ARTIKEL-29-DATENSCHUTZGRUPPE

01911/07/DE
WP 140

Stellungnahme 7/2007 zu Fragen des Datenschutzes im Zusammenhang mit dem Binnenmarkt-Informationssystem

Angenommen am 21. September 2007

INHALT

1. Einleitung 3
2. Beschreibung des IMI 4
2.1 Aufbau: Aufgaben der Kommission und einzelstaatliche Systeme 4
2.2 Die beteiligten Behörden 4
2.2.a Europäische Kommission 5
2.2.b Zuständige Behörde 5
2.2.c Nationaler IMI-Koordinator (NIMIK) 6
2.2.c Nachgeordneter IMI-Koordinator (NaIMIK) 7
2.2.e Angeschlossene Behörden 7
2.3 Rollen und Rechte im System 8
3. Verarbeitete personenbezogene Daten 9
4. Rechtliche Analyse des Systems und spezifische Fragen 9
4.1 Rechtsgrundlage für die Verarbeitung personenbezogener Daten (Artikel 7) 9
4.2 Anwendung der Grundsätze für die Qualität der Daten (Artikel 6) 12
4.2.a Qualität und Notwendigkeit der Daten 12
4.2.b Verhältnismäßigkeit 12
4.2.c Besondere Fragen hinsichtlich der Aufbewahrung von personenbezogenen Daten 13
4.2.d Besonders geschützte Daten 14
4.3 Verwendung einer nationalen Kennziffer 18
5. Rechte der betroffenen Personen 18
5.1 Auskunftsrecht 18
5.2 Rechte auf Zugang, Berichtigung, Löschung und Sperrung 19
5.3 Abhilfemaßnahmen 20
6. Sicherheit 20
7. Meldung bei der Datenschutzbehörde und Vorabkontrolle 22
8. Übermittlung von personenbezogenen Daten in Drittstaaten 22
9. Schlussfolgerungen und Empfehlungen der Artikel-29-Datenschutzgruppe 22

1. Einleitung

Das Vorhaben, ein computergestütztes System als Hilfsmittel für den Informationsaustausch hinsichtlich personenbezogener Daten einzurichten, gibt Anlass zu erheblichen Bedenken in Bezug auf die Grundrechte von Einzelpersonen, insbesondere auf das Recht auf Privatsphäre.

Aufgrund der Komplexität des Binnenmarkt-Informationssystems (Internal Market Information System — IMI) und der verschiedenen damit verbundenen Fragen ersuchte die GD Binnenmarkt der Europäischen Kommission die Artikel-29-Datenschutzgruppe um ihre Stellungnahme. Der Schwerpunkt der Stellungnahme der Artikel-29-Datenschutzgruppe liegt auf denselben Aspekten, die in den Dokumenten „Issue Paper on Data Protection in IMI" (Themenpaper über den Datenschutz im IMI; D-4784) und „General Overview" (Allgemeine Übersicht; D-1804) behandelt werden. Zweck dieser Stellungnahme ist es, die Auswirkungen des IMI hinsichtlich personenbezogener Daten, die durch die Richtlinie 95/46/EG („Datenschutzrichtlinie") und die Verordnung (EG) Nr. 45/2001 („Datenschutzverordnung") geschützt werden, zu analysieren.

> Im März 2006 gaben die Vertreter der Mitgliedstaaten im Beratenden Ausschuss für den Binnenmarkt grünes Licht für die Entwicklung des Binnenmarkt-Informationssystems (IMI), dessen Ziel die Verbesserung der Kommunikation unter den Verwaltungen der Mitgliedstaaten ist. Das IMI ist ein elektronisches Hilfsmittel, das ein System für den Informationsaustausch bietet, das den Mitgliedstaaten eine effizientere Zusammenarbeit in ihren laufenden Aktivitäten bei der Umsetzung der Binnenmarktvorschriften in den Bereichen erlauben soll, die von der Richtlinie 2006/123/EG[1] über Dienstleistungen im Binnenmarkt und der Richtlinie 2005/36/EG[2] über die Anerkennung von Berufsqualifikationen für reglementierte Berufe und Dienstleistungen abgedeckt werden. Das IMI soll dazu beitragen, dass praktische Hindernisse überwunden werden, welche die Kommunikation und Zusammenarbeit zwischen den zuständigen Behörden der Mitgliedstaaten erschweren, wie zum Beispiel unterschiedliche Verwaltungs- und Arbeitskulturen, Sprachbarrieren und das Fehlen eindeutiger Angaben zu Ansprechpartnern in anderen Mitgliedstaaten. Es soll die Verwaltungslasten verringern helfen und Effizienz und Wirksamkeit in der laufenden Zusammenarbeit unter den Mitgliedstaaten steigern.

Die Bedeutung des Ausbaus der Verwaltungszusammenarbeit zwischen den Mitgliedstaaten wurde in der erneuerten Lissabon-Strategie[3] und in der Agenda der EU für bessere Rechtsetzung[4] voll anerkannt, da sie dazu beitragen wird, die Anwendung des Gemeinschaftsrechts durch die Mitgliedstaaten zu verbessern.

Es ist Aufgabe der Mitgliedstaaten, das reibungslose und wirkungsvolle Funktionieren des Binnenmarktrechts auf ihrem eigenen Staatsgebiet sicherzustellen. Sie benötigen allerdings Hilfsmittel für die Zusammenarbeit untereinander und mit der Kommission, um zu gewährleisten, dass Bürger und Unternehmen in den Genuss aller Vorteile des Rechtsrahmens

---

1 ABl. L 376 vom 27.12.2006, S. 36.

2 ABl. L 255 vom 30.9.2005, S. 22.

3 Siehe „Jetzt aufs Tempo drücken: Die neue Partnerschaft für Wachstum und Arbeitsplätze" (KOM(2006) 30 endgültig), Seite 21.

4 Siehe „Strategische Überlegungen zur Verbesserung der Rechtsetzung in der Europäischen Union" (KOM(2006) 689 endgültig), Seite 3.

kommen. Das IMI wird derzeit entwickelt, um diesen Bedarf zu decken und die rechtliche Verpflichtung zur Einrichtung eines elektronischen Systems für den Austausch von Informationen zwischen den Mitgliedstaaten nach Artikel 34 Absatz 1 der Richtlinie 2006/123/EG über Dienstleistungen im Binnenmarkt (im Folgenden: „die Dienstleistungsrichtlinie“) zu erfüllen.

> Die erste Priorität im Rahmen des IMI wird in der Entwicklung von Anwendungen für die Richtlinie 2005/36/EG („Richtlinie über Berufsqualifikationen“) und die Dienstleistungsrichtlinie bestehen.

2. Beschreibung des IMI

Das IMI wird eine Reihe von horizontalen Anwendungen, die sprachliche Unterstützung und Hilfsmittel für die Kommunikation zwischen den zuständigen Behörden bieten, sowie vertikale Anwendungen zu spezifischen Rechtsakten umfassen. Das IMI selbst wird ein eigenständiges System sein, dessen sämtliche Funktionen über eine Website zugänglich sein werden. Die wichtigsten Nutzer der Anwendungen werden die Verwaltungen und zuständigen Behörden der Mitgliedstaaten sein.

2.1 Aufbau: Aufgaben der Kommission und einzelstaatliche Systeme

Im Hinblick auf den Aufbau des IMI liegt der Schwerpunkt darauf, den Mitgliedstaaten die Erfüllung ihrer rechtlichen Verpflichtungen zum Informationsaustausch zu erleichtern, aber es wird auch neue und komplexere Formen der Verwaltungszusammenarbeit ermöglichen. Das IMI wird eine Suchfunktion, mit der die entsprechende zuständige Behörde in einem anderen Mitgliedstaat gefunden werden kann, und einen Satz von Menüs in mehreren Sprachen aufweisen, die mit einem strukturieren Fragenkatalog den erforderlichen Informationsaustausch unterstützen. Die Artikel-29-Datenschutzgruppe betont, dass es von entscheidender Bedeutung ist, dass die Kommission die Menüs und den strukturierten Fragenkatalog so gestalten und abfassen muss, dass das Risiko einer Erfassung von Daten, die irrelevant oder unangemessen sind oder Dritte betreffen, möglichst gering gehalten wird. Es ist ebenso wichtig, dass die Nutzer des Systems (zuständige Behörden, die Daten austauschen) ihrerseits gewährleisten, dass sie das System nicht für den Austausch von Daten verwenden, die irrelevant oder unangemessen sind oder Dritte betreffen.

Das System ist so angelegt, dass es die vielfältigen Gegebenheiten der nationalen Verwaltungen in den einzelnen Mitgliedstaaten berücksichtigt (beispielsweise in unterschiedlichem Maße zentralisierte oder dezentralisierte Systeme). Somit kann jeder Mitgliedstaat die Darstellung seiner zuständigen Behörden für die Zwecke des IMI individuell anpassen und die Effizienz maximieren.

Die zentralen Akteure werden unter Bezugnahme auf das Dokument „General Overview“ nachstehend kurz beschrieben.

2.2 Die beteiligten Behörden

Die wichtigsten Akteure im Rahmen des IMI werden die zuständigen Behörden im gesamten Europäischen Wirtschaftsraum (EWR) sein, die das IMI zum Austausch von Informationen in den Bereichen der Binnenmarktvorschriften über reglementierte Berufe und Dienstleistungen verwenden werden.

Hinsichtlich der Aufgaben und Befugnisse der einzelnen Behörden bei der Verarbeitung personenbezogener Daten ist zu betonen, dass sowohl der Europäischen Kommission als auch den Mitgliedstaaten eine wichtige Rolle im IMI zukommen wird. Jeder Mitgliedstaat wird die Möglichkeit haben, seine eigenen Strukturen so zu gestalten, dass sie seinen spezifischen Bedürfnissen entsprechen, aber alle Mitgliedstaaten müssen dabei im Rahmen des IMI dieselbe Funktion erfüllen.

Die spezifischen Aufgaben der Behörden werden im folgenden Auszug aus dem von der Kommission vorgelegten Dokument „Issue Paper on Data Protection in IMI" beschrieben.

