DER EUROPÄISCHE DATENSCHUTZBEAUFTRAGTE

Stellungnahme des Europäischen Datenschutzbeauftragten zu der Mitteilung der Kommission über einen Aktionsplan zur Einführung intelligenter Verkehrssysteme in Europa und dem dazugehörigen Vorschlag für eine Richtlinie des Europäischen Parlaments und des Rates zur Festlegung eines Rahmens für die Einführung intelligenter Verkehrssysteme im Straßenverkehr und für deren Schnittstellen zu anderen Verkehrsträgern

(2010/C 47/02)

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,

gestützt 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,

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, insbesondere auf Artikel 41,

gestützt auf das am 11. Februar 2009 eingegangene Ersuchen der Europäischen Kommission um Stellungnahme nach Artikel 28 Absatz 2 der Verordnung (EG) Nr. 45/2001 —

HAT FOLGENDE STELLUNGNAHME ANGENOMMEN:

I. EINLEITUNG

1. Am 16. Dezember 2008 hat die Kommission eine Mitteilung mit einem Aktionsplan zur Einführung intelligenter Verkehrssysteme in Europa (nachstehend „Mitteilung" genannt) angenommen [1]. Die Mitteilung wird ergänzt durch einen Vorschlag für eine Richtlinie des Europäischen Parlaments und des Rates zur Festlegung eines Rahmens für die Einführung intelligenter Verkehrssysteme im Straßenverkehr und für deren Schnittstellen zu anderen Verkehrsträgern (nachstehend „Vorschlag" genannt) [2]. Die Mitteilung und der dazugehörige Vorschlag wurden dem Europäischen Datenschutzbeauftragten (EDSB) von der Kommission zwecks Konsultation gemäß Artikel 28 Absatz 2 der Verordnung (EG) Nr. 45/2001 [3] übermittelt.

2. Der EDSB begrüßt es, dass er konsultiert wird, und empfiehlt, eine Bezugnahme auf diese Konsultation in die Erwägungsgründe des Vorschlags aufzunehmen, wie dies bei verschiedenen Rechtstexten der Fall ist, zu denen er gemäß der Verordnung (EG) Nr. 45/2001 konsultiert wurde.

I.1 Mitteilung der Kommission über einen Aktionsplan zur Einführung von intelligenten Verkehrssystemen in Europa

3. „Intelligente Verkehrssysteme" („IVS") sind fortgeschrittene Anwendungen, die in die einzelnen Verkehrsträger eingebettete Informations- und Kommunikationstechnologien (IKT) für die Interaktion zwischen diesen Verkehrsträgern nutzen. Im Straßenverkehrssektor sollen die IVS verschiedenen Nutzern wie etwa Reisenden, Nutzern und Betreibern der Verkehrsinfrastruktur, Flottenmanagern und Betreibern von Notdiensten in Bezug auf die Verkehrsträger und das Verkehrsmanagement innovative Dienste bereitstellen.

4. Angesichts des zunehmenden Einsatzes von IVS bei verschiedenen Verkehrsträgern [4] in der Europäischen Union hat die Kommission einen Aktionsplan angenommen, um die Einführung und Nutzung von IVS-Anwendungen und

[1] KOM(2008) 886 endg. Der Rat (Verkehr, Telekommunikation und Energie) hat auf seiner 2935. Tagung vom 30. und 31. März 2009 Schlussfolgerungen zum Thema Kommunikation angenommen.
[2] KOM(2008) 887 endg.
[3] 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 (ABl. L 8 vom 12.1.2001, S. 1).
[4] Es gibt auf EU-Ebene verschiedene Initiativen zur Einbeziehung von IVS in verschiedene Verkehrsträger einschließlich des Luftverkehrs (SESAR), der Binnenschifffahrt (RIS), des Eisenbahnverkehrs (TSI TAG), des Seeverkehrs (VTMIS, AIS, LRIT) und des Straßenverkehrs (eToll, eCall), siehe KOM(2008) 886 endg., S. 3).

-Diensten im Bereich des Straßenverkehrs zu beschleunigen. Mit dem Plan soll ferner ihre Interaktion mit anderen Verkehrsträgern sichergestellt werden, was die Bereitstellung von multimodalen Verkehrsdiensten erleichtern wird. Die kohärente Einführung von IVS in Europa soll mehreren Zielen der Gemeinschaft dienen, wie der Verkehrseffizienz, der Nachhaltigkeit und der Straßenverkehrssicherheit, und damit den EU-Binnenmarkt und die Wettbewerbsfähigkeit der Union fördern. Inmitten der Vielfalt der mit der IVS-Einführung verfolgten Ziele werden in der Kommissionsmitteilung für den Zeitraum 2009—2014 sechs vorrangige Aktionsbereiche vorgegeben. Zur Durchführung des Plans schlägt die Kommission vor, dass auf der Ebene der EU durch eine Richtlinie ein Rechtsrahmen geschaffen wird, in dem eine Reihe von Maßnahmen in ausgewählten vorrangigen Bereichen festgelegt wird.

I.2 **Vorschlag für eine Richtlinie zur Festlegung eines Rahmens für die Einführung von IVS im Straßenverkehr und für deren Schnittstellen zu anderen Verkehrsträgern**

5. Mit dem Vorschlag wird ein Rahmen für die grenzüberschreitende Einführung von IVS-Anwendungen festgelegt, der die Bereitstellung harmonisierter grenzüberschreitender Dienste insbesondere in Bezug auf Verkehrs- und Reiseinformationen sowie Verkehrsmanagement erleichtern soll. Danach würden die Mitgliedstaaten verpflichtet, mehrere technische Maßnahmen zur Erleichterung des Datenaustauschs zwischen Nutzern, Behörden, einschlägigen Akteuren und IVS-Diensteanbietern und zur Integration von sicherheitsrelevanten IVS-Systemen in Fahrzeuge und Straßenverkehrsinfrastruktur zu treffen. Technische Spezifikationen für IVS-Anwendungen und -Systeme in vier der im Aktionsplan aufgeführten vorrangigen Aktionsbereiche ([5]) werden im Wege eines Ausschussverfahrens ([6]) festgelegt, dessen Kernkomponenten in Anhang II präzisiert werden. Es ist jedoch noch keineswegs klar, zu welchen speziellen Zwecken die IVS in diesen Bereichen verwendet werden sollen. Ferner kann die Einführung von IVS über die vier ursprünglich für die Entwicklung harmonisierter technischer Spezifikationen ausgewählten Bereiche hinaus auf viele weitere Bereiche erweitert werden. Zwar befasst sich der Vorschlag im Wesentlichen mit der Einführung zukünftiger IVS-Anwendungen und -Dienste, er wird sich aber im Rahmen des Möglichen auch auf bestehende oder derzeit in Entwicklung befindliche Technologien auf dem betreffenden Gebiet (wie etwa eCall, eToll usw.) erstrecken.

6. Der Vorschlag wurde dem Europäischen Parlament zugeleitet, das seine Stellungnahme in erster Lesung ([7]) am 23. April 2009 abgegeben hat. Im Anschluss an ein Konsultationsersuchen des Rates vom 29. Januar 2009 hat der Europäische Wirtschafts- und Sozialaussschuss am 13. Mai 2009 eine Stellungnahme zu dem Vorschlag ([8]) abgegeben.

I.3 **Schwerpunkt der Stellungnahme**

7. Der EDSB begrüßt die Anhörung zu dem vorgeschlagenen Plan zur Einführung von IVS, den die Kommission vorgelegt hat. Es ist nicht das erste Mal, dass der EDSB mit den im IVS-Aktionsplan behandelten Themen befasst ist. Der EDSB hat eine Stellungnahme zu dem Vorschlag der Kommission zur Erleichterung der grenzübergreifenden Durchsetzung von Verkehrssicherheitsvorschriften abgegeben ([9]) und zu den Arbeiten der Artikel-29-Datenschutzgruppe an einem Arbeitsdokument zur eCall-Initiative beigetragen ([10]).

