die Daten bestimmt sind;

e) die Empfänger oder Kategorien von Empfängern, an die die Daten weitergegeben werden können;

f) eine geplante Datenübertragung in Drittländer;

g) eine allgemeine Beschreibung, die es ermöglicht, vorläufig zu beurteilen, ob die Maßnahmen nach Artikel 24 zur Gewährleistung der Sicherheit der Verarbeitung angemessen sind.

2. Die Mitgliedstaaten legen die Bedingungen und Verfahren für die Meldung der in Absatz 1 genannten Angaben an die Kontrollstelle fest.

Artikel 26
Vorabkontrolle

1. Die Mitgliedstaaten legen fest, welche Verarbeitungen spezifische Risiken für die Rechte und Freiheiten der betroffenen Personen in sich bergen können, und tragen dafür Sorge, dass diese Verarbeitungen vor ihrem Beginn geprüft werden.

2. Solche Vorabprüfungen nimmt die Kontrollstelle nach Empfang der Meldung des für die Verarbeitung Verantwortlichen oder des Datenschutzbeauftragten vor, der im Zweifelsfall die Kontrollstelle konsultieren muss.

3. Die Mitgliedstaaten können eine solche Prüfung auch im Zuge der Ausarbeitung einer Maßnahme ihres Parlaments oder einer auf eine solche gesetzgeberische Maßnahme gestützten Maßnahme durchführen, die die Art der Verarbeitung festlegt und geeignete Garantien vorsieht.

KAPITEL VI
RECHTSBEHELFE UND HAFTUNG

Artikel 27
Rechtsbehelfe

Unbeschadet möglicher verwaltungsrechtlicher Beschwerdeverfahren, die vor Beschreiten des Rechtsweges insbesondere bei der in Artikel 30 genannten Kontrollstelle eingeleitet werden können, sehen die Mitgliedstaaten vor, dass jede Person im Falle der Verletzung der Rechte, die ihr nach diesem Rahmenbeschluss durch die für die betreffende Verarbeitung geltenden innerstaatlichen Rechtsvorschriften garantiert sind, bei Gericht Rechtsmittel einlegen kann.

Artikel 28
Haftung

1. Die Mitgliedstaaten sehen vor, dass jede Person, der wegen einer rechtswidrigen Verarbeitung oder einer anderen mit den innerstaatlichen Vorschriften zur Umsetzung dieses Rahmenbeschlusses nicht zu vereinbarenden Handlung ein Schaden entsteht, Anspruch auf Schadenersatz von dem für die Verarbeitung Verantwortlichen hat. Der für die Verarbeitung Verantwortliche kann teilweise oder vollständig von seiner Haftung befreit werden, wenn er nachweist, dass der Umstand, durch den der Schaden eingetreten ist, ihm nicht zur Last gelegt werden kann.

2. Eine zuständige Behörde, die personenbezogene Daten von einer zuständigen Behörde eines anderen Mitgliedstaats erhalten hat, haftet jedoch gegenüber dem Geschädigten für Schäden, die auf die Verwendung von unrichtigen oder veralteten Daten zurückzuführen sind. Sie kann die Haftung nicht mit der Begründung ablehnen, dass sie unrichtige oder veraltete Daten von einer anderen Behörde erhalten hat. Muss die empfangende Stelle wegen Verwendung unrichtiger Daten, die von der zuständigen Behörde eines anderen Mitgliedstaats übermittelt oder zur Verfügung gestellt wurden, Schadenersatz leisten, so erstattet letztere der empfangenden Stelle den Gesamtbetrag des geleisteten Ersatzes.

Artikel 29
Sanktionen

1. Die Mitgliedstaaten ergreifen geeignete Maßnahmen, um die ordnungsgemäße Anwendung der Bestimmungen dieses Rahmenbeschlusses sicherzustellen, und legen insbesondere wirksame, angemessene und abschreckende Sanktionen fest, die bei Verstößen gegen die Vorschriften zur Umsetzung dieses Rahmenbeschlusses zu verhängen sind.