2.2.a Europäische Kommission

Im Dokument „Issue Paper on Data Protection in IMI" ist Folgendes vorgesehen: „*The database will be stored on a Commission server in Luxembourg. All exchange of data will go through this server and exchanged data will be stored on that server. The Commission's responsibilities, [generally delegated to the EU System Administrator], will be related to the registration of the National IMI Coordinator in each Member State, database administration at the system level, administration of legislation-based question sets and translation of all IMI system components into all official EU languages.*" [Die Datenbank wird auf einem Server der Kommission in Luxemburg gespeichert. Der gesamte Datenaustausch wird über diesen Server erfolgen, auf dem auch die ausgetauschten Daten gespeichert werden sollen. Die Zuständigkeiten der Kommission [die im Allgemeinen an den Systemverwalter der EU delegiert werden] werden die Registrierung des nationalen IMI-Koordinators aus jedem Mitgliedstaat, das Datenbankmanagement auf Systemebene, die Verwaltung der auf den Rechtsvorschriften beruhenden Fragenkataloge und die Übersetzung aller Systemelemente des IMI in alle Amtssprachen der EU umfassen.]

Die gesamte Zuständigkeit für die Dateneingabe, die Einhaltung der Vorgaben für die Nutzung und Qualität der Daten, die Anmeldung und Pflege der Berechtigungen für den Zugang zu den Daten, ihre Änderung und Löschung liegt auf der nationalen Ebene.

Die Artikel-29-Datenschutzgruppe betont, dass die Kommission gemeinsam mit den zuständigen Behörden in den Mitgliedstaaten die Verantwortung für die Einhaltung der anwendbaren Datenschutzvorschriften tragen muss, da die Kommission auch gewisse Aufgaben im Bereich der Datenverarbeitung (i) für die Mitgliedstaaten einerseits (z. B. Speichern und Löschen von Daten) und (ii) für die Kommission selbst als Systemverwalter andererseits (Daten über die Nutzer des IMI und die Ansprechpartner) wahrnehmen wird. Die Aufgaben und Zuständigkeiten der Kommission und der zuständigen Behörden in den Mitgliedstaaten sind klar festzulegen.

2.2.b Zuständige Behörde

Im selben Dokument wird hinsichtlich der zuständigen Behörden Folgendes festgehalten: „*Public administrations in each Member State will be designated as Competent Authorities [and may be competent for more than one area of legislation]. After being registered in the system, CAs will be able to send and receive information requests via IMI.*" [In jedem Mitgliedstaat werden Stellen der öffentlichen Verwaltung als zuständige Behörden benannt werden [die für mehr als einen Rechtsbereich zuständig sein können.] Nach ihrer Registrierung im System werden die zuständigen Behörden Anfragen über das IMI senden und empfangen können.] Ungeachtet ihrer Beziehungen zu den nachgeordneten IMI-Koordinatoren (in den Mitgliedstaaten, die sich für die Benennung solcher Koordinatoren

entscheiden) werden alle zuständigen Behörden in einem bestimmten Mitgliedstaat vom nationalen IMI-Koordinator des betreffenden Mitgliedstaats überwacht.[5]

Die Artikel-29-Datenschutzgruppe weist darauf hin, dass in einigen Mitgliedstaaten nicht immer alle Informationen, die eine anfragende zuständige Behörde über einen bestimmten Wanderarbeiter oder Dienstleistungserbringer benötigt, bei einer einzigen zuständigen Behörde verfügbar sind. Es kann zum Beispiel nötig sein, zwischen der Anerkennung von Berufsabschlüssen, für die ein bestimmter Kabinettsminister zuständig sein könnte, und der Anerkennung von Berufszulassungen, für die ein Berufsverband zuständig sein könnte, zu unterscheiden. In solchen Fällen kann es notwendig sein, dass die anfragende zuständige Behörde zwei verschiedene zuständige Behörden kontaktiert. Die Artikel-29-Datenschutzgruppe begrüßt, dass die Gestalter des IMI zur Lösung dieser und ähnlicher Probleme ein Netz von Koordinatoren innerhalb jedes Mitgliedstaats vorgesehen haben, die den anfragenden zuständigen Behörden, wie in den Abschnitten 2.2.c und 2.2.d beschrieben wird, dabei helfen, die richtigen Ansprechpartner in anderen Mitgliedstaaten zu finden. Gleichzeitig betont die Artikel-29-Datenschutzgruppe, dass die Schnittstelle des IMI auch so gestaltet werden muss, dass die Gefahr von Missverständnissen darüber, welche Behörde für eine bestimmte Angelegenheit zuständig ist, gering gehalten wird.

2.2.c Nationaler IMI-Koordinator (NIMIK)

Jeder Mitgliedstaat wird einen nationalen Koordinator für das IMI bestellen, der als oberste IMI-Behörde und in der Kommunikation mit der Europäischen Kommission und den anderen Mitgliedstaaten als direkter Ansprechpartner für alle technischen Fragen des IMI und für die Fälle fungiert, in denen Verfahren zur Behandlung eskalierender Probleme nötig sind, um Antworten auf Anfragen zu erhalten.

Wie im Dokument „Issue Paper on Data Protection in IMI“ festgelegt, wird ein NIMIK eine Liste aller Anfragen einsehen können, die von den zuständigen Behörden oder den nachgeordneten IMI-Koordinatoren (NaIMIK) seines Mitgliedstaats abgesandt oder empfangen wurden, wobei diese Liste aber keine personenbezogenen Daten enthalten wird.

Die Artikel-29-Datenschutzgruppe begrüßt diese Beschränkung, da die NIMIK für die Erfüllung ihrer Aufgaben — wie die Kommission bestätigt — keinen Zugriff auf personenbezogene Daten zu benötigen scheinen. Deshalb würde ein Zugang zu personenbezogenen Daten gegen Artikel 6 Absatz 1 Buchstabe c) der Datenschutzrichtlinie verstoßen, nach dem die Mitgliedstaaten sicherstellen müssen, dass personenbezogene Daten *„den Zwecken entsprechen, für die sie erhoben und/oder weiterverarbeitet werden, dafür erheblich sind und nicht darüber hinausgehen“*.

Des Weiteren ist die Artikel-29-Datenschutzgruppe überzeugt, dass es notwendig ist, diese Beschränkung ausdrücklich festzuhalten und die Informationen, die in diesen Listen enthalten sein werden, genauer zu bestimmen.

Die Artikel-29-Datenschutzgruppe vertritt auch die Auffassung, dass die Verteilung der Kompetenzen und Pflichten zwischen der Kommission, den Koordinatoren und den zuständigen Behörden klarer zu definieren ist, zumal sich ihre Rollen im IMI am besten als eine gemeinsame Verantwortung für die Datenverarbeitung beschreiben lassen. In gewissem

[5] Die Funktionen der nachgeordneten und nationalen IMI-Koordinatoren werden in den Abschnitten 2.2.c und 2.2.d behandelt.

Maße wird nach Ansicht der Artikel-29-Datenschutzgruppe jeder Akteur im IMI in einer bestimmten Kapazität sowohl die Funktion eines Auftragsverarbeiters als auch die Funktion des für die Verarbeitung Verantwortlichen übernehmen je nachdem, welche Verarbeitungsaktivität in einer spezifischen Situation ausgeführt wird. Die Komplexität des IMI führt dazu, dass möglicherweise nicht immer klar erkennbar ist, ob die Akteure Auftragsverarbeiter, für die Verarbeitung Verantwortliche oder beides sind. Die Möglichkeit solcher Verwechslungen unterstreicht, wie wichtig es ist, das spezifische Ziel für jeden einzelnen Datenverarbeitungsschritt ausdrücklich anzugeben; dadurch können alle Beteiligten verstehen, welche Verwendung der Daten angemessen ist und wie sie die Datenschutzvorschriften auch in Fällen einhalten können, in denen ihre Handlungen gemischter oder nicht eindeutiger Natur sind.

2.2.c Nachgeordneter IMI-Koordinator (NaIMIK)

Eine dritte Funktion, deren Einrichtung im Ermessen jedes Mitgliedstaats liegt, ist der optionale NaIMIK, der die Funktionen koordiniert und überwacht, die einzelne zuständige Behörden in einem bestimmten Rechts- oder Politikbereich wahrnehmen.

Wie im „Issue Paper on Data Protection in IMI“ erläutert, kann ein NaIMIK eine Liste aller Anfragen einsehen, die von den mit ihm verbundenen zuständigen Behörden abgesandt oder empfangen wurden. Laut dem Dokument wird diese Liste für die Überwachung des Anfragenflusses durch den Koordinator ausreichende Informationen auf einer hohen Ebene, aber keine Verknüpfungen zu personenbezogenen Daten enthalten. Diese Funktion wurde eigens eingeführt, um Mitgliedstaaten mit einem zentralisierten System für zuständige Behörden eine Koordinierung mit Mitgliedstaaten zu ermöglichen, die stärker dezentralisiert sind oder viele zuständige Behörden haben.

Die Artikel-29-Datenschutzgruppe weist darauf hin, dass die unterschiedlichen Funktionen der NIMIK und NaIMIK sowie ihre Verantwortung für die Gewährleistung eines angemessenen Schutzes der personenbezogenen Daten, die unter ihrer Aufsicht ausgetauscht werden, geklärt und besser definiert werden müssen, damit ihre Auswirkungen konkreter analysiert werden können.

2.2.e Angeschlossene Behörden

Eine zuständige Behörde kann anderen Stellen der öffentlichen Verwaltung im eigenen Mitgliedstaat auch einen *„Überwachungszugang“* gewähren. Dadurch kann eine andere Stelle eine Liste aller Anfragen einsehen, die von der zuständigen Behörde abgesandt oder empfangen wurden, aber sie kann nicht auf die verarbeiteten personenbezogenen Daten zugreifen.

Diese Möglichkeit würde es fachlich relevanten Organisationen (z. B. Berufsverbänden) erlauben, eine anonymisierte Liste von Anfragen an verwandte Organisationen einzusehen, um vielleicht sicherzustellen, dass die Anfragen an die richtigen zuständigen Behörden weitergeleitet werden. Die Artikel-29-Datenschutzgruppe vertritt allerdings die Ansicht, dass die spezifischen Ziele und Vorteile der Funktion dieser angeschlossenen Behörden sowie die genauen Informationen, zu denen sie Zugang erhalten, expliziter festzulegen sind, damit gewährleistet ist, dass es tatsächlich zu keinem unbefugten Zugriff auf personenbezogene Daten kommt.

