Stellungnahme zu einer Meldung des Datenschutzbeauftragten der Europäischen Kommission für eine Vorabkontrolle des Systems zum Elektronischen Austausch von Sozialversicherungsdaten („EESSI“)

Brüssel, den 28. Juli 2011 (Fall 2011-0016)

1. Verfahren

Am 5. Januar 2011 erhielt der Europäische Datenschutzbeauftragte („EDSB“) eine Meldung des Datenschutzbeauftragten der Europäischen Kommission für eine Vorabkontrolle des Systems zum Elektronischen Austausch von Sozialversicherungsdaten („EESSI“). Es handelt sich hierbei effektiv um eine Vorabkontrolle; gemäß Durchführungszeitplan ist vorgesehen, dass das EESSI gegen Ende des Übergangszeitraums zum 1. Mai 2012 in Betrieb genommen werden wird.

1.1. Voraussetzungen für die Einrichtung des EESSI

Das EESSI ist ein von der EU entwickeltes Informationssystem, das als groß angelegtes IT-System betrachtet werden kann, da es den grenzüberschreitenden Austausch einer bestimmten Menge an personenbezogenen Daten im Bereich der System der sozialen Sicherheit zwischen allen Mitgliedstaaten vorsieht. Das EESSI hat folglich erhebliche Auswirkungen auf den Schutz der Privatsphäre und der personenbezogenen Daten der Bürger.

Die Auswirkungen eines solchen groß angelegten IT-Systems auf den Schutz der Privatsphäre und der personenbezogenen Daten der Bürger werden auf zwei Ebenen bewertet: (1) auf der legislativen Ebene ist gemäß Artikel 28 Absatz 2 der Verordnung (EG) Nr. 45/2001 vorgesehen, dass der EDSB bei einem Vorschlag für Rechtsvorschriften der EU zur Einführung eines solchen groß angelegten IT-Systems konsultiert wird; (2) auf der Durchführungsebene müssen die nationalen Datenschutzbehörden der Mitgliedstaaten und der EDSB im Hinblick auf die Datenverarbeitung seitens der EU-Organe und -Einrichtungen angemessen über die Datenverarbeitung informiert werden.

Der EDSB stellt mit Zufriedenheit fest, dass er gemäß Artikel 28 Absatz 2 der Verordnung (EG) Nr. 45/2011 von der Kommission im Hinblick auf den Entwurf der Durchführungsverordnung zur Koordinierung der Systeme der sozialen Sicherheit, die die Rechtsgrundlage des EESSI darstellt und technische Details enthält, konsultiert wurde. In seiner beratenden Stellungnahme[1] hat der EDSB den rechtlichen Rahmen für die Durchführung des EESSI kommentiert und einige spezifische Fragen aufgeworfen, bei

[1] Stellungnahme des EDSB zum Vorschlag für eine Verordnung des Europäischen Parlaments und des Rates zur Festlegung der Modalitäten für die Durchführung der Verordnung (EG) Nr. 883/2004 über die Koordinierung der Systeme der sozialen Sicherheit (KOM (2006)16 endgültig), verabschiedet am 6. März 2007.

denen aus datenschutzrechtlicher Sicht angemessene Maßnahmen ergriffen werden müssen. Einige der Fragen wurden in der Durchführungsverordnung selbst behandelt, deren endgültige Fassung einige der Vorschläge enthält, die vom EDSB unterbreitet wurden; andere dagegen machen weitere Umsetzungsschritte seitens der Mitgliedstaaten und/oder der Kommission erforderlich.

Der EDSB unterstreicht deshalb, dass die vorliegende Stellungnahme zur Vorabkontrolle, in der eine Bewertung der Durchführungsmaßnahmen vorgenommen wird, die ihm von der Kommission gemeldet wurden, gemeinsam mit der beratenden Stellungnahme zu berücksichtigen ist.

1.2. Frist für die Stellungnahme

Gemäß Artikel 27 Absatz 4 der Verordnung (EG) Nr. 45/2001 muss diese Stellungnahme innerhalb von zwei Monaten abgegeben werden, wobei diese Frist ausgesetzt werden kann, bis dem EDSB weitere von ihm erbetene Auskünfte vorliegen. Der EDSB ersuchte die Kommission am 17. Februar 2011 um weitere Informationen. Diese wurden am 3. März 2011 bzw. am 6. April 2011 übermittelt. Die Frist für die Abgabe der Stellungnahme wurde ursprünglich auf den 26. April 2011 festgesetzt (da der 24. April ein Samstag und der 25. April Ostermontag war). Angesichts der Kompliziertheit des Falles wurde die Frist gemäß Artikel 27 Absatz 4 der Verordnung um einen Monat verlängert. Am 28. April wurden weitere Fragen unterbreitet, die anlässlich einer Sitzung zwischen dem Personal des EDSB und der GD EMPL am 22. Juni 2011 erörtert wurden. Weitere Erklärungen wurden schriftlich am 6. Juli 2011 und am 8. Juli 2011 übermittelt. Der EDSB übermittelte den Entwurf seiner Stellungnahme am 18. Juli 2011 zur Stellungnahme, die am 27. Juli 2011 einging. Das Verfahren wurde insgesamt für einen Zeitraum von 182 Tagen ausgesetzt. Folglich muss die vorliegende Stellungnahme spätestens am 14. August 2011 abgegeben werden.

2. Sachverhalt

Das **EESSI** ist ein ICT-System, im Rahmen dessen die für den Bereich der sozialen Sicherheit zuständigen Behörden der Mitgliedstaaten zu Zwecken des elektronischen Datenaustauschs miteinander verbunden werden. Dieses System wurde von der Europäischen Kommission auf der Grundlage der Verordnung (EG) Nr. 883/2004, in ihrer durch die Verordnung (EG) Nr. 988/2009 (der „Grundverordnung“) geänderten Form, und der Verordnung (EG) Nr. 987/2009 (der „Durchführungsverordnung) über die Koordinierung der Systeme der sozialen Sicherheit entwickelt.

Anwendungsbereich des EESSI: Vom geographischen Gesichtspunkt aus gelten die EU-Bestimmungen im Bereich der Koordinierung der Systeme der sozialen Sicherheit nicht nur auf EU-Gebiet sondern auch in einer Reihe anderer teilnehmender Staaten[2], nämlich Island, Liechtenstein, Norwegen und die Schweiz. Die EU-Bestimmungen im Bereich der Koordinierung der Systeme der sozialen Sicherheit gelten für die Bürger der EU-Mitgliedstaaten und der teilnehmenden Staaten sowie für Drittstaatsangehörige, die sich rechtmäßig in der EU aufhalten und in mehr als einem EU-Mitgliedstaat gearbeitet haben. Der Datenaustausch wird zwischen den zuständigen Behörden aller teilnehmenden Staaten in den Bereichen erfolgen, die den Verordnungen zur Koordinierung der Systeme der sozialen Sicherheit unterliegen:

[2] Der Einfachheit halber wird in dieser Stellungnahme nur auf die „Mitgliedstaaten“ Bezug genommen. Jeder Verweis in dieser Stellungnahme auf die „Mitgliedstaaten“ ist jedoch dahingehend auszulegen, dass auch die EWR-Staaten (Island, Liechtenstein, Norwegen) und die Schweiz gemeint sind.

