

I

(Mitteilungen)

EUROPÄISCHER DATENSCHUTZBEAUFTRAGTER

Stellungnahme des Europäischen Datenschutzbeauftragten zu dem Vorschlag 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 (KOM(2005) 438 endg.)

(2005/C 298/01)

DER EUROPÄISCHE DATENSCHUTZBEAUFTRAGTE —

gestützt auf den Vertrag zur Gründung der Europäischen Gemeinschaft, insbesondere auf Artikel 286,

gestützt auf die Charta der Grundrechte der Europäischen Union, insbesondere auf Artikel 8,

gestützt auf 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 ⁽¹⁾ und auf die 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) ⁽²⁾,gestützt auf die 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 ⁽³⁾, insbesondere auf Artikel 41,

gestützt auf das am 23. September 2005 eingegangene Ersuchen der Kommission um Stellungnahme nach Artikel 28 Absatz 2 der Verordnung (EG) Nr. 45/2001 —

HAT FOLGENDE STELLUNGNAHME ANGENOMMEN:

I. Einleitung

1. Der Europäische Datenschutzbeauftragte (European Data Protection Supervisor, im Folgenden EDPS genannt) begrüßt es, dass er nach Artikel 28 Absatz 2 der Verordnung (EG) Nr. 45/2001 konsultiert wird. Da es sich bei Artikel 28 Absatz 2 der Verordnung (EG) Nr. 45/2001 um eine

zwingende Vorschrift handelt, sollte die vorliegende Stellungnahme jedoch in der Präambel der Richtlinie erwähnt werden.

2. Der EDPS sieht ein, dass die Strafverfolgungsbehörden der Mitgliedstaaten insbesondere zur Bekämpfung von Terrorismus und anderen schweren Straftaten über alle erforderlichen Rechtsinstrumente verfügen müssen. Die aus-

⁽¹⁾ ABl. L 281 vom 23.11.1995, S. 31.

⁽²⁾ ABl. L 201 vom 31.7.2002, S. 37.

⁽³⁾ ABl. L 8 vom 12.1.2001, S. 1.

reichende Verfügbarkeit bestimmter Verkehrs- und Standortdaten öffentlicher elektronischer Dienste kann für diese Strafverfolgungsbehörden ein Instrument von zentraler Bedeutung sein und zur physischen Sicherheit von Personen beitragen. Es ist allerdings darauf hinzuweisen, dass dies nicht die Notwendigkeit der im gegenwärtigen Vorschlag vorgesehenen neuen Instrumente stillschweigend impliziert.

3. Es ist offensichtlich, dass der Vorschlag erhebliche Auswirkungen auf den Schutz personenbezogener Daten hat. Betrachtet man den Vorschlag ausschließlich aus der Sicht des Datenschutzes, so sollten Verkehrs- und Standortdaten überhaupt nicht zum Zwecke der Strafverfolgung auf Vorrat gespeichert werden. In der Richtlinie 2002/58/EG wurde gerade aus Datenschutzgründen als Rechtsgrundsatz verankert, dass Verkehrsdaten gelöscht werden müssen, sobald die Speicherung nicht mehr für Zwecke erforderlich ist, die mit der Kommunikation selbst zusammenhängen (einschließlich Abrechnungszwecken). Ausnahmen von diesem Rechtsgrundsatz sind strengen Bedingungen unterworfen.

4. In der vorliegenden Stellungnahme wird der EDPS aufzeigen, welche Auswirkungen der Vorschlag für den Schutz personenbezogener Daten hat. Dabei wird der EDPS auch berücksichtigen, dass der Vorschlag trotz seiner Bedeutung für die Strafverfolgung nicht dazu führen darf, dass Menschen ihr Grundrecht auf Schutz ihrer Privatsphäre entzogen wird.

5. Diese Stellungnahme des EDPS ist vor dem Hintergrund dieser Überlegungen zu sehen. Der EDPS strebt einen ausgewogenen Ansatz an, bei dem die Notwendigkeit und die Verhältnismäßigkeit des Eingriffs in den Datenschutz eine zentrale Rolle spielen.

6. Was den Vorschlag selbst betrifft, so ist er als eine Reaktion auf die Initiative der Französischen Republik, Irlands, des Königreichs Schweden und des Vereinigten Königreichs für einen Rahmenbeschluss über die Vorratsspeicherung von Daten, die in Verbindung mit der Bereitstellung öffentlicher elektronischer Kommunikationsdienste verarbeitet und aufbewahrt werden, oder von Daten, die in öffentlichen Kommunikationsnetzen vorhanden sind, für die Zwecke der Vorbeugung, Ermittlung, Aufdeckung und Verfolgung von Straftaten einschließlich Terrorismus (nachstehend „Entwurf eines Rahmenbeschlusses“ genannt) zu sehen, der vom Europäischen Parlament (im Rahmen des Konsultationsverfahrens) abgelehnt worden ist.

7. Der EDPS ist zu dem Entwurf eines Rahmenbeschlusses weder konsultiert worden, noch hat er auf eigene Initiative eine Stellungnahme zu dem Entwurf abgegeben. Es ist auch nicht seine Absicht, jetzt eine Stellungnahme zu diesem Entwurf abzugeben — er wird jedoch in der vorliegenden

Stellungnahme auf diesen Entwurf Bezug nehmen, wenn ihm dies sinnvoll erscheint.

II. Allgemeine Bemerkungen

Die Auswirkungen des Vorschlags für den Datenschutz

8. Für den EDPS ist es von größter Bedeutung, dass in dem Vorschlag die Grundrechte gewahrt bleiben. Eine Legislativmaßnahme, durch die der Schutz beeinträchtigt würde, der durch das Gemeinschaftsrecht und insbesondere die Rechtsprechung des Gerichtshofs und des Europäischen Gerichtshofs für Menschenrechte gewährleistet ist, wäre nicht nur unannehmbar, sondern auch illegal. Die gesellschaftlichen Bedingungen können sich aufgrund von Terroranschlägen durchaus geändert haben, dies darf aber nicht dazu führen, dass die hohen Schutzstandards im derzeitigen Recht beeinträchtigt werden. Der Schutz ist durch das Recht gewährleistet, ungeachtet der aktuellen Erfordernisse der Strafverfolgung. Überdies lässt die Rechtsprechung selbst auch Ausnahmen zu, sofern diese in einer demokratischen Gesellschaft erforderlich sind.

9. Der Vorschlag hat direkte Auswirkungen für den durch Artikel 8 der Europäischen Konvention zum Schutze der Menschenrechte und Grundfreiheiten („EMRK“) gewährten Schutz. In der ständigen Rechtsprechung des Europäischen Gerichtshofs für Menschenrechte wurde Folgendes festgestellt:

- Die Speicherung von Informationen über eine Einzelperson wurde als Eingriff in das Privatleben erachtet, auch wenn diese Informationen keine sensitiven Daten enthielten (Amann ⁽¹⁾).
- Das Gleiche gilt für die Praxis der Telefongesprächserfassung, bei der ein Gerät benutzt wird, das automatisch die auf einem Telefon gewählte Nummer sowie den Zeitpunkt und die Dauer jedes einzelnen Gesprächs aufzeichnet (Malone ⁽²⁾).
- Die Gründe für den Eingriff sollten schwerer wiegen als die nachteilige Wirkung, die allein die Existenz der fraglichen Rechtsbestimmung für die betroffenen Personen haben könnte (Dudgeon ⁽³⁾).

10. Artikel 6 Absatz 2 des EU-Vertrags sieht vor, dass die Union die in der EMRK verankerten Grundrechte achtet. In der vorstehenden Nummer wurde aufgezeigt, dass die Verpflichtung zur Vorratsspeicherung von Daten nach der Rechtsprechung des Europäischen Menschenrechtsgerichtshofs in den Geltungsbereich von Artikel 8 EMRK fällt, und dass es dafür einer sehr triftigen Begründung bedarf, die das Kriterium

⁽¹⁾ Urteil des EGMR vom 16. Februar 2000 in der Rechtssache Amann, 2000-II, Nr. 27798/95.

⁽²⁾ Urteil des EGMR vom 2. August 1984 in der Rechtssache Malone, A82, Nr. 8691/79.