2.3 Rollen und Rechte im System

Die wichtigsten Datenverarbeitungsschritte im IMI erfolgen während des Informationsaustauschs zwischen den zuständigen Behörden der Mitgliedstaaten, aber auch die Kommission selbst wird personenbezogene Daten, nämlich Informationen über die zuständigen Behörden, verarbeiten. Die an der Verarbeitung personenbezogener Daten Beteiligten — seien es die zuständigen Behörden, die NIMIK oder die NaIMIK — unterliegen stets den einzelstaatlichen Rechtsvorschriften zur Umsetzung der Richtlinie 95/46/EG[6] im eigenen Mitgliedstaat. Die Kommission wiederum hat die Datenschutzverordnung einzuhalten.

Angesichts der verschiedenen Rollen und Akteure im IMI ist es nötig festzulegen, für welche Arten der Datenverarbeitung jeder dieser Akteure als der „für die Verarbeitung Verantwortliche" betrachtet wird. In Artikel 2 Buchstabe d) der Datenschutzrichtlinie wird der „für die Verarbeitung Verantwortliche" definiert als die *„natürliche oder juristische Person, Behörde, Einrichtung oder jede andere Stelle, die allein oder gemeinsam mit anderen über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheidet"*.

Im Gegensatz dazu ist der „Auftragsverarbeiter" nach Artikel 2 Buchstabe e) dieser Richtlinie *„die natürliche oder juristische Person, Behörde, Einrichtung oder jede andere Stelle, die personenbezogene Daten im Auftrag des für die Verarbeitung Verantwortlichen verarbeitet"*. Somit ist der Auftragsverarbeiter die Person oder Behörde, die die Daten gemäß den Anweisungen des für die Verarbeitung Verantwortlichen tatsächlich verarbeitet.

Des Weiteren ist in Artikel 17 Absatz 3 der Datenschutzrichtlinie vorgesehen, dass die Verarbeitung personenbezogener Daten durch einen Dritten (der nicht der für die Verarbeitung Verantwortliche ist) auf der Grundlage eines Vertrags oder Rechtsakts erfolgen muss, durch den der Auftragsverarbeiter an den für die Verarbeitung Verantwortlichen gebunden ist und der insbesondere sicherstellt, dass der Auftragsverarbeiter nur auf Weisung des für die Verarbeitung Verantwortlichen handelt.

In diesem Dokument werden nicht alle möglichen Szenarien für die Datenverarbeitung im Einzelnen analysiert. Die Artikel-29-Datenschutzgruppe vertritt allerdings die Ansicht, dass der für die Verarbeitung Verantwortliche in jedem einzelnen Verarbeitungsschritt für die Einhaltung der in diesem Dokument festgelegten Grundsätze und Garantien, unter anderem in Bezug auf Sicherheitsmaßnahmen, zuständig ist. Ein Auftragsverarbeiter seinerseits wird für die Erfüllung seiner Geheimhaltungspflichten, das Ergreifen geeigneter Sicherheitsmaßnahmen und die Gewährleistung der Befolgung der Weisungen der für die Verarbeitung Verantwortlichen zuständig sein.

Die zuständigen Behörden und die Kommission müssen klar verstehen, dass sie gemeinsam die Verantwortung für das Speichern und Löschen von Daten tragen. Es wird notwendig sein, ein Dokument zu verfassen, in dem die Rahmenbedingungen für diese Verarbeitungsschritte zwischen dem für die Verarbeitung Verantwortlichen und dem Auftragsverarbeiter dargelegt werden. In diesem Dokument sind die Aufgaben und Verantwortlichkeiten der Beteiligten klar festzulegen.

Durch den Aufbau des IMI entsteht ein außergewöhnlich komplexes Netz von für die Verarbeitung Verantwortlichen und Auftragsverarbeitern. Folglich ist es notwendig zu

[6] ABl. L 281, 23.11.1995, S. 31.

erkennen, dass die Verantwortung jedes Beteiligten je nach Art der einzelnen Handlungen variieren kann und dass nicht immer klar ist, ob ein Akteur ein für die Verarbeitung Verantwortlicher oder ein Auftragsverarbeiter ist. Unabhängig von dieser Unterscheidung müssen natürlich alle Stellen, die für die Verarbeitung von Daten verantwortlich sind oder sie selbst verarbeiten, das Niveau an Datensicherheit gewährleisten und die Datenverarbeitungsgrundsätze einhalten, die in der Datenschutzrichtlinie und in der Datenschutzverordnung festgelegt sind.

3. Verarbeitete personenbezogene Daten

Das IMI kann sich potenziell auf die Grundrechte einer großen Anzahl von Wanderarbeitern und Dienstleistungserbringern auswirken, die ihr Recht auf Freizügigkeit innerhalb der Europäischen Union ausüben. Das System speichert auch Daten über die Nutzer des IMI (Mitarbeiter der zuständigen Behörden, der NIMIK und der NaIMIK).

Laut Artikel 2 der Datenschutzrichtlinie sind personenbezogene Daten *„alle Informationen über eine bestimmte oder bestimmbare natürliche Person“*.[7] Da das IMI solche Daten für zwei unterschiedliche Zwecke verarbeiten und speichern wird, kann die Artikel-29-Datenschutzgruppe davon ausgehen, dass das System zwei verschiedene Kategorien der Verarbeitung von personenbezogenen Daten umfasst.

- Die erste betrifft die personenbezogenen Daten der zuständigen Behörden (sowie der NIMIK und NaIMIK), die das IMI verwenden. Da die betreffenden Personen Ansprechpartner der Nutzer sind, werden ihre Telefonnummern, Namen, E-Mail-Adressen und ähnliche Angaben im System gespeichert werden. Die Daten, die über diese Personen erfasst werden, sind speziell aufzulisten und dürfen gemäß der Richtlinie nur so viele Angaben umfassen, wie für die Funktionen des Systems erforderlich sind (Qualität der Daten).

- Die zweite Art der Datenverarbeitung betrifft die Arbeitnehmer und Dienstleistungserbringer im Zusammenhang mit der Dienstleistungsrichtlinie und der Richtlinie über Berufsqualifikationen. Zu diesen Daten werden der Name, die Telefonnummer, die E-Mail-Adresse, das Geburtsdatum und die Staatsangehörigkeit jedes Dienstleistungserbringers (für gewöhnlich, wenn dies für die Zwecke der Identifizierung relevant ist) sowie Angaben zu ihren Berufsqualifikationen und sensiblere Daten, wie zum Beispiel Informationen über gute Führung, Disziplinarmaßnahmen, Vorstrafen und die Rechtmäßigkeit der Niederlassung, gehören.

4. Rechtliche Analyse des Systems und spezifische Fragen

4.1 Rechtsgrundlage für die Verarbeitung personenbezogener Daten (Artikel 7)

Die Richtlinie über Berufsqualifikationen und die Dienstleistungsrichtlinie sehen beide spezifische Verpflichtungen zur Verwaltungszusammenarbeit zwischen den Mitgliedstaaten vor, in denen auch ein Austausch von Informationen, die in den meisten Fällen *„bestimmte oder bestimmbare natürliche Personen“* betreffen, enthalten ist. Das bedeutet, dass sich der relevante Rechtsrahmen durch die Übernahme dieser Richtlinien ins einzelstaatliche Recht erheblich verändern wird; die in Bezug auf das IMI eingeführten Regeln müssen allerdings

[7] Siehe Stellungnahme 4/2007 zum Begriff „personenbezogene Daten“, WP 136.

den allgemeinen Grundsätzen für den Datenschutz entsprechen, die in der Datenschutzrichtlinie und der Datenschutzverordnung festgelegt sind.

Das IMI wird zwangsläufig bedeutende Auswirkungen auf die Mechanismen der Datenverarbeitung und die damit verbundenen Überwachungs- und Kontrollaktivitäten haben, mit denen die zuständigen Behörden betraut werden.

Artikel 56 der Richtlinie über Berufsqualifikationen lautet:

„1. Die zuständigen Behörden der Aufnahme- und Herkunftsmitgliedstaaten arbeiten eng zusammen und leisten sich Amtshilfe, um die Anwendung dieser Richtlinie zu erleichtern. Sie stellen die Vertraulichkeit der ausgetauschten Informationen sicher.

2. Die zuständigen Behörden im Aufnahme- und Herkunftsmitgliedstaat unterrichten sich gegenseitig über das Vorliegen disziplinarischer oder strafrechtlicher Sanktionen oder über sonstige schwerwiegende, genau bestimmte Sachverhalte, die sich auf die Ausübung der in dieser Richtlinie erfassten Tätigkeiten auswirken könnten; dabei sind die Rechtsvorschriften über den Schutz personenbezogener Daten im Sinne der Richtlinien 95/46/EG des Europäischen Parlaments und des Rates vom 24. Oktober 1995 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr (1) und 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) einzuhalten.“

In Artikel 28 der Dienstleistungsrichtlinie wird ebenfalls Amtshilfe gefordert:

„1. Die Mitgliedstaaten leisten einander Amtshilfe und ergreifen Maßnahmen, die für eine wirksame Zusammenarbeit bei der Kontrolle der Dienstleistungserbringer und ihrer Dienstleistungen erforderlich sind…

6. Die Mitgliedstaaten stellen die von anderen Mitgliedstaaten oder von der Kommission angeforderten Informationen so schnell wie möglich auf elektronischem Wege zur Verfügung.“

Die in diesen beiden Richtlinien vorgesehene Zusammenarbeit ist sorgfältig durchzuführen, macht aber verbesserte Kapazitäten und Reaktionsfähigkeiten nötig. Daher fordert die Dienstleistungsrichtlinie die Schaffung eines elektronischen Hilfsmittels für einen vereinfachten, rascheren Informationsaustausch. Konkret ist nach Artikel 34 vorgesehen, dass die Kommission *„in Zusammenarbeit mit den Mitgliedstaaten ein elektronisches System für den Austausch von Informationen zwischen den Mitgliedstaaten [einrichtet], wobei sie bestehende Informationssysteme berücksichtigt.“*

Nach Ansicht der Artikel-29-Datenschutzgruppe ist es notwendig, klar und deutlich festzuhalten, dass das IMI den bestehenden Datenschutzvorschriften entsprechen muss. Diese Anforderung ist in Artikel 43 der Dienstleistungsrichtlinie ausdrücklich enthalten, wodurch die Bedeutung einer anhaltenden und konsequenten Anwendung der Datenschutzrichtlinie und der Richtlinie 2002/58/EG („Datenschutzrichtlinie für elektronische Kommunikation“) unterstrichen wird.