8. Intelligente Verkehrssysteme sind gestützt auf Erhebung, Verarbeitung und Austausch einer ganzen Bandbreite von Daten aus öffentlichen und privaten Quellen und sind daher von großer Daten-Intensität. Die Einführung von IVS wird weithin auf Geolokalisierungstechnologien wie der Satellitenortung und auf berührungsfrei arbeitende Technologien wie etwa RFID beruhen; dies soll die Bereitstellung einer Vielzahl von öffentlichen und/oder kommerziellen standortbasierten Diensten ermöglichen (z. B. Verkehrsinformationen in Echtzeit, eFreight, eCall, eToll, Parkplatzreservierung usw.). Einige der über IVS verarbeiteten Informationen werden aggregiert — etwa Angaben zur Verkehrslage, Unfällen und Fahrtalternativen — und beziehen sich nicht auf Einzelpersonen, wohingegen andere Informationen sich auf bestimmte oder bestimmbare Personen beziehen und somit als personenbezogene Daten im Sinne von Artikel 2 Buchstabe a der Richtlinie 95/46/EG zu gelten haben.

9. Nach Auffassung des EDSB ist es von wesentlicher Bedeutung, dass die für die Einführung von IVS geplanten Initiativen mit dem bestehenden Rechtsrahmen, wie er im Vorschlag aufgeführt ist — insbesondere mit der Datenschutzrichtlinie 95/46/EG ([11]) und der Datenschutzrichtlinie 2002/58/EG für elektronische Kommunikation ([12]) —, im Einklang stehen.

([5]) In Artikel 4 des Vorschlags ist die Festlegung technischer Maßnahmen auf folgenden Gebieten vorgesehen: i) optimale Nutzung von Straßen-, Verkehrs- und Reisedaten, ii) Kontinuität der IVS-Dienste in den Bereichen Verkehrs- und Frachtmanagement auf den europäischen Verkehrskorridoren und in Ballungsräumen, iii) Sicherheit im Straßenverkehr und iv) Einbindung des Fahrzeugs in die Verkehrsinfrastruktur.

([6]) Im Vorschlag ist ein Regelungsverfahren mit Kontrolle gemäß Artikel 5 Buchstabe a Nummern 1 bis 4 und Artikel 7 des Beschlusses 1999/46/EG vorgesehen.

([7]) Legislative Entschließung des Europäischen Parlaments vom 23. April 2009 zu dem Vorschlag für eine Richtlinie des Europäischen Parlaments und des Rates zur Festlegung eines Rahmens für die Einführung intelligenter Verkehrssysteme im Straßenverkehr und für deren Schnittstellen zu anderen Verkehrsträgern, T6-0283/2009.

([8]) Stellungnahme des Europäischen Wirtschafts- und Sozialausschusses zu dem Vorschlag für eine Richtlinie des Europäischen Parlaments und des Rates zur Festlegung eines Rahmens für die Einführung intelligenter Verkehrssysteme im Straßenverkehr und für deren Schnittstellen zu anderen Verkehrsträgern — TEN/382, 13. Mai 2009.

([9]) Stellungnahme des Europäischen Datenschutzbeauftragten zu dem Vorschlag für eine Richtlinie des Europäischen Parlaments und des Rates zur Erleichterung der grenzübergreifenden Durchsetzung von Verkehrssicherheitsvorschriften — 2008/C 310/02 (ABl. C 310 vom 5.12.2008, S. 9).

([10]) Arbeitsdokument der Artikel-29-Datenschutzgruppe über Eingriffe in den Datenschutz im Rahmen der Initiative eCall (Dok. WP 125 vom 26. September 2006). http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2006/wp125_de.pdf

([11]) 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 (ABl. L 281 vom 23.11.1995, S. 31).

([12]) 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) (ABl. L 201 vom 31.7.2002, S. 37).

10. Die noch offenen Fragen in Bezug auf den Schutz von Daten und Privatsphäre wurden von der Kommission als ein Haupthindernis für die Förderung von IVS ermittelt. Die betreffenden Aspekte werden in dieser Stellungnahme wie folgt behandelt:

— In Kapitel II wird der von der Kommission für die Einführung von IVS vorgeschlagene Rechtsrahmen unter Datenschutzgesichtspunkten analysiert.

— In Kapitel III werden die Datenschutzanliegen aufgezeigt, auf die im Hinblick auf eine ordnungsgemäße Einführung von IVS weiter eingegangen werden muss:

— Zunächst wird in der Stellungnahme darauf hingewiesen, dass bei der Entwicklung von IVS das Konzept des „eingebauten Datenschutzes" zum Tragen kommen muss; zudem sollen die wichtigen Fragen weiter erläutert werden, für die bei der Konzeption von IVS-Anwendungen und Datenverarbeitungssystemen Lösungen gefunden werden müssen.

— Sodann wird schwerpunktmäßig auf einige Erwägungen in Bezug auf den Schutz der Privatsphäre eingegangen, die im Rahmen der Erbringung von IVS-Diensten weiter zu berücksichtigen sind.

II. ANALYSE DES ZUR EINFÜHRUNG VON IVS VORGESCHLAGENEN RECHTSRAHMENS

11. Der Richtlinienvorschlag der Kommission enthält zwei Bestimmungen (Erwägungsgrund 9 und Artikel 6), in denen es um den Schutz der Privatsphäre und um die Sicherheit und Weiterverwendung von Informationen geht. Nach Artikel 6 Absatz 1 des Vorschlags müssen bei der Anwendung von IVS die unter anderem in den Richtlinien 95/46/EG und 2002/58/EG enthaltenen Datenschutzvorschriften eingehalten werden. Artikel 6 Absatz 2 des Vorschlags stellt auf konkrete Datenschutzmaßnahmen — hauptsächlich unter Sicherheitsaspekten — ab und besagt: „ Insbesondere stellen die Mitgliedstaaten sicher, dass IVS-Daten und -Aufzeichnungen gegen Missbrauch, wie unberechtigten Zugang, Änderung oder Verlust, geschützt sind.". Schließlich gilt nach Artikel 6 Absatz 3 des Vorschlags die Richtlinie 2003/98/EG.

12. Das Europäische Parlament hat in erster Lesung Abänderungen an Artikel 6 vorgeschlagen. Insbesondere werden in Artikel 6 Absatz 1 drei neue Unterabsätze angefügt; sie betreffen die etwaige Verwendung anonymer Daten, die Verarbeitung sensibler Daten nur nach einer in Kenntnis der Sachlage gegebenen Einwilligung des Betroffenen und die Gewähr dafür, dass personenbezogene Daten nur dann verarbeitet werden, „wenn ihre Verarbeitung für den Betrieb von IVS-Anwendungen und/oder -Diensten erforderlich ist". Ferner wird Artikel 6 Absatz 2 durch einen Zusatz dahingehend abgeändert, dass IVS-Daten und -Aufzeichnungen „nicht zu anderen als den in dieser Richtlinie genannten Zwecken verwendet werden dürfen".

13. Der EDSB begrüßt es, dass der Datenschutz bei der Formulierung des Vorschlags berücksichtigt wurde und als eine generelle Voraussetzung für die ordnungsgemäße Einführung vorgegeben wird. Ferner ist sich der EDSB dessen bewusst, dass eine kohärente Harmonisierung der Datenprozesse auf EU-Ebene erforderlich ist, um die europaweite Einsatzfähigkeit der IVS-Anwendungen und -Dienste zu gewährleisten.

14. Der EDSB stellt jedoch fest, dass der vorgeschlagene Rechtsrahmen zu weit gefasst und zu allgemein gehalten ist, um den mit der Einführung von IVS in den Mitgliedstaaten verbundenen Datenschutzanliegen gerecht zu werden. Es ist nicht klar, wann der Betrieb von IVS-Diensten zur Erhebung und Verarbeitung personenbezogener Daten führen wird, für welche speziellen Zwecke eine Datenverarbeitung erfolgt und aufgrund welcher Rechtsgrundlage die betreffende Verarbeitung gerechtfertigt ist. Ferner bringt der Einsatz von Ortungstechnologien für die Einführung von IVS die Gefahr mit sich, dass Dienste entwickelt werden, welche die Privatsphäre verletzen, wenn sie mit der Erhebung und dem Austausch von personenbezogenen Daten verbunden sind. Ferner sind in dem Vorschlag die Funktionen und Zuständigkeiten der einzelnen an der Einführung der IVS beteiligten Akteure nicht eindeutig bestimmt, so dass sich nur schwer ermitteln lässt, bei welchen Akteuren es sich um für die Datenverarbeitung Verantwortliche handelt, die dann ([13]) für die Einhaltung der Datenschutzpflichten Sorge tragen müssen. Die IVS-Betreiber werden mit erheblichen Problemen konfrontiert sein, wenn nicht all diese Aspekte in der Rechtsvorschrift präzisiert sind, denn die Durchführung der in der vorgeschlagenen Richtlinie niedergelegten Maßnahmen wird letztendlich ihnen obliegen.