⁽³⁾ Urteil des EGMR vom 22. Oktober 1981 in der Rechtssache Dudgeon, A45, Nr. 7525.

des Dudgeon-Urteils erfüllt. Die Notwendigkeit und die Verhältnismäßigkeit der Verpflichtung zur Vorratsspeicherung von Daten — mit ihrer ganzen Tragweite — muss nachgewiesen werden.

11. Überdies hat der Vorschlag erhebliche Auswirkungen auf die im Gemeinschaftsrecht verankerten Grundsätze des Datenschutzes:

- Die Daten müssen über einen Zeitraum auf Vorrat gespeichert werden, der viel länger ist als die Zeiträume, die für die Vorratsspeicherung durch Anbieter öffentlich zugänglicher elektronischer Kommunikationsdienste oder Betreiber eines öffentlichen Kommunikationsnetzes (für beide Dienste wird im Folgenden der Begriff „Betreiber“ benutzt) üblich sind.
- Nach der Richtlinie 2002/58/EG, insbesondere nach Artikel 6, dürfen Daten nur aus Gründen erhoben und gespeichert werden, die in direkter Beziehung zu der Nachricht selbst stehen, einschließlich zu Abrechnungszwecken⁽¹⁾. Danach sind die Daten zu löschen (außer in Ausnahmefällen). Nach dem gegenwärtigen Vorschlag ist die Vorratsspeicherung zum Zwecke der Strafverfolgung Pflicht. Die Ausgangspositionen stehen somit im Widerspruch zueinander.
- Die Richtlinie 2002/58/EG gewährleistet die Sicherheit und die Vertraulichkeit. Der vorliegende Vorschlag darf nicht zu Gesetzeslücken auf diesem Gebiet führen; strenge Schutzmechanismen sind erforderlich, und der Zweck sollte deutlich eingegrenzt werden.
- Die Einführung einer Pflicht zur Vorratsspeicherung von Daten, wie sie im Vorschlag vorgesehen ist, führt zu umfangreichen Datenbanken und birgt für den Betroffenen besondere Risiken. So könnten die Daten beispielsweise gewerblich genutzt oder von den Strafverfolgungsbehörden und von den nationalen Sicherheitsdiensten zu Ausforschungszwecken und/oder für Data Mining benutzt werden.

12. Außerdem wurden sowohl der Schutz des Privatlebens als auch der Schutz personenbezogener Daten in der Grundrechtecharta anerkannt, wie in der Begründung des Vorschlags angeführt wird.

13. Die Auswirkungen des Vorschlags für den Schutz personenbezogener Daten müssen gründlich untersucht werden. Bei dieser Untersuchung wird der EDPS die oben genannten Aspekte berücksichtigen und zu dem Schluss kommen, dass mehr Schutzmechanismen erforderlich sind. Ein einfacher Verweis auf den geltenden Rechtsrahmen zum Datenschutz (insbesondere die Richtlinien 95/46/EG und 2002/58/EG) ist nicht ausreichend.

Die Notwendigkeit, Verkehrs- und Standortdaten auf Vorrat zu speichern

14. Der EDPS erinnert an die Schlussfolgerung der Datenschutzgruppe „Artikel 29“ vom 9. November 2004 zu dem Entwurf eines Rahmenbeschlusses. Die Gruppe stellte fest, dass die verbindlich vorgeschriebene Vorratsspeicherung von Verkehrsdaten unter den in dem Entwurf eines Rahmenbeschlusses vorgesehenen Bedingungen nicht annehmbar ist. Die Schlussfolgerung ergab sich unter anderem daraus, dass kein Beweis dafür erbracht wurde, dass die Vorratsspeicherung zu Zwecken der öffentlichen Ordnung erforderlich ist, da eine entsprechende Analyse ergab, dass die von den Strafverfolgungsbehörden nachgefragten Daten größtenteils nicht älter als sechs Monate waren.

15. Nach Auffassung des EDPS sollten die oben dargestellten Überlegungen der Datenschutzgruppe den Ausgangspunkt für die Beurteilung des vorliegenden Vorschlags darstellen. Allerdings kann das Ergebnis dieser Überlegungen nicht einfach auf den vorliegenden Vorschlag übertragen werden. Es ist zu berücksichtigen, dass sich die Umstände ändern können. Nach Ansicht des EDPS könnten die nachstehenden Entwicklungen für die Beurteilung von Relevanz sein.

16. Erstens wurden einige Zahlen vorgelegt, um nachzuweisen, dass die Strafverfolgungsbehörden in der Praxis um Verkehrsdaten ersuchen, die bis zu einem Jahr alt sind. Sowohl die Kommission als auch der Vorsitz des Rates messen einer Studie der Polizei des Vereinigten Königreichs⁽²⁾ Bedeutung bei, aus der hervorgeht, dass zwar 85 % der von der Polizei benötigten Verkehrsdaten weniger als 6 Monate alt waren, dass aber bei komplexen Untersuchungen zu schwereren Straftaten zwischen 6 und 12 Monate alte Daten verwendet wurden. Es wurden auch einige Beispiele für solche Fälle gegeben. Die Speicherungsfrist im Vorschlag — für Telefondaten ein Jahr — spiegelt diese Praxis der Strafverfolgungsbehörden wider.

17. Der EDPS ist nicht davon überzeugt, dass diese Zahlen den Beweis dafür erbringen, dass die Vorratsspeicherung von Verkehrsdaten für bis zu einem Jahr erforderlich ist. Die Tatsache, dass die Verfügbarkeit von Verkehrs- und/oder Standortdaten in einigen Fällen zur Aufklärung eines Verbrechens beigetragen hat, bedeutet nicht zwangsläufig, dass diese Daten (generell) als Instrument für die Strafverfolgung benötigt werden. Die Zahlen dürfen allerdings auch nicht ignoriert werden. Sie stellen zumindest den ernsthaften Versuch dar, nachzuweisen, dass die Vorratsspeicherung erforderlich ist. Außerdem zeigen die Zahlen deutlich, dass aus Sicht der gegenwärtigen Strafverfolgungspraxis kein Bedarf an einer Speicherungsfrist von mehr als einem Jahr besteht.

18. Zweitens wird die nach der Richtlinie 2002/58/EG für die Betreiber bestehende Möglichkeit, Verkehrsdaten zu Abrechnungszwecken auf Vorrat zu speichern, nicht immer genutzt, da in einer immer größeren Zahl von Fällen gar keine Datenspeicherung zu Abrechnungszwecken mehr erfolgt (Prepaid-Karten für Mobiltelefone, Pauschaltarife usw.). In

⁽¹⁾ Siehe auch Nr. 3 dieser Stellungnahme.

⁽²⁾ „Liberty and security, striking the right balance“. Dokument des britischen Vorsitzes der Europäischen Union vom 7. September 2005.

diesen Fällen — die in der Praxis häufiger geworden sind — werden Verkehrs- und Standortdaten gar nicht gespeichert, sondern sofort nach der Kommunikation gelöscht. Dasselbe gilt für erfolglose Anrufversuche. Dies wirkt sich möglicherweise auf die Effizienz der Strafverfolgung aus.

19. Diese Entwicklung bei den Telekommunikationsdiensten kann außerdem zu Störungen des Funktionierens des Binnenmarktes führen, unter anderem aufgrund der (bevorstehenden) Annahme von Legislativmaßnahmen nach Artikel 15 der Richtlinie 2002/58/EG in den Mitgliedstaaten. So hat z. B. die italienische Regierung vor kurzem eine Verordnung veröffentlicht, die die Betreiber verpflichtet, Telefondaten vier Jahre lang zu speichern. Diese Verpflichtung wird in bestimmten Mitgliedstaaten, wie Italien, zu erheblichen Kosten führen.

