STELLUNGNAHMEN

DER EUROPÄISCHE DATENSCHUTZBEAUFTRAGTE

Stellungnahme des Europäischen Datenschutzbeauftragten zum Vorschlag der Kommission für eine Verordnung des Europäischen Parlaments und des Rates über die Verwaltungszusammenarbeit mithilfe des Binnenmarkt-Informationssystems („IMI")

(2012/C 48/02)

DER EUROPÄISCHE DATENSCHUTZBEAUFTRAGTE —

gestützt auf den Vertrag über die Arbeitsweise der Europäischen Union, insbesondere auf Artikel 16,

gestützt auf die Charta der Grundrechte der Europäischen Union, insbesondere auf Artikel 7 und 8,

gestützt auf die Richtlinie 95/46/EG des Europäischen Parlaments und des Rates vom 24. Oktober 1995 über den Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr [1],

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 [2],

gestützt auf ein Ersuchen um eine Stellungnahme gemäß Artikel 28 Absatz 2 der Verordnung (EG) Nr. 45/2001,

HAT FOLGENDE STELLUNGNAHME ANGENOMMEN:

1. EINLEITUNG

1.1 Konsultation des EDSB

1. Am 29. August 2011 nahm die Kommission einen Vorschlag für eine Verordnung („Vorschlag" oder „vorgeschlagene Verordnung") des Europäischen Parlaments und des Rates über die Verwaltungszusammenarbeit mithilfe des Binnenmarkt-Informationssystems („IMI") an [3]. Der Vorschlag wurde dem EDSB noch am selben Tag zur Konsultation übermittelt.

2. Vor der Annahme des Vorschlags hatte der EDSB Gelegenheit, informelle Kommentare zu dem Vorschlag sowie zuvor auch zur Mitteilung der Kommission „Eine bessere Governance für den Binnenmarkt mittels verstärkter administrativer Zusammenarbeit: Eine Strategie für den Ausbau und die Weiterentwicklung des Binnenmarkt-Informationssystems (‚IMI')" („IMI-Strategie-Mitteilung") abzugeben [4], die dem Vorschlag voranging. Viele dieser Kommentare wurden im Vorschlag berücksichtigt, sodass im Ergebnis die Datenschutzgarantien im Vorschlag gestärkt wurden.

3. Der EDSB begrüßt seine formelle Konsultation durch die Kommission und den Verweis auf diese Stellungnahme in der Präambel des Vorschlags.

1.2 Ziele und Anwendungsbereich des Vorschlags

4. Das IMI ist ein IT-Tool, mit dessen Hilfe die zuständigen Behörden in den Mitgliedstaaten im Zusammenhang mit der Anwendung der Binnenmarktrechtsvorschriften untereinander Informationen austauschen. Mit Hilfe des IMI können nationale, regionale und lokale Behörden in EU-Mitgliedstaaten schnell und einfach mit ihren Partnereinrichtungen in anderen europäischen Ländern kommunizieren. Dabei werden auch personenbezogene Daten einschließlich sensibler Daten verarbeitet.

5. Das IMI war ursprünglich als Instrument für den Informationsaustausch zwischen zwei Teilnehmern im Rahmen der Richtlinie über die Anerkennung von Berufsqualifikationen [5] und der Dienstleistungsrichtlinie [6] konzipiert. Das IMI hilft den Nutzern bei der Suche nach der richtigen Behörde in einem anderen Land und bei der Kommunikation mit dieser Behörde mit Hilfe von bereits übersetzten Standardfragen und -antworten [7].

[1] ABl. L 281 vom 23.11.1995, S. 31.
[2] ABl. L 8 vom 12.1.2001, S. 1.
[3] KOM(2011) 522 endgültig.
[4] KOM(2011) 75.
[5] Richtlinie 2005/36/EG des Europäischen Parlaments und des Rates vom 7. September 2005 über die Anerkennung von Berufsqualifikationen (ABl. L 255 vom 30.9.2005, S. 22).
[6] Richtlinie 2006/123/EG des Europäischen Parlaments und des Rates vom 12. Dezember 2006 über Dienstleistungen im Binnenmarkt (ABl. L 376 vom 27.12.2006, S. 36).
[7] Zur Illustration eine typische Frage, die sensible Daten enthält: „Ist das beigefügte Dokument ein ordnungsgemäßer Beleg dafür, dass (gegen den zuwandernden Berufsangehörigen) kein Verdacht oder Verbot der Ausübung einschlägiger beruflicher Tätigkeit wegen schwerer beruflicher Verfehlung oder einer Straftat besteht?".

6. Das IMI ist jedoch als flexibles, horizontales System gedacht, das verschiedene Bereiche der Binnenmarktrechtsvorschriften unterstützen kann. In Zukunft soll seine Nutzung schrittweise auf weitere Rechtsbereiche ausgedehnt werden.

7. Auch die Funktionalitäten des IMI sollen ausgebaut werden. Neben dem Informationsaustausch zwischen zwei Teilnehmern sind weitere Funktionalitäten vorgesehen oder bereits umgesetzt, wie „Meldeverfahren, Warnmechanismen, Amtshilfevereinbarungen und Problemlösungsverfahren" ([8]) sowie „Datenspeicher, auf die IMI-Akteure künftig zugreifen können" ([9]). Bei vielen, wenn auch nicht allen dieser Funktionalitäten kann es auch zur Verarbeitung personenbezogener Daten kommen.

8. Ziel des Vorschlags ist es, eine klare Rechtsgrundlage und einen umfassenden Datenschutzrahmen für IMI zu schaffen.

1.3 **Hintergrund des Vorschlags: ein schrittweiser Ansatz zum Aufbau eines umfassenden Datenschutzrahmens für IMI**

9. Im Frühjahr 2007 forderte die Kommission eine Stellungnahme der Artikel 29-Datenschutzgruppe („WP29") zur Überprüfung der datenschutzrechtlichen Implikationen des IMI an. Die Artikel 29-Datenschutzgruppe gab ihre Stellungnahme am 20. September 2007 ab ([10]). Die Stellungnahme empfahl der Kommission die Schaffung einer klareren Rechtsgrundlage und spezifische Datenschutzgarantien für den Datenaustausch innerhalb des IMI. Der EDSB nahm aktiv an den Arbeiten der IMI-Unterarbeitsgruppe teil und schloss sich den Schlussfolgerungen der Stellungnahme der Artikel 29-Datenschutzgruppe an.

10. In der Folge beriet der EDSB die Kommission weiter bei der schrittweisen Einführung eines umfassenderen Datenschutzrahmens für das IMI ([11]). Im Rahmen dieser Zusammenarbeit und seit der Annahme seiner Stellungnahme zur Umsetzung des IMI am 22. Februar 2008 ([12]), hat sich der EDSB immer wieder für einen im ordentlichen Gesetzgebungsverfahren angenommenen neuen Rechtsakt ausgesprochen, mit dem ein umfassenderer Datenschutzrahmen für das IMI und Rechtssicherheit geschaffen werden soll. Der Vorschlag für einen solchen Rechtsakt liegt nun vor ([13]).

([8]) Siehe Erwägungsgrund 10.
([9]) Siehe Artikel 13 Absatz 2.
([10]) Stellungnahme Nr. 7/2007 der Artikel 29-Datenschutzgruppe zu Fragen des Datenschutzes im Zusammenhang mit dem Binnenmarkt-Informationssystem, WP140. Abrufbar unter http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2007/wp140_de.pdf
([11]) Die wichtigsten Dokumente zu dieser Zusammenarbeit sind zu finden auf der IMI-Website der Kommission unter http://ec.europa.eu/internal_market/imi-net/data_protection_en.html sowie auf der Website des EDSB unter http://www.edps.europa.eu
([12]) Stellungnahme des EDSB zur Entscheidung 2008/49/EG der Kommission vom 12. Dezember 2007 über den Schutz personenbezogener Daten bei der Umsetzung des Binnenmarktinformationssystems (ABl. C 270 vom 25.10.2008, S. 1).
([13]) Auch die Artikel 29-Datenschutzgruppe plant, sich zu dem Vorschlag zu äußern. Der EDSB hat die Arbeiten in der einschlägigen Unterarbeitsgruppe der Artikel 29-Datenschutzgruppe verfolgt und hierzu Kommentare vorgelegt.