- Leistungen bei Krankheit, Leistungen bei Mutterschaft und gleichgestellte Leistungen bei Vaterschaft
- Altersrenten, Leistungen für den Vorruhestand und bei Invalidität
- Leistungen für Hinterbliebene und Sterbegeld
- Arbeitslosengeld
- Familienleistungen
- Leistungen im Falle von Arbeitsunfällen und Berufskrankheiten

Zweck des EESSI ist es, den Schutz der Rechte der Bürger zu stärken, indem der elektronische Austausch von personenbezogenen Sozialversicherungsdaten von Wanderarbeitnehmern innerhalb der EU zwischen den zuständigen Behörden der Mitgliedstaaten ermöglicht wird. Ziel ist es, die 200 Papierformulare, die derzeit für die Kommunikation zwischen den Behörden verwendet werden, durch das EESSI zu ersetzen. Mit diesem System für den rechnergestützten Austausch von Daten im Rahmen des EESSI wird insbesondere (1) die Entscheidungsfindung bei der Berechnung und Auszahlung von Sozialversicherungsleistungen erleichtert und beschleunigt; (2) eine effizientere Datenprüfung ermöglicht; (3) eine flexiblere und benutzerfreundliche Schnittstelle zwischen verschiedenen Systemen bereitgestellt und (4) eine genaue Erhebung statistischer Daten über den europäischen Datenaustausch ermöglicht.
Zeitrahmen: Die Verordnungen zur Koordinierung der Systeme der sozialen Sicherheit traten am 1. Mai 2010 in Kraft; es wurde jedoch ein Übergangszeitraum von zwei Jahren vorgesehen, um es den Mitgliedstaaten zu gestatten, ihre nationalen Anwendungen mit dem EESSI-System zu verbinden. Ab dem 1. Mai 2012 sollten alle Behörden mit dem EESSI verbunden sein und Informationen austauschen können.

Verantwortliche der Datenverarbeitung: Rollen und Verantwortlichkeiten
Der Betrieb des EESSI macht eine gemeinsame Verantwortung der Mitgliedstaaten und der Kommission erforderlich:

- **Auf der Ebene der Mitgliedstaaten** werden die personenbezogenen Daten von den zuständigen Behörden der Mitgliedstaaten entsprechend den nationalen Datenschutzbestimmungen zur Umsetzung der Richtlinie 95/46/EG erfasst. Jede zuständige Behörde ist für die eigene Datenverarbeitung und für den Austausch personenbezogener Daten im EESSI verantwortlich entsprechend den Bestimmungen gemäß den Artikeln 77[3] und 78[4] der Grundverordnung. Gemäß Richtlinie 95/46/EG können die für den Bereich der Sozialversicherung zuständigen Behörden als für die Datenverarbeitung Verantwortlichen identifiziert werden und haben folglich alle entsprechenden Pflichten und Verantwortlichkeiten.

[3] Artikel 77 sieht Folgendes vor: „*Werden personenbezogene Daten aufgrund dieser Verordnung oder der Durchführungsverordnung von den Behörden oder Trägern eines Mitgliedstaats den Behörden oder Trägern eines anderen Mitgliedstaats übermittelt, so gilt für diese Datenübermittlung das Datenschutzrecht des übermittelnden Mitgliedstaats. Für jede Weitergabe durch die Behörde oder den Träger des Empfängermitgliedstaats sowie für die Speicherung, Veränderung oder Löschung der Daten durch diesen Mitgliedstaat gilt das Datenschutzrecht des Empfängermitgliedstaats. Die für die Anwendung dieser Verordnung und der Durchführungsverordnung erforderlichen Daten werden durch einen Mitgliedstaat an einen anderen Mitgliedstaat unter Beachtung der Gemeinschaftsbestimmungen über den Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und den freien Datenverkehr übermittelt.*“

[4] Artikel 78 Absatz 2 sieht insbesondere Folgendes vor: „*Jeder Mitgliedstaat betreibt seinen Teil der elektronischen Datenverarbeitungsdienste in eigener Verantwortung unter Beachtung der Gemeinschaftsbestimmungen über den Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und den freien Datenverkehr*“.

- **Rolle der Kommission bei der Bestimmung des Zwecks und der Mittel der Datenverarbeitung im EESSI**: Gemäß der Meldung an den EDSB ist die Kommission im Hinblick auf ihre Rolle im EESSI ein für die Datenverarbeitung Verantwortlicher. Die Kommission ist verantwortlich für die Koordinierung des EESSI, sie übernimmt das Sekretariat des Lenkungsausschusses des Projekts EESSI und nimmt mit beratender Rolle an der Verwaltungskommission für die Koordinierung der Systeme der sozialen Sicherheit teil (der „Verwaltungskommission")[5]. Die Kommission ist auch für die zentrale Infrastruktur und für die Gewährleistung der Sicherheit der ausgetauschten Daten verantwortlich. Dies bedeutet, dass die Europäische Kommission als für die Datenverarbeitung Verantwortlicher gemäß Verordnung (EG) Nr. 45/2001 einige Verantwortlichkeiten und Pflichten im Hinblick auf das EESSI hat. Außerdem ist die Kommission auch ein für die Datenverarbeitung Verantwortlicher[6] im Hinblick auf die öffentliche Datenbank, die gemäß Artikel 88 Absatz 4 der Durchführungsverordnung eingerichtet werden wird und in der die zuständigen Behörden der einzelnen Mitgliedstaaten und deren Ansprechstellen aufgelistet sein werden.

- **Zukünftige Rolle der Kommission als Benutzer des Systems:** Obgleich eine derartige Rolle bei der ersten Einführung des EESSI nicht geplant ist, ist langfristig vorgesehen, dass die Kommission (PMO) als zuständige Behörde zum Nutzer des EESSI wird. Die zuständige Dienststelle der Kommission, die für die Datenverarbeitung verantwortlich ist, wird zum für die Datenverarbeitung Verantwortlichen und wird die entsprechenden Pflichten und Verantwortlichkeiten gemäß Verordnung (EG) Nr. 45/2001 haben. Diese Rolle wird eine separate Meldung zur Vorabkontrolle an den EDSB erforderlich machen; aus diesem Grund wird diese in der vorliegenden Stellungnahme weder beschrieben noch erörtert.

Die **primäre Verantwortlichkeit** für die Verarbeitung zu Zwecken des Betriebs der EESSI-Infrastruktur seitens der Kommission obliegt dem Referat „Freizügigkeit der Arbeitnehmer, Koordinierung der Systeme der sozialen Sicherheit" der GD Beschäftigung, soziale Angelegenheiten und Integration (GD EMPL, B.4). Im Rahmen von Standardarbeitsverfahren innerhalb der GD EMPL wird das Referat B.4 vom Referat G.4 im Hinblick auf technische Kenntnisse, Erfahrungen und Unterstützung im IT-Bereich unterstützt. Das Referat G.4 ist verantwortlich für die Entwicklung, Wartung und die Unterstützung des Systems zum elektronischen Austausch von Nachrichten.

[5] Die Verwaltungskommission ist der Europäischen Kommission zur Seite gestellt und das Hauptkontrollorgan im Bereich der Koordinierung der Systeme der sozialen Sicherheit auf EU-Ebene. Sie besteht aus Vertretern aller teilnehmenden Staaten sowie einem Vertreter der Europäischen Kommission. Die von dieser Verwaltungskommission getroffenen Beschlüsse im Hinblick auf die Durchführung des EESSI betreffen alle politischen, organisatorischen und technischen Aspekte bezüglich des Einsatzes, der Durchführung und des Betriebs des Systems. So fasste die Verwaltungskommission beispielsweise Beschlüsse über den Inhalt und das Format der SEDs. Im Hinblick auf die Datenverarbeitung wird die Verwaltungskommission beraten vom Fachausschuss für Datenverarbeitung.

[6] Die Datenverarbeitung seitens der Kommission im Zusammenhang mit der Bereitstellung der EESSI-Verzeichnisdienste ist nicht Gegenstand der Vorabkontrolle seitens des EDSB. Da diese jedoch ein wesentlicher Bestandteil des EESSI sind, wird diese Verarbeitung in der vorliegenden Stellungnahme beschrieben.