15. Es besteht daher die Gefahr, dass die mangelnde Präzision des vorgeschlagenen Rechtsrahmens zu Unterschieden bei der Einführung von IVS in Europa führen wird und anstatt des Abbaus von Diskrepanzen zwischen den Mitgliedstaaten vielmehr infolge unterschiedlicher Datenschutzniveaus ein beträchtliches Maß an Unsicherheit, Fragmentierung und Inkohärenz zur Folge haben wird. Dies wiederum führt möglicherweise zur mangelhaften Einhaltung wesentlicher Datenschutzgarantien. Der EDSB betont, dass in Bezug auf diese Aspekte eine weitere Harmonisierung auf der Ebene der EU erforderlich ist. Daher schlägt er von Datenschutzerwägungen getragene Änderungen an dem vorgeschlagenen Rechtsrahmen vor. Er empfiehlt nachdrücklich, dass das Europäische Parlament und der Rat die vorgeschlagenen Abänderungen und, soweit durchführbar, zusätzliche Bestimmungen zur Klärung der noch offenen Fragen (wie etwa Bestimmung und Zuständigkeiten der IVS-Akteure, Entwicklung von Standardaufträgen zur Erbringung von IVS-Diensten usw.) in den Vorschlag aufnehmen.

([13]) Gemäß Artikel 2 Buchstabe d, Artikel 6 Absatz 2 und Artikel 23 der in der Fußnote 11 aufgeführten Richtlinie 95/46/EG.

Ferner betont er, dass auch die Mitgliedstaaten Verantwortung dafür tragen, dass die Richtlinie ordnungsgemäß umgesetzt wird, damit die Akteure dann Systeme und Dienste entwickeln können, die europaweit ein angemessenes Datenschutzniveau bieten.

II.1 **Datenverarbeitungstätigkeiten bedürfen einer geeigneten Rechtsgrundlage**

16. Es ist nicht klar, zu welchem Zeitpunkt nach dem Einbau von IVS-Geräten in ein Fahrzeug mit der Verarbeitung personenbezogener Daten begonnen wird und auf welcher rechtlichen Grundlage die Verarbeitung erfolgt. Die Betreiber können sich auf unterschiedliche Rechtsgrundlagen für die Datenverarbeitung stützen, unter anderem auf die zweifelsfrei feststehende Einwilligung der Nutzer, einen Vertrag oder eine rechtliche Verpflichtung, die der für die Datenverarbeitung Verantwortliche einzuhalten hat. Die Rechtsgrundlage für die Durchführung der Datenverarbeitung in IVS muss harmonisiert werden, damit die Systeme europaweit funktionieren und die Nutzer nicht unter unterschiedlichen Vorgehensweisen bei der Datenverarbeitung in den einzelnen EU-Mitgliedstaaten zu leiden haben.

17. In einer Reihe von Fällen werden die IVS-Systeme bereits standardmäßig in die Fahrzeuge integriert sein. Dies gilt insbesondere für sicherheitsrelevante IVS-Systeme, die dem Vorschlag zufolge in die Fahrzeuge integriert sein müssen. Im Vorschlag findet sich jedoch keine Bestimmung des Begriffs „sicherheitsrelevante IVS-Systeme", weshalb näher präzisiert werden muss, worum es sich bei den in die Fahrzeuge zu integrierenden IVS-Anwendungen und -Diensten eigentlich handelt. Ferner sollte präzisiert werden, ob die Aktivierung und Verwendung des betreffenden Geräts durch den Nutzer freiwillig oder vorgeschrieben ist. Die Entscheidung für eine obligatorische Durchführung der Datenverarbeitung sollte nur für spezielle Zwecke unter Berücksichtigung von zwingenden Gründen (beispielsweise ordnungsgemäße Kontrolle des Frachtmanagements) und mit geeigneten Garantien hinsichtlich der Verarbeitung personenbezogener Daten getroffen werden. Ist die Verwendung von IVS fakultativ, so sollten angemessene Garantien zum Tragen kommen, um zu verhindern, dass aufgrund des bloßen Vorhandenseins des Systems im Fahrzeug davon ausgegangen wird, dass die Nutzer stillschweigend in seine Verwendung eingewilligt haben.

18. Der EDSB gibt einer Erbringung von IVS-Diensten auf freiwilliger Grundlage den Vorzug. Dies bedeutet, dass die Nutzer in der Lage sein müssen, in freier Entscheidung der Verwendung des Systems und den speziellen Zwecken, für die es verwendet werden soll, zuzustimmen. Wenn die erbrachten Dienste auf standortbezogenen Daten beruhen, muss der Nutzer (insbesondere nach Artikel 9 der Richtlinie 2002/58/EG) darüber angemessen unterrichtet werden und in der Lage sein, seine Zustimmung zurückzuziehen. In der Praxis setzt dies die Einführung einer einfach durchzuführenden Deaktivierung des Geräts und/oder der Funktion voraus, wobei dem Nutzer keine technischen oder finanziellen Beschränkungen auferlegt werden dürfen ([14]), wenn er mit der weiteren Verwendung des Systems und/oder einer besonderen Funktion desselben nicht länger einverstanden ist. Es sollten weitere Garantien zum Tragen kommen, damit die Nutzer nicht diskriminiert werden, wenn sie die Nutzung eines Dienstes ablehnen.

19. In den Fällen, in denen bestimmte Verarbeitungstätigkeiten verbindlich vorgeschrieben sind und andere die Einwilligung des Nutzers voraussetzen, ist die Transparenz in Bezug auf die verschiedenen durchgeführten Datenverarbeitungsvorgänge zu gewährleisten, indem die Nutzer angemessen über den obligatorischen und/oder fakultativen Charakter jeder einzelnen Datenverarbeitungstätigkeit und deren Tragweite unterrichtet werden. Ferner ist es von entscheidender Bedeutung, dass angemessene Sicherheitsvorkehrungen getroffen werden, damit außerhalb des rechtlich vorgeschriebenen und/oder freiwillig akzeptierten Rahmens keine Daten erhoben und verarbeitet werden.

20. In Anbetracht der grenzüberschreitenden Auswirkungen von IVS-Diensten empfiehlt der EDSB ferner, europaweit einheitliche Standardaufträge auszuarbeiten, damit gewährleistet ist, dass die mit den IVS erbrachten Dienste in ganz Europa dasselbe Schutzniveau bieten und dass insbesondere die den Nutzern bereitgestellten Informationen hinreichend präzise die verwendeten spezifischen Funktionsmerkmale, die Wirkungen der Nutzung der spezifischen Technologien auf den Schutz ihrer Daten und das Verfahren für die Ausübung ihrer Rechte beschreiben. Werden neue Funktionen hinzugefügt, so sollten von den Diensteanbietern zusätzliche Maßnahmen getroffen werden, um den Nutzern präzise und konkrete Informationen zu diesen Zusatzfunktionen zu vermitteln und in geeigneter Form ihre Einwilligung in die Nutzung dieser neuen Funktionen einzuholen.

II.2 **Die Zwecke und Modalitäten der Datenverarbeitung sind näher zu bestimmen**

21. Der EDSB stellt fest, dass im Vorschlag die spezifischen Dienste und Zwecke, für die IVS-Anwendungen verwendet werden könnten, nicht genau bestimmt sind und somit im Unklaren bleiben. Dies ermöglicht in der Praxis ein flexibles Vorgehen, bedeutet aber auch, dass möglicherweise noch offene Fragen des Schutzes der Privatsphäre und des Datenschutzes — die ja von der Kommission als eines der Haupthindernisse für die Förderung von IVS ermittelt wurden (siehe Nummer 10) — ungelöst bleiben und einer ausgewogenen Durchführung der vorgeschlagenen Maßnahmen im Wege stehen könnten.