2. **ANALYSE DES VORSCHLAGS**

2.1 **Generelle Meinung des EDSB zum Vorschlag und zu den Hauptproblemen bei der Regulierung des IMI**

11. Generell beurteilt der EDSB das IMI positiv. Der EDSB unterstützt das Ziel der Kommission, ein elektronisches System für den Informationsaustausch aufzubauen und dessen Datenschutzaspekte zu regeln. Ein solches gestrafftes System dürfte nicht nur die Effizienz der Zusammenarbeit steigern, sondern auch dafür sorgen, dass die Datenschutzgesetze einheitlicher eingehalten werden. Dies könnte durch klare Vorgaben dazu erreicht werden, welche Informationen mit wem und unter welchen Bedingungen ausgetauscht werden dürfen.

12. Der EDSB begrüßt ferner, dass die Kommission einen horizontalen Rechtsakt für das IMI in Form einer Verordnung des Rates und des Parlaments vorschlägt. Er ist erfreut darüber, dass in dem Vorschlag ausführlich auf die größten Datenschutzprobleme des IMI eingegangen wird. Seine Kommentare sind vor diesem positiven Grundtenor zu lesen.

13. Dessen ungeachtet möchte der EDSB davor warnen, dass der Aufbau eines einzigen zentralisierten elektronischen Systems für mehrere Bereiche der Verwaltungszusammenarbeit auch Risiken schafft. Dazu gehört vor allem, dass mehr Daten weiter verbreitet werden könnten, als für eine wirksame Zusammenarbeit eigentlich erforderlich wäre, und dass Daten — auch möglicherweise veraltete und unrichtige Daten — länger als notwendig im System verbleiben. Auch die Sicherheit des in 27 Mitgliedstaaten abfragbaren Informationssystems ist ein Problem, da das Gesamtsystem nur so sicher sein wird wie das schwächste Glied in der Kette es zulässt.

Zentrale Herausforderungen

14. Im Hinblick auf den Rechtsrahmen für das IMI, der mit der vorgeschlagenen Verordnung geschaffen werden soll, weist der EDSB auf zwei zentrale Herausforderungen hin:

— es muss Kohärenz bei gleichzeitiger Wahrung der Vielfalt gewährleistet sein, und

— es muss ein ausgewogenes Verhältnis zwischen Flexibilität und Rechtssicherheit gefunden werden.

15. Diese zentralen Herausforderungen sind wichtige Eckpunkte und bestimmten zu einem großen Teil die Auffassungen, die der EDSB in dieser Stellungnahme vertritt.

Kohärenz bei gleichzeitiger unter Wahrung der Vielfalt

16. Zunächst einmal gilt, dass das IMI ein System ist, das in 27 Mitgliedstaaten genutzt wird. Beim derzeitigen Stand der Harmonisierung europäischer Rechtsvorschriften bestehen erhebliche Unterschiede zwischen den nationalen Verwaltungsverfahren sowie zwischen den nationalen Datenschutzvorschriften. Das IMI muss so gestaltet sein, dass Nutzer in jedem einzelnen dieser 27 Mitgliedstaaten beim Austausch personenbezogener Daten über das IMI in der Lage sind, ihre eigenen nationalen Gesetze einschließlich der Datenschutzvorschriften einzuhalten. Dabei müssen die betroffenen Personen aber sichergehen können,

dass ihre Daten unabhängig von einer Datenübertragung per IMI an einen anderen Mitgliedstaat einheitlich geschützt sind. Kohärenz bei gleichzeitiger Wahrung der Vielfalt ist eine der zentralen Herausforderungen beim Aufbau sowohl der technischen wie der rechtlichen Infrastruktur des IMI. Unnötige Komplexität und Fragmentierung sollten vermieden werden. Die Datenverarbeitungsvorgänge innerhalb des IMI müssen transparent sein, und die Verantwortlichkeiten für Entscheidungen bezüglich der Gestaltung des Systems, seine Pflege in der täglichen Praxis und Nutzung und auch für die Überwachung des Systems müssen klar zugeordnet sein.

Ausgewogenes Verhältnis zwischen Flexibilität und Rechtssicherheit

17. Zweitens ist das IMI im Gegensatz zu anderen IT-Großsystemen wie dem Schengener Informationssystem, dem Visa-Informationssystem, dem Zoll-Informationssystem oder Eurodac, in deren Mittelpunkt die Zusammenarbeit in besonderen, klar umrissenen Bereichen steht, ein horizontales Instrument für den Informationsaustausch und kann zur Erleichterung des Informationsaustauschs in vielen verschiedenen Politikbereichen eingesetzt werden. Es ist ferner vorgesehen, den Anwendungsbereich des IMI schrittweise auf weitere Politikbereiche auszudehnen; damit können sich seine Funktionalitäten ändern und bislang noch nicht spezifizierte Arten der Verwaltungszusammenarbeit umfassen. Diese Besonderheiten des IMI erschweren eine klare Definition der Funktionalitäten des Systems und des Datenaustauschs, der im System stattfinden kann. Somit ist es auch schwieriger, eindeutig die angemessenen Datenschutzgarantien festzulegen.

18. Der EDSB räumt ein, dass Bedarf an Flexibilität besteht und nimmt den Wunsch der Kommission zur Kenntnis, die Verordnung „zukunftsfest" zu machen. Dies sollte jedoch nicht zur Folge haben, dass es bei den Funktionalitäten des Systems und den umzusetzenden Datenschutzgarantien an Klarheit oder Rechtssicherheit mangelt. Aus diesem Grund sollte der Vorschlag überall dort, wo dies möglich ist, spezifischer formuliert sein und nicht nur die Hauptgrundsätze des Datenschutzes wiederholen, die in der Richtlinie 95/46/EG und in der Verordnung (EG) Nr. 45/2001 festgelegt sind ([14]).

2.2 **Anwendungsbereich des IMI und seine geplante Ausdehnung (Artikel 3 und 4)**

2.2.1 *Einleitung*

19. Der EDSB begrüßt den im Vorschlag klar abgesteckten derzeitigen Anwendungsbereich des IMI und die Tatsache, dass in Anhang I die einschlägigen Rechtsakte der Union aufgeführt werden, auf deren Grundlage Informationen ausgetauscht werden dürfen. Dazu gehört die Zusammenarbeit aufgrund der entsprechenden Bestimmungen der Richtlinie über die Anerkennung von Berufsqualifikationen, der Dienstleistungsrichtlinie und der Richtlinie über die Ausübung der Patientenrechte in der grenzüberschreitenden Gesundheitsversorgung ([15]).

20. Da der Anwendungsbereich des IMI erweitert werden soll, sind mögliche Ziele einer Erweiterung in Anhang II aufgeführt. Punkte aus Anhang II können mit einem nach einer Folgenabschätzung von der Kommission angenommenen delegierten Rechtsakt in den Anhang I verschoben werden ([16]).

21. Der EDSB begrüßt diese Vorgehensweise, da sie i) den Anwendungsbereich des IMI klar abgrenzt und ii) Transparenz gewährleistet, gleichzeitig aber iii) Flexibilität in Fällen ermöglicht, in denen das IMI in der Zukunft für weitere Arten des Informationsaustausches eingesetzt werden wird. Sie gewährleistet ferner, dass kein Informationsaustausch über das IMI erfolgen kann ohne i) eine angemessene Rechtsgrundlage in einem Binnenmarktrechtsakt, der den Informationsaustausch erlaubt oder vorsieht ([17]), und ii) einen Verweis auf diese Rechtsgrundlage in Anhang I der Verordnung.

22. Dessen ungeachtet sind aber noch nicht alle Frage geklärt, die den Anwendungsbereich des IMI, die Politikbereiche, auf die das IMI ausgedehnt werden könnte sowie die Funktionalitäten der IMI betreffen, die das IMI umfasst bzw. künftig umfassen könnte.

23. Erstens kann nicht ausgeschlossen werden, dass der Anwendungsbereich des IMI über die in Anhang I und Anhang II aufgeführten Politikbereiche hinaus erweitert wird. Dies könnte geschehen, wenn der Einsatz des IMI für bestimmte Arten des Informationsaustauschs nicht in einem delegierten Rechtsakt der Kommission, sondern in einem in Anhang II nicht vorgesehenen Fall in einem von Parlament und Rat angenommenen Rechtsakt geregelt wird ([18]).

([14]) Siehe hierzu auch unsere Kommentare in Abschnitt 2.2 zur geplanten Ausdehnung des IMI.

([15]) Richtlinie 2011/24/EG des Europäischen Parlaments und des Rates vom 9. März 2011 über die Ausübung der Patientenrechte in der grenzüberschreitenden Gesundheitsversorgung (ABl. L 88 vom 4.4.2011, S. 45).