20. Drittens haben sich auch die Arbeitsmethoden der Strafverfolgungsbehörden weiterentwickelt: Proaktive Ermittlungen und der Einsatz technischer Hilfsmittel sind wichtiger geworden. Die Entwicklungen führen dazu, dass die Behörden über angemessene und genau umrissene Instrumente verfügen müssen, um ihre Arbeit unter gebührender Achtung der Datenschutzgrundsätze verrichten zu können. Ein Instrument, über das die Behörden in den Mitgliedstaaten gewöhnlich verfügen, ist die Sicherungsspeicherung von Daten bzw. die Aufbewahrung von Kommunikationsdaten auf Verlangen im Rahmen einer konkreten Ermittlung. Es wurde festgestellt, dass dieses Instrument, das geringere Auswirkungen auf die Datenschutzgrundsätze als das nun vorgeschlagene Instrument (Vorratsspeicherung von Daten) hat, nicht immer ausreichend sein könnte, insbesondere, wenn es darum geht, Personen aufzuspüren, die in Terrorismus oder andere schwere Straftaten verwickelt sind und zuvor keiner kriminellen Aktivität verdächtigt wurden. Es sind jedoch mehr Beweise erforderlich, um festzustellen, ob dies tatsächlich zutrifft.

21. Viertens ist die Sorge in Bezug auf Terroranschläge gewachsen. Der EDPS teilt die im Zusammenhang mit den Vorschlägen zur Vorratsspeicherung von Daten geäußerte Ansicht, dass die physische Sicherheit an sich von allergrößter Bedeutung ist. Gesellschaften bedürfen des Schutzes. Aus diesem Grund sind die Regierungen im Falle eines Angriffs auf die Gesellschaft verpflichtet, unter Beweis zu stellen, dass sie dieses Schutzbedürfnis ernst nehmen, und auszuforschen, ob sie mit der Einführung neuer Legislativmaßnahmen reagieren müssen. Selbstverständlich unterstützt der EDPS in vollem Umfang die Aufgabe der Regierungen — sowohl auf nationaler als auch auf europäischer Ebene —, die Gesellschaft zu schützen und unter Beweis zu stellen, dass sie alles Notwendige unternehmen, um Schutz zu bieten, einschließlich der Annahme neuer, rechtmäßiger und effizienter Maßnahmen als Ergebnis ihrer Nachforschungen.

22. Der EDPS erkennt zwar an, dass sich die Umstände verändert haben, ist aber trotzdem noch nicht davon überzeugt, dass eine Vorratsspeicherung von Verkehrs- und Standortdaten zu Strafverfolgungszwecken, wie sie in dem Vorschlag vorgesehen ist, erforderlich ist. Er betont die Bedeutung des in der Richtlinie 2002/58/EG verankerten Rechtsgrundsatzes, wonach Verkehrsdaten gelöscht werden müssen, sobald die Speicherung nicht mehr für Zwecke

erforderlich ist, die mit der Kommunikation selbst zusammenhängen. Außerdem belegen die vorgelegten Zahlen weder, dass der bestehende Rechtsrahmen nicht die für den Schutz der physischen Sicherheit erforderlichen Instrumente bietet, noch, dass die Mitgliedstaaten ihre Befugnisse nach europäischem Recht in vollem Umfang ausüben, um zusammenzuarbeiten, wie es ihnen der bestehende Rechtsrahmen gestattet (ohne dass dies die erforderlichen Ergebnisse erbringen würde).

23. Wenn aber das Europäische Parlament und der Rat — nach sorgfältiger Abwägung der Interessen, die auf dem Spiel stehen — zu dem Schluss kommen, dass die Notwendigkeit der Vorratsspeicherung von Verkehrs- und Standortdaten ausreichend nachgewiesen ist, so lässt sich die Vorratsspeicherung nach Auffassung des EDPS nach dem Gemeinschaftsrecht nur dann rechtfertigen, wenn, wie in dieser Stellungnahme dargelegt, der Grundsatz der Verhältnismäßigkeit gewahrt bleibt und für angemessene Schutzmechanismen gesorgt wird.

Verhältnismäßigkeit

24. Die Verhältnismäßigkeit der vorgeschlagenen neuen Legislativmaßnahme hängt vom Inhalt ihrer Bestimmungen ab: Stellt die Maßnahme eine geeignete und angemessene Reaktion auf die Bedürfnisse der Gesellschaft dar?

25. Die erste Überlegung betrifft die Geeignetheit des Vorschlags: Kann davon ausgegangen werden, dass der Vorschlag die physische Sicherheit der Bewohner der Europäischen Union erhöht? Ein häufig in der öffentlichen Diskussion genannter Grund, die Geeignetheit zu bezweifeln, ist, dass Verkehrs- und Standortdaten nicht immer mit einer bestimmten Person in Verbindung stehen; die Kenntnis einer Telefonnummer (oder einer Internet-Protokoll-Adresse) führt nicht zwangsläufig zur Identifizierung einer Person. Ein anderer — und schwerwiegenderer — Grund für Zweifel liegt in der Frage, ob riesige Datenbanken die Strafverfolgungsbehörden tatsächlich in die Lage versetzen, leicht zu finden, was sie in einem ganz bestimmten Fall suchen.

26. Der EDPS ist der Ansicht, dass die Vorratsspeicherung von Verkehrs- und Standortdaten allein keine geeignete oder wirksame Reaktion darstellt. Es sind zusätzliche Maßnahmen erforderlich, um sicherzustellen, dass die Behörden zielsicher und schnell auf die in einem ganz bestimmten Fall benötigten Daten zugreifen können. Die Vorratsspeicherung von Daten ist nur dann geeignet und wirksam, wenn es auch effiziente Suchmaschinen gibt.

27. Die zweite Überlegung betrifft die Angemessenheit der Reaktion. Damit der Vorschlag angemessen ist,

— sollten die Speicherungsfristen im Vorschlag begrenzt werden. Diese Fristen müssen den nachgewiesenen Erfordernissen der Strafverfolgungsbehörden entsprechen;

— sollte die Anzahl der zu speichernden Daten im Vorschlag begrenzt werden. Diese Anzahl muss den nachgewiesenen Erfordernissen der Strafverfolgungsbehörden entsprechen, und es muss sichergestellt werden, dass kein Zugang zu Inhaltsdaten möglich ist;

— sollten im Vorschlag geeignete Schutzmechanismen enthalten werden, so dass der Zugang und die Weiterverwendung begrenzt werden, die Sicherheit der Daten gewährleistet ist und sichergestellt wird, dass die Betroffenen selbst ihre Rechte ausüben können.

28. Der EDPS hebt hervor, wie wichtig diese strengen Begrenzungen mit geeigneten Schutzmechanismen zur Beschränkung des Zugangs sind. Er ist der Ansicht, dass die Mitgliedstaaten angesichts der Bedeutung der unter der vorstehenden Nummer genannten drei Punkte keine zusätzlichen nationalen Maßnahmen in Bezug auf diese drei Punkte ergreifen dürfen, die die Verhältnismäßigkeit berühren. Diese Notwendigkeit der Harmonisierung wird in Abschnitt IV eingehender behandelt.

Geeignete Sicherheitsmaßnahmen

29. Der Vorschlag führt dazu, dass die Betreiber über Datenbanken verfügen werden, in denen große Mengen von Verkehrs- und Standortdaten gespeichert sein werden.

30. Erstens muss in dem Vorschlag sichergestellt werden, dass der Zugang zu den Daten und ihre Weiterverwendung begrenzt werden und nur unter bestimmten Umständen und zu einer eingeschränkten Zahl konkreter Zwecke erfolgen dürfen.

31. Zweitens müssen die Datenbanken ausreichend geschützt werden (Datensicherheit). Zu diesem Zweck ist sicherzustellen, dass die Daten nach Ablauf der Speicherungsfristen effizient gelöscht werden. Es sollte keine „wilde Entsorgung von Daten“ und keine Auswertung der Daten geben. Kurz gesagt bedarf es dazu einer hohen Datensicherheit und geeigneter technischer und organisatorischer Sicherheitsmaßnahmen.

32. Eine hohe Datensicherheit ist umso wichtiger, als das bloße Vorhandensein der Daten zu Ersuchen von mindestens drei interessierten Gruppen um Zugang und Verwendung führen könnte:

- die Betreiber selbst. Sie könnten versucht sein, die Daten für ihre eigenen kommerziellen Zwecke zu nutzen. Es sind Sicherheitsmechanismen erforderlich, mit denen das Kopieren der betreffenden Dateien verhindert wird;
- die für die Strafverfolgung zuständigen Behörden: Der Vorschlag gibt ihnen ein Zugangsrecht, aber nur in ganz bestimmten Fällen und nach Maßgabe der nationalen Rechtsvorschriften (Artikel 3 Absatz 2 des Vorschlags). Es sollte keinen Zugang für Data Mining oder zu Ausforschungszwecken geben. Der Austausch von Daten mit Behörden in anderen Mitgliedstaaten sollte klar geregelt werden;
- Nachrichtendienste (mit Zuständigkeit für die nationale Sicherheit).