Ganz allgemein findet sich die Rechtsgrundlage für die Datenverarbeitung in den Mitgliedstaaten in Artikel 7 der Datenschutzrichtlinie, in dem die Bedingungen für rechtmäßige Datenverarbeitungsaktivitäten festgelegt sind. Insbesondere dürfen personenbezogene Daten nach Artikel 7 Buchstabe c) verarbeitet werden, wenn dies „für die Erfüllung einer rechtlichen Verpflichtung erforderlich [ist], der der für die Verarbeitung Verantwortliche unterliegt“. *Artikel 5 Buchstabe b) der Datenschutzverordnung enthält ähnliche Bestimmungen.*

Wie oben erwähnt, schafft Artikel 34 der Dienstleistungsrichtlinie diese rechtliche Verpflichtung für die für die Verarbeitung Verantwortlichen und erlaubt es ihnen daher (nach der Übernahme der Richtlinie in einzelstaatliches Recht), die relevanten personenbezogenen Daten zu verarbeiten. Diese Rechtsgrundlage wirft jedoch mehrere potenziell problematische Fragen auf.

Erstens wird in der Richtlinie über Berufsqualifikationen zwar auch die Zusammenarbeit gefordert, aber es ist darin kein elektronisches Hilfsmittel für den Austausch von Informationen vorgesehen. In Artikel 56 Absatz 2 ist tatsächlich eine Verpflichtung zum Austausch von Informationen zwischen den zuständigen Behörden der Mitgliedstaaten über disziplinarische oder strafrechtliche Sanktionen oder über sonstige schwerwiegende, genau bestimmte Sachverhalte festgelegt, die sich auf die Ausübung der in dieser Richtlinie erfassten Tätigkeiten auswirken könnten, aber die Einrichtung eines elektronischen Systems für diesen Zweck wird darin nicht erwähnt. Nach anderen Bestimmungen der Richtlinie sollen auch Informationen in dem Maße ausgetauscht werden, als eine zuständige Behörde berechtigte Zweifel in Bezug auf einen gewissen Aspekt hat. Obwohl die Rechtsgrundlage für den Informationsaustausch nach Ansicht der GD MARKT in diesen spezifischen Bestimmungen zu finden ist, ist es fraglich, ob sie für die Datenverarbeitung mit Hilfe des IMI im Rahmen der Zusammenarbeit nach der Richtlinie über Berufsqualifikationen wirklich ausreicht.

Zweitens müssen die Richtlinie über Berufsqualifikationen und die Dienstleistungsrichtlinie in einzelstaatliches Recht übernommen worden sein, damit Artikel 7 Buchstabe c) als Rechtsgrundlage für die Datenverarbeitung herangezogen werden kann. Wenn ein bestimmter Mitgliedstaat die Richtlinien nicht umgesetzt hat, ist es wiederum fraglich, ob eine geeignete Rechtsgrundlage besteht und ob somit die Verarbeitung von Daten über das IMI zulässig ist.

Darüber hinaus betont die Artikel-29-Datenschutzgruppe auch, dass sichergestellt werden muss, dass jeder einzelne Datenaustausch gerechtfertigt ist, selbst wenn die Dienstleistungsrichtlinie und die Richtlinie über Berufsqualifikationen nach ihrer Umsetzung im einzelstaatlichen Recht eine Rechtsgrundlage allgemeiner Natur bieten. Insbesondere muss jeder einzelne Fall der Datenverarbeitung einen genau bestimmten, eindeutigen und rechtmäßigen Zweck sowie eine angemessene eigene Rechtsgrundlage für diesen Zweck haben.

Des Weiteren weist die Artikel-29-Datenschutzgruppe schließlich darauf hin, dass Artikel 7 Buchstabe e) der Datenschutzrichtlinie wohl auch eine zusätzliche, ergänzende Rechtsgrundlage für die Verarbeitung darstellen könnte: *„die Verarbeitung ist erforderlich für die Wahrnehmung einer Aufgabe, die im öffentlichen Interesse liegt oder in Ausübung öffentlicher Gewalt erfolgt und dem für die Verarbeitung Verantwortlichen oder dem Dritten, dem die Daten übermittelt werden, übertragen wurde“*. Zweck des IMI ist es, Informationen bereitzustellen und die Zusammenarbeit der verschiedenen zuständigen Behörden in den einzelnen Mitgliedstaaten zu erleichtern. Dies liegt im öffentlichen Interesse, da es dazu

beiträgt, das reibungslose Funktionieren des Binnenmarkts für diejenigen Personen zu gewährleisten, die das Recht auf Niederlassungsfreiheit und freien Dienstleistungsverkehr in der Ausübung ihrer beruflichen Tätigkeit nutzen wollen.

Angesichts der aufgezeigten rechtlichen Unsicherheiten empfiehlt die Artikel-29-Datenschutzgruppe trotz der potenziellen Verfügbarkeit von Artikel 7 Buchstaben c) und e), dass als Ad-hoc-Lösung zur Unterstützung der Rechtsgrundlage, wie von der Kommission selbst vor Kurzem beschlossen, eine Kommissionsentscheidung zur Festlegung der Durchführungsbestimmungen angenommen wird. Neben der Stärkung der Rechtsgrundlage für die Datenverarbeitung sollte in der Entscheidung auch festgelegt werden, welche Datenfelder in die Datenbank aufgenommen werden und welchen Mindestinhalt die Anfragen, Antworten und Datenflüsse haben sollen. Des Weiteren sollten darin die Rollen und Verantwortlichkeiten der verschiedenen Akteure und die rechtlichen Erfordernisse vom Standpunkt des Datenschutzes definiert werden.

4.2 Anwendung der Grundsätze für die Qualität der Daten (Artikel 6)

4.2.a Qualität und Notwendigkeit der Daten

Das IMI ist ein Hilfsmittel, das eigens darauf ausgelegt ist, Informationen auszutauschen und den zuständigen Behörden bei Bedarf Zugang zu diesen Informationen zu ermöglichen. Dies stellt einen Informationsfluss dar, der zum Teil sensible Daten umfasst (wobei die Daten, wie nachstehend in Abschnitt 4.2.c dargelegt, sechs Monate lang gespeichert werden) und der deshalb den Grundsätzen entsprechen muss, die in Artikel 8 der Datenschutzrichtlinie festgelegt sind. Das IMI unterliegt ausdrücklich den Garantien der Datenschutzrichtlinie für die Wahrung der legitimen Rechte der betroffenen Personen, die in allen Mitgliedstaaten in das einzelstaatliche Recht übernommen worden sind.

Erstens ist das Erfordernis der Qualität der Daten nach Artikel 6 der Datenschutzrichtlinie zu erfüllen. Gemäß diesem Grundsatz dürfen personenbezogene Daten nur zur Erreichung festgelegter, eindeutiger und rechtmäßiger Zwecke erhoben und nicht in einer mit diesen Zweckbestimmungen unvereinbaren Weise weiterverarbeitet werden. Dementsprechend erfordert die Einhaltung dieses Grundsatzes, dass klar definiert wird, für welchen Zweck personenbezogene Daten mit dem IMI erhoben und verarbeitet werden.

Zweitens ist es nötig, die Erfüllung der Grundsätze der Verhältnismäßigkeit und der Rechtmäßigkeit unter Berücksichtigung der Risiken für den Datenschutz, der Grundrechte von Einzelpersonen und insbesondere der eventuellen Notwendigkeit einer Weitergabe von Informationen über disziplinarrechtliche Maßnahmen zu analysieren.

4.2.b Verhältnismäßigkeit

Die Verhältnismäßigkeit ist ein wesentlicher Grundsatz im Rechtsrahmen, der von der Richtlinie 95/46/EG und der Verordnung (EG) Nr. 45/2001 abgesteckt wird. Er erfordert, dass die zuständigen Behörden in den Fragebögen, die zum Informationsaustausch im IMI verwendet werden, keine Informationen übermitteln dürfen, die im Hinblick auf das festgelegte Ziel des Austauschs irrelevant oder unangemessen sind. Deshalb muss der Zweck des Informationsaustauschs bezüglich eines Wanderarbeiters oder Dienstleistungserbringers im Voraus definiert werden.

Ein vollständiger Bericht über jeglichen Informationsaustausch kann in allen Amtssprachen der EU durch benannte Personen ausgedruckt werden. Das IMI wird auch Kapazitäten für das Laden und Speichern von relevanten zusätzlichen Dokumenten oder Bildern bieten.

Des Weiteren empfiehlt die Artikel-29-Datenschutzgruppe im Zusammenhang mit der Anwendung des Grundsatzes der Verhältnismäßigkeit, dass die für das IMI verantwortliche zuständige Behörde sorgfältig prüft, ob es zweckmäßig ist, die Anzahl der Personen zu beschränken, die zum Absenden und Beantworten von Anfragen berechtigt sind.

Darüber hinaus ist es wichtig, dass der Fragenkatalog, über den die zuständigen Behörden im IMI Informationen austauschen können, unter Beachtung des Grundsatzes der Verhältnismäßigkeit ausgearbeitet wird. Dazu wäre die sicherste Option vom Standpunkt des Datenschutzes her, alle Datenfelder (d. h. alle vorgegebenen Fragen und Antworten) in der vorgeschlagenen Kommissionsentscheidung zur Festlegung der Durchführungsbestimmungen genau aufzuführen (siehe Abschnitt 4.1). Die Artikel-29-Datenschutzgruppe räumt allerdings ein, dass die Entwickler des Systems voraussichtlich ein gewisses Maß an Flexibilität für künftige Anpassungen und Verbesserungen des IMI gewährleisten wollen. Um diese gegensätzlichen Anliegen abzudecken und gleichzeitig auch den Informationsaustausch transparent zu halten, empfiehlt die Artikel-29-Datenschutzgruppe, dass in der neuen Kommissionsentscheidung mit den Durchführungsbestimmungen ausdrücklich festgelegt werden sollte, dass (i) alle vorgegebenen Fragen direkt aus den Bestimmungen der Richtlinie über Berufsqualifikationen und der Dienstleistungsrichtlinie (oder aus weiteren Richtlinien, die in der Zukunft möglicherweise in einen aktualisierten Anhang der Kommissionsentscheidung aufgenommen werden) abgeleitet werden müssen, (ii) sie in Absprache mit Betroffenen in den Mitgliedstaaten formuliert werden müssen und (iii) die vorgegebenen Fragen und Antworten auf der Website des IMI öffentlich zugänglich gemacht werden müssen.