([16]) Im Verordnungsentwurf selber wird eine Folgenabschätzung nicht erwähnt. Auf S. 7 der Begründung des Vorschlags erläutert die Kommission jedoch, sie werde ermächtigt sein, „im Anschluss an eine Bewertung der technischen Durchführbarkeit, der Kosteneffizienz, der Benutzerfreundlichkeit und der Gesamtauswirkungen auf das System sowie gegebenenfalls der Ergebnisse einer etwaigen Testphase die Liste der in Anhang I genannten Bereiche im Wege eines delegierten Rechtsakts zu aktualisieren".

([17]) Dies gilt mit Ausnahme von SOLVIT (siehe Anhang II I(1)), wo es nur „soft law", nämlich eine Empfehlung der Kommission, gibt. Aus datenschutzrechtlicher Sicht könnte nach Auffassung des EDSB im Sonderfall SOLVIT die Rechtgrundlage für die Verarbeitung in der „Einwilligung" der betroffenen Person gefunden werden.

([18]) Dies kann auf Anregung der Kommission geschehen, es lässt sich aber auch nicht ausschließen, dass der Gedanke an den Einsatz des IMI in einem bestimmten Politikbereich erst später im Gesetzgebungsverfahren aufkommt und dann vielleicht vom Parlament oder vom Rat vorgeschlagen wird. So war es bereits der Fall bei der Richtlinie über die Ausübung der Patientenrechte in der grenzüberschreitenden Gesundheitsversorgung. Bei einem solchen Fall müsste klarer geregelt sein, welches „Verfahren" für die Erweiterung gilt; bisher scheint man sich fast ausschließlich mit dem Fall der Erweiterung per delegiertem Rechtsakt befasst zu haben (vgl. die Bestimmungen zu Folgenabschätzung, zu delegierten Rechtsakten und zur Aktualisierung von Anhang I).

24. Zweitens mag in einigen Fällen die Ausdehnung des Anwendungsbereichs auf neue Politikbereiche nur wenige oder gar keine Änderungen der bestehenden Funktionalitäten des Systems erfordern ([19]), während andere Erweiterungen neue und andere Funktionalitäten oder erhebliche Änderungen an bestehenden Funktionalitäten notwendig machen:

— Im Vorschlag wird zwar auf mehrere bestehende oder geplante Funktionalitäten verwiesen, doch sind diese Verweise häufig nicht ausreichend klar oder ausreichend detailliert. Dies gilt, wenn auch in unterschiedlichem Ausmaß, für die Verweise auf Warnungen, externe Akteure, Datenspeicher, Amtshilfevereinbarungen und Problemlösungsverfahren ([20]). Als Beispiel sei das Wort „Warnung" herausgegriffen, mit dem auf eine bestehende Kernfunktionalität verwiesen wird; es wird nur ein einziges Mal erwähnt, nämlich in Erwägungsgrund 10;

— nach der vorgeschlagenen Verordnung können neue Arten von Funktionalitäten beschlossen werden, die im Vorschlag überhaupt nicht erwähnt werden;

— bisher wurde das IMI stets als IT-Tool für den Informationsaustausch beschrieben, also als Kommunikationsinstrument (siehe z. B. Artikel 3 des Vorschlags). Einige der im Vorschlag aufgeführten Funktionalitäten einschließlich des „Datenspeichers" scheinen jedoch weit darüber hinauszugehen. Auch die vorgeschlagene Verlängerung der Aufbewahrungsfristen deutet eher auf eine Entwicklung in Richtung „Datenbank" hin. Mit derartigen Entwicklungen würde sich der Charakter des IMI grundlegend wandeln ([21]).

2.2.2 *Empfehlungen*

25. Zur Beseitigung dieser Unsicherheiten empfiehlt der EDSB einen zweigleisigen Ansatz. Als erstes schlägt er vor, dass bereits absehbare Funktionalitäten klarer formuliert und ausdrücklicher angesprochen werden, und als zweites sollten angemessene Verfahrensgarantien angewandt werden, um sicherzustellen, dass der Datenschutz auf bei der künftigen Weiterentwicklung des IMI sorgfältig beachtet wird.

Klarere Formulierung bereits verfügbarer oder absehbarer Funktionalitäten (z. B. Informationsaustausch zwischen zwei Teilnehmern, Warnmechanismen, Problemlösungsverfahren und externe Akteure)

26. Der EDSB empfiehlt, in der Verordnung deutlichere Aussagen zu bereits bekannten Funktionalitäten zu machen, wie bei dem in Anhang I und II erwähnten Informationsaustausch.

27. So könnten beispielsweise konkretere und klare Maßnahmen zur Integration von SOLVIT ([22]) in das IMI (Bestimmungen für „externe Akteure" und „Problemlösungsverfahren") und für Verzeichnisse von Fachkräften und Dienstleistern (Bestimmungen für „Datenspeicher") vorgesehen werden.

28. Weitere Klarstellungen könnten auch bei „Warnungen" vorgenommen werden, die bereits nach der Dienstleistungsrichtlinie verwendet werden und die auch in weitere Bereiche Eingang finden könnte. „Warnung" als Funktionalität sollte insbesondere in Artikel 5 definiert werden (zusammen mit anderen Funktionalitäten wie Informationsaustausch zwischen zwei Teilnehmern und Datenspeicher). Auch die Zugangsrechte und Aufbewahrungsfristen für Warnungen sollten klargestellt werden ([23]).

Verfahrensgarantien (Datenschutz-Folgenabschätzung und Konsultation der Datenschutzbehörden)

29. Sollte die Absicht bestehen, die Verordnung im Hinblick auf weitere, langfristig unter Umständen erforderliche Funktionalitäten „zukunftsfest" zu machen und somit weitere, in der Verordnung noch nicht festgelegte Funktionalitäten zuzulassen, sollte es hierfür angemessene Verfahrensgarantien geben, mit denen gewährleistet wird, dass angemessene Maßnahmen vorgesehen werden, mit denen die erforderlichen Datenschutzgarantien noch vor dem Anlaufen der neuen Funktionalität umgesetzt werden. Gleiches sollte für Erweiterungen auf neue Bereiche gelten, bei denen Auswirkungen auf den Datenschutz zu erwarten sind.

30. Der EDSB empfiehlt einen klaren Mechanismus, mit dem gewährleistet wird, dass vor jeder Erweiterung von Funktionalitäten oder der Ausdehnung auf neue Politikbereiche Datenschutzanliegen sorgfältig bewertet werden und erforderlichenfalls zusätzliche Garantien oder technische Vorkehrungen in die IMI-Architektur aufgenommen werden. Insbesondere gilt:

— Die auf S. 7 der Begründung erwähnte Folgenabschätzung sollte auch in der Verordnung selbst ausdrücklich gefordert werden und sollte auch eine Datenschutz-Folgenabschätzung umfassen, in der genau angegeben wird, ob und wenn ja welche Änderungen am IMI erforderlich sind, damit es auch weiterhin angemessene Datenschutzgarantien enthält, die auch neue Politikbereiche und/oder Funktionalitäten abdecken.

— Die Verordnung sollte ausdrücklich vorsehen, dass vor jeder Erweiterung des IMI eine Konsultation des EDSB und nationaler Datenschutzbehörden erforderlich ist. Diese Konsultation könnte mit Hilfe des in Artikel 20 vorgesehenen Mechanismus der koordinierten Überwachung erfolgen.

([19]) So folgt beispielsweise der Informationsaustausch zwischen zwei Teilnehmern nach der Richtlinie über die Anerkennung von Berufsqualifikationen und der Richtlinie über die Ausübung der Patientenrechte in der grenzüberschreitenden Gesundheitsversorgung im Wesentlichen der gleichen Struktur und kann unter Verwendung ähnlicher Funktionalitäten erledigt werden, die ähnlichen Datenschutzvorkehrungen unterliegen.

([20]) Siehe Erwägungsgründe 2, 10, 12, 13 und 15 sowie Artikel 5 Buchstabe b, Artikel 5 Buchstabe i, Artikel 10 Absatz 7 und Artikel 13 Absatz 2.

([21]) Sollte übrigens die Absicht bestehen, mit dem IMI bestehende Dateienverwaltungs- und Archivierungssysteme zu ersetzen oder zu ergänzen und/oder das IMI als Datenbank einzusetzen, sollte dies in Artikel 3 klarer zum Ausdruck gebracht werden.