33. Was den Zugang von Nachrichtendiensten anbelangt, so weist der EDPS darauf hin, dass Maßnahmen im Rahmen der dritten und der ersten Säule nach Artikel 33 EU-Vertrag und Artikel 64 EG-Vertrag nicht die Wahrnehmung der Zuständigkeiten der Mitgliedstaaten für die Aufrechterhaltung der öffentlichen Ordnung und den Schutz der inneren Sicherheit berühren. Nach Auffassung des EDPS bedeuten diese Bestimmungen, dass die Europäische Union nicht befugt ist, den Zugang von Sicherheits- oder Nachrichtendiensten zu den von den Betreibern auf Vorrat gespeicherten Daten zu kontrollieren. Mit anderen Worten: Das Recht der Europäischen Union berührt weder den Zugang dieser Dienste zu den Verkehrs- und Standortdaten der Betreiber noch die Weiterverwendung der von diesen Diensten eingeholten Informationen. Dies ist ein Aspekt, der bei der Beurteilung des Vorschlags zu berücksichtigen ist. Es ist Sache der Mitgliedstaaten, die erforderlichen Maßnahmen zu ergreifen, um den Zugang der Nachrichtendienste zu regeln.

34. Drittens haben die in den vorstehenden Nummern beschriebenen Wirkungen des Vorschlags potenziell Folgen für den Betroffenen. Es sind zusätzliche Schutzmechanismen erforderlich, um sicherzustellen, dass er seine Rechte als Betroffener auf einfache Weise und zügig ausüben kann. Der EDPS weist darauf hin, dass der Zugang zu den Daten und ihre Weiterverwendung wirksam kontrolliert werden müssen, vorzugsweise durch die Justizbehörden in den Mitgliedstaaten. Die Schutzmechanismen sollten auch in Bezug auf den Zugang und die Weiterverwendung der Verkehrsdaten durch Behörden in anderen Mitgliedstaaten gelten.

35. Der EDPS verweist in diesem Zusammenhang auf die Initiativen für einen neuen, den Datenschutz betreffenden Rechtsrahmen, der Anwendung auf die Strafverfolgung finden soll (in der dritten Säule des EU-Vertrags). Seines Erachtens erfordert ein solcher Rechtsrahmen zusätzliche Schutzmechanismen und darf sich nicht darauf beschränken, die allgemeinen Grundsätze des Datenschutzes in der ersten Säule zu bekräftigen. ⁽¹⁾

36. Viertens besteht eine direkte Beziehung zwischen der Geeignetheit der Sicherheitsmaßnahmen und den Kosten dieser Maßnahmen. Ein geeignetes Gesetz zur Vorratsspeicherung von Daten muss daher den Betreibern Anreize für Investitionen in die technische Infrastruktur bieten. Ein solcher Anreiz könnte darin bestehen, dass den Betreibern die zusätzlichen Kosten geeigneter Sicherheitsmaßnahmen zurückerstattet werden.

37. Fazit: Geeignete Sicherheitsmaßnahmen sollten

- den Zugang zu den Daten und ihre Weiterverwendung einschränken;
- für geeignete technische und organisatorische Sicherheitsmaßnahmen zum Schutz der Datenbanken sorgen. Dazu gehört die wirksame Löschung der Daten nach Ablauf der Speicherungsfrist und die Anerkennung der

⁽¹⁾ Siehe im gleichen Sinne das auf der Frühjahrskonferenz der Europäischen Datenschutzbehörden vom 25./26. April 2005 in Krakau angenommene Positionspapier zum Thema Strafverfolgung und Informationsaustausch in der EU.

Tatsache, dass es von Seiten verschiedener interessierter Gruppen Anfragen nach dem Zugang zu den Daten und ihrer Verwendung geben könnte;

- gewährleisten, dass die Betroffenen ihre Rechte ausüben können, und zwar nicht nur, indem die allgemeinen Grundsätze des Datenschutzes bekräftigt werden;
- Anreize für die Betreiber beinhalten, damit diese in die technische Infrastruktur investieren.

III. Die Rechtsgrundlage und der Entwurf eines Rahmenbeschlusses

38. Der Vorschlag ist auf den EG-Vertrag, insbesondere auf Artikel 95, gestützt und hat laut Artikel 1 die Harmonisierung der Pflichten der Betreiber hinsichtlich der Verarbeitung und Vorratsspeicherung von Verkehrs- und Standortdaten zum Ziel. In dem Vorschlag ist vorgesehen, dass die Daten nur in Einzelfällen im Zusammenhang mit Straftaten an die zuständigen nationalen Behörden weitergegeben werden; die genauere Definition des Zweckes sowie die Regelung des Zugangs zu den Daten und ihrer Weiterverwendung werden hingegen vorbehaltlich der Schutzmechanismen des bestehenden Gemeinschaftsrahmens zum Datenschutz in das Ermessen der Mitgliedstaaten gelegt.

39. In dieser Hinsicht hat der Vorschlag einen stärker eingegrenzten Geltungsbereich als der Entwurf eines Rahmenbeschlusses, der auf Artikel 31 Absatz 1 Buchstabe c des EU-Vertrags gestützt ist, und der zusätzliche Bestimmungen über den Zugang zu den auf Vorrat gespeicherten Daten und über Anträge auf Zugang aus anderen Mitgliedstaaten enthält. In der Begründung des Richtlinienvorschlags wird ein Grund für diese Eingrenzung des Geltungsbereichs genannt. Es wird dort festgestellt, dass Fragen des Zugangs zu den Informationen und des Austauschs zwischen den einschlägigen Strafverfolgungsbehörden nicht in den Anwendungsbereich des EG-Vertrags fallen.

40. Diese in der Begründung enthaltene Erklärung überzeugt den EDPS nicht. Eine auf Artikel 95 des EG-Vertrags (Binnenmarkt) gestützte Intervention der Gemeinschaft muss die Beseitigung von Handelshemmnissen zum Hauptziel haben. Nach der Rechtsprechung des Europäischen Gerichtshofs muss eine solche Maßnahme tatsächlich dazu geeignet sein, zur Beseitigung eines solchen Hemmnisses beizutragen. Der Europäische Gesetzgeber muss allerdings bei seiner Intervention die Grundrechte achten (Artikel 6 Absatz 2 des EU-Vertrags; siehe Abschnitt II dieser Stellungnahme). Aus diesen Gründen könnte die Einführung von Vorschriften zur Vorratsspeicherung von Daten auf Gemeinschaftsebene im Interesse des Binnenmarktes erforderlich machen, dass auch die Achtung der Grundrechte auf der Ebene der Europäischen Gemeinschaft behandelt wird. Wenn der Gemeinschaftsgesetzgeber keine Vorschriften über den Zugang zu Daten und über ihre Verwendung festlegen könnte, so könnte er seinen Pflichten nach Artikel 6 des EU-Vertrags nicht nachkommen, da die in diesem Artikel enthaltenen Vorschriften unverzichtbar sind, um sicherzustellen, dass die Vorratsspeicherung unter gebührender Achtung der Grundrechte erfolgt. Mit anderen Worten: Nach Auffassung des EDPS sind Vorschriften über den Zugang, die Verwendung und den Austausch von Daten nicht von der Pflicht zur Vorratsspeicherung der Daten zu trennen.

41. Was die Einrichtung der zuständigen Behörden anbelangt, so räumt der EDPS ein, dass dies in der Verantwortung der Mitgliedstaaten liegt. Das Gleiche gilt für die Organisation der Strafverfolgung und des gerichtlichen Schutzes. Allerdings können den Mitgliedstaaten in einem Rechtsakt der Gemeinschaft Bedingungen in Bezug auf die Benennung zuständiger Behörden, die gerichtliche Kontrolle oder den Zugang der Bürger zur Justiz auferlegt werden. Mit solchen Bestimmungen wird sichergestellt, dass auf nationaler Ebene geeignete Mechanismen vorhanden sind, die die uneingeschränkte Wirksamkeit des Rechtsakts gewährleisten, einschließlich der uneingeschränkten Einhaltung der Datenschutzvorschriften.