4.2.c Besondere Fragen hinsichtlich der Aufbewahrung von personenbezogenen Daten

Die Kommission beabsichtigt, eine automatische sechsmonatige Aufbewahrungsfrist vorzusehen und auch automatische Meldungen zur Erinnerung an das Löschen der Daten in die Systemarchitektur einzubauen.

Die Datenschutzrichtlinie schreibt vor, dass personenbezogene Daten nicht länger aufbewahrt werden, als es für die Realisierung der Zwecke erforderlich ist, für die sie erhoben oder weiterverarbeitet werden (siehe Artikel 6 Absatz 1 Buchstabe e) der Datenschutzrichtlinie und Verordnung (EG) Nr. 45/2001). Dies ist von wesentlicher Bedeutung für die Einhaltung des Grundsatzes der Verhältnismäßigkeit bei der Verarbeitung von personenbezogenen Daten.

Die Artikel-29-Datenschutzgruppe vertritt die Ansicht, dass die von der Kommission vorgeschlagene sechsmonatige Aufbewahrungsdauer auf den ersten Blick angemessen erscheinen kann, zumal Rückfragen zu einem bestimmten Fall zwischen den zuständigen Behörden auftreten könnten. Allerdings empfiehlt die Artikel-29-Datenschutzgruppe, dass die Gründe, weshalb die Daten genau für diesen Zeitraum aufbewahrt werden sollen, in der künftigen Kommissionsentscheidung zur Festlegung der Durchführungsbestimmungen erläutert werden sollten.

4.2.c.i Aufbewahrung von Daten durch die Kommission

Die auf dem Server der Kommission in Luxemburg gespeicherten Daten müssen ähnlichen Datenschutzregeln unterliegen wie die Daten, die in den Datenbanken der Mitgliedstaaten aufbewahrt werden. Insbesondere dürfen diese Daten nur so lange im IMI belassen werden, wie sie für die Erreichung der Zwecke benötigt werden, für die sie erfasst wurden.

Die auf dem Server gespeicherten Daten dürfen nicht für andere Zwecke oder Anfragen verwendet werden und müssen stets im Einklang mit dem Datenschutzrecht verarbeitet werden. Es ist von entscheidender Bedeutung, dass sie gegen unbefugte Zugriffe geschützt sind.

Die Bestimmung der angemessenen Aufbewahrungsdauer innerhalb von sechs Monaten und somit der Einhaltung von Artikel 4 Buchstabe e) der Verordnung (EG) Nr. 45/2001 erfordert ein eindeutiges, ausdrücklich festgelegtes Verständnis des Ziels oder des Zwecks jeder einzelnen Datenverarbeitung, wobei auch ein Schutz der Daten gegen unerlaubten Zugang wesentlich ist.

4.2.c.ii Aufbewahrungsfrist für die von nationalen Behörden verarbeiteten und gespeicherten Daten

Falls nationale Behörden ebenfalls personenbezogene Daten aufbewahren, so dürfen diese Daten nur bis zum Abschluss des Austauschs oder der Transaktion, für die sie erfasst wurden, gespeichert werden, wobei die im einzelstaatlichen Recht der Mitgliedstaaten festgelegten besonderen Fristen für die Löschung der Daten einzuhalten sind.

Dieses Erfordernis wird äußerst wichtig in Fällen, in denen ein Bediensteter der zuständigen Behörde in der Lage ist, diese Informationen auf der lokalen Festplatte oder einem anderen Speichermedium seines eigenen Computers aufzubewahren. Die Beschränkung der Aufbewahrungsdauer kommt auch hier zum Tragen, und die Daten müssen gesperrt werden, sobald sie für die Zwecke, für die sie erhoben wurden, nicht mehr benötigt werden. Selbstverständlich gilt diese Anforderung zusätzlich zu den Verpflichtungen, die sich aus den Datenschutzregeln auf nationaler Ebene ergeben.

4.2.d Besonders geschützte Daten

Die Verarbeitung sensibler Daten erfordert besondere Aufmerksamkeit für die Einhaltung der Datenschutzbestimmungen. Die für sensible Daten geltenden Bedingungen und Einschränkungen sind in Artikel 8 der Datenschutzrichtlinie und in Artikel 10 der Verordnung (EG) Nr. 45/2001 festgelegt.

Zu diesen Daten gehören Angaben über die rassische oder ethnische Herkunft, politische Meinungen, religiöse oder philosophische Überzeugungen, eine Gewerkschaftszugehörigkeit, die Gesundheit oder das Sexualleben. Die Verarbeitung von Daten, die Straftaten, strafrechtliche Verurteilungen oder Sicherungsmaßregeln betreffen, werden nach der Richtlinie (und der Verordnung (EG) Nr. 45/2001) ebenfalls zu den sensiblen Daten gezählt. Die Mitgliedstaaten können Angaben über administrative Strafen oder zivilrechtliche Urteile ebenfalls als sensible Daten einstufen.

Laut dem Dokument „Issue Paper on Data Protection in IMI“ ist *„not intended“* [nicht beabsichtigt], derartige sensible Daten mit dem IMI zu verarbeiten. Der Informationsaustausch über das IMI könnte jedoch möglicherweise Angaben über die Gesundheit enthalten — zum Beispiel im Falle von Personen mit Behinderungen, die sich um einen Arbeitsplatz bewerben.

Die Artikel-29-Datenschutzgruppe vertritt die Ansicht, dass die Formulierung *„not intended“* zu vage und zu wenig streng ist. Um die Einhaltung der Datenschutzbestimmungen sicherzustellen, muss ein verbindlicher Wortlaut gewählt werden: sensible Daten „dürfen nicht verarbeitet werden“. Jegliche Ausnahmen sollten klar und deutlich angegeben werden und zusätzlichen Garantien unterliegen.

In Artikel 8 der Datenschutzrichtlinie wird eindeutig festgelegt, dass die *„Mitgliedstaaten […] die Verarbeitung personenbezogener Daten, aus denen die rassische und ethnische Herkunft, politische Meinungen, religiöse oder philosophische Überzeugungen oder die Gewerkschaftszugehörigkeit hervorgehen, sowie von Daten über Gesundheit oder Sexualleben [untersagen].“* Artikel 10 der Verordnung (EG) Nr. 45/2001 enthält eine ähnliche Formulierung.

Insbesondere ist in Artikel 8 Absatz 5 Folgendes vorgesehen: *„Die Verarbeitung von Daten, die Straftaten, strafrechtliche Verurteilungen oder Sicherungsmaßregeln betreffen, darf nur unter behördlicher Aufsicht oder aufgrund von einzelstaatlichem Recht, das angemessene Garantien vorsieht, erfolgen, wobei ein Mitgliedstaat jedoch Ausnahmen aufgrund innerstaatlicher Rechtsvorschriften, die geeignete besondere Garantien vorsehen, festlegen kann. Ein vollständiges Register der strafrechtlichen Verurteilungen darf allerdings nur unter behördlicher Aufsicht geführt werden.*

Die Mitgliedstaaten können vorsehen, dass Daten, die administrative Strafen oder zivilrechtliche Urteile betreffen, ebenfalls unter behördlicher Aufsicht verarbeitet werden müssen.“

Die Richtlinie über Berufsqualifikationen bietet in Artikel 56 Absatz 2 eine Rechtsgrundlage für eine gegenseitige Unterrichtung über das Vorliegen disziplinarischer oder strafrechtlicher Sanktionen, wobei bekräftigt wird, dass der Austausch solcher Daten den oben genannten Bestimmungen entsprechen muss. Die spezifischen Bedingungen für den Austausch von strafrechtlichen Informationen sollten allerdings auf den einzelstaatlichen Rechtsvorschriften zur Umsetzung der Richtlinie 95/46/EG beruhen.

„Die zuständigen Behörden im Aufnahme- und Herkunftsmitgliedstaat unterrichten sich gegenseitig über das Vorliegen disziplinarischer oder strafrechtlicher Sanktionen oder über sonstige schwerwiegende, genau bestimmte Sachverhalte, die sich auf die Ausübung der in dieser Richtlinie erfassten Tätigkeiten auswirken könnten; dabei sind die Rechtsvorschriften über den Schutz personenbezogener Daten im Sinne der Richtlinien 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 [Datenschutzrichtlinie] und 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) einzuhalten.“

Des Weiteren sind in Artikel 33 der Dienstleistungsrichtlinie spezifische Regeln für den Austausch von Informationen über die Zuverlässigkeit von Dienstleistungserbringern vorgesehen. Diese Bestimmungen sind rechtzeitig vor der Umsetzung umfassend zu analysieren, um ihre Folgen für den Datenschutz zu bewerten. *„Auf Ersuchen einer zuständigen Behörde eines anderen Mitgliedstaats übermitteln die Mitgliedstaaten unter Beachtung ihres nationalen Rechts Informationen über Disziplinar- oder Verwaltungsmaßnahmen oder strafrechtliche Sanktionen und Entscheidungen wegen Insolvenz oder Konkurs mit betrügerischer Absicht, die von ihren zuständigen Behörden gegen einen Dienstleistungserbringer verhängt wurden und die von direkter Bedeutung für die Kompetenz oder berufliche Zuverlässigkeit des Dienstleistungserbringers sind. Der Mitgliedstaat, der die Informationen zur Verfügung stellt, informiert den Dienstleistungserbringer darüber."*

Was die rechtlichen Bestimmungen anbelangt, welche die Datenverarbeitung legitimieren, müssen die Grundsätze der Datenschutzrichtlinie berücksichtigt werden, in der die Begriffe Verhältnismäßigkeit, Qualität der Daten und Verwendungsbeschränkungen im Datenschutz konkreter erklärt werden. Es ist unerlässlich sicherzustellen, dass personenbezogene Informationen sowohl richtig als auch aktuell sind, wenn sensible Daten ausgetauscht werden. Veraltete Angaben aus Strafregistern sollten zum Beispiel nicht ausgetauscht werden.