([22]) Siehe Anhang II, I(1).

([23]) Siehe nachstehende Abschnitte 2.4 und 2.5.5.

31. Diese Verfahrensgarantien (Datenschutz-Folgenabschätzung und Konsultation) sollten für Erweiterungen sowohl im Wege eines delegierten Rechtsaktes der Kommission (Verschiebung eines Bereichs von Anhang II in Anhang I) als auch per Verordnung des Parlaments und des Rates gelten, mit der ein noch nicht in Anhang II aufgeführter Bereich dort aufgenommen wird.

32. Schließlich empfiehlt der EDSB, in der Verordnung klarzustellen, ob der Anwendungsbereich der delegierten Rechtsakte, zu deren Annahme die Kommission gemäß Artikel 23 ermächtigt sein wird, außer der Verschiebung von Bereichen von Anhang II nach Anhang I noch andere Punkte umfassen wird. Falls machbar, sollte die Kommission in der Verordnung dazu ermächtigt werden, spezifische Durchführungs- oder delegierte Rechtsakte anzunehmen, in denen weitere Funktionalitäten des Systems festgelegt oder etwaig in Zukunft auftretende Datenschutzbedenken behandelt werden können.

2.3 **Rollen, Zuständigkeiten und Verantwortlichkeiten (Artikel 7 bis 9)**

33. Der EDSB begrüßt, dass ein ganzes Kapitel (Kapitel II) vorgesehen ist, um die Aufgaben und Verantwortlichkeiten der am IMI beteiligten Akteure festzulegen. Diese Bestimmungen sollten folgendermaßen verstärkt werden.

34. Artikel 9 beschreibt die Verantwortlichkeiten, die sich aus der Rolle der Kommission als für die Verarbeitung Verantwortlicher ergeben. Der EDSB empfiehlt darüber hinaus die Aufnahme einer weiteren Bestimmung zur Rolle der Kommission, die dafür zu sorgen hat, dass das System nach dem Grundsatz des „eingebauten Datenschutzes" konzipiert wird, sowie zu ihrer Rolle als Koordinator in Datenschutzfragen.

35. Der EDSB stellt erfreut fest, dass zu den in Artikel 7 aufgeführten Aufgaben der IMI-Koordinatoren nunmehr auch die Koordinierung beim Datenschutz gehört, wobei der Koordinator als Ansprechpartner der Kommission fungiert. Er empfiehlt eine Klarstellung dahingehend, dass diese Koordinierungsaufgaben auch die Kontakte zu den nationalen Datenschutzbehörden umfassen.

2.4 **Zugangsrechte (Artikel 10)**

36. Artikel 10 bietet Garantien bezüglich des Zugangsrechts. Der EDSB begrüßt, dass diese Bestimmungen nach seinen Kommentaren spürbar verstärkt wurden.

37. In Anbetracht des horizontalen und expansiven Charakters des IMI ist unbedingt dafür zu sorgen, dass das System die Anwendung so genannter „chinesischer Mauern" vorsieht, mit denen die in einem Politikbereich verarbeiteten Daten auf diesen Bereich begrenzt bleiben. IMI-Nutzer sollten i) Zugang zu den Informationen nur haben, wenn sie über diese unbedingt verfügen müssen, und ii) nur zu einem Bereich Zugang haben.

38. Sollte es sich nicht vermeiden lassen, dass ein IMI-Nutzer Zugang zu mehreren Bereichen haben darf (dies kann beispielsweise in einigen Büros lokaler Behörden der Fall sein), sollte das System zumindest nicht zulassen, dass aus verschiedenen Bereichen stammende Informationen zusammenkommen. Bei Bedarf könnten Ausnahmen in Durchführungsrechtsakten oder einem Rechtsakt der Union geregelt werden, wobei der Grundsatz der Zweckbindung strengstens zu beachten wäre.

39. Diese Grundsätze finden sich derzeit zwar im Wortlaut der Verordnung, doch könnten sie deutlicher und operationeller formuliert werden.

40. Mit Blick auf die Zugangsrechte der Kommission begrüßt der EDSB die Tatsache, dass in Artikel 9 Absatz 2, Artikel 9 Absatz 4 sowie Artikel 10 Absatz 6 des Vorschlags bestimmt ist, dass die Kommission keinen Zugang zu den zwischen Mitgliedstaaten ausgetauschten personenbezogenen Daten hat; ausgenommen hiervon sind Fälle, in denen die Kommission an Verfahren der Verwaltungszusammenarbeit mitwirkt.

41. Auch die Zugangsrechte externer Akteure und die Zugangsrechte zu Warnungen sollten näher spezifiziert werden ([24]). Bezüglich der Warnungen empfiehlt der EDSB, in der Verordnung vorzusehen, dass Warnungen nicht standardmäßig an alle einschlägigen zuständigen Behörden in allen Mitgliedstaaten gesandt werden, sondern nach dem Need-to-know-Prinzip nur an die eigentlich betroffenen. Damit ist natürlich nicht ausgeschlossen, dass in bestimmten Fällen oder in bestimmten Bereichen Warnungen an alle Mitgliedstaaten gehen, sofern alle betroffen sind. Ähnlich ist fallweise darüber zu entscheiden, ob die Kommission Zugang zu diesen Warnungen haben soll.

2.5 **Aufbewahrung personenbezogener Daten (Artikel 13 und 14)**

2.5.1 *Einleitung*

42. In Artikel 13 des Vorschlags wird die Aufbewahrungsfrist für die Daten im IMI von derzeit sechs Monaten (gezählt ab Abschluss des Falls) auf fünf Jahre verlängert, wobei die Daten nach 18 Monaten „gesperrt" werden. Während der „Sperr"-Frist ist ein Zugriff auf die Daten nur mit einem besonderen Abrufverfahren möglich, das nur auf Verlangen der betroffenen Person oder in Fällen eingeleitet werden darf, in denen die Daten „zum Zweck des Nachweises eines Informationsaustauschs über das IMI" benötigt werden.

43. Die Daten werden also im IMI in drei verschiedenen Phasen gespeichert:

— vom Hochladen bis zum Abschluss des Falls;

— ab dem Abschluss des Falls für einen Zeitraum von 18 Monaten ([25]);

— nach Ablauf der 18 Monate in gesperrter Form für weitere dreieinhalb Jahre (also bis zu fünf Jahren nach dem Abschluss des Falls).

([24]) Siehe auch Abschnitt 2.2.2.

([25]) Nach Artikel 13 Absatz 1 sind die 18 Monate eine „Höchst"-Frist; es kann also auch ein kürzerer Zeitraum bestimmt werden. Das hätte jedoch keinerlei Auswirkung auf die Gesamtaufbewahrungsfrist, die auf jeden Fall erst fünf Jahre nach Abschluss des Falls enden würde.

44. Über diese allgemeinen Vorschriften hinaus erlaubt Artikel 13 Absatz 2 die Speicherung von Daten in einem „Datenspeicher" so lange, wie es zu diesem Zweck erforderlich ist, wenn der Betroffene seine Einwilligung gegeben hat, oder wenn „dies erforderlich ist, um einem Rechtsakt der Union nachzukommen". Artikel 14 sieht einen ähnlichen Sperrmechanismus für die Aufbewahrung von personenbezogenen Daten über IMI-Nutzer vor, und zwar fünf Jahre ab dem Zeitpunkt, an dem sie nicht mehr zu den IMI-Nutzern zählen.

45. Weitere spezifische Bestimmungen bestehen nicht. Daher sollen vermutlich die allgemeinen Vorschriften nicht nur für den Informationsaustausch zwischen zwei Teilnehmern gelten, sondern auch für Warnungen, Problemlösungen (wie in SOLVIT ([26])) und für alle anderen Funktionalitäten, bei denen personenbezogene Daten verarbeitet werden.

46. Der EDSB hegt im Lichte von Artikel 6 Absatz 1 Buchstabe e der Richtlinie 95/46/EG und von Artikel 4 Absatz 1 Buchstabe e der Verordnung (EG) Nr. 45/2001 mehrere Bedenken bezüglich der Aufbewahrungsfristen; beide Rechtsakte fordern, dass personenbezogene Daten nur so lange aufbewahrt werden dürfen, wie dies für die Zwecke, für die sie erhoben oder weiterverarbeitet werden, erforderlich ist.