2. Die Mitgliedstaaten sehen wirksame, angemessene und abschreckende strafrechtliche Sanktionen für vorsätzliche Straftaten vor, die schwere Verstöße gegen die innerstaatlichen Vorschriften zur Umsetzung dieses Rahmenbeschlusses, vor allem gegen die Bestimmungen über die Geheimhaltung und die Sicherheit der Verarbeitung darstellen.

KAPITEL VII
KONTROLLSTELLE UND GRUPPE FÜR DEN SCHUTZ VON PERSONEN BEI DER VERARBEITUNG PERSONENBEZOGENER DATEN

Artikel 30
Kontrollstelle

1. Die Mitgliedstaaten sehen vor, dass eine oder mehrere öffentliche Stellen beauftragt werden, die Anwendung der von den Mitgliedstaaten zur Umsetzung dieses Rahmenbeschlusses erlassenen innerstaatlichen Vorschriften in ihrem Hoheitsgebiet

zu überwachen. Diese Stellen nehmen die ihnen zugewiesenen Aufgaben in völliger Unabhängigkeit wahr.

2. Die Mitgliedstaaten sehen vor, dass die Kontrollstellen bei der Ausarbeitung von Rechts- oder Verwaltungsvorschriften zum Schutz der Rechte und Freiheiten von Personen bei der Verarbeitung personenbezogener Daten zur Verhütung, Aufdeckung, Untersuchung und Verfolgung von Straftaten konsultiert werden.

3. Jede Kontrollstelle verfügt insbesondere über:

   – Untersuchungsbefugnisse, wie das Recht auf Zugang zu Daten, die Gegenstand von Verarbeitungen sind, und das Recht auf Einholung aller für die Erfüllung ihres Überwachungsauftrags erforderlichen Informationen,

   – wirksame Einwirkungsbefugnisse, wie beispielsweise die Möglichkeit, im Einklang mit Artikel 26 vor der Durchführung der Verarbeitungen Stellungnahmen abzugeben und für eine geeignete Veröffentlichung der Stellungnahmen zu sorgen, oder die Befugnis, die Sperrung, Löschung oder Vernichtung von Daten oder das vorläufige oder endgültige Verbot einer Verarbeitung anzuordnen, oder die Befugnis, den für die Verarbeitung Verantwortlichen zu verwarnen oder zu ermahnen oder die Parlamente oder andere Regierungseinrichtungen zu befassen,

   – das Klagerecht oder eine Anzeigebefugnis bei Verstößen gegen die innerstaatlichen Vorschriften zur Umsetzung dieses Rahmenbeschlusses.

   Gegen beschwerende Entscheidungen der Kontrollstelle kann Rechtsmittel eingelegt werden.

4. Jede Person kann sich zum Schutz der die Person betreffenden Rechte und Freiheiten bei der Verarbeitung personenbezogener Daten an jede Kontrollstelle mit einer Eingabe wenden. Die betroffene Person ist darüber zu informieren, wie mit der Eingabe verfahren wurde.

5. Jede Kontrollstelle legt regelmäßig einen Bericht über ihre Tätigkeit vor. Dieser Bericht wird veröffentlicht.

6. Jede Kontrollstelle ist unabhängig von dem auf die jeweilige Verarbeitung anwendbaren innerstaatlichen Recht im Hoheitsgebiet ihres Mitgliedstaats für die Ausübung der ihr gemäß Absatz 3 übertragenen Befugnisse zuständig. Jede Kontrollstelle kann von einer Kontrollstelle eines anderen Mitgliedstaats zur Ausübung ihrer Befugnisse aufgefordert werden.