Auftragsverarbeiter: Die Kommission hat das DIGIT-Datenzentrum der Kommission zum **Auftragsverarbeiter** ernannt. Das DIGIT-Datenzentrum der Kommission ist der Host und Betreiber der zentralen Komponenten des EESSI (insbesondere die sTESTA-Infrastruktur, die als Kommunikationsnetzwerk zur Verbindung der nationalen Netzwerke der Mitgliedstaaten untereinander und mit dem DIGIT-Datenzentrum dient). Das Datenzentrum versendet Daten und erhebt statistische Daten. Die GD EMPL und DIGIT haben sich auf ein Hosting-Angebot zum Betrieb der zentralen EESSI-Infrastruktur beim DIGIT-Datenzentrum der Kommission geeinigt. Eine Dienstleistungsvereinbarung zwischen der GD EMPL und DIGIT steht kurz vor dem Abschluss. Ein Entwurf einer Standard-Dienstleistungsvereinbarung wurde dem EDSB vorgelegt; Seite 9 dieser Standard-Dienstleistungsvereinbarung enthält die Datenschutzbestimmungen, mit denen Artikel 23 der Verordnung umgesetzt wird.

Beschreibung der Verarbeitung: Die personenbezogene Daten werden von kommunalen, regionalen und nationalen Behörden erfasst und dann über das EESSI im Rahmen eines gemeinsamen sicheren Netzwerks an die zuständigen Behörden der anderen Mitgliedstaaten übermittelt. Eine gemeinsame europäische Systemarchitektur für den elektronischen Datenaustausch wurde von der Verwaltungskommission definiert, deren wichtigsten Merkmale wie folgt dargestellt werden können:

EESSI High Level Architecture: Das System sieht eine Sterntopologie mit einem zentralen Koordinierungsknoten (CN) und Endpunkten vor, die als Zugangsportale bezeichnet werden und die in den Mitgliedstaaten eingerichtet werden. Das EESSI besteht im Wesentlichen aus (1) einer zentralen Einheit (dem Koordinierungsknoten), die im DIGIT-Datenzentrum der Kommission untergebracht ist und die die EESSI-Verzeichnisdienste umfasst und (2) den internationalen Bereichen der Zugangsportale der Mitgliedstaaten, die über ein sicheres Netzwerk (sTesta) mit dem Koordinierungsknoten verbunden sind und über die alle elektronischen Daten zwischen den Mitgliedstaaten ausgetauscht werden müssen.

Die gemeinsame EU-Infrastruktur wird auf EU-Ebene entwickelt, während die Mitgliedstaaten dafür verantwortlich sind, die nötigen Schritte zu ergreifen, um mit dem System insgesamt verbunden zu werden. Zu diesem Zweck haben die Mitgliedstaaten mindestens ein und maximal fünf Zugangsportale benannt, über die die Daten zwischen den Mitgliedstaaten übermittelt werden. Das EESSI betrifft ausschließlich den Datenaustausch zwischen Mitgliedstaaten über deren Zugangsportale. Die Datenübertragung von den nationalen Teilen des Zugangsportals bzw. der Zugangsportale an die nationalen Sozialversicherungseinrichtungen bleibt weiterhin voll und ganz im Zuständigkeitsbereich der Mitgliedstaaten.

EESSI AP_RI und WEBIC (Web interface for clerks): Die Kommission hat eine Referenzimplementierungssoftware entwickelt, die die Mitgliedstaaten auf freiwilliger Basis benutzen können. Diese Referenzimplementierung umfasst ein vordefiniertes internationales und nationales Zugangsportal (das AP_RI) und eine Standard-Webapplikation für Anwender (das WEBIC).

SED-Nachrichten und Flüsse: Der Austausch von Sozialversicherungsdaten erfolgt mittels SEDs (Structured Electronic Documents), die nach einem Business-Protokoll ausgetauscht werden. Sowohl die Nachrichtenstruktur als auch das Protokoll werden von den zuständigen Lenkungsausschüssen und Arbeitsgruppen genehmigt. Die SEDs können nur innerhalb von vorab definierten Arbeitsflüssen ausgetauscht werden. Zu diesem Zweck wurden etwa 100 Flüsse definiert, innerhalb derer die SEDs ausgetauscht werden können. Diese Flüsse sind eine Übertragung der Prozesse des Datenaustauschs zwischen

den Behörden, die in der Durchführungsverordnung definiert wurden. Die Flüsse können nur zwischen zwei zuständigen Behörden ausgetauscht werden; wenn Daten an verschiedene Empfänger übermittelt werden sollen, dann muss die absendende Behörde den Vorgang entsprechend der Anzahl der Empfänger wiederholen. Es ist nicht möglich, die Daten an alle Empfänger gleichzeitig zu senden.

Suchfunktionen im EESSI: Die Bediensteten der zuständigen Behörden können eine Suche in Datenflüssen durchführen, die über das EESSI abgewickelt werden. Sie werden Zugang zu den Kopfzeilen aller Flüsse haben, werden aber nur dann Zugang zum Inhalt einer bestimmten SED-Nachricht erhalten, wenn sie dazu berechtigt sind, d.h. wenn sie der Sender bzw. der genannte Empfänger des jeweiligen Flusses sind.

Zentrales Verzeichnis des EESSI[7]: Ein zentrales Verzeichnis im Datenzentrum der Kommission enthält Informationen zu den Sozialversicherungsbehörden. Im zentralen Verzeichnis werden die Kontaktdaten der Sozialversicherungsbehörden ebenso verarbeitet wie die personenbezogenen Daten der Kontaktpersonen bei den zuständigen Behörden. Dieses Verzeichnis wird wie folgt verwendet:

- Von den Zugangsportalen, um die Adresse des Zugangsportals des Empfängers ausfindig zu machen. Zu diesem Zweck wird das Hauptverzeichnis in regelmäßigen Abständen an die Zugangsportale übermittelt.
- Vom zentralen Koordinierungsknoten (CN) zur Validierung der Adresse des Zugangsportals bei Übertragung der SED-Nachrichten.
- Von den Bediensteten der Behörden eines Mitgliedstaates zur Identifizierung der Behörden eines anderen Mitgliedstaats (unter Verwendung der örtlichen Replikation des Hauptverzeichnis, das beim Zugangsportal vorliegt).
- Von den EU-Bürgern, um Informationen über die Behörden über die öffentliche EESSI-Website zu erhalten (unter Verwendung einer Replikation des Hauptverzeichnisses mit dem Namen „öffentliches Verzeichnis“).

Informationsverwaltungssystem: Es wird ein Informationsverwaltungssystem geben, um den interessierten Kreisen allgemeine EESSI-Informationen zur Verfügung zu stellen (z. B. EESSI-Musterdokumentation, Designdokumente, Softwareupdates, etc.).

Betroffene Personen sind Arbeitnehmer und deren Familienangehörige, die in mehr als einem Mitgliedstaat gearbeitet haben und einen Antrag auf Sozialversicherungsleistungen gestellt haben[8]. Die Verordnungen im Bereich der sozialen Sicherheit sehen auch eine Koordinierung der Sozialversicherungsrechte von Nichterwerbstätigen vor, die Verbindungen zu mehr als einem Mitgliedstaat haben. Die Verordnungen gelten auch für Drittstaatsangehörige, die sich gemäß Verordnung (EG) Nr. 1231/2010[9] des Rates rechtmäßig in der EU aufhalten.

Im Rahmen des EESSI ausgetauschte personenbezogene Daten: Spezifische Bestimmungen der Grundverordnung definieren den Anwendungsbereich der

[7] Siehe Fußnote 6.