Ferner werden Situationen auftreten, in denen Angaben im Zusammenhang mit administrativen Strafen für die Ausübung eines Berufs in einem bestimmten Mitgliedstaat nicht unbedingt nötig sind. In diesem Fall ist das berufliche Statut sowohl im Herkunftsmitgliedstaat als auch im Zielmitgliedstaat eines Dienstleistungserbringers zu beachten. Ohne Bedachtnahme auf die besondere Relevanz der Daten in einer solchen Situation muss die Datenverarbeitung über das IMI dem in der Datenschutzrichtlinie vorgesehenen Grundsatz der Verhältnismäßigkeit entsprechen.[8]

In Bezug auf Informationen über offene Schulden und strafrechtliche Vergehen wird im „Arbeitspapier über Schwarze Listen" (WP 65)[9] Folgendes aufgeführt:

„Artikel 8 der Richtlinie 95/46/EG nennt in den Absätzen 5 und 6 die Verarbeitung von Daten, die Straftaten oder strafrechtliche Verurteilungen betreffen, und legt allgemein fest, dass eine solche Verarbeitung nur unter behördlicher Aufsicht erfolgen darf. Allerdings kann ein Mitgliedstaat Ausnahmen aufgrund einzelstaatlicher Rechtsvorschriften festlegen, die zum einen geeignete Garantien vorsehen müssen, welche die Grundrechte der Bürger schützen, und die zum anderen der Europäischen Kommission mitzuteilen sind.

Die Legitimierung für die Verarbeitung derartiger Verzeichnisse, die Daten, die strafrechtliche Vergehen betreffen, enthalten, findet sich in der Pflicht der Staatsgewalt, die Aufrechterhaltung der öffentlichen Sicherheit und Ordnung zu gewährleisten. Dies ist gemäß den Bestimmungen von Artikel 7 Buchstabe e der Richtlinie zweifellos ein Grundsatz, der eine

---

[8] In der Richtlinie 2002/92/EG über Versicherungsvermittlung wird beispielsweise genau dargelegt, inwieweit Informationen über Straftaten und Zuverlässigkeit für die Ausübung dieses Berufes relevant sind. Nach Artikel 4 Absatz 2 müssen *„Versicherungs- und Rückversicherungsvermittler […] einen guten Leumund besitzen. Als Mindestanforderung dürfen sie nicht im Zusammenhang mit schwerwiegenden Straftaten in den Bereichen Eigentums- oder Finanzkriminalität ins Strafregister oder ein gleichwertiges einzelstaatliches Register eingetragen und sollten nie in Konkurs gegangen sein, es sei denn, sie sind gemäß nationalem Recht rehabilitiert worden."*

[9] WP 65. http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2002/wp65_de.pdf.

derartige Verarbeitung rechtfertigt, sofern die im vorstehenden Absatz genannten Einschränkungen eingehalten werden.

Was die Verarbeitung personenbezogener Daten, die strafrechtliche Vergehen betreffen, anbelangt, so gibt es in den meisten Mitgliedstaaten Verzeichnisse, die derartige Daten enthalten und die unter behördlicher Aufsicht stehen. …

Bei dieser Art der Verarbeitung müssen in jedem Fall die Grundsätze der Qualität der gespeicherten Daten und insbesondere der sachlichen Richtigkeit und der Aktualisierung gewährleistet sein. Besonders berücksichtigt werden muss auch das Recht auf offizielle oder automatische Berichtigung und Löschung der Daten der betroffenen Person nach Ablauf der gesetzlich festgesetzten Speicherdauer und unter entsprechender Anwendung der verschiedenen Mechanismen, die dies ermöglichen, da die Speicherung personenbezogener Daten in diesen Verzeichnissen über die gesetzlich festgesetzte Dauer hinaus für die Betroffenen nachteilige Folgen haben kann.

Besondere Bedeutung kommt diesen Punkten im Fall von Freisprüchen, Verjährung oder Rehabilitierung zu; bei einer weiteren Speicherung entsprechender Daten wäre die Zweckbestimmung nicht mehr gegeben. Hierzu ist festzustellen, dass diese Aspekte in den meisten Mitgliedstaaten im Strafrecht geregelt sind, wobei es allerdings eine gewisse Bandbreite von Kriterien gibt.

Ein weiterer grundsätzlicher Punkt, den es zu berücksichtigen gilt, betrifft den Zugang zu den Daten bzw. die Frage, welche Personen oder Institutionen berechtigt sind, von den in den Verzeichnissen enthaltenen Daten Kenntnis zu erhalten. Darüber hinaus müssen die betroffenen Personen in jedem Fall das Recht auf Zugang zu den sie betreffenden, in einem Verzeichnis enthaltenen Daten haben.

Diese Möglichkeit des Zugangs kann schwierige und problematische Situationen zur Folge haben wie z. B. den Fall, dass sich der Betroffene um einen Arbeitsplatz bewirbt und — in Mitgliedstaaten, in denen dies zulässig ist — der Arbeitgeber im Rahmen des Auswahlverfahrens von dem Bewerber ein polizeiliches Führungszeugnis verlangt, das von einer für das Verzeichnis verantwortlichen Behörde ausgestellt wurde. Der Bewerber würde in diesem Fall das geforderte Zeugnis erhalten, das ggf. Angaben über strafrechtliche Verurteilungen oder andere Sicherungsmaßregeln enthalten würde. Auf diese Weise erhielte der Arbeitgeber Zugang zu Dateninhalten, über die er auf direktem Wege rechtmäßig keine Kenntnis erlangen würde.

Durch eine spätere Nutzung entsprechender Informationen durch den Arbeitgeber könnte dieser angenommene Fall noch komplizierter werden, denn im Prinzip stünde die reine Heranziehung der ihm durch den Bewerber im Rahmen des Auswahlverfahrens zur Verfügung gestellten Informationen nicht im Widerspruch zu den Bestimmungen von Artikel 8 Absatz 5 der Richtlinie, eine spätere manuelle oder automatische Verarbeitung jedoch schon."

Um die unnötige Übermittlung dieser sensiblen, aber nicht immer relevanten Daten auf ein Mindestmaß zu beschränken, empfiehlt die Artikel-29-Datenschutzgruppe, dass in allen Fällen, in denen die Weiterleitung von konkreten Auskünften aus dem Strafregister nicht absolut notwendig ist, die vorgegebenen Fragen und Antworten in der Nutzerschnittstelle des IMI keine Angaben aus dem Strafregister fordern und anders formuliert werden sollten, um den Austausch sensibler Daten zu minimieren. Die zuständige Behörde eines Gastlandes kann

sich beispielsweise mit der Information zufrieden geben, dass ein zuwandernder Rechtsanwalt in seinem Heimatland ordnungsgemäß in das Anwaltsverzeichnis eingetragen ist und keine disziplinarischen Sanktionen der Rechtsanwaltskammer gegen ihn vorliegen, und muss nicht davon Kenntnis erlangen, dass ein Verstoß gegen Verkehrsvorschriften in seinem Strafregister aufscheint, wenn dies in seinem Heimatland kein Hindernis für die Ausübung des Anwaltsberufs darstellt.

4.3 Verwendung einer nationalen Kennziffer

Im „Issue Paper on Data Protection in IMI" heißt es: "*Finally, Member states, in accordance with Article 8 para 7. of Directive 95/46/CE shall determine the conditions under which a national identification number or any other identifier of general application may be processed. Processing such personal data will certainly make the information exchange between competent authorities easier to the extent that it will facilitate the identification of the provider concerned. National restrictions on such an exchange of data would not therefore seem justified*." [Schließlich müssen die Mitgliedstaaten im Einklang mit Artikel 8 Absatz 7 der Richtlinie 95/46/EG die Bedingungen bestimmen, unter denen eine nationale Kennziffer oder andere Kennzeichen allgemeiner Bedeutung verarbeitet werden dürfen. Die Verarbeitung solcher personenbezogener Daten werden den Informationsaustausch zwischen den zuständigen Behörden insofern vereinfachen, als sie die Identifizierung des betreffenden Dienstleistungserbringers erleichtern. Nationale Beschränkungen eines solchen Datenaustauschs würden daher nicht gerechtfertigt erscheinen.]

Dies ist eine äußerst heikle Frage. Die Regelung der Verarbeitung von nationalen Kennziffern liegt nach Artikel 8 Absatz 7 der Datenschutzrichtlinie ausdrücklich im Ermessen der Mitgliedstaaten: *„Die Mitgliedstaaten bestimmen, unter welchen Bedingungen eine nationale Kennziffer oder andere Kennzeichen allgemeiner Bedeutung Gegenstand einer Verarbeitung sein dürfen."* Daher sind die Mitgliedstaaten dafür zuständig, alle Bedingungen und Modalitäten, einschließlich möglicher Beschränkungen, festzulegen, unter denen eine nationale Kennziffer über das IMI übermittelt werden darf. In einigen Mitgliedstaaten ist zum Beispiel die Verwendung von Kennziffern streng geregelt und erfordert die Genehmigung eines speziellen Ausschusses, der bei der Datenschutzbehörde eingerichtet ist. Eine solche Beschränkung ist nach der Datenschutzrichtlinie zulässig und gilt daher auch im Zusammenhang mit dem IMI.

5. Rechte der betroffenen Personen

5.1 Auskunftsrecht

Gemäß den Artikeln 10 und 11 der Datenschutzrichtlinie müssen die für die Verarbeitung Verantwortlichen die betroffenen Personen über die Verarbeitung ihrer Daten informieren. Die Datenschutzverordnung enthält ebenfalls diese Verpflichtung zur Information der betroffenen Personen. Für die Fälle, in denen die Daten direkt bei der betroffenen Person erhoben werden, schreibt Artikel 10 der Datenschutzrichtlinie die Erteilung klarer und vollständiger Auskünfte über das System vor und verpflichtet den für die Verarbeitung Verantwortlichen dazu, die betroffenen Personen über das Bestehen, die Zweckbestimmung und die Funktionsweise des Systems, die Empfänger der Daten und das Recht auf Zugang, Berichtigung und Löschung zu informieren.