2.5.2 *Vom Hochladen bis zum Abschluss des Falls: Fälle müssen rechtzeitig abgeschlossen werden*

47. Mit Blick auf den ersten Zeitraum zwischen dem Hochladen von Informationen und dem Abschluss des Falls hegt der EDSB Bedenken ob der Gefahr, dass manche Fälle nie oder erst nach einer unverhältnismäßig langen Zeit abgeschlossen werden. Damit könnten einige personenbezogene Daten länger als erforderlich oder sogar unendlich lange in der Datenbank gespeichert bleiben.

48. Nach Auffassung des EDSB hat die Kommission auf der praktischen Ebene durchaus Fortschritte bei der Beseitigung von Verzögerungen im IMI erzielt und besteht jetzt ein System für den Informationsaustausch zwischen zwei Teilnehmern, bei dem auf einen rechtzeitigen Abschluss der Fälle geachtet wird und in regelmäßigen Abständen diejenigen ermahnt werden, die zurückliegen. Außerdem ist es dank einer Änderung bei den Funktionalitäten des Systems und gestützt auf das Konzept des „eingebauten Datenschutzes" nunmehr möglich, mit dem Klicken auf eine einzige Schaltfläche eine Antwort zu akzeptieren und damit gleichzeitig den Fall abzuschließen. Zuvor waren hierfür zwei Schritte erforderlich; dies könnte einige der noch immer im System vorhandenen ruhenden Fälle hervorgerufen haben.

49. Der EDSB begrüßt diese Bemühungen auf der praktischen Ebene. Er empfiehlt jedoch, im Wortlaut der Verordnung Garantien dafür vorzusehen, dass Fälle im IMI so schnell wie möglich abgeschlossen werden und dass ruhende Fälle (also Fälle ohne Aktivitäten in der jüngsten Vergangenheit) aus der Datenbank gelöscht werden.

([26]) Siehe Anhang II, I(1).

2.5.3 *Vom Abschluss eines Falls bis zu 18 Monaten: Ist die Verlängerung der Frist von sechs Monaten gerechtfertigt?*

50. Nach Auffassung des EDSB sollte erneut geprüft werden, ob die Verlängerung der derzeitigen Sechsmonatsfrist auf 18 Monate nach Abschluss des Falls wirklich gerechtfertigt ist, und falls dem so sein sollte, ob dies nur für Informationsaustausche zwischen zwei Teilnehmern oder auch für andere Funktionalitäten gilt. Das IMI besteht nun schon seit mehreren Jahren, und deshalb sollten die diesbezüglichen praktischen Erfahrungen genutzt werden.

51. Wenn das IMI ein Instrument für den Informationsaustausch bleiben soll (und kein Dateienverwaltungssystem, keine Datenbank und kein Archivierungssystem werden soll), und wenn weiter die zuständigen Behörden über Mittel verfügen, aus dem System die von ihnen empfangenen Informationen wieder abzurufen (entweder elektronisch oder auf Papier, aber auf jeden Fall so, dass sie die abgerufenen Informationen als Beweis verwenden können ([27])), dürfte nur geringer Bedarf an irgendeiner Speicherung der Daten im IMI nach Abschluss des Falls bestehen.

52. Beim Informationsaustausch zwischen zwei Teilnehmern mag unter Umständen der potenzielle Bedarf an Anschlussfragen auch nach Akzeptanz einer Antwort und damit dem Abschluss des Falls eine (relativ kurze) Speicherfrist auch nach Abschluss des Falls rechtfertigen. Auf den ersten Blick dürfte für diesen Zweck der derzeitige Zeitraum von sechs Monaten vollkommen ausreichen.

2.5.4 *Von 18 Monaten auf fünf Jahre: „gesperrte" Daten*

53. Nach Ansicht des EDSB hat die Kommission die Notwendigkeit und Verhältnismäßigkeit einer Aufbewahrung „gesperrter" Daten für einen Zeitraum von bis zu fünf Jahren nicht ausreichend begründet.

54. In der Begründung (S. 8) wird auf das Urteil des Gerichtshofes in der Sache *Rijkeboer* Bezug genommen ([28]). Der EDSB empfiehlt der Kommission, die Implikationen dieses Falls auf die Datenaufbewahrung im IMI zu berücksichtigen. Seiner Ansicht nach muss nach *Rijkeboer* das IMI nicht so konfiguriert sein, das es Daten fünf Jahre nach Abschluss eines Falls aufbewahrt.

55. Nach Auffassung des EDSB ist ein Verweis auf das Urteil *Rijkeboer* oder auf das Recht betroffener Personen, Auskunft über ihre Daten zu erhalten, keine ausreichende und angemessene Rechtfertigung der Speicherung von Daten im IMI fünf Jahre nach Abschluss eines Falls. Die Aufbewahrung nur von Log-Daten (eng definiert, um Inhalte wie Anlagen oder sensible Daten auszuschließen) könnte eine weniger in die Privatsphäre eindringende Lösung sein, die vielleicht näher zu prüfen wäre. Derzeit ist der EDSB jedoch nicht davon überzeugt, dass selbst dieses erforderlich oder verhältnismäßig wäre.

([27]) Soweit wir wissen, hat man sich bemüht, dies in der Praxis sicherzustellen.

([28]) C-553/07 *Rijkeboer* [2009] Slg. I-3889.

56. Weiterhin ist problematisch, dass nicht feststeht, wer Zugang zu den „gesperrten" Daten haben darf und zu welchen Zwecken. Ein einfacher Verweis auf eine Verwendung „zum Zweck des Nachweises eines Informationsaustauschs" (wie in Artikel 13 Absatz 3) reicht nicht aus. Sollte die Bestimmung über das „Sperren" beibehalten werden, sollte auf jeden Fall näher ausgeführt werden, wer einen Nachweise eines Informationsaustauschs und in welchem Kontext verlangen kann. Wären neben der betroffenen Person auch andere zugangsbefugt? Wenn ja: Wären dies nur die zuständigen Behörden und dies auch nur, um zu beweisen, dass ein bestimmter Informationsaustausch mit einem bestimmten Inhalt stattgefunden hat (falls ein solcher Austausch von der zuständigen Behörde, die die Nachricht versendet oder erhalten hat, bestritten wird)? Sind andere mögliche Verwendungen zum „Zweck des Nachweises eines Informationsaustauschs" vorgesehen ([29])?

2.5.5 *Warnungen*

57. Der EDSB empfiehlt eine klarere Unterscheidung zwischen Warnungen und Datenspeichern. Es ist eine Sache, eine Warnung als Kommunikationsinstrument einzusetzen, um zuständige Behörden über ein bestimmtes Fehlverhalten oder einen Verdacht zu informieren, und es ist ein völlig andere Sache, diese Warnung für einen längeren oder gar unbegrenzten Zeitraum in einer Datenbank zu speichern. Die Speicherung von Warnungsdaten würde weitere Bedenken hervorrufen und besondere Vorschriften und zusätzliche Datenschutzgarantien erfordern.

58. Der EDSB empfiehlt daher, in der Verordnung standardmäßig vorzusehen, dass i) — falls in vertikalen Rechtsvorschriften nicht anders bestimmt und vorbehaltlich weiterer Garantien — für Warnungen eine Aufbewahrungsfrist von sechs Monaten gelten sollte, und dass ii) diese Frist ab dem Zeitpunkt der Sendung der Warnung läuft.

59. Alternativ empfiehlt der EDSB, in der vorgeschlagenen Verordnung ausdrücklich detaillierte Garantien im Hinblick auf Warnungen vorzusehen. Der EDSB ist gerne bereit, die Kommission und den Gesetzgeber diesbezüglich zu beraten, sollte diese zweite Lösung gewählt werden.

2.6 **Besondere Datenkategorien (Artikel 15)**

60. Der EDSB begrüßt die Unterscheidung zwischen den personenbezogenen Daten, die in Artikel 8 Absatz 1 der Richtlinie 95/46/EG genannt werden, einerseits und den personenbezogenen Daten nach Artikel 8 Absatz 5 andererseits. Des Weiteren begrüßt er, dass es in der Verordnung unmissverständlich heißt, dass besondere Datenkategorien nur gestützt auf einen in Artikel 8 der Richtlinie 95/46/EG genannten Grund verarbeitet werden dürfen.