22. Nach Auffassung des EDSB ist es besonders wichtig, dass die im Hinblick auf die Erbringung spezifischer IVS-Dienste durchgeführten Datenverarbeitungsvorgänge nicht nur auf eine geeignete Rechtsgrundlage gestützt sind, sondern auch für festgelegte eindeutige und rechtmäßige Zwecke erhoben werden, und dass die geplante Datenverarbeitung für diese Zwecke angemessen und notwendig ist (Artikel 6 der Richtlinie 95/46/EG). Daher sollte geprüft werden, ob es möglicherweise erforderlich ist, auf der Ebene der EU weitere Rechtsvorschriften in Bezug auf die spezifischen Verwendungszwecke von IVS zu erlassen, damit für die geplanten Datenverarbeitungstätigkeiten eine geeignete harmonisierte Rechtsgrundlage zur Verfügung steht und es bei der Einführung von IVS-Diensten nicht zu Diskrepanzen zwischen den Mitgliedstaaten kommt.

23. Der vorgeschlagene Rahmen enthält noch keine Entscheidung über die Modalitäten der Datenverarbeitung und des Datenaustauschs bei der Verwendung von IVS. Viele technische Parameter, deren Wahl sich jeweils unterschiedlich auf den Schutz der Privatsphäre und den Datenschutz auswirken wird, sollen erst zu einem späteren Zeitpunkt im

([14]) Siehe das in Fußnote 10 auf Seite 4 aufgeführte Dok. WP 125 zu eCall.

Wege des Ausschussverfahrens beschlossen werden. In Anbetracht des besonderen Schutzes der Privatsphäre und des Datenschutzes als Grundrechte nach Artikel 8 der Europäischen Konvention zum Schutze der Menschenrechte und Grundfreiheiten und den Artikeln 7 und 8 der Charta der Grundrechte der Europäischen Union ist fraglich, ob und inwieweit die Bestimmung von Datenverarbeitungsvorgängen im Wege des Ausschussverfahrens erfolgen sollte.

24. In einer demokratischen Gesellschaft sollten Entscheidungen über Grundprinzipien und Einzelheiten, die sich auf Grundrechte auswirken, im Rahmen eines vollständigen Gesetzgebungsverfahrens, das die geeigneten Kontroll- und Gegenkontrollmechanismen einschließt, getroffen werden. Im vorliegenden Fall bedeutet dies, dass Entscheidungen, die mit erheblichen Auswirkungen auf den Schutz von Privatsphäre und personenbezogenen Daten verbunden sind — wie etwa Verwendungszweck und Modalitäten verbindlich vorgeschriebener Datenverarbeitungstätigkeiten und die Festlegung von Modalitäten der Einführung von IVS in neuen Bereichen — vom Europäischen Parlament und vom Rat und nicht im Wege des Ausschussverfahrens getroffen werden sollten.

25. Vor diesem Hintergrund empfiehlt der EDSB nachdrücklich, dass die Artikel-29-Datenschutzgruppe und der EDSB im Wege einer möglichst frühzeitigen Anhörung schon im Vorfeld der Ausarbeitung einschlägiger Maßnahmen an den Arbeiten des mit Artikel 8 des Vorschlags eingesetzten Ausschusses und an künftigen Initiativen im Hinblick auf die Einführung von IVS beteiligt werden, wenn dies angebracht ist.

26. Ferner nimmt der EDSB die vom Europäischen Parlament zu Artikel 6 des Vorschlags angenommenen Abänderungen zur Kenntnis. Der EDSB stellt zunächst fest, dass die Abänderung in Bezug auf die etwaige Förderung der Verwendung anonymer Daten zwar grundsätzlich zu begrüßen ist, aber nicht alle Datenschutzprobleme lösen wird, da es sich möglicherweise bei vielen der über IVS erhobenen und ausgetauschten Daten um personenbezogene Daten handelt. Damit personenbezogene Daten anonym verarbeitet werden können, darf es keiner Person zu irgendeinem Zeitpunkt der Verarbeitung — unter Berücksichtigung aller Mittel, die vernünftigerweise entweder von dem für die Verarbeitung Verantwortlichen oder von einem Dritten eingesetzt werden könnten — möglich sein, die Daten mit Daten zu verknüpfen, die sich auf eine bestimmte Person beziehen, da diese Daten ansonsten personenbezogene Daten im Sinne von Artikel 2 Buchstabe a der Richtlinie 95/46/EG darstellen ([15]). Des Weiteren empfiehlt der EDSB auf der Grundlage der vom Europäischen Parlament vorgeschlagenen Abänderungen, Artikel 6 des Vorschlags folgendermaßen zu ändern:

— Die Bewertung, ob eine Verarbeitung personenbezogener Daten durch IVS notwendig ist, sollte im Hinblick auf die festgelegten eindeutigen und rechtmäßigen Zwecke der Datenverarbeitung vorgenommen werden. Der Betrieb der IVS-Anwendung ([16]) kann für sich allein genommen kein rechtmäßiger Zweck sein, der die Datenverarbeitung rechtfertigen würde, da die Anwendung lediglich ein Mittel zur Erhebung und zum Austausch von Daten darstellt, deren Verwendung zwangsläufig speziellen Zwecken dienen sollte.

— Die Abänderung betreffend das Verbot der Verwendung von IVS-Daten und -Aufzeichnungen „zu anderen als den in dieser Richtlinie genannten Zwecken“ ([17]) bietet keine ausreichende Schutzgarantie, da insbesondere die spezifischen Zwecke und Dienste, zu denen bzw. für die die IVS verwendet werden, in der Richtlinie nicht präzise und vollständig genug dargelegt werden. In Anbetracht des Umstands, dass die Datenverarbeitungstätigkeiten über IVS vielen sehr unterschiedlichen Zwecken dient, sollte sichergestellt werden, dass die im Laufe der Datenverarbeitung für einen spezifischen Zweck erhobenen Daten nicht für mit diesen Zweckbestimmungen nicht zu vereinbarende Zwecke weiterverarbeitet werden. Daher empfiehlt der EDSB, dass Artikel 6 Absatz 2 noch weiter geändert werden sollte, um dafür zu sorgen, dass IVS-Daten und -Aufzeichnungen „nicht in einer mit diesen Zweckbestimmungen nicht zu vereinbarenden Weise weiterverarbeitet werden“.

III. DATENSCHUTZ BEI INTELLIGENTEN VERKEHRSSYSTEMEN

27. Es ist ganz besonders wichtig, dass die Funktionen der einzelnen an IVS beteiligten Akteure präzisiert werden, um zu bestimmen, wer dafür verantwortlich ist, dass die Systeme in datenschutzrechtlicher Hinsicht ordnungsgemäß funktionieren. Daher sollte genauer angegeben werden, wer die Verantwortung für den Einsatz der Anwendungen und Systeme, deren Ausgestaltung im Wege des Ausschussverfahrens spezifiziert werden soll, tragen sollte und wer in der Kette der Akteure bei der Datenverarbeitung für die Einhaltung der Datenschutzvorschriften verantwortlich (d. h. der für die Datenverarbeitung Verantwortliche) sein sollte. Der EDSB wird im Folgenden auf einige der Anliegen in Bezug auf Schutz der Privatsphäre und Datenschutz hinweisen, denen im Rahmen des Ausschussverfahrens und von den für die Datenverarbeitung Verantwortlichen bei der Konzeption der Anwendungen und der Systemarchitektur Rechnung getragen werden sollte. Ferner wird er einige Datenschutzfragen darlegen, auf die der Gesetzgeber und die für die Datenverarbeitung Verantwortlichen hinsichtlich der Erbringung von IVS-Diensten eingehen müssen.

III.1 „Eingebauter Datenschutz“

28. Die ordnungsgemäße Anwendung der in der Richtlinie 95/46/EG niedergelegten Datenschutzgrundsätze ist eine Grundvoraussetzung für die erfolgreiche Einführung von IVS in der Gemeinschaft. Diese Grundsätze haben Auswirkungen auf die Konzeption der Systemarchitektur und der Anwendungen. Der EDSB empfiehlt, dass bereits in einer frühen Phase der Konzeption von IVS ein Konzept des

([15]) In Erwägungsgrund 26 der Richtlinie 95/46/EG heißt es: „Bei der Entscheidung, ob eine Person bestimmbar ist, sollten alle Mittel berücksichtigt werden, die vernünftigerweise entweder von dem Verantwortlichen für die Verarbeitung oder von einem Dritten eingesetzt werden könnten, um die betreffende Person zu bestimmen.“.