7. Die Kontrollstellen arbeiten mit den anderen Kontrollstellen sowie mit den nach Titel VI des Vertrags über die Europäische Union eingesetzten Kontrollinstanzen und dem Europäischen Datenschutzbeauftragten, insbesondere durch den Austausch sachdienlicher Informationen, zusammen, soweit dies zur Erfüllung ihrer Aufgaben notwendig ist.

8. Die Mitgliedstaaten sehen vor, dass die vertraulichen Informationen, zu denen Mitglieder und Bedienstete der Kontrollstellen Zugang haben, dem Berufsgeheimnis unterliegen, an das diese auch nach ihrem Ausscheiden aus dem Dienst gebunden sind.

9. Die Befugnisse der Kontrollstellen schränken die Unabhängigkeit der Justiz nicht ein und Entscheidungen der Kontrollstelle ergehen unbeschadet der Wahrnehmung der rechtmäßigen Aufgaben der Justizbehörden bei der Verfolgung von Strafsachen.

Artikel 31
Gruppe für den Schutz von Personen bei der Verarbeitung personenbezogener Daten zum Zwecke der Verhütung, Aufdeckung, Untersuchung und Verfolgung von Straftaten

1. Es wird eine Gruppe für den Schutz von Personen bei der Verarbeitung personenbezogener Daten zum Zwecke der Verhütung, Aufdeckung, Untersuchung und Verfolgung von schweren Straftaten eingesetzt (nachstehend "Gruppe" genannt). Die Gruppe ist unabhängig und hat beratende Funktion.

2. Die Gruppe besteht aus einem Vertreter aller von den Mitgliedstaaten bestimmten Kontrollstellen und einem Vertreter des Europäischen Datenschutzbeauftragten sowie einem Vertreter der Kommission.

   Jedes Mitglied der Gruppe wird von der Einrichtung, der Stelle bzw. Stellen, die es vertritt, benannt. Hat ein Mitgliedstaat mehrere Kontrollstellen benannt, so ernennen diese einen gemeinsamen Vertreter.

   Die Vorsitzenden der nach Titel VI des Vertrags über die Europäische Union eingesetzten gemeinsamen Kontrollinstanzen haben das Recht, an den Sitzungen der Gruppe teilzunehmen oder einen Vertreter zu entsenden. Die von Island, Norwegen und der Schweiz benannte Kontrollstelle bzw. Kontrollstellen hat bzw. haben das Recht, an den Sitzungen der Gruppe teilzunehmen, wenn Fragen des Schengen-Besitzstands behandelt werden.

3. Die Gruppe beschließt mit der einfachen Mehrheit der Vertreter der Kontrollstellen der Mitgliedstaaten.

4. Die Gruppe wählt ihren Vorsitzenden. Die Dauer der Amtszeit des Vorsitzenden beträgt zwei Jahre. Wiederwahl ist möglich.

5. Die Sekretariatsgeschäfte der Gruppe werden von der Kommission wahrgenommen.

6. Die Gruppe gibt sich eine Geschäftsordnung.

7. Die Gruppe prüft die Fragen, die der Vorsitzende von sich aus oder auf Antrag des Vertreters einer Kontrollstelle, der Kommission, des Europäischen Datenschutzbeauftragten oder der Vorsitzenden der gemeinsamen Kontrollinstanzen auf die Tagesordnung gesetzt hat.

Artikel 32

Aufgaben

1. Die Gruppe hat die Aufgabe,

   a) alle Fragen im Zusammenhang mit der Anwendung der innerstaatlichen Vorschriften zur Umsetzung dieses Rahmenbeschlusses zu prüfen, um auf eine einheitliche Anwendung hinzuwirken;

   b) eine Stellungnahme zum Schutzniveau in den Mitgliedstaaten und in Drittländern und internationalen Einrichtungen abzugeben, um insbesondere sicherzustellen, dass zur Gewährleistung eines angemessenen Datenschutzes personenbezogene Daten gemäß Artikel 15 dieses Rahmenbeschlusses an Drittländer oder internationale Einrichtungen übertragen werden,