[8] Es ist vorgesehen, dass in der Zukunft EU-Beamte und andere Kategorien von Personen, die für EU-Organe und -Einrichtungen tätig sind, ebenfalls betroffene Personen im Rahmen des EESSI sein werden. Die vorliegende Stellungnahme geht auf diese Aspekte jedoch nicht ein, die im Rahmen einer separaten Vorabkontrolle geprüft werden, sobald eine Meldung auf Vorabkontrolle beim EDSB vom zuständigen für die Verarbeitung Verantwortlichen im Hinblick auf die Verarbeitung als zuständige Behörde im EESSI eingeht.

[9] Verordnung (EG) Nr. 1231/2010 Verordnung (EG) Nr. 1231/2010 zur Ausdehnung der Verordnung (EG) Nr. 883/2004 und der Verordnung (EG) Nr. 987/2009 auf Drittstaatsangehörige, die ausschließlich aufgrund ihrer Staatsangehörigkeit nicht bereits unter diese Verordnungen fallen.

personenbezogenen Daten, die zwischen den zuständigen Behörden ausgetauscht werden sollen. Die von der Verwaltungskommission eingesetzten Arbeitsgruppen haben ein EESSI-Modell vereinbart, in dem die Inhalte der im Rahmen von SEDs auszutauschenden Daten und die Flusstypen definiert werden. Insgesamt wurden 350 SEDs definiert. Die SEDs werden überarbeitet werden, nachdem gewisse Erfahrungen mit der Verwendung der SEDs und der Flüsse gesammelt wurden. Je nach beantragter Sozialversicherungsleistung und anderen Faktoren können folgende Arten personenbezogener Daten über das EESSI ausgetauscht werden:

- Name, Geschlecht, Anschrift, Geburtsdatum und -ort, Wohnsitzdaten, Familienstand, Zusammensetzung des Haushalts und Daten der Personen (einschließlich z. B. Kinderadoption) zu den aktuellen und verstorbenen Mitgliedern des Haushalts, Informationen über Sozialversicherungsansprüche (Sozialversicherungsnummer, PIN (persönliche Identifikationsnummer) bei der betroffenen Sozialversicherungsbehörde (Beginn, Ende, mögliche Zurückweisungsgründe, etc.), Informationen über die Gesundheit des Patienten (einschließlich z. B. ärztliche Untersuchungen/Behandlungen) und Unfälle, Informationen über bezogene Leistungen, finanzielle Informationen (einschließlich Bankkonto, Steuernummer und Handelregistereintrag, Einkommen), Beschäftigungsstatus und Beschäftigungszeiten (einschließlich dem Grund für die Beendigung). Daten über die sexuelle Orientierung können in bestimmten Fällen vom Familienstand abgeleitet werden.

Datenübermittlung: Die Empfänger der über das EESSI ausgetauschten Daten sind die Bediensteten der zuständigen Behörden der Mitgliedstaaten im betroffenen spezifischen Bereich des Systems der sozialen Sicherheit. Die Kommission stellt den Austausch der personenbezogenen Daten zwischen den Mitgliedstaaten sicher, wird jedoch keinen Zugang zum Inhalt der personenbezogenen Daten haben, die in verschlüsselter Form über das EESSI übermittelt werden (die Kommission hat – wie unten erläutert – nur Zugang zu den Kopfzeilen der Nachrichten zu statistischen Zwecken). Die Mitarbeiter von DIGIT haben Zugang zu bestimmten vom Benachrichtigungssystem verwendeten technischen Daten in ihrer Eigenschaft als Kommissions-Administratoren des Koordinierungsknotens zu Zwecken des Managements des Koordinierungsknotens und zur Erfassung von statistischen Daten. Die Bediensteten der GD EMPL, G.4, haben in ihrer Eigenschaft als EC-Administratoren[10] und DS-Administratoren[11] des EESSI-Hauptverzeichnisses im Rahmen des EESSI Zugang zu bestimmten Daten.

Die betroffenen Personen haben **ein Recht auf Zugang** zu ihren Daten und auf deren Berichtigung, indem sie die örtliche, regionale oder nationale Behörde kontaktieren, an die sie einen Antrag auf Sozialversicherungsleistungen gestellt haben oder jede andere nationale zuständige Behörde, an die dieser gerichtet ist. Gemäß den Verordnungen im Bereich der sozialen Sicherheit sind die Mitgliedstaaten dafür verantwortlich, sicherzustellen, dass die betroffenen Personen in der Lage sind, ihre Datenschutzrechte uneingeschränkt auszuüben. Da die Kommission keine personenbezogenen Daten erfasst und keinen Zugang zu den personenbezogenen Daten der betroffenen Personen hat, kann sie diesen keinen Zugang gewähren und deren Daten nicht berichtigen. Die Kommission wird jedoch die Ausübung der Rechte seitens der betroffenen Personen erleichtern, indem sie auf der EESSI-Website eine Datenschutzerklärung veröffentlicht, aus der hervorgeht,

[10] Vom EC-Administrator wird verlangt, dass er die zentralen Konfigurationseinstellungen der Datenbank wartet.

[11] Der DS-Administrator ist eine Art Supernutzer, der verpflichtet ist, die Konfiguration einer leeren Verzeichnisdienst-Datenbank zu starten.

wie diese ihre Rechte ausüben können. Falls die betroffenen Personen die Kommission im Hinblick auf den Zugang zu ihren Daten kontaktieren sollten, wird die Kommission sie auffordern, sich an die nationale Behörde zu wenden. Was die Datenverarbeitung seitens der Kommission angeht, können die betroffenen Personen auf dem Postweg oder per E-Mail eine Anfrage an den für die Datenverarbeitung Verantwortlichen richten (die Kontaktdaten stehen auf der EESSI-Website zur Verfügung).

Auskünfte an die betroffenen Personen werden von der örtlichen, regionalen oder nationalen Behörde erteilt, bei der die betroffenen Personen einen Antrag auf eine Sozialversicherungsleistung gestellt haben. Außerdem hat die Kommission eine Datenschutzmitteilung verfasst, die auf der EESSI-Website veröffentlicht wird, in der Informationen über die Verarbeitung der personenbezogenen Daten im Rahmen des EESSI sowie über die jeweilige Verantwortung der Mitgliedstaaten und der Kommission zur Verfügung gestellt werden.

Personenbezogene Daten werden **nicht im EESSI-System aufbewahrt** sondern in den Repositorien der Zugangsportale der nationalen Behörden unter deren Verantwortung. Die Daten können auch von den Behörden der Mitgliedstaaten in lokalen Datenbanken gespeichert werden, sofern es nationale IT-Systeme gibt. Personenbezogene Daten werden zu Zwecken aufbewahrt, die in Zusammenhang stehen mit dem Antrag der betroffenen Personen unter der Verantwortung der nationalen Behörden, die diese austauschen. Die betroffenen Personen werden angewiesen, die Behörde zu kontaktieren, bei der sie den Antrag eingereicht haben, um in Erfahrung zu bringen, die Aufbewahrungsfristen jeweils gelten.

Die Kommission speichert in der unter ihre Verantwortung fallenden Infrastruktur keine personenbezogenen Daten. Falls es erforderlich sein sollte, Daten aus technischen Gründen kurzfristig zu speichern, werden die personenbezogenen Daten auf jeden Fall in verschlüsselter Form aufbewahrt werden. Durchlaufende Nachrichten werden aus technischen Gründen vorübergehend für höchstens zwei Tagen im DIGIT-Datenzentrum auf verschlüsselte Weise aufbewahrt. Sie werden so bald wie technisch möglich an das empfangende Zugangsportal übermittelt.