([16]) Nach Abänderung 34 (Aufnahme des neuen Absatzes 1b in Artikel 6) ist Folgendes vorgesehen: „Personenbezogene Daten werden nur dann verarbeitet, wenn ihre Verarbeitung für den Betrieb von IVS-Anwendungen und/oder -Diensten erforderlich ist.“.

([17]) Nach Abänderung 36 wird Artikel 6 Absatz 2 durch folgende Formulierung ergänzt: „ … und nicht zu anderen als den in dieser Richtlinie genannten Zwecken verwendet werden dürfen.“.

„eingebauten Datenschutzes“ für die Festlegung von Architektur, Betrieb und Management der Anwendungen und Systeme beschlossen wird. Dieses Konzept wird insbesondere in der Richtlinie 1999/5/EG in Bezug auf die Konzeption von Funkanlagen und Telekommunikations-Endeinrichtungen hervorgehoben ([18]).

29. Die Konzeption von IVS-Anwendungen und Systemen erfolgt in mehreren Phasen durch unterschiedliche Akteure, die aber alle den Belangen des Schutzes der Privatsphäre und des Datenschutzes Rechnung tragen sollten. Die Kommission und der IVS-Ausschuss tragen zu Anfang besondere Verantwortung bei der Festlegung — im Wege des Ausschussverfahrens — von Maßnahmen, Standardisierungsinitiativen, Verfahren und bewährter Verfahren, die dem Konzept des „eingebauten Datenschutzes“ dienen sollten.

30. Das Konzept des „eingebauten Datenschutzes“ sollte in allen Phasen und bei allen Formen der einzelnen Prozesse gefördert werden.

— Auf organisatorischer Ebene sollte dem Schutz der Privatsphäre bei der Festlegung der erforderlichen Verfahren für den Datenaustausch zwischen allen einschlägigen Datenaustauschbeteiligten Rechnung getragen werden; dies hat möglicherweise direkte Auswirkungen auf die Art des Datenaustauschs und die Art der ausgetauschten Daten.

— Die Anforderungen zum Schutz der Privatsphäre und der Sicherheit sollten in Normen, bewährte Verfahren, technische Spezifikationen und Systeme integriert werden.

— In technischer Hinsicht empfiehlt der EDSB, dass — beispielsweise im Wege des Ausschussverfahrens — für den Schutz der Privatsphäre, den Datenschutz und die Sicherheit in bestimmten Sektoren und/oder für spezielle Zwecke „beste verfügbare Techniken“ ([19]) (BVT) entwickelt werden, mit denen die einzelnen während der gesamten Lebensdauer des Systems geltenden Sicherheitsparameter festgelegt werden sollen, um die Einhaltung des EU-Regelungsrahmens zu gewährleisten.

31. Der EDSB geht im Folgenden auf einige der Aspekte ein, denen bei der Konzeption der Anwendungen und der Systemarchitektur besonders Rechnung zu tragen ist. Sie betreffen die erhobenen Daten, die Interoperabilität der Systeme und die Datensicherheit.

III.1.a) *Datenminimierung und Anonymität*

32. Nach Artikel 6 Absatz 1 Buchstabe c der Richtlinie 95/46/EG dürfen nur personenbezogene Daten erhoben und verarbeitet werden, die für spezielle Zwecke notwendig und erheblich sind.

33. Der EDSB betont, dass die Informationen und Daten, die über ein IVS verarbeitet werden sollen, auf geeignete Weise eingestuft werden müssen, um eine massenhafte und unangebrachte Erhebung personenbezogener Daten zu vermeiden. In diesem Zusammenhang ist Folgendes zu berücksichtigen:

— Herkunft der Daten (ob aus öffentlichen Quellen oder aber von Telekommunikationsunternehmen, IVS-Diensteanbietern, anderen Betreibern, Fahrzeugen, Fahrzeugnutzern oder anderen betroffenen Personen);

— Art der Daten (z. B. aggregierte Informationen, anonyme Daten, personenbezogene Daten, sensible Daten);

— Zweck bzw. Zwecke, für den bzw. die die Daten verwendet werden sollen, und

— bei kooperativen Systemen Präzisierung, welche Daten vom Fahrzeug empfangen bzw. angefordert werden, mit anderen Fahrzeugen und/oder der Infrastruktur oder zwischen Infrastrukturen ausgetauscht werden, und zu welchen Zwecken dies geschieht.

34. Die einzelnen Funktionen sollten mit Blick auf die verfolgten Zwecke sorgfältig analysiert werden, um zu bewerten, ob die Erhebung personenbezogener Daten nötig ist. Der EDSB weist darauf hin, dass ein angemessenes Gleichgewicht zwischen den Grundrechten der betroffenen Personen und den Interessen der einzelnen beteiligten Akteure zu wahren ist, was bedeutet, dass möglichst wenige personenbezogene Daten verarbeitet werden. Soweit wie möglich sollte die Architektur der Anwendungen und Systeme so konzipiert sein, dass nur die personenbezogenen Daten erhoben werden, die im Hinblick auf die zu erfüllenden Zwecke unverzichtbar sind.

35. Wenn personenbezogene Daten nicht oder nur in einer frühen Phase der Verarbeitung benötigt werden, sollten sie erst gar nicht erhoben oder aber so bald wie möglich anonymisiert werden. Es ist daher besonders wichtig, nicht nur zu bewerten, ob Daten erhoben werden müssen, sondern auch, ob sie in den einzelnen Systemen vorgehalten werden müssen. Für alle einzelnen Akteure in der Dienstleistungskette sollten spezifische Fristen für die Speicherung personenbezogener Daten festgelegt werden, die nach der Art der Daten und nach dem Erhebungszweck zu differenzieren sind ([20]). Daher sollten Daten, die für die Erfüllung der mit der Erhebung oder Weiterverarbeitung verbundenen Zwecke nicht länger vorgehalten werden müssen, anonymisiert werden, d. h. nicht länger bestimmten oder bestimmbaren Personen zugeordnet sein.

36. Systemarchitektur und Datenaustauschverfahren sollten so konzipiert sein, dass sie mit der Verarbeitung von möglichst wenigen personenbezogenen Daten auskommen. Diesbezüglich sollten alle Stufen der Verarbeitung und alle Akteure in der Kette der Erbringung von IVS-Diensten berücksichtigt werden. Während einige Daten unter Wahrung der Anonymität ausgetauscht und verarbeitet werden können, sind möglicherweise andere Daten, auch wenn sie

([18]) Vor allem in Artikel 3 Absatz 3 Buchstabe c der Richtlinie 1999/5/EG des Europäischen Parlaments und des Rates vom 9. März 1999 über Funkanlagen und Telekommunikationsendeinrichtungen und die gegenseitige Anerkennung ihrer Konformität.

([19]) Unter der „besten verfügbaren Technik“ ist der effizienteste und fortschrittlichste Entwicklungsstand von Tätigkeiten und entsprechenden Betriebsmethoden zu verstehen, der spezielle Techniken als praktisch geeignet erscheinen lässt, prinzipiell als Grundlage für informationstechnische und sicherheitstechnische Anwendungen und Systeme herangezogen zu werden, die mit den Anforderungen an den Schutz der Privatsphäre und den Datenschutz- und Sicherheitsanforderungen gemäß dem Regelungsrahmen der EU vereinbar sind.

([20]) So regelt beispielsweise die Richtlinie 2006/24/EG des Europäischen Parlaments und des Rates vom 15. März 2006 über die Vorratsspeicherung von Daten, die bei der Bereitstellung öffentlich zugänglicher elektronischer Kommunikationsdienste oder öffentlicher Kommunikationsnetze erzeugt oder verarbeitet werden, und zur Änderung der Richtlinie 2002/58/EG die Vorratsspeicherung von Verkehrsdaten und Standortdaten in Verbindung mit öffentlich zugänglichen elektronischen Kommunikationsdiensten.

ohne Personenbezug ausgetauscht werden, mit Daten verknüpft, die sich auf bestimmte Personen beziehen, und stellen daher personenbezogene Daten im Sinne von Artikel 2 Buchstabe a der Richtlinie 95/46/EG dar ([21]). In Anbetracht der Verwendungszwecke der IVS dürfte schwerlich zu gewährleisten sein, dass ein großer Teil der über sie zusammengetragenen Daten unter Wahrung der Anonymität verarbeitet wird, da bis zu einem gewissen Maß die Identität der betreffenden Person — etwa für die Zwecke der Rechnungsstellung — benötigt wird. Es bedarf im Endergebnis spezieller Maßnahmen technischer, organisatorischer und rechtlicher Art, um in bestimmten Bereichen die Anonymität zu gewährleisten.