   c) die Kommission und die Mitgliedstaaten bei jeder Vorlage zur Änderung dieses Rahmenbeschlusses, zu zusätzlichen oder spezifischen Maßnahmen zum Schutz der Rechte und Freiheiten natürlicher Personen bei der Verarbeitung personenbezogener Daten zum Zweck der Verhütung, Aufdeckung, Untersuchung und Verfolgung von Straftaten sowie zu allen anderen vorgeschlagenen Maßnahmen zu beraten, die sich auf diese Rechte und Freiheiten auswirken.

2. Stellt die Gruppe Unterschiede zwischen den Rechtsvorschriften und der Praxis der Mitgliedstaaten fest, die die Gleichwertigkeit des Schutzes von Personen bei der Verarbeitung personenbezogener Daten in der Europäischen Union beeinträchtigen könnten, so teilt sie dies dem Rat und der Kommission mit.

3. Die Gruppe kann von sich aus oder auf Veranlassung der Kommission oder des Rates Empfehlungen zu allen Fragen abgeben, die den Schutz von Personen bei der Verarbeitung personenbezogener Daten in der Europäischen Union zum Zweck der Verhütung, Aufdeckung, Untersuchung und Verfolgung von Straftaten betreffen.

4. Die Stellungnahmen und Empfehlungen der Gruppe werden dem Rat, der Kommission, dem Europäischen Parlament und dem in Artikel 16 vorgesehenen Ausschuss übermittelt.

5. Die Kommission teilt der Gruppe auf der Grundlage der von den Mitgliedstaaten vorgelegten Informationen mit, welche Maßnahmen sie aufgrund der Stellungnahmen und Empfehlungen getroffen hat. Sie verfasst hierzu einen Bericht, der auch dem Europäischen Parlament und dem Rat übermittelt wird. Dieser Bericht wird veröffentlicht. Die Mitgliedstaaten unterrichten die Gruppe über jede Maßnahme, die sie gemäß Absatz 1 ergriffen haben.

6. Die Gruppe verfasst jährlich einen Bericht über den Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten in der Europäischen Union zum Zweck der Verhütung, Aufdeckung, Untersuchung und Verfolgung von Straftaten in der Europäischen Union und in Drittländern, den sie der Kommission, dem Europäischen Parlament und dem Rat übermittelt. Dieser Bericht wird veröffentlicht.

KAPITEL VIII
Schlussbestimmungen

Artikel 33
Änderung des Schengener Übereinkommens

In Bezug auf Angelegenheiten, die in den Anwendungsbereich des EU-Vertrags fallen, ersetzt dieser Rahmenbeschluss die Artikel 126 bis 130 des Schengener Übereinkommens.

Artikel 34
Beziehung zu anderen Instrumenten für die Verarbeitung und den Schutz personenbezogener Daten

1. Dieser Rahmenbeschluss ersetzt Artikel 23 des Übereinkommens über die Rechtshilfe in Strafsachen zwischen den Mitgliedstaaten der Europäischen Union.

2. Bezugnahmen auf das Übereinkommen Nr. 108 des Europarats vom 28. Januar 1981 zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten sind als Bezugnahmen auf diesen Rahmenbeschluss zu verstehen.

Artikel 35
Umsetzung

1. Die Mitgliedstaaten treffen die erforderlichen Maßnahmen, um diesem Rahmenbeschluss bis spätestens 31. Dezember 2006 nachzukommen.

2. Zur gleichen Frist legen die Mitgliedstaaten dem Generalsekretariat des Rates und der Kommission den Wortlaut der Bestimmungen zur Umsetzung der Vorschriften dieses Rahmenbeschlusses in innerstaatliches Recht sowie Angaben zu der bzw. den nach Artikel 29 benannten Kontrollstelle(n) vor. Der Rat prüft vor dem 31. Dezember 2007 anhand eines auf der Grundlage dieser Informationen erstellten Berichts und eines schriftlichen Berichts der Kommission, ob die Mitgliedstaaten die erforderlichen Maßnahmen getroffen haben, um diesem Rahmenbeschluss nachzukommen.