42. Der EDPS möchte einen weiteren Punkt im Zusammenhang mit der Rechtsgrundlage ansprechen. Es ist Sache des Europäischen Gesetzgebers, die geeignete Rechtsgrundlage und dementsprechend das geeignete Gesetzgebungsverfahren zu wählen. Diese Entscheidung geht über den Auftrag des EDPS hinaus. Angesichts der ganz wesentlichen Fragen, um die es sich hierbei handelt, spricht sich der EDPS in der gegenwärtigen Situation jedoch eindeutig für das Mitentscheidungsverfahren aus. Nur dieses Verfahren stellt ein transparentes Beschlussfassungsverfahren unter umfassender Beteiligung der drei einbezogenen Organe und unter gebührender Achtung der Grundsätze dar, auf die sich die Union gründet.

IV. Notwendigkeit der Harmonisierung

43. In dem Richtlinienvorschlag werden die Art der auf Vorrat zu speichernden Daten, die Speicherungsfristen für diese Daten sowie die Zwecke, zu denen die Daten an die zuständigen Behörden weitergegeben werden dürfen, harmonisiert. In dem Vorschlag ist eine vollständige Harmonisierung dieser Aspekte vorgesehen. In dieser Hinsicht unterscheidet sich der Richtlinienvorschlag grundlegend von dem Entwurf eines Rahmenbeschlusses, der Mindestvorschriften festlegt.

44. Der EDPS betont, dass diese Aspekte mit Blick auf das Funktionieren des Binnenmarktes, die Erfordernisse der Strafverfolgung und — nicht zuletzt — die EMRK und die Grundsätze des Datenschutzes uneingeschränkt harmonisiert werden müssen.

45. Was das Funktionieren des Binnenmarktes anbelangt, so begründet die Harmonisierung der Pflicht zur Vorratsspeicherung der Daten die Wahl der Rechtsgrundlage des Vorschlags (Artikel 95 des EG-Vertrags). Die vorhandenen Störungen im Binnenmarkt für elektronische Kommunikation, die unter anderem durch die (unmittelbar bevorstehende) Verabschiedung von Legislativmaßnahmen nach Artikel 15 der Richtlinie 2002/58/EG in den Mitgliedstaaten verursacht werden (siehe Nr. 19 dieser Stellungnahme), werden nicht ausgeräumt, wenn zugelassen wird, dass sich die Rechtsvorschriften der Mitgliedstaaten wesentlich unterscheiden.

46. Dies ist umso wichtiger, als für einen großen Teil der elektronischen Kommunikation die Zuständigkeit von mehr als einem Mitgliedstaat relevant ist. Beispiele dafür sind: grenzüberschreitende Telefongespräche, Roaming, Grenzüberschreitung während einer Mobilfunkkommunikation und der Rückgriff auf einen Betreiber in einem anderem Mitgliedstaat als dem, in dem die betreffende Person ihren Wohnsitz hat.

47. Überdies würde in diesem Zusammenhang eine mangelnde Harmonisierung den Erfordernissen der Strafverfolgung zuwiderlaufen, da die zuständigen Behörden unterschiedliche Rechtsvorschriften einhalten müssen. Dies könnte den Informationsaustausch zwischen den Behörden der Mitgliedstaaten behindern.

48. Schließlich hebt der EDPS — unter Verweis auf seine Verantwortung nach Artikel 41 der Verordnung (EG) Nr. 45/2001 — hervor, dass eine vollständige Harmonisierung der wichtigsten im Vorschlag enthaltenen Aspekte unbedingt erforderlich ist, um der EMRK und den Grundsätzen des Datenschutzes zu entsprechen. Wenn eine Legislativmaßnahme, die zur Vorratsspeicherung von Verkehrs- und Standortdaten verpflichtet, aus Sicht des Datenschutzes annehmbar sein und den Vorgaben der Notwendigkeit und Verhältnismäßigkeit entsprechen soll, müssen in dieser Maßnahme die Anzahl der auf Vorrat zu speichernden Daten, die Speicherungsfristen und der (Zweck des) Zugang(s) zu den Daten und ihre(r) Weiterverwendung eindeutig begrenzt werden.

V. Bemerkungen zu den Artikeln des Vorschlags

Artikel 3: Vorratsspeicherungspflicht

49. Artikel 3 ist die zentrale Bestimmung des Vorschlags. Mit Artikel 3 Absatz 1 wird die Pflicht zur Vorratsspeicherung von Verkehrs- und Standortdaten eingeführt, während Artikel 3 Absatz 2 dem Grundsatz der Zweckbindung Wirkung verleiht. In Artikel 3 Absatz 2 sind drei wichtige Begrenzungen vorgesehen. Die auf Vorrat gespeicherten Daten werden nur

- an die zuständigen nationalen Behörden,
- in ganz bestimmten Fällen,
- zum Zwecke der Vorbeugung, Ermittlung, Aufdeckung und Verfolgung von schweren Straftaten wie Terrorismus und organisierter Kriminalität

weitergegeben. In Artikel 3 Absatz 2 wird, was die Festlegung weiterer Einschränkungen anbelangt, auf die nationalen Rechtsvorschriften der Mitgliedstaaten verwiesen.

50. Der EDPS begrüßt Artikel 3 Absatz 2 als eine wichtige Bestimmung, ist jedoch der Ansicht, dass die Begrenzungen nicht präzise genug sind, dass der Zugang zu den Daten und ihre Weiterverwendung im Rahmen dieser Richtlinie explizit geregelt werden sollten, und dass zusätzliche Schutzmechanismen erforderlich sind. Wie bereits in Abschnitt III dieser Stellungnahme dargelegt, ist der EDPS nicht davon überzeugt, dass die Nichtaufnahme (präziser) Bestimmungen über den Zugang zu den Verkehrs- und Standortdaten und über ihre Weiterverwendung eine unvermeidliche Folge der Rechtsgrundlage des Vorschlags (Artikel 95) ist. Dies gibt Anlass zu den nachstehenden Bemerkungen.

51. Erstens: Es wird nicht präzise festgelegt, dass andere Interessengruppen, wie etwa der Betreiber selbst, keinen

Zugang zu den Daten haben. Nach Artikel 6 der Richtlinie 2002/58/EG dürfen die Betreiber Verkehrsdaten nur bis zum Ende des Zeitraums verarbeiten, während dessen die Daten zu Abrechnungszwecken auf Vorrat gespeichert werden. Nach Auffassung des EDPS gibt es außer dem in der Richtlinie 2002/58/EG vorgesehenen Zugang, der den Bedingungen dieser Richtlinie unterliegt, keinen anderen gerechtfertigten Zugang des Betreibers oder sonstiger Interessierter zu den Daten.

52. Der EDPS empfiehlt, dem Text eine Bestimmung hinzuzufügen, um sicherzustellen, dass niemand anders als die zuständigen Behörden Zugang zu den Daten hat. Diese Bestimmung könnte folgendermaßen formuliert sein: „Der Zugang zu den Daten und/oder ihre Verarbeitung ist nur zu dem in Artikel 3 Absatz 2 genannten Zweck gestattet“ oder „die Betreiber gewährleisten, dass nur den zuständigen Behörden Zugang zu den Daten gewährt wird“.

53. Zweitens: Die Begrenzung auf ganz bestimmte Fälle scheint einen routinemäßigen Zugang zu Ausforschungszwecken oder für Data-Mining-Aktivitäten zu verbieten. Es sollte aber trotzdem in dem Text präzisiert werden, dass die Daten nur dann zur Verfügung gestellt werden können, wenn dies im Zusammenhang mit einer spezifischen Straftat erforderlich ist.