III.1.b) *Interoperabilität, Datenqualität und Zweckbindung*

37. Die Interoperabilität der Anwendungen und Systeme ist eine Grundvoraussetzung für die erfolgreiche Einführung der IVS. Es sollen Harmonisierungsarbeiten durchgeführt werden, um die technischen Spezifikationen der in Anwendungen und Systeme zu integrierenden Schnittstellen festzulegen, damit diese Anwendungen und Systeme mit anderen in andere Verkehrsträger und/oder Systeme eingebetteten Anwendungen interagieren können. Während die Interoperabilität der Systeme zur Erleichterung der Erbringung einer Vielfalt von Diensten und zur Sicherstellung einer europaweit kontinuierlichen Erbringung dieser Dienste beitragen wird, birgt sie in datenschutzrechtlicher Hinsicht eine Reihe von Risiken, wie etwa die Gefahr der Zweckentfremdung oder des Missbrauchs der Daten. Eine Vernetzung von Datenbanken sollte unter gebührender Beachtung der Datenschutzgrundsätze und praktischer Sicherheitsvorkehrungen erfolgen ([22]) (siehe auch Abschnitt III.1.c).

38. Der in Artikel 6 Buchstabe d der Richtlinie 95/46/EG aufgeführte Grundsatz der Datenqualität ist im Zusammenhang mit der Interoperabilität von Anwendungen und Systemen von besonderer Bedeutung. Die für die Konzeption der Schnittstellen festzulegenden technischen Spezifikationen sollten die Richtigkeit der durch Vernetzung von Anwendungen und Systemen gewonnenen Daten gewährleisten.

39. Da die Interoperabilität der Systeme die Vernetzung von Datenbanken und den Abgleich der Daten zu weiteren Zwecken erleichtern wird, betont der EDSB, dass jede Vernetzung unter sorgfältiger Beachtung des in Artikel 6 Absatz 1 Buchstabe d der Richtlinie 95/46/EG niedergelegten Grundsatzes der Zweckbindung erfolgen sollte. Es ist besonders wichtig, dass bei der Konzeption der IVS-Systemarchitektur jede nicht den Zwecken der ursprünglichen Erhebung dienende Weiterverwendung ausgeschlossen wird. In das System müssen geeignete Sicherheitsschutzmaßnahmen integriert werden, um einer Zweckentfremdung, einer unbefugten Offenlegung oder einem unbefugten Zugang sowie unerwünschten Nebenwirkungen von Geräten vorzubeugen. So sollten ausreichende Schutzvorkehrungen getroffen werden, damit nicht unbefugte Dritte auf Mobilgeräte zugreifen können, um entgegen den mit dem System verfolgten Zwecken Personen zu identifizieren und ihre Standortänderungen zu verfolgen.

40. Die Rechtmäßigkeit der Vernetzung selbst wird im Einzelfall unter Berücksichtigung der Art der über die Systeme zugänglich gemachten und ausgetauschten Daten und der ursprünglichen Zweckbestimmung der Daten zu bewerten sein.

III.1.c) *Datensicherheit*

41. Die Sicherheit von personenbezogenen Daten ist ein zentraler Aspekt bei der Einführung von IVS. Der EDSB begrüßt die Tatsache, dass die Sicherheit im Aktionsplan und im Richtlinienvorschlag ausdrücklich genannt wird. Die Sicherheit sollte nicht nur während des Betriebs des IVS-Geräts (innerhalb des bordeigenen Systems und im Übertragungsprotokoll) gewährleistet sein, sondern auch über den Betrieb des Geräts hinaus, d. h. in den Datenbanken, in denen die Daten verarbeitet und/oder gespeichert werden. Für alle Verarbeitungsstufen sollten geeignete technische, administrative und organisatorische Anforderungen festgelegt werden, die ein ausreichendes Maß an Sicherheit gemäß den Artikeln 16 und 17 der Richtlinie 95/46/EG (sowie gegebenenfalls den Artikeln 4 und 5 der Richtlinie 2002/58/EG) gewährleisten.

42. Geeignete Sicherheitsmaßnahmen sollten erst dann festgelegt werden, wenn sowohl die konkreten Zwecke, für die IVS eingesetzt werden sollen, als auch die Modalitäten der Verarbeitung einer sorgfältigen Prüfung unterzogen wurden. In diesem Zusammenhang empfiehlt der EDSB, für bestimmte Sektoren und/oder Verwendungszwecke (z. B. für sicherheitsrelevante IVS-Systeme, Frachtmanagementsysteme usw.) Folgenabschätzungen hinsichtlich der Auswirkungen auf die Privatsphäre und den Datenschutz durchzuführen. Mit der Durchführung einer Folgenabschätzung hinsichtlich der Auswirkungen auf die Privatsphäre und den Datenschutz und dem Einsatz der „besten verfügbaren Techniken“ zum Schutz von Privatsphäre und Daten wird dazu beigetragen, dass die am besten geeigneten Sicherheitsmaßnahmen für die jeweilige Verarbeitung festgelegt werden.

III.2 **Weitere Erwägungen zum Schutz von Daten und Privatsphäre bei der Bereitstellung von IVS-Diensten**

43. Die Modalitäten der Einführung von IVS-Diensten müssen auf EU-Ebene weiter harmonisiert werden, damit Diskrepanzen bei der Einführung dieser Dienste vermieden werden. Der EDSB weist diesbezüglich auf die beiden folgenden Aspekte hin, die vor allem unter dem Gesichtspunkt des Schutzes von Privatsphäre und Daten weiterer Untersuchungen bedürfen:

— Die Verwendung von Ortungsinstrumenten für die Bereitstellung standortbasierter öffentlicher und kommerzieller Dienste erfordert zusätzliche Sicherheitsvorkehrungen. In diesem Zusammenhang sollte besonders darauf geachtet werden, ob und wann standortbasierte IVS-Dienste für private bzw. berufliche Zwecke genutzt werden und wie sich die Verwendung eines derartigen Systems auf Personen, die ein Fahrzeug für berufliche Zwecke nutzen, auswirken könnte.

— Bei integrierten Systemen ist es besonders wichtig, dass die Aufgaben und Verantwortlichkeiten der unterschiedlichen Parteien, die an der Einführung von IVS beteiligt sind, eindeutig festgelegt werden.

([21]) Siehe Fußnote 15.

([22]) Vgl. auch die Kommentare des EDSB vom 10. März 2006 zu der Mitteilung der Kommission über die Interoperabilität der europäischen Datenbanken: http://www.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consultation/Comments/2006/06-03-10_Interoperability_DE.pdf

III.2.a) *Sicherheitsvorkehrungen bei der Verwendung von Ortungsinstrumenten für die Bereitstellung standortbasierter IVS-Dienste*

44. Die Einführung von IVS wird die Entwicklung von Anwendungen für die Überwachung und Verfolgung von Waren fördern und die Einführung von standortbasierten kommerziellen und öffentlichen Diensten ermöglichen. Für derartige Dienste werden Technologien wie satellitengestützte Ortung und RFID-Etiketten genutzt werden ([23]). Navigationssysteme und Systeme zur Überwachung und Verfolgung sind für verschiedene Zwecke bestimmt, wie etwa die Fernüberwachung von Fahrzeugen und Fracht (z. B. bei Gefahrgut- oder Tiertransporten), die Erhebung fahrzeugbezogener Entgelte aufgrund verschiedener Parameter wie zurückgelegte Fahrstrecke und Tageszeit (z. B. Mauterhebung, elektronische Mautsysteme) sowie die Überwachung von Fahrern zum Zwecke der Rechtsdurchsetzung, wie etwa die Kontrolle der Lenkzeiten (anhand digitaler Fahrtenschreiber) und die Verhängung von Strafen (durch elektronische Fahrzeugerkennung).