Darüber hinaus müssen die für die Verarbeitung Verantwortlichen nach Artikel 11 der Datenschutzrichtlinie die betroffenen Personen davon unterrichten, wenn ihre personenbezogenen Daten bei einem Dritten und nicht direkt von ihnen erhoben werden. Das Auskunftsrecht erlaubt auch die Ausübung der oben angeführten Rechte.

Zur Vereinfachung dieses Auskunftsrechts würde die Artikel-29-Datenschutzgruppe eine abgestufte Vorgehensweise bei der Information der betroffenen Personen empfehlen.

Dadurch könnten mehrere Maßnahmen berücksichtigt werden, wie zum Beispiel eine Mitteilung darüber, dass die Informationen nach den Artikeln 10 und 11 der Richtlinie — nämlich die Identität des für die Verarbeitung Verantwortlichen und die Zweckbestimmung der Verarbeitung — vorab der betroffenen Person übermittelt werden müssen, um eine Verarbeitung nach Treu und Glauben zu gewährleisten.

Erstens sollte auf der Website der Kommission ein ausführlicher Hinweis angebracht werden, der die Informationen gemäß den Artikeln 10 und 11 der Datenschutzrichtlinie und den entsprechenden Bestimmungen der Datenschutzverordnung enthält, die Rolle der Kommission und der zuständigen Behörden genau beschreibt und die Rechte der betroffenen Personen klar und deutlich aufzeigt.

Zweitens sollte jede zuständige Behörde auf ihrer eigenen Website einen Datenschutzhinweis anbringen, der auch einen Link zum entsprechenden Hinweis auf der Website der Kommission enthält.

Drittens müssen schließlich im IMI ebenso wie in anderen Zusammenhängen die erforderlichen Mitteilungen und Auskünfte auch direkt, individuell und unverzüglich erfolgen, sobald Dokumente von Bürgern oder zuständigen Behörden erfasst werden. Alle Akteure im IMI sollten ausdrücklich auf diese Verpflichtung aufmerksam gemacht werden.

5.2 Rechte auf Zugang, Berichtigung, Löschung und Sperrung

Artikel 12 der Datenschutzrichtlinie, der das Recht auf Zugang zu Daten und auf deren Berichtigung betrifft, räumt jeder betroffenen Person das Recht ein, Zugang zu den über sie gespeicherten Daten zu erhalten, um deren Richtigkeit zu prüfen und diese zu korrigieren, falls sie unrichtig, unvollständig oder veraltet sind. Das IMI muss so aufgebaut sein, dass die Wahrung des Rechts von Einzelpersonen auf den Zugang zu den Daten und auf Berichtigung von falschen, unvollständigen oder veralteten Daten sichergestellt ist.

Des Weiteren müssen die betroffenen Personen das Recht haben, ihre Daten zu berichtigen oder zu löschen, wenn die Verarbeitung solcher Daten, insbesondere aufgrund ihrer Unvollständigkeit oder Unrichtigkeit, gegen die Bestimmungen der Datenschutzrichtlinie verstößt (gemäß Artikel 12 Buchstabe b)).

Im Falle einer Berichtigung oder Sperrung von unrichtigen oder aus anderen Gründen ungültigen Daten muss der für die Verarbeitung Verantwortliche alle zuständigen Behörden informieren, die ebenfalls an der unrechtmäßigen Verarbeitung beteiligt waren. Diese Verantwortung ist ausdrücklich darzulegen. Die Aufnahme einer eigenen Schnittstelle für die Durchführung solcher Verständigungen in das IMI wäre für alle Betroffenen höchst hilfreich. Es könnte auch nötig sein, ein Verfahren einzuführen, das bei Ausübung des Rechts auf die Löschung von Daten durch die Bürger sicherstellt, dass diese Daten tatsächlich aus allen

Datenbanken, auch aus denjenigen außerhalb des IMI, entfernt werden, wobei auch eine Koordinierung zwischen den zuständigen Behörden eingerichtet wird.

Jegliche Verweigerung des Zugangs muss auf einer spezifischen Ausnahme nach den anwendbaren einzelstaatlichen Datenschutzvorschriften beruhen und muss hinreichend begründet sein.

Wenn die betreffende Behörde nicht innerhalb eines angemessenen Zeitraums antwortet oder keine Einwände erhebt, kann die Behörde, bei welcher der Antrag auf Einsichtnahme in die Daten gestellt wurde, auf der Grundlage ihres eigenen einzelstaatlichen Rechts entscheiden. Wenn sich die Behörden nicht einig sind, ob der Zugang zu den Daten gewährt werden sollte, dann sollte die Behörde, welche die Informationen bereitgestellt hat, diejenige sein, welche letztlich die Kriterien für die Entscheidung über den Zugang ansetzt.

Wenn der Zugang verweigert wird, müssen die Gründe dafür klar dargelegt werden und die betroffenen Personen darauf hingewiesen werden, dass sie sich stattdessen an eine andere zuständige Behörde wenden können, um Zugang zu den Daten erhalten, oder die Datenschutzbehörde nach Artikel 28 unbeschadet des Rechts auf Einleitung eines Gerichtsverfahrens kontaktieren können.

Ähnliche Verfahren für die Zusammenarbeit sollten im Zusammenhang mit der Berichtigung, Löschung oder Sperrung von Daten vorhanden sein.

Wenn ein Ersuchen um Zugang zu Daten an die Kommission gerichtet wird, darf die Kommission nur Zugang zu den Daten gewähren, zu denen sie selbst rechtmäßig Zugang hat, so dass die betroffenen Personen an die Behörde zu verweisen sind, die Zugang zu den Informationen hat, wobei die in der Datenschutzverordnung festgelegten Garantien zu beachten sind.

5.3 Abhilfemaßnahmen

Es ist ebenfalls unbedingt notwendig sicherzustellen, dass betroffene Personen in Fällen, in denen ihre garantierten Rechte verletzt werden, Rechtsmittel ergreifen können. Personen, für die die nicht ordnungsgemäße oder unrechtmäßige Verarbeitung ihrer personenbezogenen Daten negative Auswirkungen nach sich zieht, müssen auch das Recht haben, eine Wiedergutmachung des erlittenen Schadens zu fordern.

6. Sicherheit

Nach Artikel 17 der Datenschutzrichtlinie müssen die für die Verarbeitung Verantwortlichen geeignete technische und organisatorische Maßnahmen ergreifen, um personenbezogene Daten vor zufälliger oder unrechtmäßiger Zerstörung, zufälligem Verlust, unberechtigter Weitergabe oder unberechtigtem Zugang zu schützen. Diese Sicherheitsmaßnahmen sollten im Verhältnis zu den Zwecken, für welche die Daten erhoben werden, angemessen sein und den Sicherheitsregelungen der einzelnen Mitgliedstaaten entsprechen. Ähnliche Anforderungen sind auch in den entsprechenden Bestimmungen der Datenschutzverordnung enthalten.

Die Rechtmäßigkeit eines Datenverarbeitungssystems mit einem außerordentlich hohen Risikopotenzial hängt von der Aufrechterhaltung eines ausreichend hohen Niveaus der Datensicherheit für jeden Aspekt der Funktionsweise des Systems ab.

Um die Sicherheit des Systems angesichts der möglichen Verarbeitung von besonders sensiblen Daten (z. B. Informationen über strafrechtliche Sanktionen) zu gewährleisten, erachtet es die Artikel-29-Datenschutzgruppe zudem als wesentlich, die Umsetzung einer Reihe spezifischer Maßnahmen technischer und organisatorischer Natur vorzuschreiben, welche eine Veränderung, einen Verlust oder eine unberechtigte Verarbeitung der Daten oder einen unberechtigten Zugang zu ihnen verhindern und so die Geheimhaltung und Integrität der Informationen gewährleisten. Auch wenn in diesem Dokument keine spezifischen technologischen Rahmen oder Hilfsmittel für die Datensicherheit empfohlen werden, sind diese Kriterien zu erfüllen, damit das IMI personenbezogene Daten angemessen schützt.

Die Sicherheitsmaßnahmen müssen ausreichen, um sicherzustellen, dass:

- unbefugte Personen nicht auf das System zugreifen können;
- überprüft werden kann, welche Daten wann und von wem verarbeitet wurden;
- die Dateneingabe kontrolliert wird, um ein unbefugtes Hinzufügen oder Verändern von Daten zu verhindern;
- Zugangskontrollen vorhanden sind, die gewährleisten, dass die Nutzer lediglich zu den Daten Zugang erhalten, zu deren Verarbeitung sie befugt sind;
- die Kommunikation kontrolliert wird, um bestimmen zu können, welche Behörden berechtigt sind, gewisse Daten weiterzugeben;
- die Datenübermittlung sicher ist, um ein unbefugtes Zugreifen, Kopieren, Verändern oder Unterdrücken von Daten während des Informationsaustauschs zu verhindern.

Der Schwerpunkt weiterer Maßnahmen liegt auf der Erstellung von Sicherungskopien, der Datenwiederherstellung, der Erprobung des Systems anhand von echten Daten vor der Implementierung und der Übertragung über Telekommunikationsnetze entweder durch Kodierung der Informationen oder mit Hilfe anderer Mechanismen, die gewährleisten, dass die Informationen von Dritten nicht verstanden und auch nicht manipuliert werden können.

Die Kommission wird für diese Maßnahmen im Zusammenhang mit der Funktionsweise und Sicherheit des zentralen Servers verantwortlich sein, aber sichere Verfahren der Vernetzung sind auch auf Ebene der Mitgliedstaaten von entscheidender Bedeutung.

Des Weiteren unterliegt die Kommission den Sicherheitsvorschriften der Datenschutzverordnung, die aber im Lichte der am besten bewährten Verfahren in den Mitgliedstaaten ausgelegt werden sollten.