54. Drittens: Der EDPS begrüßt es, dass der Zweck des Zugangs auf schwere Straftaten wie Terrorismus und organisierte Kriminalität begrenzt ist. In weniger schweren Fällen dürfte ein Zugang zu Verkehrs- und Standortdaten nicht so leicht angemessen sein. Der EDPS bezweifelt jedoch, dass diese Begrenzung präzise genug ist, insbesondere, wenn im Zusammenhang mit anderen schweren Straftaten als Terrorismus und organisierte Kriminalität um Zugang ersucht wird. Die Praxis in den Mitgliedstaaten wird unterschiedlich aussehen. Der EDPS hat in Abschnitt IV dieser Stellungnahme betont, dass die wesentlichen in diesem Vorschlag enthaltenen Aspekte vollständig harmonisiert werden müssen. Daher empfiehlt der EDPS, die Bestimmung auf bestimmte schwere Straftaten einzuschränken.

55. Viertens: Im Gegensatz zum Entwurf eines Rahmenbeschlusses enthält der Vorschlag keine Bestimmung über den Zugang zu den Daten. Nach Auffassung des EDPS sollten der Zugang zu den Daten und ihre Weiterverwendung im Vorschlag nicht ignoriert werden. Sie sind fester Bestandteil des Gegenstands (siehe Abschnitt III dieser Stellungnahme).

56. Der EDPS empfiehlt, dem Vorschlag einen oder mehrere Artikel über den Zugang der zuständigen Behörden zu den Standort- und Verkehrsdaten und über die Weiterverwendung der Daten hinzuzufügen. Mit diesen Artikeln sollte sichergestellt werden, dass die Daten zu den in Artikel 3 Absatz 2 genannten Zwecken genutzt werden, dass die Behörden Sorge für die Qualität, Vertraulichkeit und Sicherheit der an sie weitergegebenen Daten tragen, und dass die Daten gelöscht werden, wenn sie nicht länger für die Vorbeugung, Ermittlung,

Aufdeckung und Verfolgung der spezifischen Straftat benötigt werden. Ferner sollte festgelegt werden, dass der Zugang in ganz bestimmten Fällen der gerichtlichen Kontrolle in den Mitgliedstaaten unterliegt.

57. Fünftens: Der Vorschlag enthält keine zusätzlichen Schutzmechanismen für den Datenschutz. In den Erwägungsgründen wird auf Schutzmechanismen in den geltenden Rechtsvorschriften, insbesondere in den Richtlinien 95/46/EG und 2002/58/EG, verwiesen. Der EDPS ist mit diesem begrenzten Ansatz des Datenschutzes trotz der besonderen Bedeutung von (zusätzlichen) Schutzmechanismen (siehe Abschnitt II dieser Stellungnahme) nicht einverstanden.

58. Der EDPS empfiehlt daher, einen Absatz zum Datenschutz aufzunehmen. In diesen Absatz könnten die vorstehenden Empfehlungen zu Artikel 3 Absatz 2 aufgenommen werden sowie weitere Bestimmungen zum Datenschutz, wie Bestimmungen in Bezug auf die Ausübung der Rechte des Betroffenen (siehe Abschnitt II dieser Stellungnahme), auf die Qualität und die Sicherheit der Daten sowie auf Standort- und Verkehrsdaten von Personen, die nicht einer Straftat verdächtig sind.

Artikel 4: Für die Vorratsspeicherung in Frage kommende Datenkategorien

59. Im Allgemeinen begrüßt der EDPS diesen Artikel und den Anhang aufgrund

- des gewählten Aufbaus, bei der die funktionalen Beschreibungen im verfügbaren Teil der Richtlinie und die technischen Einzelheiten in einem Anhang enthalten sind. Dieser Aufbau ist flexibel genug, damit angemessen auf technische Entwicklungen reagiert werden kann, und bietet den Bürgern Rechtssicherheit;

- der Unterscheidung zwischen Telefon- und Internetdaten, obgleich diese Unterscheidung technisch betrachtet an Bedeutung verliert. Aus der Sicht des Datenschutzes ist diese Unterscheidung jedoch wichtig, da es im Internet keine klare Grenze zwischen Inhaltsdaten und Verkehrsdaten gibt (siehe z. B. Artikel 1 Absatz 2 der Richtlinie, in dem festgelegt wird, dass es sich bei im Internet eingesehenen Informationen um Inhaltsdaten handelt);

- des Maßes der Harmonisierung: Der Vorschlag sieht ein hohes Maß an Harmonisierung mit einer erschöpfenden Aufzählung der für die Vorratsspeicherung in Frage kommenden Datenkategorien vor (im Gegensatz zu dem Entwurf eines Rahmenbeschlusses, der eine Mindestliste enthält und den Mitgliedstaaten viel Spielraum zur Einbeziehung weiterer Daten lässt). Aus der Sicht des Datenschutzes ist eine vollständige Harmonisierung von wesentlicher Bedeutung (siehe Abschnitt IV).

60. Der EDPS schlägt die folgenden Änderungen vor:

- Artikel 4 Absatz 2 sollte mehr sachliche Kriterien enthalten, um sicherzustellen, dass keine Inhaltsdaten aufgenommen werden. Folgender Satz sollte hinzugefügt werden: „In den Anhang dürfen keine Daten aufgenommen werden, die den Inhalt einer Kommunikation offen legen.“

- Artikel 5 eröffnet die Möglichkeit einer Überarbeitung des Anhangs durch eine Richtlinie der Kommission („Komitologie“). Der EDPS empfiehlt, dass Überarbeitungen des Anhangs, die wesentliche Auswirkungen auf den Datenschutz haben, vielmehr im Wege einer Richtlinie nach dem Mitentscheidungsverfahren vorgenommen werden. ⁽¹⁾

Artikel 7: Speicherungsfristen

61. Der EDPS begrüßt den Umstand, dass die Speicherungsfristen in dem Vorschlag erheblich kürzer sind als die in dem Entwurf eines Rahmenbeschlusses vorgesehenen Fristen.

- Unter Rückverweis auf die Zweifel, die in dieser Stellungnahme in Bezug auf den Nachweis der Notwendigkeit einer Vorratsspeicherung von Verkehrsdaten für bis zu einem Jahr geäußert wurden, ist festzustellen, dass die Frist von einem Jahr der Praxis der Strafverfolgung entspricht, *wie sie aus den* von der Kommission und dem Vorsitz des Rates vorgelegten Zahlen *hervorgeht*.

- Aus diesen Zahlen geht ebenfalls hervor, dass eine Vorratsspeicherung von Daten über längere Zeiträume — Sonderfälle ausgenommen — nicht der Praxis der Strafverfolgung entspricht.

- Die kürzere Frist von sechs Monaten für Daten in Verbindung mit elektronischen Nachrichtenübermittlungen, die ganz oder überwiegend unter Verwendung des Internet-Protokolls vorgenommen werden, ist aus der Sicht des Datenschutzes wichtig, da die Speicherung von Ergebnissen der Internet-Kommunikation zu großen Datenbanken führt (diese Daten werden gewöhnlich nicht zu Abrechnungszwecken gespeichert), die Grenze zu den Inhaltsdaten unscharf ist und eine Vorratsspeicherung von mehr als sechs Monaten nicht der Praxis der Strafverfolgung entspricht.

62. Es sollte im Text präzisiert werden, dass

- die Vorratsspeicherungsfristen von sechs Monaten bzw. einem Jahr die Höchstdauer der Vorratsspeicherung darstellen;

⁽¹⁾ Siehe in demselben Sinne auch die Stellungnahme des EDPS vom 23. März 2005 zu dem Vorschlag für eine Verordnung des Europäischen Parlaments und des Rates über das Visa-Informationssystem (VIS) und den Datenaustausch zwischen Mitgliedstaaten über Visa für den kurzfristigen Aufenthalt (Abschnitt 3.12).

- die Daten nach Ablauf der Vorratsspeicherungsfrist gelöscht werden. Im Text sollte ebenfalls präzisiert werden, wie die Löschung erfolgen sollte. Nach Auffassung des EDPS muss ein Betreiber die Daten auf automatische Weise löschen, und zwar mindestens einmal pro Tag.

Artikel 8: Anforderungen an die Vorratsspeicherung

63. Dieser Artikel steht in enger Verbindung zu Artikel 3 Absatz 2 und enthält eine wichtige Bestimmung, mit der sichergestellt werden kann, dass in ganz bestimmten Fällen der Zugang zu den Daten auf die Daten beschränkt wird, die speziell für diese Fälle benötigt werden. Nach Artikel 8 und Artikel 3 Absatz 2 ist davon auszugehen, dass die benötigten Daten von den Betreibern an die Behörden weitergeleitet werden und die Behörden keinen direkten Zugang zu den Datenbanken haben. Der EDPS empfiehlt, dies im Text ausdrücklich aufzunehmen.