45. Die Verwendung von Standortbestimmungstechnologien stellt unter dem Gesichtspunkt des Schutzes der Privatsphäre einen besonders einschneidenden Eingriff dar, weil sie die Ortung der Fahrer und die Erhebung unterschiedlichster Daten in Bezug auf ihre Fahrgewohnheiten ermöglicht. Wie die Artikel-29-Datenschutzgruppe betont hat ([24]), ist die Verarbeitung von Standortdaten eine besonders sensible Angelegenheit, die die zentrale Frage des Anspruchs von Personen auf Anonymität ihrer Bewegungen berührt und besondere Schutzvorkehrungen erfordert, um die Überwachung von Personen und den Missbrauch von Daten zu verhindern.

46. Der EDSB unterstreicht, dass die Verwendung von Ortungsinstrumenten rechtmäßig sein muss, d.h. sie muss auf einer geeigneten Rechtsgrundlage beruhen, für eindeutige und rechtmäßige Zwecke erfolgen und in einem angemessenen Verhältnis zu den verfolgten Zwecken stehen. Die Rechtmäßigkeit der Datenverarbeitung wird in erheblichem Maße davon abhängen, in welcher Weise und zu welchen Zwecken Ortungsinstrumente eingesetzt werden. Wie die Artikel-29-Datenschutzgruppe in ihrer Stellungnahme zur eCall-Initiative betont hat, wäre „im Hinblick auf die mögliche Aktivierung von eCall-Geräten eine permanente Verbindung derartiger Geräte mit den Kommunikationsnetzen und damit eine permanente Lokalisierbarkeit der Fahrzeuge unter dem Aspekt des Datenschutzes nicht akzeptabel" ([25]). Es ist daher wichtig, dass die konkreten Umstände, unter denen ein Fahrzeug geortet wird, und die damit verbundenen Folgen für den Nutzer präzisiert werden. Auf jeden Fall sollte die Verwendung von Ortungsinstrumenten durch ein legitimes Erfordernis (z.B. die Überwachung des Transports von Waren) gerechtfertigt und streng auf das für diesen Zweck erforderliche Maß begrenzt werden. Daher ist es wichtig, dass genau festgelegt wird, welche Standortdaten erhoben werden, wo und wie lange sie gespeichert werden und mit wem und für welche Zwecke sie ausgetauscht werden und dass alle erforderlichen Maßnahmen ergriffen werden, um eine unsachgemäße oder missbräuchliche Verwendung der Daten zu vermeiden.

47. Darüber hinaus ist die Verarbeitung von Standortdaten in Bezug auf die Nutzer von öffentlichen Kommunikationsnetzen oder öffentlich zugänglichen Kommunikationsdiensten in Artikel 9 der Richtlinie 2002/58/EG streng geregelt. Dort ist insbesondere festgelegt, dass Standortdaten nur dann verarbeitet werden dürfen, wenn sie anonymisiert wurden oder wenn der Nutzer seine Einwilligung erteilt hat. Dies bedeutet, dass die Nutzer vor ihrer Zustimmung zur Verwendung eines Ortungsinstruments angemessen unterrichtet werden müssen, unter anderem darüber, welche Standortdaten verarbeitet werden, für welche Zwecke und wie lange das geschieht, und ob die Daten zum Zwecke der Bereitstellung des Dienstes mit Zusatznutzen an einen Dritten weitergegeben werden. Die Nutzer müssen die Möglichkeit haben, die Verarbeitung von Standortdaten für jede Verbindung zum Netz und jede Übertragung einer Nachricht auf einfache Weise und gebührenfrei zeitweise zu untersagen. Die Verarbeitung der Standortdaten sollte strikt auf Personen beschränkt werden, die im Auftrag des Betreibers des öffentlichen Kommunikationsnetzes oder öffentlich zugänglichen Kommunikationsdienstes oder des Dritten, der den Dienst mit Zusatznutzen anbietet, handeln.

48. Werden Standortdaten von Fahrzeugen erhoben, die im Rahmen einer beruflichen Tätigkeit genutzt werden, sind zusätzliche Sicherheitsvorkehrungen zu treffen, um zu verhindern, dass die Standortbestimmungstechnologie zur unrechtmäßigen Überwachung von Arbeitnehmern genutzt wird. Auf jeden Fall sollte die Verarbeitung auf Standortdaten beschränkt sein, die während der Arbeitszeit erhoben werden; folglich müssen die Arbeitnehmer die Möglichkeit haben, die Standortbestimmungsfunktion außerhalb der Arbeitszeit und/oder während der privaten Nutzung des Fahrzeugs auszuschalten.

49. Es besteht die Gefahr, dass Dritte (z. B. Versicherungsunternehmen, Arbeitgeber und Strafverfolgungsbehörden) Zugang zu Daten verlangen, die durch Navigations- und Ortungssysteme für rechtmäßige und festgelegte Zwecke erhoben wurden (z. B. die Überwachung von Waren, die elektronische Mauterhebung usw.), um diese Daten für sekundäre Zwecke zu nutzen, wie etwa die Kontrolle von Lenk- und Ruhezeiten oder die Überprüfung der Einhaltung der Straßenverkehrsvorschriften und die Verhängung von Strafen. Ein Zugriff auf Daten für sekundäre Zwecke ist grundsätzlich nicht statthaft, wenn dieser Zugriff zu Zwecken dient, die mit den Zwecken, für die die Daten erhoben wurden, nicht vereinbar sind. Abweichend von diesem Grundsatz kann ein Zugriff nur dann gestattet werden, wenn die Bedingungen für diesen Zugriff die strengen Kriterien nach Artikel 13 der Richtlinie 95/46/EG erfüllen. Infolgedessen sollte ein Zugriff auf Standortdaten durch Dritte nur im Einklang mit dem Recht und in transparenter Weise gewährt werden und auf eine rechtliche Maßnahme

([23]) Siehe die durch die Verwendung von RFID aufgeworfenen Fragen hinsichtlich des Schutzes von Privatsphäre und Daten in der Stellungnahme des Europäischen Datenschutzbeauftragten zu der Mitteilung der Kommission an das Europäische Parlament, den Rat, den Europäischen Wirtschafts- und Sozialausschuss und den Ausschuss der Regionen zum Thema „Funkfrequenzkennzeichnung (RFID) in Europa: Schritte zu einem ordnungspolitischen Rahmen" (KOM(2007) 96); ABl. C 101 vom 23.4.2008, S. 1. http://www.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consultation/Opinions/2007/07-12-20_RFID_DE.pdf

([24]) Artikel-29-Datenschutzgruppe, Stellungnahme zur Nutzung von Standortdaten für die Bereitstellung von Diensten mit Zusatznutzen, WP 115, November 2005. http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2005/wp115_de.pdf

([25]) Siehe das in Fußnote 10 auf Seite 5 genannte Dokument WP 125 zur Initiative eCall.

gestützt sein, die geeignete Verfahren und Modalitäten für den Zugriff auf die Daten für bestimmte Zwecke festlegt und ausreichende Garantien für die betroffenen Personen entsprechend den weiteren Zwecken, für die ihre Daten verwendet werden könnten, vorsieht.

III.2.b) *Aufgaben und Verantwortlichkeiten von IVS-Akteuren*

50. Es ist noch nicht klar, wer für die einzelnen Teile der Verarbeitung verantwortlich sein wird. In vielen Fällen werden die IVS-Diensteanbieter wahrscheinlich für die Verarbeitung der Daten verantwortlich sein, entweder allein (für die personenbezogenen Daten, die für die Bereitstellung ihrer eigenen IVS-Dienste verarbeitet werden) oder gemeinsam (in den Fällen, in denen die Verarbeitung zusammen mit anderen für die Datenverarbeitung Verantwortlichen durchgeführt wird). Für Betreiber, die in unterschiedlichen Eigenschaften an IVS beteiligt sind, sollten Aufgaben und Verantwortlichkeiten als für die Verarbeitung Verantwortlicher und als Auftragsverarbeiter für jeden Teil der Verarbeitung eindeutig festgelegt werden (z. B. Telekommunikationsbetreiber, die sowohl Kommunikationsdienste als auch IVS-Dienste erbringen).

51. Diejenigen Personen, die als für die Datenverarbeitung Verantwortliche agieren, werden dafür sorgen müssen ([26]), dass die Systeme und Dienste alle Datenschutzanforderungen erfüllen, und insbesondere die Aufgabe haben, Systeme mit „eingebautem Datenschutz" einzurichten, die den Grundsätzen der Datenqualität und der Zweckbindung entsprechen und ein ausreichendes Maß an Datensicherheit gewährleisten, wie vorstehend unter III.1 beschrieben.