Artikel 36
Inkrafttreten

Dieser Rahmenbeschluss tritt am zwanzigsten Tag nach seiner Veröffentlichung im Amtsblatt der Europäischen Union in Kraft.

Geschehen zu Brüssel am […]

Im Namen des Rates
Der Präsident

ANHANG

FINANZBOGEN

Politikbereich(e): Justiz und Inneres

Tätigkeit(en): 1806 – Aufbau eines europäischen Straf- und Zivilrechtsraums

BEZEICHNUNG DES VORGESCHLAGENEN RECHTSAKTS: VORSCHLAG FÜR EINEN RAHMENBESCHLUSS DES RATES ÜBER DEN SCHUTZ PERSONENBEZOGENER DATEN, DIE IM RAHMEN DER POLIZEILICHEN UND JUSTIZIELLEN ZUSAMMENARBEIT IN STRAFSACHEN VERARBEITET WERDEN

1. HAUSHALTSLINIE (NUMMER UND BEZEICHNUNG)

entfällt

2. ALLGEMEINE ZAHLENANGABEN

2.1. Gesamtmittelausstattung der Maßnahme (Teil B): Mio. EUR (VE)

entfällt

2.2. Laufzeit:

beginnt 2006

2.3. Mehrjährige Gesamtvorausschätzung der Ausgaben:

a) Fälligkeitsplan für Verpflichtungsermächtigungen/Zahlungsermächtigungen (finanzielle Intervention) (*vgl. Ziffer 6.1.1*)

in Mio. € (*bis zur 3. Dezimalstelle*)

	[2006]	[2007]	[2008]	[2009]	[2010]	[2011]	Gesamt
Verpflichtungs-ermächtigungen							
Zahlungs-ermächtigungen							

b) Technische und administrative Hilfe (ATA) und Unterstützungsausgaben (DDA) (*vgl. Ziffer 6.1.2*)

Verpflichtungs-ermächtigungen							
Zahlungs-ermächtigungen							

Zwischensumme a+b							
Verpflichtungs-ermächtigungen							
Zahlungs-ermächtigungen							

c) Gesamtausgaben für Humanressourcen und Verwaltung *(Ziffer 7.2 und 7.3)*

Verpflichtungs-ermächtigungen / Zahlungs-ermächtigungen	0.389	0.389	0.389	0.389	0.389	0.389	2,334

a+b+c insgesamt							
Verpflichtungs-ermächtigungen							
Zahlungs-ermächtigungen							

2.4. Vereinbarkeit mit der Finanzplanung und der Finanziellen Vorausschau

entfällt

2.5. Finanzielle Auswirkungen auf die Einnahmen

Der Vorschlag hat keine finanziellen Auswirkungen.

3. HAUSHALTSTECHNISCHE MERKMALE

Art der Ausgaben		**Neu**	**EFTA-Beitrag**	**Beiträge von Bewerber-ländern**	**Rubrik der Finanziellen Vorausschau**
NOA	NGM	entfällt	entfällt	entfällt	Nein n.v.