64. Die Bestimmung sollte präzisiert werden, indem ausgeführt wird, dass

- die benötigten Daten von den Betreibern an die Behörden weitergeleitet werden (siehe Nr. 63);
- die Betreiber die erforderlichen technischen Einrichtungen, einschließlich Suchmaschinen, installieren sollten, um den gezielten Zugriff auf die benötigten Daten zu erleichtern;
- die Betreiber sicherstellen sollten, dass nur Mitarbeiter, die für bestimmte technische Aufgaben verantwortlich sind, aus technischen Gründen Zugang zu den Datenbanken haben, und dass sich diese Mitarbeiter des sensitiven Charakters der Daten bewusst sind und nach strengen internen Vertraulichkeitsregeln arbeiten;
- die Weiterleitung nicht nur unverzüglich, sondern auch so erfolgen sollte, dass keine anderen Verkehrs- und Standortdaten weitergegeben werden als die, die für die Zwecke der Anfrage benötigt werden.

Artikel 9: Statistik

65. Die Pflicht der Betreiber, jährlich eine Statistik zu übermitteln, hilft den Gemeinschaftsorganen, die Effizienz der Umsetzung und der Anwendung des vorliegenden Vorschlags zu überwachen. Es bedarf ausreichender Informationen.

66. Nach Auffassung des EDPS verleiht diese Verpflichtung dem Grundsatz der Transparenz Wirkung. Der europäische Bürger hat das Recht, zu wissen, wie effizient die Vorratsspeicherung von Daten ist. Aus diesem Grund sollte der Betreiber zusätzlich verpflichtet werden, Protokolle zu führen und systematisch (Selbst-)Kontrollen durchzuführen, um so den nationalen Datenschutzbehörden zu ermöglichen, die praktische Anwendung der Datenschutzvorschriften zu überwachen⁽¹⁾. Der Vorschlag sollte dementsprechend geändert werden.

Artikel 10: Kosten

67. Wie bereits in Abschnitt II dargelegt, besteht eine direkte Beziehung zwischen der Eignung der Sicherheitsmaßnahmen und den Kosten für diese Maßnahmen, oder, mit anderen Worten, zwischen Sicherheit und Kosten. Der EDPS hält daher Artikel 10, der die Erstattung von nachweislich entstandenen Zusatzkosten vorsieht, für eine wichtige Bestimmung, die für die Betreiber ein Anreiz sein könnte, in die technische Infrastruktur zu investieren.

68. Nach den Schätzungen, die in der dem EDPS von der Kommission vorgelegten Folgenabschätzung enthalten sind, sind die mit der Vorratsspeicherung verbundenen Kosten beträchtlich. Für einen großen Netzbetreiber und Diensteanbieter würden sich die Kosten für eine einjährige Vorratsspeicherung auf mehr als 150 Mio. EUR belaufen, wobei die jährlichen Betriebskosten rund 50 Mio. EUR ausmachen würden.⁽²⁾ Es gibt allerdings weder Zahlen zu den Kosten für zusätzliche Sicherheitsmaßnahmen, wie teure Suchmaschinen (siehe die Bemerkung zu Artikel 6), noch zu den (geschätzten) finanziellen Konsequenzen einer vollständigen Erstattung zusätzlicher Kosten des Betreibers.

69. Nach Auffassung des EDPS sind präzisere Zahlen erforderlich, damit der Vorschlag in seiner ganzen Tragweite beurteilt werden kann. Er regt an, die finanziellen Konsequenzen des Vorschlags in der Begründung des Vorschlags klar darzulegen.

70. Was im Einzelnen die Bestimmung von Artikel 10 betrifft, so sollte die Beziehung zwischen der Eignung der Sicherheitsmaßnahmen und den Kosten im Text der Bestimmung klar zum Ausdruck gebracht werden. Überdies sollten im Vorschlag Mindeststandards für die Sicherheitsmaßnahmen vorgesehen werden, die die Betreiber ergreifen müssen, um Anspruch auf eine Rückerstattung durch einen Mitgliedstaat zu haben. Nach Auffassung des EDPS kann die Festlegung dieser Standards nicht ausschließlich den Mitgliedstaaten

(1) Siehe in demselben Sinne auch die Stellungnahme des EDPS vom 23. März 2005 zu dem Vorschlag für eine Verordnung des Europäischen Parlaments und des Rates über das Visa-Informationssystem (VIS) und den Datenaustausch zwischen Mitgliedstaaten über Visa für den kurzfristigen Aufenthalt (Abschnitt 3.9).

(2) Die Kommission verweist auf Zahlen des ETNO (Europäischer Verband der Telekommunikationsbetreiber) und auf einen Bericht des MEP Alvaro zu dem Entwurf eines Rahmenbeschlusses.

überlassen werden. Dies könnte sich auf den mit der Richtlinie angestrebten Grad der Harmonisierung schädlich auswirken. Außerdem sollte berücksichtigt werden, dass die finanziellen Konsequenzen der Erstattung von den Mitgliedstaaten getragen werden.

Artikel 11: Änderung der Richtlinie 2002/58/EG

71. Die Beziehung zu Artikel 15 Absatz 1 der Richtlinie 2002/58/EG sollte geklärt werden, da der vorliegende Vorschlag dieser Bestimmung viel von ihrem Inhalt nimmt. Die Bezugnahmen in Artikel 15 Absatz 1 der Richtlinie 2002/58/EG auf die Artikel 6 und 9 (derselben Richtlinie) sollten gestrichen oder zumindest geändert werden, um zu präzisieren, dass die Mitgliedstaaten nicht länger die Befugnis haben, Straftaten betreffende Rechtsvorschriften anzunehmen, die einen Zusatz zu diesem Vorschlag darstellen. Jegliche Unklarheit in Bezug auf ihre verbleibenden Befugnisse — z. B. was die Vorratsspeicherung von Daten im Zusammenhang mit weniger schweren Straftaten anbelangt — muss ausgeräumt werden.

Artikel 12: Bewertung

72. Der EDPS begrüßt, dass der Vorschlag einen Artikel enthält, wonach spätestens drei Jahre nach ihrem Inkrafttreten eine Bewertung der Richtlinie vorzulegen ist. Eine Bewertung ist umso wichtiger, da Zweifel an der Notwendigkeit und der Verhältnismäßigkeit des Vorschlags bestehen.

73. Vor diesem Hintergrund rät der EDPS dazu, eine noch strengere Verpflichtung einzuführen, die Folgendes enthalten sollte:

- Bei der Bewertung sollte auch evaluiert werden, wie effizient die Umsetzung der Richtlinie aus der Sicht der Strafverfolgung ist und welche Auswirkungen die Richtlinie auf die Grundrechte des Betroffenen hat. Die Kommission sollte dabei alle Nachweise berücksichtigen, die Auswirkungen auf die Bewertung haben könnten.
- Die Bewertung sollte in regelmäßigen Abständen vorgenommen werden (zumindest alle zwei Jahre).
- Die Kommission sollte verpflichtet sein, gegebenenfalls Änderungen am Vorschlag vorzulegen (wie in Artikel 18 der Richtlinie 2002/58/EG).

VI. Schlussfolgerungen

Voraussetzungen

74. Für den EDPS ist es ganz wichtig, dass in dem Vorschlag die Grundrechte gewahrt bleiben. Eine Legislativmaßnahme,

durch die der Schutz beeinträchtigt würde, den das Gemeinschaftsrecht und insbesondere die Rechtsprechung des Gerichtshofs und des Europäischen Gerichtshofs für Menschenrechte gewährleisten, ist nicht nur unannehmbar, sondern auch illegal.

75. Die Notwendigkeit und die Verhältnismäßigkeit der Pflicht zur Vorratsspeicherung — in ihrer ganzen Tragweite — bleibt nachzuweisen.