Die zuständigen Behörden werden für die Einhaltung der Datenschutzvorschriften in ihrem jeweiligen Mitgliedstaat sowie der Anforderungen für die Datensicherheit nach Artikel 17 der Datenschutzrichtlinie verantwortlich sein.

Zumal die Kommission keine Notwendigkeit für einen Zugang zu den personenbezogenen Daten der Wanderarbeiter oder Dienstleistungserbringer, die auf dem zentralen Server gespeichert sind, sieht, empfiehlt die Artikel-29-Datenschutzgruppe auch, dass diese Daten verschlüsselt werden sollten, um eine sichere Kommunikation zwischen den zuständigen Behörden der Mitgliedstaaten zu ermöglichen, wodurch die Kommission effektiv daran gehindert würde, auf diese Daten zuzugreifen.

7. Meldung bei der Datenschutzbehörde und Vorabkontrolle

In Anwendung der Artikel 18 bis 20 der Datenschutzrichtlinie werden Organisationen, die das IMI nutzen, die Bestimmungen über die Meldepflicht oder Vorabkontrolle durch zumindest einige nationale Datenschutzbehörden erfüllen müssen.

In den Mitgliedstaaten, die ein solches Verfahren vorsehen, unterliegt die Verarbeitung möglicherweise einer Vorabkontrolle durch die nationale Datenschutzbehörde, soweit diese Verarbeitungen ein spezifisches Risiko für die Rechte und Freiheiten der Betroffenen beinhalten können. Dies könnte der Fall sein, wenn einzelstaatliche Rechtsvorschriften die Verarbeitung von Daten über mutmaßliche Straftaten nur unter besonderen Bedingungen erlauben (zu denen wiederum eine Vorabkontrolle durch die zuständige einzelstaatliche Aufsichtsbehörde gehören kann).

Dies könnte ferner der Fall sein, wenn die nationale Behörde der Auffassung ist, dass die Verarbeitung gemeldete Personen möglicherweise von einem Recht, einem Vorteil oder einem Vertrag ausschließt. Die Abwägung, ob solche Verarbeitungen unter die Vorabkontrolle fallen, obliegt der einzelstaatlichen Gesetzgebung und den Praktiken der nationalen Datenschutzbehörde.

Nach Artikel 20 der Datenschutzrichtlinie kann die Vorabkontrolle auch im Zuge der Ausarbeitung einer Maßnahme des nationalen Parlaments oder einer auf eine solche gesetzgeberische Maßnahme gestützten Maßnahme durchgeführt werden, die die Art der Verarbeitung festlegt und geeignete Garantien vorsieht.

Die Europäische Kommission ihrerseits hat einen Datenschutzbeauftragten gemäß Artikel 24 der Datenschutzverordnung bestellt. Die auf Ebene der Kommission durchgeführten Datenverarbeitungen werden ihm im Einklang mit Artikel 25 der Verordnung gemeldet werden. Das IMI wird nach Artikel 26 auch in das Register des Datenschutzbeauftragten aufgenommen werden. Angesichts der Rolle der Kommission bei den Datenverarbeitungen in diesem spezifischen Fall ist eine Vorabkontrolle durch den europäischen Datenschutzbeauftragten wahrscheinlich nicht nötig (Artikel 27 der Datenschutzverordnung).

8. Übermittlung von personenbezogenen Daten in Drittstaaten

Das IMI soll nicht der internationalen Übermittlung von Daten in Länder außerhalb der Europäischen Gemeinschaft dienen; sein in Artikel 34 der Dienstleistungsrichtlinie festgelegter Zweck besteht im Austausch von Informationen zwischen den Mitgliedstaaten.

Die Artikel-29-Datenschutzgruppe möchte betonen, dass diese Daten nicht außerhalb des Rahmens des IMI übermittelt werden dürfen, da dies alleine schon die Grenzen des ursprünglich festgelegten Zwecks der Verarbeitung überschreiten würde. Die Übermittlung von Daten aus dem IMI in Drittstaaten würde daher gegen die Verwendungsbeschränkung nach Artikel 6 Absatz 1 Buchstabe b) der Datenschutzrichtlinie verstoßen.

9. Schlussfolgerungen und Empfehlungen der Artikel-29-Datenschutzgruppe

1. Das IMI muss vollständig im Einklang mit den Grundsätzen gestaltet werden, welche in anwendbaren Datenschutzvorschriften, einschließlich der Datenschutzrichtlinie und der Datenschutzverordnung, festgelegt sind. Die Grundsätze des Datenschutzes sind

im System ordnungsgemäß zu implementieren, wenn das Potenzial des IMI zur besseren Wahrung des Grundrechts auf den Schutz personenbezogener Daten ausgeschöpft werden soll.

2. Daher möchte die Artikel-29-Datenschutzgruppe betonen, wie wichtig es ist, dass die Erfordernisse des Datenschutzes hinsichtlich der Qualität der Daten, der Notwendigkeit und der Verhältnismäßigkeit eingehalten werden. Diese sollten in jeder Phase der Entwicklung des IMI und von allen Akteuren im System berücksichtigt werden — bei der Formulierung von standardisierten Anfragen, bei der Auswahl der zuständigen Behörden usw. Das IMI sollte den Datenschutzbehörden in den Mitgliedstaaten, in denen solche Verfahren gemäß Artikel 18 der Datenschutzrichtlinie vorgesehen sind, gemeldet werden und von diesen einer Vorabkontrolle unterzogen werden.

3. Das IMI ist ein komplexes System, das den Prozess des Informationsaustauschs durch Bereitstellung zusätzlicher Hilfsmittel für die Mitgliedstaaten vereinfachen kann. Diese Veränderungen müssen allerdings mit der genauen Einhaltung der Grundsätze aus der Datenschutzrichtlinie Hand in Hand gehen. Die Nutzer des IMI müssen besonders aufmerksam die Einhaltung der nationalen Gesetze und der Richtlinie gewährleisten, da ihre Möglichkeiten der Informationsübermittlung durch die digitale Kommunikation und durch die Beilage von Dokumenten ausgebaut werden. Des Weiteren muss die Aufsichtsrolle der nationalen Datenschutzbehörden und anderer Kontrollen, die in den verschiedenen Mitgliedstaaten vorhanden sind, erforderlichenfalls gewahrt werden. Die einzigartige Funktion der Europäischen Kommission muss samt den damit verbundenen Pflichten auch im Rahmen des IMI ausdrücklich anerkannt werden.

4. Um die zuständigen Behörden besser in die Lage zu versetzen, das IMI auf eine mit den Datenschutzvorschriften vereinbare Weise zu verwenden, ist es nötig, die genauen Funktionen aller Nutzer im System klarzustellen. Die IMI-Koordinatoren und die angeschlossenen Behörden sind besser zu definieren und ihre Rechte und Pflichten, einschließlich der spezifischen Informationen, zu denen sie Zugang erhalten werden, sind ausdrücklich festzulegen. Dadurch wird die unnötige Verarbeitung von Daten auf ein Mindestmaß beschränkt, der Schutz der Rechte der Bürger und der Mitarbeiter der zuständigen Behörden gewährleistet und gleichzeitig die Effizienz des IMI gesteigert.

5. Es ist wichtig, die Kompetenzen und Pflichten der Kommission, der Koordinatoren und der zuständigen Behörden klar abzugrenzen, da sich ihre Funktionen im IMI am besten als gemeinsame Verantwortung für die Datenverarbeitung beschreiben lassen.

6. Im Zuge der Weiterentwicklung des IMI muss eine sorgfältige Neubewertung der potenziellen Anwendungen des Systems für die Übermittlung sensibler Daten erfolgen, was selbst im Zusammenhang der ersten Implementierung für die Richtlinie über Berufsqualifikationen und die Dienstleistungsrichtlinie gilt. Solche Anwendungen sind keine abstrakten Wahrscheinlichkeiten; sie sind vielmehr schon jetzt festgelegt (zum Beispiel in Artikel 56 der Richtlinie über Berufsqualifikationen, wo der Austausch von Informationen aus dem Strafregister angeführt wird, die nun über das IMI übermittelt werden können). Da das IMI beinahe sicher für die Verarbeitung von Daten über die Gesundheit, Vorstrafen oder anderer geschützter

Informationen eingesetzt wird, müssen auch die vorhandenen Garantien im Bereich der Sicherheitsmaßnahmen und Kontrollen neu überdacht und verbessert werden.

7. Es ist von größter Bedeutung, dass jede einzelnen Datenverarbeitungsmaßnahme auf einer eigenen, legitimen Rechtsgrundlage beruht, die auf ihre spezifischen Zwecke und Ziele zugeschnitten ist.

8. Die Notwendigkeit einer konkreteren Rechtsgrundlage für jede einzelne Transaktion im IMI zeigt sehr deutlich auf, dass eine ausdrückliche Festlegung der Ziele der Datenverarbeitungen in diesem System erforderlich ist. Nur wenn ein klares Ziel definiert ist, können sich die Akteure im IMI sicher sein, dass sie die Grundsätze der Notwendigkeit, der Qualität der Daten und der Verhältnismäßigkeit einhalten. Jedes dieser Kriterien bezieht sich direkt auf den Zweck der Verarbeitung. Auch die Fristen für die Aufbewahrung der Daten hängen von einem genauen Verständnis des Ziels der Maßnahme ab; man kann nicht wissen, ob eine Aufgabe abgeschlossen ist, wenn man sich über ihr gewünschtes Ergebnis unsicher ist. In einem Netz von Datenverarbeitungsbeziehungen, das so komplex ist wie im IMI, in dem unklar sein kann, wer welche Funktion erfüllt, ist eine ausdrückliche Festlegung der Ziele der Datenverarbeitung absolut unerlässlich, um unter ungewissen Umständen Entscheidungen über das Verhalten auf der Grundlage von fundierten Informationen zu erlauben.

9. Das IMI kann niemals 27 unterschiedlichen einzelstaatlichen Rechtssystemen untergeordnet werden. Aus diesem Grund ist eine spezifischere Kommissionsentscheidung nötig; diese muss genaue Bestimmungen enthalten und sollte die oben erläuterten Bereiche, in denen Bedenken auftreten, behandeln.

Brüssel, den _____ 2007

Für die Datenschutzgruppe

Der Vorsitzende
Peter Schaar