4. RECHTSGRUNDLAGE

Artikel 30, 31 und 34 Absatz 2 Buchstabe b EUV

5. BESCHREIBUNG UND BEGRÜNDUNG

5.1. Notwendigkeit einer Maßnahme der Gemeinschaft

5.1.1. Ziele

Der vorgeschlagene Rahmenbeschluss führt einheitliche Vorschriften für den Schutz personenbezogener Daten ein, die von zuständigen Behörden im Rahmen von Tätigkeiten verarbeitet werden, die in Titel VI des Vertrags über die Europäische Union (polizeiliche und justizielle Zusammenarbeit in Strafsachen) vorgesehen sind. Unabhängige öffentliche Kontrollstellen sollen die Anwendung der innerstaatlichen Bestimmungen zur Umsetzung des Rahmenbeschlusses in den Mitgliedstaaten überwachen. Auf Ebene der EU wird eine Gruppe für den Schutz von Personen bei der Verarbeitung personenbezogener Daten zum Zwecke der Verhütung, Aufdeckung, Untersuchung und Verfolgung von schweren Straftaten eingesetzt. Die Gruppe besteht aus einem Vertreter aller von den Mitgliedstaaten bestimmten Kontrollstellen und einem Vertreter des Europäischen Datenschutzbeauftragten sowie einem Vertreter der Kommission. Sie prüft alle Fragen im Zusammenhang mit der Anwendung der innerstaatlichen Vorschriften zur Umsetzung dieses Rahmenbeschlusses, um auf eine einheitliche Anwendung hinzuwirken. Sie gibt eine Stellungnahme zum Datenschutzniveau in den Mitgliedstaaten und in Drittländern ab und berät die Kommission und die Mitgliedstaaten zu jeder Vorlage zur Änderung des Rahmenbeschlusses sowie zu zusätzlichen oder spezifischen Maßnahmen zum Schutz von Grundrechten.

In Artikel 16 des Rahmenbeschlusses ist zudem vorgesehen, dass die Kommission bei der Bewertung des Datenschutzniveaus in einem Drittland gegebenenfalls von einem Ausschuss unterstützt wird, der sich aus Vertretern der Mitgliedstaaten zusammensetzt und in dem der Vertreter der Kommission den Vorsitz führt

*5.1.2. Maßnahmen im Zusammenhang mit der **Ex-ante**-Bewertung*

Vertreter der Regierungen, der unabhängigen Kontrollstellen der Mitgliedstaaten, der Kontrollstellen Islands, Norwegens und der Schweiz, des Europäischen Datenschutzbeauftragten, von Europol und Eurojust wurden gehört. Unter Berücksichtigung der einzelnen Stellungnahmen schlägt die Kommission vor, die genannte Gruppe einzusetzen. Bei der Veranschlagung der möglichen Kosten dieser Maßnahme stützte sich die Kommission auf die Kosten (Reisekosten, Sekretariatsunterstützungen für die Vorbereitung und Organisation der Sitzungen), die der nach Artikel 29 der Richtlinie 95/46/EG eingesetzten Gruppe entstehen.

5.2. Geplante Einzelmaßnahmen und Modalitäten der Intervention zu Lasten des Gemeinschaftshaushalts

Die genannte Gruppe wird voraussichtlich etwa fünf Mal im Jahr zusammenkommen. Der in Artikel 16 genannte Ausschuss wird tagen, wenn dies nötig ist und sooft dies erforderlich ist, möglicherweise auch fünf Mal pro Jahr. Die Kosten der Teilnahme eines Vertreters aus jedem Mitgliedstaat und aus den Schengen-Staaten (Island, Norwegen) sind zu erstatten. Die Tätigkeit der Gruppe wird sich an der der Gruppen orientieren, die nach Artikel 29 und 31 der Richtlinie 95/46/EG des Europäischen Parlaments und des Rates vom 24. Oktober 1995 zum

Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr eingesetzt wurden.

5.3. Durchführungsmodalitäten

Veranstalter und Gastgeber aller Treffen wird die Kommission sein. Sie übernimmt die Sekretariatsarbeiten für die Gruppe und den Ausschuss, bereitet die Sitzungen vor und führt sie durch.