Statistische Daten über den europäischen Datenaustausch: Die Mitgliedstaaten sind verantwortlich für die Erfassung statistischer Daten bezüglich der betroffenen Personen. Artikel 91 der Grundverordnung sieht vor, dass gemäß dem Plan und der Methode, die von der Verwaltungskommission definiert werden, statistische Daten erfasst und organisiert werden; dieser Plan und diese Methoden wurden noch nicht vereinbart und befinden sich in Ausarbeitung. Die Kommission wird anonyme Daten erfassen, die in der Kopfzeile bzw. im Umschlag der Nachrichten enthalten sind, die zwischen den Behörden ausgetauscht werden, um so eine Statistik über den europäischen Datenaustausch über das EESSI zu erarbeiten. Folgende in der Kopfzeile enthaltenen Daten können zu statistischen Zwecken verwendet werden: SED-ID (die ID-Nummer zur Identifizierung eines besonderen SEDs), SED-Typ, SED-Version, Fluss-ID, Fluss-Typ, Fluss-Version, Ursprung der mit dem SED verbundenen Informationen (Staat, Zugangsportal, Träger, der das SED erstellt hat), Empfänger der SED-Informationen (Staat, Zugangsportal, Bestimmungsträger), ID der Leistungskategorie, zeitbezogene Informationen (Absendedatum und SED-Fälligkeitsdatum, sofern anwendbar), Aktionstyp (Notifizierung, Ersuchen, Antwort, Überarbeitung, Löschung oder Anfechtung). Die SED-ID wird nur als einmalige Referenznummer für die Zwischenbearbeitungsschritte verwendet und bei der abschließenden Statistik nicht berücksichtigt, aus der nur die aggregierten Daten hervorgehen.

Sicherheitsanforderungen im EESSI **(...)**

3. Rechtliche Aspekte

3.1. Vorabkontrolle

Anwendbarkeit der Verordnung (EG) Nr. 45/2001 („die Verordnung"): Was die Tätigkeiten der Kommission betrifft, unterliegt die gemeldete Verarbeitung der Verordnung und der Überwachung seitens des EDSB.[12]

Die Kommission wird als für die Verarbeitung Verantwortlicher betrachtet im Hinblick auf die Verarbeitung, die im EESSI erfolgt. Wie in der Stellungnahme der Artikel-29-Datenschutzgruppe zu den Begriffen „für die Verarbeitung Verantwortliche" und „Auftragsverarbeiter"[13] unterstrichen wurde, muss ausgehend von Fakten und nicht nur theoretisch bestimmt werden, wer als für die Verarbeitung Verantwortlicher zu betrachten ist. Angesichts der zur Verfügung stehenden Informationen geht der EDSB davon aus, dass die Kommission im Rahmen ihrer beratenden Teilnahme an der Verwaltungskommission dazu beiträgt, den Zweck und die Mittel zu definieren, die im EESSI zur Verarbeitung der personenbezogenen Daten verwendet werden. Die Kommission ist auch verantwortlich für die zentrale Infrastruktur und für die Gewährleistung der Sicherheit der im Rahmen der gemeinsamen Infrastruktur ausgetauschten Daten. Die Europäische Kommission trägt als für die Verarbeitung Verantwortlicher gemäß Verordnung (EG) Nr. 45/2001 folglich einen Teil der Verantwortung und der Pflichten im Hinblick auf das EESSI.

Die Übermittlung personenbezogener Daten über ein von der Kommission unterhaltenes elektronisches Datenaustauschsystem stellt eine Verarbeitung personenbezogener Daten dar; die Tatsache, dass die Daten verschlüsselt sind, ändert nichts an der Schlussfolgerung, dass die übermittelten Daten personenbezogene Daten sind, da sie sich auf „*eine bestimmte oder bestimmbare natürliche Person*" (Artikel 2 Absatz a der Verordnung) beziehen. Die Datenverarbeitung erfolgt von einem EU-Organ im Rahmen von Tätigkeiten, die in den Anwendungsbereich des Gemeinschaftsrechts fallen (Artikel 3 Absatz 1 der Verordnung unter Berücksichtigung des Vertrags von Lissabon). Die Datenverarbeitung erfolgt mithilfe von automatischen Mitteln. Folglich findet die Verordnung (EG) Nr. 45/2011 Anwendung.

Begründung der Vorabkontrolle: Artikel 27 Absatz 1 der Verordnung sieht Folgendes vor: „*Verarbeitungen, die aufgrund ihres Charakters, ihrer Tragweite oder ihrer Zweckbestimmungen besondere Risiken für die Rechte und Freiheiten der betroffenen Personen beinhalten können, werden vom Europäischen Datenschutzbeauftragten vorab kontrolliert*". Artikel 27 Absatz 2 der Verordnung enthält eine Liste der Verarbeitungen, bei denen es wahrscheinlich ist, dass derartige Risiken bestehen. Der Informationsaustausch im Rahmen des EESSI umfasst auch personenbezogene Daten, die in Zusammenhang mit der Gesundheit stehen. Die Verarbeitung von Daten über die Gesundheit unterliegt gemäß Artikel 27 Absatz 2 Buchstabe a der Verordnung der Vorabkontrolle durch den EDSB.

[12] Für jede zuständige Behörde besteht das anwendbare Recht im jeweiligen innerstaatlichen Datenschutzgesetz (in Übereinstimmung mit der Richtlinie 94/46/EG), und die Tätigkeit einer jeden zuständigen Behörde wird überwacht durch die jeweilige nationale/regionale Datenschutzbehörde.

[13] Stellungnahme 1/2010 zum Begriff „für die Verarbeitung Verantwortlicher" und „Auftragsverarbeiter", angenommen am 16.2.2010.

Anwendungsbereich der Stellungnahme: Die im Rahmen der vorliegenden Stellungnahme ausgesprochenen Empfehlungen sind an die Kommission gerichtet im Hinblick auf deren Rolle bei der Gestaltung und dem Betrieb der EESSI-Infrastruktur, da diese Verarbeitung den Austausch von sensiblen Daten zwischen den zuständigen Behörden erleichtert und aus den oben dargelegten Gründen einer Vorabkontrolle unterliegt.

Obgleich in dieser Stellungnahme nicht auf den Grad der Einhaltung der Datenschutzbestimmungen im EESSI auf nationaler Ebene eingegangen wird, können viele der darin erteilten Empfehlungen auch die Einhaltung der Datenschutzbestimmungen seitens der Benutzer des Systems erleichtern, wie zum Beispiel seitens der zuständigen Behörden der Mitgliedstaaten. Aus diesem Grund können die vom EDSB an die Kommission ausgesprochenen Empfehlungen dazu beitragen, insgesamt ein hohes Datenschutzniveau innerhalb des EESSI zu gewährleisten.

Des Weiteren, wie oben auf Seite 4 festgestellt, unterstreicht der EDSB, dass bevor eine Verarbeitung durch die Kommission (PMO) in ihrer Eigenschaft als zuständige Behörde stattfinden kann, bei der sie als Benutzer des EESSI-Systems auftritt, um natürlichen Personen Rechte in Bezug auf deren Sozialversicherungsansprüche einzuräumen, der betreffende für die Verarbeitung Verantwortliche dem EDSB eine derartige Verarbeitung zur Vorabkontrolle gemäß Artikel 27 Absatz 2 Buchstabe a der Verordnung melden muss.

3.2. Rechtmäßigkeit der Verarbeitung

Artikel 5 der Verordnung enthält Kriterien dafür, dass die Verarbeitung von personenbezogenen Daten rechtmäßig ist. Gemäß Artikel 5 Absatz a) ist die Verarbeitung rechtmäßig, wenn sie „*für die Wahrnehmung einer Aufgabe erforderlich [ist], die aufgrund der Verträge [...] oder anderer aufgrund dieser Verträge erlassener Rechtsakte im öffentlichen Interesse [...] ausgeführt wird*".