76. Was die Notwendigkeit anbelangt, so sieht der EDPS ein, dass sich die Umstände verändert haben; er ist aber trotzdem noch nicht davon überzeugt, dass eine Vorratsspeicherung von Verkehrs- und Standortdaten zu Strafverfolgungszwecken, wie sie in dem Vorschlag vorgesehen ist, erforderlich ist.

77. Der EDPS legt in dieser Stellungnahme trotzdem auch seine Auffassung zur Verhältnismäßigkeit des Vorschlags dar. Das heißt erstens, dass die Vorratsspeicherung von Verkehrs- und Standortdaten an sich keine geeignete oder wirksame Reaktion darstellt. Es sind zusätzliche Maßnahmen erforderlich, um sicherzustellen, dass die Behörden in einem ganz bestimmten Fall einen gezielten und schnellen Zugriff auf die erforderlichen Daten haben. Zweitens sollten

- die Speicherungsfristen im Vorschlag begrenzt sein. Diese Fristen müssen den Erfordernissen der Strafverfolgungsbehörden entsprechen;
- die Anzahl der zu speichernden Daten im Vorschlag begrenzt sein. Diese Anzahl muss den Erfordernissen der Strafverfolgungsbehörden entsprechen und Gewähr dafür bieten, dass kein Zugang zu Inhaltsdaten möglich ist;
- im Vorschlag geeignete Schutzmechanismen enthalten sein.

Allgemeine Beurteilung

78. Der EDPS betont die Bedeutung der Tatsache, dass in dem gegenwärtigen Text die vollständige Harmonisierung der wichtigsten Aspekte des Vorschlags vorgesehen ist, insbesondere die Harmonisierung der auf Vorrat zu speichernden Daten, die Zeiträume, während deren die Daten gespeichert werden sollen, sowie der (Zweck des) Zugang(s) zu den Daten und ihre(r) Weiterverwendung.

79. In einigen Punkten bedarf es einer weiteren Präzisierung, um z. B. sicherzustellen, dass nach Ablauf der Vorratsspeicherungsfrist eine entsprechende Löschung der Daten erfolgt, und um wirksam zu verhindern, dass verschiedene Interessengruppen Zugang zu den Daten haben und sie nutzen.

80. Nach Auffassung des EDPS sind folgende Punkte von größter Bedeutung, damit der Vorschlag aus Sicht des Datenschutzes annehmbar wird:

- Dem Vorschlag sollten als wesentlicher und fester Bestandteil seines Gegenstands konkrete Bestimmungen über den Zugang der zuständigen Behörden zu den Verkehrs- und Standortdaten und über die Weiterverwendung der Daten hinzugefügt werden.
- Dem Vorschlag sollten zusätzliche Sicherheitsmechanismen für den Datenschutz hinzugefügt werden (im Gegensatz zu einem einfachen Verweis auf Sicherheitsmechanismen in geltenden Rechtsvorschriften, insbesondere auf die Richtlinien 95/46/EG und 2002/58/EG), u. a. um sicherzustellen, dass der Betroffene seine Rechte ausüben kann.
- Der Vorschlag sollte um weitere Anreize — auch finanzieller Art — für die Betreiber ergänzt werden, damit diese in eine angemessene technische Infrastruktur investieren. Diese Infrastruktur kann nur dann angemessen sein, wenn es auch entsprechende effiziente Suchmaschinen gibt.

Empfehlungen zur Änderung des Vorschlags

81. Zu Artikel 3 Absatz 2:

- Aufnahme einer Bestimmung, damit sichergestellt wird, dass niemand anders als die zuständigen Behörden Zugang zu den Daten hat. Diese Bestimmung könnte folgendermaßen formuliert sein: „Der Zugang zu den Daten und/oder ihre Verarbeitung ist nur zu dem in Artikel 3 Absatz 2 genannten Zweck gestattet“ oder „die Betreiber gewährleisten, dass nur den zuständigen Behörden Zugang zu den Daten gewährt wird“;
- Präzisierung, dass die Daten nur weitergegeben werden dürfen, wenn dies im Zusammenhang mit einer spezifischen Straftat erforderlich ist;
- Begrenzung der Bestimmung auf *bestimmte* schwere Straftaten;
- Aufnahme eines oder mehrerer Artikel über den Zugang der zuständigen Behörden zu den Standort- und Verkehrsdaten und über die Weiterverwendung der Daten sowie einer Bestimmung in den Vorschlag, wonach der Zugang in ganz bestimmten Fällen der gerichtlichen Kontrolle in den Mitgliedstaaten unterliegen sollte;
- Aufnahme eines Absatzes zum Datenschutz.

82. Zu den Artikeln 4 und 5:

- Aufnahme des folgenden Satzes in Artikel 4 Absatz 2: „In den Anhang dürfen keine Daten aufgenommen werden, die den Inhalt einer Kommunikation offen legen.“;
- Präzisierung, dass Überarbeitungen des Anhangs, die wesentliche Auswirkungen auf den Datenschutz haben, vorzugsweise im Wege einer Richtlinie nach dem Mitentscheidungsverfahren vorgenommen werden.

83. Zu Artikel 7: Präzisierung im Text, dass

- die Vorratsspeicherungsfristen von sechs Monaten bzw. einem Jahr die Höchstdauer der Vorratsspeicherung darstellen;
- die Daten nach Ablauf der Vorratsspeicherungsfrist gelöscht werden. Im Text sollte ebenfalls präzisiert werden, wie die Löschung erfolgen sollte, nämlich durch den Betreiber auf automatische Weise, und zwar mindestens einmal pro Tag.

84. Zu Artikel 8: Präzisierung im Text, dass

- die benötigten Daten von den Betreibern an die Behörden weitergeleitet werden;
- die Betreiber die erforderlichen technischen Einrichtungen einschließlich Suchmaschinen installieren sollten, um einen gezielten Zugriff auf die benötigten Daten zu erleichtern;
- die Betreiber sicherstellen sollten, dass nur Mitarbeiter, die für bestimmte technische Aufgaben verantwortlich sind, aus technischen Gründen Zugang zu den Datenbanken haben, und dass sich diese Mitarbeiter des sensitiven Charakters der Daten bewusst sind und nach strengen internen Vertraulichkeitsregeln arbeiten;
- die Datenübermittlung nicht nur unverzüglich, sondern auch so erfolgen sollte, dass keine anderen Verkehrs- und Standortdaten weitergegeben werden als die, die für die Zwecke der Anfrage benötigt werden.

85. Zu Artikel 9:

- Aufnahme einer Bestimmung, mit der der Betreiber zusätzlich verpflichtet wird, Protokolle zu führen und systematisch (Selbst-)Kontrollen durchzuführen, um so den nationalen Datenschutzbehörden zu ermöglichen, die praktische Anwendung der Datenschutzvorschriften zu überwachen.

86. Zu Artikel 10:

- Präzisierung der Beziehung zwischen der Eignung der Sicherheitsmaßnahmen und den Kosten im Text der Bestimmung;
- Aufnahme von Mindeststandards für die Sicherheitsmaßnahmen, die die Betreiber ergreifen müssen, um Anspruch auf eine Rückerstattung durch einen Mitgliedstaat zu haben;
- klare Darstellung der finanziellen Konsequenzen des Vorschlags in seiner Begründung.

87. Zu Artikel 11:

- Änderung von Artikel 15 Absatz 1 der Richtlinie 2002/58/EG, indem die Verweise auf die Artikel 6 und 9 (derselben Richtlinie) gestrichen oder zumindest

abgeändert werden, um zu präzisieren, dass die Mitgliedstaaten nicht länger die Befugnis haben, Straftaten betreffende Rechtsvorschriften anzunehmen, die einen Zusatz zu diesem Vorschlag darstellen.

88. Zu Artikel 12: Änderung der Bestimmung über die Bewertung:

- Bei der Bewertung sollte auch evaluiert werden, wie effizient die Umsetzung der Richtlinie ist;
- die Bewertung sollte in regelmäßigen Abständen vorgenommen werden (zumindest alle zwei Jahre);
- die Kommission sollte verpflichtet sein, gegebenenfalls Änderungen zum Vorschlag vorzulegen (wie in Artikel 18 der Richtlinie 2002/58/EG).

Geschehen zu Brüssel am 26. September 2005.

Peter HUSTINX
Europäischer Datenschutzbeauftragter