61. Der EDSB deutet dies so, dass das IMI erhebliche Mengen von sensiblen Daten verarbeiten wird, die unter Artikel 8 Absatz 2 der Richtlinie 95/46/EG fallen. Das IMI war nämlich anfänglich, als es zunächst zur Unterstützung der Amtshilfe nach der Dienstleistungsrichtlinie und der Richtlinie über die Anerkennung von Berufsqualifikationen eingesetzt wurde, für die Verarbeitung solcher Daten konzipiert, insbesondere von Daten über Strafregisterauszüge und Verwaltungsstrafen, die sich auf das Recht einer Fachkraft oder eines Dienstleisters auf Arbeit/Erbringung einer Dienstleistung in einem anderen Mitgliedstaat auswirken.

62. Außerdem dürften in erheblichem Maße sensible Daten nach Artikel 8 Absatz 1 (hauptsächlich Gesundheitsdaten) im IMI verarbeitet werden, sobald das IMI um ein Modul für SOLVIT erweitert worden ist ([30]). Schließlich kann nicht ausgeschlossen werden, dass künftig mit dem IMI *ad hoc* oder systematisch noch weitere sensible Daten erhoben werden.

2.7 **Sicherheit (Artikel 16 und Erwägungsgrund 16)**

63. Der EDSB stellt erfreut fest, dass in Artikel 16 ausdrücklich von der Verpflichtung der Kommission die Rede ist, ihre eigenen Vorschriften einzuhalten, die gemäß Artikel 22 der Verordnung (EG) Nr. 45/2001 angenommen wurden, und einen Sicherheitsplan für das IMI anzunehmen und zu aktualisieren.

64. Zur weiteren Stärkung dieser Bestimmungen empfiehlt der EDSB, dass die Verordnung vor jeder Ausdehnung des IMI auf einen neuen Bereich oder vor der Hinzufügung einer neuen Funktionalität mit Auswirkungen auf den Datenschutz eine Risikobewertung und Überprüfung des Sicherheitsplans verlangt ([31]).

65. Weiter hält der EDSB fest, dass in Artikel 16 und in Erwägungsgrund 16 nur von den Pflichten der Kommission und der Aufsichtsrolle des EDSB die Rede ist. Dieser Verweis könnte irreführend sein. Es trifft zwar zu, dass die Kommission Betreiber des Systems und damit zu einem großen Teil für die Erhaltung der Sicherheit des IMI ist, doch auch die zuständigen Behörden, die wiederum der Aufsicht durch die nationalen Datenschutzbehörden unterliegen, haben gewisse Pflichten. Artikel 16 und Erwägungsgrund 16 sollten daher auch von den in der Richtlinie 95/46/EG aufgeführten Sicherheitspflichten der übrigen IMI-Akteure und von den Aufsichtsbefugnissen nationaler Datenschutzbehörden sprechen.

2.8 **Information der Betroffenen und Transparenz (Artikel 17)**

2.8.1 *In den Mitgliedstaaten gegebene Informationen*

66. Im Hinblick auf Artikel 17 Absatz 1 empfiehlt der EDSB spezifischere Bestimmungen in der Verordnung, mit denen gewährleistet wird, dass die betroffenen Personen über die Verarbeitung ihrer Daten im IMI umfassend unterrichtet werden. In Anbetracht der Tatsache, dass das IMI von zahlreichen zuständigen Behörden einschließlich kleiner Stellen lokaler Behörden ohne ausreichende Personalausstattung genutzt wird, wird nachdrücklich empfohlen, die Bereitstellung des Datenschutzhinweises auf nationaler Ebene zu regeln.

([29]) Obwohl die Aufbewahrung personenbezogener Daten im Vergleich ein geringeres Risiko für die Privatsphäre bedeutet, ist der EDSB trotzdem der Auffassung, dass die Aufbewahrung personenbezogener Daten von IMI-Nutzern für fünf Jahre, nachdem sie keinen Zugang mehr zum IMI haben, ebenfalls nicht hinreichend begründet worden ist.

([30]) Siehe Anhang II, I(1).

([31]) Siehe auch Abschnitt 12 mit Empfehlungen zu Audits.

2.8.2 *Von der Kommission gegebene Informationen*

67. Laut Artikel 17 Absatz 2 ist die Kommission aufgefordert, gemäß Artikel 10 und 11 der Verordnung (EG) Nr. 45/2001 einen Datenschutzhinweis zu ihren eigenen Datenverarbeitungsaktivitäten bereitzustellen. Gemäß Artikel 17 Absatz 2 Buchstabe b hat die Kommission auch Informationen über „die Datenschutzaspekte der Verfahren der Verwaltungszusammenarbeit im Rahmen des IMI gemäß Artikel 12" zu geben. Laut Artikel 17 Absatz 2 Buchstabe c schließlich hat die Kommission Informationen über „Ausnahmen von den Rechten der Betroffenen" gemäß Artikel 19 zu geben.

68. Der EDSB nimmt erfreut diese Bestimmungen zur Kenntnis, die einen Beitrag zur Transparenz der Datenverarbeitungen im IMI leisten. Wie bereits in Abschnitt 2.1. festgestellt, kommt es bei einem in 27 Mitgliedstaaten eingesetzten IT-System im Wesentlichen darauf an, beim Betrieb des Systems, den Datenschutzgarantien und den den Betroffenen gegebenen Informationen für Kohärenz zu sorgen ([32]).

69. Die Bestimmungen von Artikel 17 Absatz 2 sollten daher weiter gestärkt werden. Die Kommission als Betreiber des Systems ist wohl am ehesten in der Lage, eine proaktive Rolle bei der Bereitstellung einer ersten „Schicht" von Datenschutzhinweis und weiteren einschlägigen Informationen für betroffene Personen auf ihrer mehrsprachigen Website zu spielen, auch „im Namen" zuständiger Behörden, also zur Abdeckung der in Artikel 10 oder 11 der Richtlinie 95/46/EG geforderten Angaben. Häufig würde es dann genügen, wenn die zuständigen Behörden in den Mitgliedstaaten in ihrem Hinweis auf den Hinweis der Kommission verwiesen und ihn nur bei Bedarf mit Zusatzinformationen ergänzten, die nach dem nationalen Recht ausdrücklich zu geben wären.

70. In Artikel 17 Absatz 2 Buchstabe b sollte klargestellt werden, dass die von der Kommission gegebenen Informationen alle Bereiche, alle Arten von Amtshilfeverfahren und alle Funktionalitäten des IMI abdecken und auch die gegebenenfalls verarbeiteten Datenkategorien umfassen. Dazu sollte auch die Veröffentlichung der Fragengruppen gehören, die schon heute in der praktischen Zusammenarbeit zwischen zwei Teilnehmern auf der IMI-Website verwendet werden.

2.9 **Recht auf Auskunft, Berichtigung und Löschung (Artikel 18)**

71. Wie schon in Abschnitt 2.1 verweist der EDSB erneut darauf, dass der Kohärenz zwischen dem Betrieb des Systems und den angewandten Datenschutzgarantien zentrale Bedeutung zukommt. Daher würde der EDSB die Bestimmungen über das Recht auf Auskunft, Berichtigung und Löschung gerne näher spezifiziert haben.

72. In Artikel 18 sollte gesagt werden, an wen sich betroffene Personen mit einem Antrag auf Auskunft wenden sollen. Diese Frage sollte im Hinblick auf den Datenzugriff während der verschiedenen Zeiträume geklärt werden.

— vor dem Abschluss eines Falls

— nach dem Abschluss eines Falls, aber vor Ablauf der Aufbewahrungsfrist von 18 Monaten

— und schließlich während der „Sperrfrist".

73. Die Verordnung sollte ferner von den zuständigen Behörden bei Bedarf die Zusammenarbeit bei Auskunftsersuchen fordern. Berichtigung und Löschung sollten „so bald wie möglich, aber spätestens nach 60 Tagen" und nicht „innerhalb von 60 Tagen" vorgenommen werden. Es sollte auch auf die Möglichkeit eines Datenschutzmoduls und von Lösungen „mit eingebautem Datenschutz" für die Zusammenarbeit zwischen Behörden bezüglich der Auskunftsrechte verwiesen werden, sowie auf „mehr Befugnisse für betroffene Personen", indem ihnen beispielsweise unmittelbar Auskunft über ihre Daten erteilt wird, wo immer dies erheblich und machbar ist.

2.10 **Überwachung (Artikel 20)**

74. In den letzten Jahren wurde das Modell der „koordinierten Überwachung" entwickelt. Dieses Überwachungsmodell, das bereits bei EURODAC und Teilen des Zoll-Informationssystems gilt, ist auch vom Visa-Informationssystem (VIS) und vom Schengener Informationssystems der zweiten Generation (SIS-II) übernommen worden.