Die Rechtsgrundlage für die Verarbeitung seitens der Kommission ist in der Grundverordnung zur Koordinierung der Systeme der sozialen Sicherheit und in Artikel 4 Absatz 2 der Durchführungsverordnung (EG) Nr. 987/2009 wie folgt enthalten: „*Die Datenübermittlung zwischen den Trägern oder Verbindungsstellen erfolgt elektronisch entweder unmittelbar oder mittelbar über die Zugangsstellen in einem gemeinsamen sicheren Rahmen, in dem die Vertraulichkeit und der Schutz der ausgetauschten Daten gewährleistet werden kann*".

Im Hinblick auf die Notwendigkeit der Verarbeitung stellt der EDSB fest, dass die Erleichterung der Freizügigkeit der Arbeitnehmer ein rechtmäßiges Ziel ist, das von der EU seit Gründung der Europäischen Gemeinschaften verfolgt wird, was unter anderem auch die Koordinierung der Systeme der sozialen Sicherheit innerhalb der EU umfasst. Artikel 48 des Vertrags über die Arbeitsweise der EU definiert die Zuständigkeiten der EU im Bereich der Koordinierung der sozialen Sicherheit. Des Weiteren ist das Recht auf soziale Sicherheit ein Grundrecht, das in Artikel 34 der Charta der Grundrechte der Europäischen Union geschützt wird. Aus diesem Grund können die auf EU-Ebene entwickelten Maßnahmen zur Koordinierung der Systeme der sozialen Sicherheit der EU-Mitgliedstaaten als zur effektiven Ausübung dieses Grundrechts notwendig erachtet werden.

Der EDSB begrüßt die Tatsache, dass diese Verarbeitung, die besondere Datenkategorien betrifft, auf einer soliden Rechtsgrundlage basiert. Der EDSB begrüßt ebenfalls, dass die Grundverordnung zur Koordinierung der sozialen Sicherheit ergänzt wurde durch die

Durchführungsverordnung, die allgemeine Durchführungsmaßnahmen enthält, und dass die spezifischen Einzelheiten der Verarbeitung klar aus den Entscheidungen der Verwaltungskommission hervorgehen[14].

3.3. Verarbeitung besonderer Datenkategorien

Im Rahmen des EESSI werden personenbezogene Daten verarbeitet, die in Zusammenhang mit der Gesundheit und Daten stehen, aus denen die sexuelle Orientierung von Personen abgeleitet werden kann (wie dem Familienstand). Die Verarbeitung von personenbezogenen Daten über die Gesundheit und das Sexualleben ist gemäß Artikel 10 Absatz 1 der Verordnung verboten, es sei denn, die Gründe gemäß Artikel 10 Absatz 2, Artikel 10 Absatz 3 oder Artikel 10 Absatz 4 der Verordnung sind gegeben.

Artikel 10 Absatz 4 der Verordnung sieht Folgendes vor „*Vorbehaltlich angemessener Garantien können aus Gründen eines wichtigen öffentlichen Interesses [...] Ausnahmen durch die Verträge zur Gründung der Europäischen Gemeinschaften oder andere auf der Grundlage dieser Verträge erlassene Rechtsakte oder, falls notwendig, im Wege einer Entscheidung des Europäischen Datenschutzbeauftragten vorgesehen werden*". Die Verarbeitung seitens der Kommission erfolgt zum Zweck der Sicherstellung der Umsetzung der EU-Verordnungen zur Koordinierung der Systeme der sozialen Sicherheit, was die effektive Inanspruchnahme der Rechte der Personen im Hinblick auf die soziale Sicherheit erleichtern wird. Die Verarbeitung erfolgt aufgrund eines wichtigen öffentlichen Interesses gemäß den EU-Verordnungen zur Koordinierung der sozialen Sicherheit. Der EDSB betrachtet die Verarbeitung besonderer Datenkategorien seitens der Kommission im Kontext der Betreibung der EESSI-Infrastruktur als gemäß Artikel 10 Absatz 4 der Verordnung gerechtfertigt.

Angesichts der beschränkten Rolle der Kommission bei der Verarbeitung dieser Daten stellt der EDSB jedoch fest, dass es eine angemessene Maßnahme ist vorzusehen, dass die Kommission nur verschlüsselte Daten überträgt, so dass sie keinen Zugang zum Inhalt der sensiblen Daten hat, die durch das EESSI übertragen werden.

3.4 Datenqualität

Zweckmäßigkeit, Erheblichkeit und Verhältnismäßigkeit: Gemäß Artikel 4 Absatz 1 Buchstabe c der Verordnung dürfen personenbezogene Daten nur „*den Zwecken entsprechen, für die sie erhoben und/oder weiterverarbeitet werden, dafür erheblich sein und nicht darüber hinausgehen*". Um die Verhältnismäßigkeit der ausgetauschten Daten sicherzustellen wird in spezifischen Bestimmungen der Verordnungen zur sozialen Sicherheit der Anwendungsbereich der Daten definiert, die zwischen den zuständigen Behörden ausgetauscht werden sollen. In der Praxis wurden von der Verwaltungskommission für jede Art des Anspruchs Standardformulare (Structured Electronic Documents) definiert, die strukturierte obligatorische und Pflichtfelder zum Ausfüllen enthalten, wodurch die Menge und die Art der zu verarbeiteten Daten auf diejenigen eingeschränkt werden, die für einen bestimmten Anspruch erforderlich sind. Die verarbeiteten Daten scheinen für die Bewertung des Anspruchs der Personen auf spezifische Sozialversicherungsleistungen notwendig zu sein. Folglich geht der EDSB davon aus, dass die ihm vorgelegten Informationen über die verarbeiteten Daten die Bedingungen gemäß Artikel 4 Absatz 1 Buchstabe c erfüllen.

[14] Siehe Fußnote 5.

Sachliche Richtigkeit: Artikel 4 Absatz 1 Buchstabe d der Verordnung sieht vor, dass personenbezogene Daten „*sachlich richtig und, wenn nötig, auf den neuesten Stand gebracht*" sein müssen und sieht Folgendes vor*:* „*es sind alle angemessenen Maßnahmen zu treffen, damit im Hinblick auf die Zwecke, für die sie erhoben oder weiterverarbeitet werden, unrichtige oder unvollständige Daten gelöscht oder berichtigt werden*". Die meisten der Daten werden von einer zuständigen Behörde an eine andere übermittelt. Angesichts der Tatsache, dass die Daten in den meisten Fällen nicht direkt bei den betroffenen Personen eingeholt werden, sind die Rechte auf Zugang und auf Berichtigung wichtige Mittel zur Sicherstellung der Richtigkeit der Daten, die den betroffenen Personen gewährt werden müssen (siehe Punkt 3.7).

Verarbeitung nach Treu und Glauben und Rechtmäßigkeit: Artikel 4 Absatz 1 Buchstabe a der Verordnung 45/2001 legt fest, dass personenbezogene Daten „*nach Treu und Glauben und auf rechtmäßige Weise verarbeitet werden*". Die Rechtmäßigkeit wurde bereits erörtert (siehe Punkt 3.2) und die Verarbeitung nach Treu und Glauben wird im Zusammenhang mit den Informationen erörtert, die den betroffenen Personen zur Verfügung gestellt werden (siehe Punkt 3.8).

3.5. Datenaufbewahrung

Artikel 4 Absatz 1 Buchstabe e der Verordnung (EG) Nr. 45/2001 legt fest, dass personenbezogene Daten „*so lange, wie es für die Erreichung der Zwecke, für die sie erhoben oder weiterverarbeitet werden, erforderlich ist, in einer Form gespeichert werden, die die Identifizierung der betroffenen Person ermöglicht.*"

Was die Aufbewahrung der SED-Nachrichten seitens der Kommission angeht, ist der EDSB einverstanden mit der kurzen Aufbewahrungsfrist von zwei Tagen, die festgelegt wurde, um die Übertragung der Nachrichten sicherzustellen, sowie damit, dass die aufbewahrten Daten verschlüsselt werden. Die Aufbewahrung der SED-Nachrichten seitens der Kommission ist mit Artikel 4 Absatz 1 Buchstabe e der Verordnung vereinbar.