52. Die für die Verarbeitung Verantwortlichen werden dafür sorgen müssen, dass auf allen Ebenen der Kette von Akteuren, die an der Einführung von IVS beteiligt sind, geeignete Sicherheitsvorkehrungen getroffen werden. Dazu wird insbesondere erforderlich sein, dass sie mit allen Interessenträgern, die am Austausch und an der Verarbeitung von Daten beteiligt sind, geeignete vertragliche Vereinbarungen eingehen, die angemessene Datenschutzgarantien bieten (insbesondere hinsichtlich der Artikel 16 und 17 der Richtlinie 95/46/EG und der Artikel 4 und 5 der Richtlinie 2002/58/EG). Wichtig ist unter dem Gesichtspunkt des Datenschutzes, dass die für die Datenverarbeitung Verantwortlichen dafür Sorge tragen müssen, dass der Datenschutz auf allen Verarbeitungsstufen gewährleistet ist und dass sie überdies für die Verarbeitung verantwortlich bleiben und ihre Verantwortlichkeit nicht vertraglich ausschließen können.

IV. **FAZIT**

53. Der EDSB begrüßt den von der Kommission vorgeschlagenen Plan zur Einführung von IVS, der darauf abzielt, die Datenverarbeitungsprozesse europaweit zu harmonisieren, um die Bereitstellung von IVS-Diensten zu erleichtern, und in dem der Datenschutz als Grundvoraussetzung für die ordnungsgemäße Einführung von IVS in Europa genannt wird.

54. Der EDSB stellt fest, dass mit der vorgeschlagenen Richtlinie ein allgemeiner Rahmen vorgegeben wird, der eine Reihe von Fragen zum Schutz der Privatsphäre und zum Datenschutz aufwirft, auf die auf der Ebene der EU und auf einzelstaatlicher Ebene weiter eingegangen werden muss:

— Es besteht die Gefahr, dass die mangelnde Präzision des vorgeschlagenen Rechtsrahmens zu Diskrepanzen bei der Einführung von IVS in Europa führen wird, die wiederum bewirken, dass es in Europa zu unterschiedlichen Datenschutzniveaus kommt. Der EDSB betont, dass es in Bezug auf diese Fragen einer weiteren Harmonisierung auf EU-Ebene bedarf, um die noch offenen Fragen zu klären (etwa die Bestimmung der Funktionen und Zuständigkeiten der IVS-Akteure, die Frage, welche spezifischen IVS-Anwendungen und -Systeme in Fahrzeuge zu integrieren sind, die Ausarbeitung einheitlicher Aufträge zur Erbringung von IVS-Diensten, die spezifischen Verwendungszwecke von IVS und die entsprechenden Einzelheiten der Verwendung usw.). Es ist besonders wichtig, zu bestimmen, wer bei der vorgenommenen Datenverarbeitung der für die Verarbeitung Verantwortliche sein wird, da dieser die Verantwortung dafür tragen wird, dass den Belangen des Schutzes der Privatsphäre und des Datenschutzes auf allen Ebenen der Verarbeitungskette Rechnung getragen wird.

— Entscheidungen über bestimmte Modalitäten der Verarbeitung, die sich erheblich auf das Recht der Personen auf Schutz ihrer Privatsphäre und ihrer Daten auswirken könnten, sollten vom Europäischen Parlament und vom Rat und nicht im Wege des Ausschussverfahrens getroffen werden.

— Es ist von höchster Bedeutung, dass dem Schutz der Privatsphäre und dem Datenschutz bereits in der Anfangsphase und dann auf allen weiteren Stufen der Verarbeitung Rechnung getragen wird; der Rückgriff auf das Konzept des „eingebauten Datenschutzes" bei der Konzeption von IVS-Anwendungen und -Systemen sollte gefördert werden und das Konzept in Normen, bewährte Verfahren, technische Spezifikationen und Systeme Eingang finden.

— Jede Vernetzung von Anwendungen und Systemen sollte unter gebührender Beachtung der Datenschutzgrundsätze und praktischer Sicherheitsvorkehrungen erfolgen.

— Angesichts der Ungewissheiten, die hinsichtlich der Modalitäten der Einführung von IVS weiterhin bestehen, begrüßt der EDSB ganz besonders die in der Mitteilung der Kommission vorgebrachte Initiative, dass bis 2011 eine Folgenabschätzung hinsichtlich der Auswirkungen auf die Privatsphäre durchgeführt werden soll. Der EDSB empfiehlt zudem nachdrücklich, dass Folgenabschätzungen hinsichtlich der Auswirkungen auf die Privatsphäre und den Datenschutz für bestimmte Sektoren und/oder Verwendungszwecke durchgeführt werden, um geeignete Sicherheitsmaßnahmen festzulegen, und dass die „besten verfügbaren Techniken" für den Schutz von Privatsphäre und Daten sowie für die Sicherheit in IVS entwickelt wird.

— Der EDSB betont ferner, dass die Mitgliedstaaten die Verantwortung dafür tragen, dass die Richtlinie ordnungsgemäß umgesetzt wird, damit die IVS-Betreiber Systeme und Dienste entwickeln, die europaweit ein angemessenes Datenschutzniveau bieten.

([26]) Siehe Fußnote 13.

— Die für die Datenverarbeitung verantwortlichen Akteure, die IVS-Dienste bereitstellen, müssen geeignete Sicherheitsvorkehrungen treffen, damit die Verwendung von Standortbestimmungstechnik, wie etwa satellitengestützte Ortung oder RFID-Etiketten, nicht die Privatsphäre von Personen verletzt, die Fahrzeuge rein privat oder zu beruflichen Zwecken nutzen. Dies erfordert insbesondere, dass die Verarbeitung streng auf die Daten beschränkt wird, die für den betreffenden Zweck benötigt werden, wobei dafür zu sorgen ist, dass geeignete Sicherheitsmaßnahmen in die Systeme integriert werden, damit die Standortdaten nicht Unbefugten zugänglich gemacht werden, und den Nutzern ein wirksames Mittel zur Deaktivierung des Ortungsgeräts bzw. der Ortungsfunktion zur Verfügung gestellt werden.

55. Der EDSB empfiehlt, Artikel 6 des Vorschlags im Einklang mit der Richtlinie 95/46/EG folgendermaßen zu ändern:

— Bei der Datenverarbeitung über IVS sollte die Datenminimierung gefördert werden. Diesbezüglich wird empfohlen, Artikel 6 Absatz 1 Buchstabe b des Vorschlags wie folgt zu formulieren: „Personenbezogene Daten werden nur dann verarbeitet, wenn ihre Verarbeitung für den spezifischen Verwendungszweck der IVS erforderlich ist und im Einklang mit einer geeigneten Rechtsgrundlage erfolgt."

— Es ist wichtig, dass die über interoperable Systeme verarbeiteten personenbezogenen Daten nicht für andere als die ihrer Erhebung zugrundeliegenden Zwecke weiterverwendet werden. Daher wird empfohlen, Artikel 6 Absatz 2 folgendermaßen zu formulieren: „ … und nicht zu anderen als zu den ihrer Erhebung zugrundeliegenden Zwecken in einer mit diesen Zwecken nicht zu vereinbarenden Weise verwendet werden dürfen".

— Der EDSB schlägt vor, in Artikel 6 ausdrücklich auf das Konzept des „eingebauten Datenschutzes" hinsichtlich der Konzeption von IVS-Anwendungen und -Systemen zu verweisen. Ferner empfiehlt er, dass die Artikel-29-Datenschutzgruppe und der EDSB über weitere Maßnahmen in dieser Frage, die im Wege des Ausschussverfahrens getroffen werden, unterrichtet und dazu konsultiert werden.

56. Der EDSB empfiehlt ferner, eine Bezugnahme auf diese Konsultation in die Erwägungsgründe des Vorschlags aufzunehmen.

57. Aufgrund dieser Erwägungen empfiehlt der EDSB, dass die Datenschutzbehörden — insbesondere über die Artikel-29-Datenschutzgruppe — und der EDSB im Wege einer rechtzeitig vor der Ausarbeitung einschlägiger Maßnahmen durchzuführenden Konsultation eng in die Initiativen zur Einführung von IVS einbezogen werden.

Brüssel, den 22. Juli 2009

Peter HUSTINX

Europäischer Datenschutzbeauftragter