75. Das Modell besteht aus drei Schichten:

— Die Überwachung auf nationaler Ebene erfolgt durch die nationalen Datenschutzbehörden;

— die Überwachung auf EU-Ebene erfolgt durch den EDSB;

— die Koordinierung erfolgt über regelmäßige Sitzungen und andere koordinierte Aktivitäten, die vom EDSB, der als Sekretariat für diesen Koordinierungsmechanismus fungiert, unterstützt werden.

76. Dieses Modell hat sich als erfolgreich und effektiv erwiesen und sollte künftig für andere Informationssysteme in Erwägung gezogen werden.

77. Der EDSB begrüßt, dass Artikel 20 des Vorschlags ausdrücklich eine koordinierte Überwachung durch die nationalen Datenschutzbehörden und den EDSB vorsieht, die sich weitgehend auf das in den Verordnungen über VIS und SIS-II festgelegte Modell stützt ([33]).

([32]) Bei diesen Bemühungen um Kohärenz ist natürlich, sofern erforderlich und begründet, nationalen Unterschieden angemessen Rechnung zu tragen.

([33]) Siehe Verordnung (EG) Nr. 1987/2006 des Europäischen Parlaments und des Rates vom 20. Dezember 2006 über die Einrichtung, den Betrieb und die Nutzung des Schengener Informationssystems der zweiten Generation (SIS II) (ABl. L 381 vom 28.12.2006, S. 4) und Verordnung (EG) Nr. 767/2008 des Europäischen Parlaments und des Rates vom 9. Juli 2008 über das Visa-Informationssystem (VIS) und den Datenaustausch zwischen den Mitgliedstaaten für einen kurzfristigen Aufenthalt (VIS-Verordnung), (ABl. L 218 vom 13.8.2008, S. 60).

78. Der EDSB würde die Bestimmungen über die koordinierte Überwachung in einigen Punkten stärken und sich zu dem Zweck für Bestimmungen einsetzen, wie es sie beispielsweise beim Visa-Informationssystem (Artikel 41-43 der VIS-Verordnung) und bei Schengen II (Artikel 44-46 der SIS-II-Verordnung) gibt und wie sie für Eurodac geplant sind ([34]). So wäre es hilfreich, wenn die Verordnung

— in Artikel 20 Absatz 1 und 2 die jeweiligen Überwachungspflichten der nationalen Datenschutzbehörden und des EDSB regeln und klarer voneinander trennen würde ([35]);

— in Artikel 20 Absatz 3 besagen würde, dass die nationalen Datenschutzbehörden und der EDSB in ihrem jeweiligen Zuständigkeitsbereich „aktiv zusammenarbeiten" und „eine koordinierte Überwachung des IMI gewährleisten" (und nicht nur von einer koordinierten Aufsicht spräche, ohne die aktive Zusammenarbeit zu erwähnen) ([36]); und

— näher spezifizieren würde, was die Zusammenarbeit beinhalten könnte, indem sie zum Beispiel fordert, dass die nationalen Datenschutzbehörden und der EDSB „im Rahmen ihrer jeweiligen Zuständigkeiten einschlägige Informationen austauschen, sich gegenseitig bei Überprüfungen und Inspektionen unterstützen, Schwierigkeiten bei der Auslegung oder Anwendung der IMI-Verordnung prüfen, Problemen bei der Wahrnehmung der unabhängigen Überwachung oder der Ausübung der Rechte betroffener Personen nachgehen, harmonisierte Vorschläge im Hinblick auf gemeinsame Lösungen für etwaige Probleme ausarbeiten und erforderlichenfalls das Bewusstsein für die Datenschutzrechte fördern" ([37]).

79. Der EDSB ist sich natürlich der derzeitig geringeren Größe, der anderen Art der verarbeiteten Daten und des sich weiter entwickelnden Charakters des IMI bewusst. Er räumt daher ein, dass bei der Häufigkeit von Zusammenkünften und Prüfungen mehr Flexibilität angeraten sein könnte. Zusammenfassend empfiehlt der EDSB, dass die Verordnung die erforderlichen Mindestvorschriften enthalten sollte, die eine wirksame Zusammenarbeit gewährleisten, jedoch keinen unnötigen Verwaltungsaufwand schaffen sollte.

80. Artikel 20 Absatz 3 des Vorschlags fordert keine regelmäßigen Sitzungen, sondern sieht einfach nur vor, dass der EDSB „die nationalen Überwachungsbehörden bei Bedarf zu Zusammenkünften einladen kann". Der EDSB begrüßt, dass diese Bestimmungen den betroffenen Parteien die Entscheidung darüber überlassen, wie oft und nach welchen Modalitäten sie zusammenkommen, und auch selber andere Einzelheiten der Verfahren ihrer Zusammenarbeit festlegen können. Dies kann in den im Vorschlag erwähnten Verfahrensregeln bestimmt werden.

81. Bezüglich der regelmäßigen Prüfungen wäre es unter Umständen auch wirksamer, wenn es den kooperierenden Behörden überlassen bliebe, in ihren Verfahrensregeln festzulegen, wann und wie häufig solche Prüfungen durchgeführt werden sollen. Dies hängt von einer ganzen Reihe von Faktoren ab und kann sich im Zeitverlauf auch ändern. Der EDSB schließt sich daher der Kommission an, die auch in diesem Bereich größere Flexibilität zulässt.

2.11 **Nationale Nutzung des IMI**

82. Der EDSB begrüßt, dass der Vorschlag eine klare Rechtsgrundlage für die nationale Nutzung des IMI bietet und dass eine solche Verwendung mehreren Bedingungen unterliegt; so müssen beispielsweise die nationalen Datenschutzbehörden konsultiert werden und diese Nutzung im Einklang mit einzelstaatlichem Recht stehen.

2.12 **Informationsaustausch mit Drittländern (Artikel 22)**

83. Der EDSB begrüßt die in Artikel 22 Absatz 1 festgelegten Anforderungen für einen Informationsaustausch sowie die Tatsache, dass Artikel 22 Absatz 3 die Transparenz der Erweiterung im Wege der Veröffentlichung einer aktualisierten Liste der das IMI nutzenden Drittländer im Amtsblatt gewährleistet (Artikel 22 Absatz 3).

84. Der EDSB empfiehlt der Kommission weiter, den Verweis auf die Ausnahmen nach Artikel 26 der Richtlinie 95/46/EG einzuengen und nur Artikel 26 Absatz 2 zu erwähnen. Mit anderen Worten: Zuständige Behörden oder andere externe Akteure in einem Drittland, das keinen angemessenen Schutz bietet, dürften nur auf der Grundlage angemessener vertraglicher Klauseln unmittelbaren Zugang zum IMI haben. Diese Klauseln sollten auf EU-Ebene ausgehandelt werden.

85. Der EDSB unterstreicht, dass andere Ausnahmen wie „die Übermittlung ist aus wichtigen Gründen öffentlichen Interesses oder zur Feststellung, Ausübung oder Verteidigung von Rechtsansprüchen erforderlich oder rechtlich geboten" nicht zur Begründung von Datenübermittlungen an Drittländer durch direkten Zugang zum IMI herangezogen werden sollten ([38]).

2.13 **Rechenschaftspflicht (Artikel 26)**

86. Mit Blick auf die erwartete Stärkung der Regelungen für mehr Rechenschaftspflicht bei der Überarbeitung des EU-Datenschutzrahmens ([39]), empfiehlt der EDSB, dass die Verordnung einen klaren Rahmen für angemessene interne Kontrollmechanismen abstecken sollte, die die Einhaltung der Datenschutzvorschriften gewährleisten und sie belegen und zumindest die nachstehend aufgeführten Elemente enthalten.

([34]) Verordnung (EG) Nr. 2725/2000 des Rates vom 11. Dezember 2000 über die Einrichtung von „Eurodac" für den Vergleich von Fingerabdrücken zum Zwecke der effektiven Anwendung des Dubliner Übereinkommens (ABl. L 316 vom 15.12.2000, S. 1); wird derzeit überarbeitet. In diesem Zusammenhang werden ähnliche Bestimmungen wie in der VIS- und der SIS II-Verordnung erwogen.
([35]) Siehe zum Beispiel Artikel 41 und 42 der VIS-Verordnung.
([36]) Siehe zum Beispiel Artikel 43 Absatz 1 der VIS-Verordnung.
([37]) Siehe zum Beispiel Artikel 43 Absatz 2 der VIS-Verordnung.
([38]) Ein ähnlicher Ansatz wurde auch in Artikel 22 Absatz 2 für die Kommission als IMI-Akteur verfolgt.
([39]) Siehe Abschnitt 2.2.4 der Mitteilung der Kommission an das Europäische Parlament, den Rat, den Europäischen Wirtschafts- und Sozialausschuss und den Ausschuss der Regionen: „Gesamtkonzept für den Datenschutz in der Europäischen Union", KOM(2010) 609 endgültig. Siehe ferner Abschnitt 7 der Stellungnahme des EDSB zu dieser Mitteilung der Kommission vom 14. Januar 2011.