Was die Aufbewahrung der Logdatei-Informationen angeht, gehen wir davon aus, dass die Kommission die Logdateien der durchgeführten Transaktionen im Koordinierungsknoten aufbewahrt, was zur Überprüfung und zum Verständnis dafür notwendig ist, wie sich spezifische technische Probleme bei einem spezifischen Fluss/Nachricht entwickelt haben, oder um zu überprüfen, ob es gegebenenfalls zu bestimmten Zeiten oder Intervallen zu Ereignissen gekommen ist. Da dies aktuell noch in keinem spezifischen Dokument definiert ist, empfiehlt der EDSB, dass die von der Kommission im EESSI aufbewahrten Logdateien sowie die Zeitfristen für deren Aufbewahrung angemessen dokumentiert werden. Der EDSB unterstreicht, dass gemäß Artikel 37 der Verordnung die Logdateien, die von der Kommission zum Betrieb der EESSI-Infrastruktur erfasst werden, „*so schnell wie möglich, spätestens aber sechs Monate nach ihrer Erhebung, zu löschen*" sind. Angesichts dieser Tatsache stellt der EDSB fest, dass die Aufbewahrungsfrist von 10 Tagen, die gemäß den Richtlinien des DIGIT-Datenzentrums vorgesehen ist, die Anforderungen der Verordnung erfüllt.

Was die Aufbewahrung der Daten seitens der Kommission zu statistischen Zwecken angeht, muss die Kommission gemäß Artikel 4 Absatz 1 Buchstabe e der Verordnung sicherstellen, dass die Daten nur in anonymisierter Form oder, wenn dies nicht möglich ist, nur mit verschlüsselter Identität der Betroffenen gespeichert werden. In dieser Hinsicht könnte die Aufbewahrung der SED-ID eine indirekte Identifizierung der Person ermöglichen, auf die sich die SED-Nachricht bezieht; folglich könnten die zu statistischen Zwecken gespeicherten Daten nicht vollständig anonymisiert sein. Die Tatsache jedoch,

dass die SED-Daten verschlüsselt sind, sollte verhindern, dass die Kommission die Daten auf eine spezifische Person zurückführt.

3.6. Datenübermittlung

Die Daten werden zwischen den ernannten zuständigen Behörden der Mitgliedstaaten über eine Infrastruktur übermittelt, die von der Kommission unterhalten wird. Der größte Teil des Datenaustausches erfolgt zwischen Empfängern, die die Richtlinie 95/46/EG anwenden, und muss folglich gemäß Artikel 8 der Verordnung bewertet werden, während ein anderer Teil zwischen Empfängern erfolgt, die nicht der Richtlinie 95/46/EG unterliegen, weshalb eine Erörterung auf der Grundlage von Artikel 9 der Verordnung zu erfolgen hat.

Die Kommission nimmt Teil an der Datenübermittlung an Drittparteien, die der Richtlinie 94/46/EG unterliegen (EU-Staaten und EWR-Staaten, die die Richtlinie 95/46/EG anwenden). Artikel 8 Buchstabe a der Verordnung sieht vor, dass die Datenübermittlung erfolgen kann *„wenn der Empfänger nachweist, dass die Daten für die Wahrnehmung einer Aufgabe, die im öffentlichen Interesse liegt oder zur Ausübung der öffentlichen Gewalt gehört, erforderlich sind*". Im vorliegenden Fall ist die Datenübermittlung ganz klar zur Wahrnehmung der Aufgaben der zuständigen Sozialversicherungsbehörden erforderlich; folglich erfüllen diese die Bestimmungen gemäß Artikel 8 Buchstabe a der Verordnung.

Des Weiteren kann eine Datenübermittlung auch mit Staaten erfolgen, die der Richtlinie 95/46/EG nicht unterliegen, namentlich mit der Schweiz. Eine derartige Datenübermittlung muss ausgehend von Artikel 9 der Verordnung erörtert werden. Artikel 9 sieht insbesondere vor, dass die Übermittlung nur dann erfolgt, wenn ein angemessenes Schutzniveau in dem Land des Empfängers gewährleistet ist und diese Übermittlung ausschließlich die Wahrnehmung von Aufgaben ermöglichen soll, die in die Zuständigkeit des für die Verarbeitung Verantwortlichen fallen. Bezüglich der Schweiz gibt es eine Angemessenheitsentscheidung der Kommission[15], der zu entnehmen ist, dass ein angemessenes Schutzniveau im Hinblick auf den Datenschutz gewährleistet ist. Die Übermittlung erfolgt nur an Sozialversicherungsbehörden zur Wahrnehmung der Aufgaben dieser Behörden. Folglich ist Artikel 9 der Verordnung erfüllt.

3.7. Rechte der betroffenen Personen

Artikel 12 der Richtlinie 95/46/EG und die entsprechenden Artikel 13 und 14 der Verordnung sehen ein Auskunftsrecht auf Anfrage der betroffenen Person in Bezug auf ihre Daten vor und – unter gewissen Umständen – ein Recht auf Berichtigung oder Löschung dieser Daten.

Der EDSB stellt fest, dass die Kommission Maßnahmen ergriffen hat, um die Inanspruchnahme der Rechte der betroffenen Personen in einem grenzüberschreitenden Kontext zu erleichtern, indem sie festgelegte, dass die Behörde, an die der Antrag gestellt wurde, der Ansprechpartner für die Inanspruchnahme dieser Rechte ist. Die Kommission wird jedoch im Hinblick auf die Gewährleistung der Rechte der betroffenen Personen keine Rolle spielen; bei etwaigen Anträgen wird sie lediglich die betroffene Person an den jeweiligen Ansprechpartner verweisen.

[15] Entscheidung 2000/518/EG der Kommission vom 26. Juli 2000 - ABl. L 215/1 vom 25. August 2000.

Der EDSB begrüßt die von der Kommission vorgestellte Lösung und die Benennung eines „einzigen Ansprechpartners" für die Ausübung der Rechte der betroffenen Personen, was die effektive Ausübung dieser Rechte seitens der betroffenen Personen in einem grenzüberschreitenden Kontext erleichtern sollte. Der EDSB unterstreicht, dass der Ansprechpartner dafür verantwortlich sein wird, sicherzustellen, dass die Rechte der betroffenen Personen wahrgenommen werden können. Die volle Inanspruchnahme der Rechte der betroffenen Personen im grenzüberschreitenden Kontext wird es insbesondere erforderlich machen, dass zwischen den zuständigen Behörden Verfahren eingerichtet werden, um (1) eine angemessene Prüfung der angefochtenen Informationen durchzuführen und (2) alle betroffenen Behörden davon in Kenntnis zu setzen, dass ein Antrag auf Berichtigung/Löschung gestellt wurde.

3.8. Informationspflicht gegenüber den betroffenen Personen

Die zuständigen Behörden sind gemäß Artikel 10 und 11 der Richtlinie 95/46/EG verpflichtet, den betroffenen Personen bestimmte Informationen bezüglich der Verarbeitung zur Verfügung zu stellen. Die entsprechenden Bestimmungen der Verordnung (Artikel 11 und 12) sehen ähnliche Anforderungen an die Kommission im Hinblick auf die von ihr verarbeiteten Daten vor.