6. FINANZIELLE AUSWIRKUNGEN

6.1. Finanzielle Gesamtbelastung für Teil B des Haushalts (während des gesamten Planungszeitraums)

6.1.1. Finanzielle Intervention

entfällt

6.1.2. Technische und administrative Hilfe, Unterstützungsausgaben und IT-Ausgaben (Verpflichtungsermächtigungen)

entfällt

6.2. Berechnung der Kosten für jede zu Lasten von Teil B vorgesehene Einzelaktion (während des gesamten Planungszeitraums)

entfällt

7. AUSWIRKUNGEN AUF PERSONAL- UND VERWALTUNGSAUSGABEN

Der Bedarf an Human- und Verwaltungsressourcen wird aus den Mitteln der zuständigen Generaldirektion im Rahmen der jährlichen Mittelzuweisung gedeckt.

Die Zuteilung von Planstellen hängt auch von der Verteilung von Aufgaben und Mitteln im Rahmen der Finanziellen Vorausschau 2007-2013 ab.

7.1. Auswirkungen im Bereich der Humanressourcen

Art der Stellen		Zur Durchführung der Maßnahme einzusetzendes Personal: vorhandene und/oder zusätzliche Mitarbeiter		Gesamt	Beschreibung der Aufgaben, die im Zuge der vorgeschlagenen Maßnahme auszuführen sind
		Zahl der Dauerplanstellen	Zahl der Planstellen auf Zeit		
Beamte oder Bedienstete auf Zeit	A B C	0,25 A 0,50 B 1,00 C		0,25A 0,50B 1,00C	Sekretariatsunterstützung, Vorbereitung der Sitzungen der Gruppe und des Ausschusses
Sonstiges Personal					

Gesamt				

7.2. Gesamtkosten für zusätzliches Personal

Art des Personals	Beträge (in EUR)	Berechnungsmethode*
Beamte Bedienstete auf Zeit	1. Jahr: 189. 000	1 X 108 000 0,5 X 108 000 0,25 X 108.000 = 189 .000
Sonstiges Personal (Angabe der Haushaltslinie)		
Gesamt	189.000	

Anzugeben sind jeweils die Beträge, die den Gesamtausgaben für 12 Monate entsprechen.

7.3. Sonstige Verwaltungsausgaben im Zusammenhang mit der Maßnahme

Haushaltslinie (Nummer und Bezeichnung)	Betrag in €	Berechnungsweise
Gesamtmittelausstattung (Titel A-7) A0701 - Dienstreisen A-7030 - Sitzungen A07031 - Obligatorische Ausschüsse A07032 - Nichtobligatorische Ausschüsse A07040 - Konferenzen A0705 - Untersuchungen und Konsultationen Sonstige Ausgaben (im Einzelnen anzugeben)	200.000	10 Sitzungen * 27 * 740€
Informationssysteme (A-5001/A-4300)		
Andere Ausgaben - Teil A (im Einzelnen anzugeben)		
Gesamt	200.000	

Anzugeben sind jeweils die Beträge, die den Gesamtausgaben für 12 Monate entsprechen.

Angabe des jeweiligen Ausschusses sowie der Gruppe, der dieser angehört.

I.	Jährlicher Gesamtbetrag (7.2. + 7.3.)	€389.000
II.	Dauer der Maßnahme	
III.	Beurteilung der Anmeldung	Gesamtaufwand

für die Maßnahme (I x II)

8. BEGLEITUNG UND BEWERTUNG

8.1. Überwachung

Die Gruppe und der Ausschuss geben sich eine Geschäftsordnung und legen darin auch Geheimhaltungsbestimmungen fest. Das Europäische Parlament wird entsprechend den Bestimmungen des Artikels 7 des Beschlusses 99/468/EG des Rates vom 28. Juni 1999 zur Festlegung der Modalitäten für die Ausübung der der Kommission übertragenen Durchführungsbefugnisse unterrichtet (ABl. L 184 vom 17.7.1999, S. 23).

8.2. Modalitäten und Periodizität der vorgesehenen Bewertung

entfällt

9. BETRUGSBEKÄMPFUNGSMASSNAHMEN

entfällt

XXX