87. Vor diesem Hintergrund begrüßt der EDSB die in Artikel 26 Absatz 2 der Verordnung enthaltene Anforderung an die Kommission, dem EDSB alle drei Jahre Bericht über datenschutzrechtliche Aspekte einschließlich der Sicherheit zu erstatten. Es wäre ratsam, in der Verordnung deutlich zu sagen, dass der EDSB wiederum im Rahmen der in Artikel 20 erwähnten koordinierten Überwachung den Bericht der Kommission an die nationalen Datenschutzbehörden weiterzuleiten hat. Hilfreich wäre auch eine klare Aussage darüber, dass sich der Bericht mit Blick auf die einzelnen Politikbereiche und Funktionalitäten mit der Frage beschäftigen sollte, wie in der Praxis mit den wichtigsten Datenschutzgrundsätzen und -anliegen (z. B. Information der betroffenen Personen, Zugangsrechte, Sicherheit) umgegangen wurde.

88. Darüber hinaus sollte in der Verordnung klar geregelt werden dass der Rahmen für interne Kontrollmechanismen auch Datenschutz-Folgenabschätzungen (auch mit einer Analyse der Sicherheitsrisiken), ein auf der Grundlage der Ergebnisse dieser Folgenabschätzung angenommenes Datenschutzkonzept (einschließlich Sicherheitsplan) sowie in regelmäßigen Abständen durchgeführte Überprüfungen und Kontrollen enthalten sollte.

2.14 **Eingebauter Datenschutz**

89. Der EDSB begrüßt den Verweis auf diesen Grundsatz in Erwägungsgrund 6 der Verordnung ([40]). Er empfiehlt, über diesen Verweis hinauszugehen und in die Verordnung besondere Garantien für diesen eingebauten Datenschutz aufzunehmen; dazu könnten gehören:

— ein Datenschutzmodul, mit dessen Hilfe betroffene Personen ihre Rechte wirksamer ausüben könnten ([41]);

— eine klare Trennung der verschiedenen Politikbereiche innerhalb des IMI („Chinesische Mauern") ([42]);

— besondere technische Lösungen zur Einschränkung der Suchmöglichkeiten in Verzeichnissen, Warnungen usw., um die Zweckbindung zu gewährleisten;

— besondere Maßnahmen um sicherzustellen, dass Fälle, in denen keine Aktivitäten zu verzeichnen sind, abgeschlossen werden ([43]);

— angemessene Verfahrensgarantien vor dem Hintergrund künftiger Entwicklungen ([44]).

3. **SCHLUSSFOLGERUNGEN**

90. Generell beurteilt der EDSB das IMI positiv. Der EDSB unterstützt das Ziel der Kommission, ein elektronisches System für den Informationsaustausch aufzubauen und dessen Datenschutzaspekte zu regeln. Der EDSB begrüßt ferner, dass die Kommission einen horizontalen Rechtsakt für das IMI in Form einer Verordnung des Rates und des Parlaments vorschlägt. Er ist erfreut darüber, dass in dem Vorschlag ausführlich auf die größten Datenschutzprobleme des IMI eingegangen wird.

91. Im Hinblick auf den Rechtsrahmen für das IMI, der mit der vorgeschlagenen Verordnung geschaffen werden soll, weist der EDSB auf zwei zentrale Herausforderungen hin:

— es muss Kohärenz bei gleichzeitiger Wahrung der Vielfalt gewährleistet sein, und

— es muss ein ausgewogenes Verhältnis zwischen Flexibilität und Rechtssicherheit gefunden werden.

92. Bereits absehbare Funktionalitäten des IMI sollten klar dargestellt und genauer umrissen werden.

93. Mit angemessenen Verfahrensgarantien sollte gewährleistet werden, dass der Datenschutz bei künftigen Entwicklungen des IMI sorgfältig berücksichtigt wird. Hierzu sollten eine Folgenabschätzung und die Konsultation des EDSB und der nationalen Datenschutzbehörden vor jeder Erweiterung des Anwendungsbereichs des IMI auf einen neuen Politikbereich und/oder neue Funktionalitäten gehören.

94. Die Zugangsrechte externer Akteure und die Zugangsrechte zu Warnungen sollten näher spezifiziert werden.

95. Zu den Aufbewahrungsfristen:

— Die Verordnung sollte Garantien dafür vorsehen, dass Fälle im IMI so schnell wie möglich abgeschlossen werden und dass ruhende Fälle (also Fälle ohne Aktivitäten in der jüngsten Vergangenheit) aus der Datenbank gelöscht werden;

— es sollte überdacht werden, ob es wirklich Gründe für die Verlängerung des derzeitigen Sechsmonatszeitraums auf 18 Monate nach Abschluss des Falls gibt;

— die Kommission hat die Notwendigkeit und Verhältnismäßigkeit der Speicherung „gesperrter" Daten für bis zu fünf Jahre nicht ausreichend begründet; der Vorschlag sollte diesbezüglich noch einmal überdacht werden;

— es sollte klarer zwischen Warnungen und Datenspeichern unterschieden werden: Die Verordnung sollte standardmäßig vorsehen, dass i) — falls in vertikalen Rechtsvorschriften nicht anders bestimmt und vorbehaltlich weiterer Garantien — für Warnungen eine Aufbewahrungsfrist von sechs Monaten gilt, und dass ii) diese Frist ab dem Zeitpunkt der Sendung der Warnung läuft.

96. Die Verordnung sollte vor jeder Ausdehnung des IMI auf einen neuen Bereich oder vor der Hinzufügung einer neuen Funktionalität mit Auswirkungen auf den Datenschutz eine Risikobewertung und Überprüfung des Sicherheitsplans verlangen.

97. Die Bestimmungen über die Information betroffener Personen und über Zugangsrechte sollten verstärkt werden und auf einen kohärenteren Ansatz abheben.

([40]) a.a.O.
([41]) Siehe vorstehenden Abschnitt 2.9.
([42]) Siehe vorstehenden Abschnitt 2.4.
([43]) Siehe vorstehenden Abschnitt 2.5.2.
([44]) Siehe vorstehenden Abschnitt 2.2.2.

98. Der EDSB würde in einigen Punkten die Bestimmungen über die koordinierte Überwachung stärken und zu diesem Zweck für Bestimmungen plädieren, die denen ähnlich sind, die es beispielsweise schon im Zusammenhang mit dem Visa-Informationssystem und Schengen II gibt, und die für Eurodac geplant sind. Bezüglich der Häufigkeit von Zusammenkünften und Kontrollen stimmt der EDSB dem flexiblen Ansatz der Vorschlags zu, mit dem gewährleistet werden soll, dass die Verordnung die erforderlichen Mindestregeln für eine effiziente Zusammenarbeit enthält, aber keinen überflüssigen Verwaltungsaufwand schafft.

99. Die Verordnung sollte dafür sorgen, dass zuständige Behörden oder andere externe Akteure in einem Drittland, das keinen angemessenen Schutz bietet, nur auf der Grundlage angemessener vertraglicher Klauseln unmittelbaren Zugang zum IMI haben. Diese Klauseln sollten auf EU-Ebene ausgehandelt werden.

100. Die Verordnung sollte einen klaren Rahmen für angemessene interne Kontrollmechanismen abstecken, die die Einhaltung der Datenschutzvorschriften gewährleisten und belegen; dazu gehören auch Datenschutz-Folgenabschätzungen (auch mit einer Analyse der Sicherheitsrisiken), ein auf der Grundlage der Ergebnisse dieser Folgenabschätzung angenommenes Datenschutzkonzept (einschließlich Sicherheitsplan) sowie in regelmäßigen Abständen durchgeführte Überprüfungen und Kontrollen.

101. Ferner sollte die Verordnung besondere Garantien für einen eingebauten Datenschutz enthalten.

Geschehen zu Brüssel am 22. November 2011.

Giovanni BUTTARELLI

Stellvertretender Europäischer Datenschutzbeauftragter