Der EDSB stellt fest, dass zusätzlich zur spezifischen Datenschutzmitteilung, die von den zuständigen Behörden zu dem Zeitpunkt zur Verfügung gestellt werden muss, an dem eine Person einen Antrag stellt, die Kommission eine eigene Datenschutzmitteilung verabschiedet hat, in der Informationen über die Datenverarbeitung innerhalb des EESSI zur Verfügung gestellt werden und die auf der EESSI-Website veröffentlicht werden wird. Die Datenschutzmitteilung der Kommission enthält alle in den Artikeln 11 und 12 der Verordnung vorgesehenen Punkte. Der EDSB begrüßt diese Maßnahme, die dazu beiträgt, die Verarbeitung transparenter zu machen, und die den betroffenen Personen nützliche Informationen zur Verfügung stellt, um die Inanspruchnahme ihrer Rechte im Hinblick auf den Datenschutz zu erleichtern.

3.9. Verarbeitung von Daten im Auftrag des für die Verarbeitung Verantwortlichen

Der EDSB geht in der Regel davon aus, dass ein Auftragsverarbeiter eine externe Organisation ist, an die die EU-Organe und -Einrichtungen bestimmte Aufgaben extern vergeben. Angesichts der Größe der Kommission, hat der EDSB akzeptiert, dass die Kommission ein formelles System eingerichtet hat, in dem die Rolle des für die Verarbeitung Verantwortlichen innerhalb ihrer Organisation delegiert wird.

Der EDSB stellt fest, dass der Entwurf der Standard-Dienstleistungsvereinbarung mit DIGIT, der dem EDSB vorgelegt wurde, Bestimmungen enthält, die die Anforderungen gemäß Artikel 23 der Verordnung erfüllen würden. Der EDSB unterstreicht jedoch, dass – wie in Artikel 23 Absatz 2 vorgesehen – die Verarbeitung seitens eines Auftragsverarbeiters *„auf der Grundlage eines Vertrags oder Rechtsakts [erfolgt], durch den der Auftragsverarbeiter an den für die Verarbeitung Verantwortlichen gebunden ist*". Der EDSB fordert demzufolge die GD EMPL auf, mit DIGIT so bald wie möglich eine Dienstleistungsvereinbarung zu unterzeichnen, auf jeden Fall jedoch bevor das System voll in Kraft tritt.

Des Weiteren empfiehlt der EDSB der Kommission, die jeweiligen Rollen der DIGIT und der GD EMPL, G.4., im Hinblick auf deren Zugang zu den Daten und die Verarbeitung in den verschiedenen IT-Systemen innerhalb des EESSI angemessen zu dokumentieren.

3.10. Sicherheitsmaßnahmen

Die Sicherheit von Gesundheitsdaten im grenzüberschreitenden Kontext ist von besonderer Bedeutung. Der Europäische Gerichtshof für Menschenrechte hat der Vertraulichkeit von Gesundheitsdaten eine besondere Bedeutung beigemessen, indem er erklärte, dass die *„Achtung der Vertraulichkeit von Gesundheitsdaten ein zentraler Grundsatz der Rechtsordnungen aller Vertragsparteien der Konvention sei. Es sei äußerst wichtig, nicht nur die Privatsphäre eines Patienten zu achten, sondern auch sein Vertrauen in den medizinischen Berufsstand und in die Gesundheitsdienste im Allgemeinen zu bewahren.*“[16]

Der EDSB stellt fest, dass die interessierten Kreise des EESSI spezifische Maßnahmen zur Wahrung der Vertraulichkeit der Informationen vereinbart haben, die über das EESSI übermittelt werden, wobei berücksichtigt wurde, dass es sich hierbei um sensible Daten handelt.

(...)

Der EDSB stellt jedoch auch fest, dass die Sicherheitsrichtlinien in einigen Bereichen sehr detailliert sind, während dies in anderen Bereichen nicht der Fall ist. Der EDSB empfiehlt der Kommission, die Sicherheitsrichtlinien in den Bereichen zu ergänzen, in denen dies erforderlich ist.

Außerdem hat der EDSB keine Informationen im Hinblick auf eine konkrete Planung von Überprüfungen des Systems erhalten. Wie in den Sicherheitsrichtlinien vorgesehen, sollte[17] regelmäßig eine Überprüfung durchgeführt werden, um festzustellen, ob die Sicherheitsrichtlinien und -verfahren eingehalten und umgesetzt werden, die Frequenz dieser Überprüfungen muss jedoch noch von der Verwaltungskommission festgelegt werden. Der EDSB erkennt an, dass es um eine Brücke von der Theorie zur Praxis zu schlagen, sehr nützlich wäre, wenn eine oder mehrere Sicherheitsprüfungen bei Aufnahme des Betriebs des Systems, nach bedeutenden Systemänderungen oder in regelmäßigen Abständen durchgeführt werden würden. Diese Überprüfung würde einen Überblick darüber geben, inwieweit die Sicherheitsrichtlinien effektiv umgesetzt werden und wo weitere Maßnahmen erforderlich sind. Insofern würde diese Überprüfung ein wertvolles Verwaltungsinstrument darstellen. Der EDSB empfiehlt deshalb der Kommission, einen durchführbaren Überprüfungsplan festzulegen und eine oder mehrere Sicherheitsüberprüfungen des Systems durchzuführen.

4. Schlussfolgerungen

Der EDSB stellt fest, dass es keinen Grund zur Annahme gibt, dass die Bestimmungen der Verordnung (EG) Nr. 45/2001 verletzt werden, sofern die Kommission die obigen Ausführungen voll und ganz berücksichtigt, bevor das EESSI-System in Kraft tritt. Die Kommission sollte insbesondere:

- nur verschlüsselte Daten übermitteln, so dass sie keinen Zugang zum Inhalt der sensiblen Daten hat, die über das EESSI übermittelt werden;

[16] Siehe EGMR-Urteil vom 17. Juli 2008, I. gegen Finnland (Individualbeschwerde Nr. 20511/03), Randnr. 38.

[17] Im Sicherheitspolitikdokument impliziert die Verwendung von „sollte“ eine deutliche Empfehlung (im Gegensatz zu einer wesentlichen und zwingend vorgeschriebenen Sicherheitskontrolle und zu einer einfachen Empfehlung).

- die Kategorien der Logdateien angemessen dokumentieren, die von ihr aufbewahrt werden, sowie deren Zeitfristen für die Aufbewahrung;

- dazu beitragen sicherzustellen, dass die betroffenen Personen ihre Rechte bei den zuständigen Ansprechstellen im Mitgliedstaat wahrnehmen können. Dies wird es insbesondere erforderlich machen, dass zwischen den zuständigen Behörden Verfahren zur Benennung einer zentralen Ansprechstelle für die betroffene Person eingerichtet werden, um die angefochtene Information zu überprüfen und im Falle der Einreichung eines Berichtigungs-/Löschungsantrags alle betroffenen Behörden davon in Kenntnis zu setzen;

- eine verbindliche Dienstleistungsvereinbarung mit DIGIT abzuschließen, die angemessene Klauseln erhält, mit denen die Vorgaben von Artikel 23 der Verordnung erfüllt werden, bevor das System vollständig in Kraft tritt;

- die jeweiligen Rollen der DIGIT und der GD EMPL, G.4., im Hinblick auf deren Zugang zu den Daten und deren Verarbeitung in den verschiedenen IT-Systemen innerhalb des EESSI angemessen zu dokumentieren;

- die Sicherheitsrichtlinien mit detaillierten Bestimmungen zu ergänzen, insbesondere in den Bereichen, in denen diese Richtlinien nicht ins Detail gehen;

- einen durchführbaren Überprüfungsplan festzulegen und eine oder mehrere Sicherheitsüberprüfungen des Systems durchzuführen;

- dem EDSB alle etwaigen wesentlichen Änderungen am Aufbau des Systems mitzuteilen, die Auswirkungen auf das Datenschutzniveau des EESSI haben könnten.

Brüssel, den 28. Juli 2011

(**unterzeichnet**)

Giovanni BUTTARELLI
Stellvertretender Europäischer Datenschutzbeauftragter