UNIVERSITÉ DE FRIBOURG
UNIVERSITÄT FREIBURG

Institut für Europarecht
Institut de droit européen

Astrid Epiney / Daniela Nüesch

Datenschutzrechtliche Anforderungen für den Betrieb von Informationssystemen im Bereich der Koordinierung der Systeme sozialer Sicherheit zwischen der Schweiz und der EU

Aufgezeigt am Beispiel der AHV, der IV
und der Unterstellung

2015

Cahiers fribourgeois de droit européen no 18
Freiburger Schriften zum Europarecht Nr. 18

FACULTÉ DE DROIT
INSTITUT DE DROIT EUROPÉEN

RECHTSWISSENSCHAFTLICHE FAKULTÄT
INSTITUT FÜR EUROPARECHT

Astrid Epiney / Daniela Nüesch

Datenschutzrechtliche Anforderungen für den Betrieb von Informationssystemen im Bereich der Koordinierung der Systeme sozialer Sicherheit zwischen der Schweiz und der EU

Aufgezeigt am Beispiel der AHV, der IV
und der Unterstellung

L'Institut de droit européen, dirigé par les Professeurs Marc Amstutz, Samantha Besson et Astrid Epiney, contribue, en tant que centre de compétence des Facultés de droit des Universités de Berne, Neuchâtel et Fribourg, à ce que les ressources des trois universités dans ce domaine soient utilisées le plus efficacement possible. Ses activités englobent, hormis les tâches relatives à l'enseignement du droit européen, la gestion d'une bibliothèque et d'un centre de documentation européenne, l'organisation de manifestations pour la formation continue ainsi que la recherche scientifique en droit européen, des avis de droit et des expertises.

Les Cahiers fribourgeois de droit européen proposent des textes, en français, en allemand, en anglais et en italien, qui, pour différentes raisons, ne se prêtent pas à une publication commerciale, tels que des «papers» de discussion de doctorants, des avis de droit ou des versions écrites de conférences données à l'Université de Fribourg.

Das Institut für Europarecht unter der Leitung von Professor Marc Amstutz und den Professorinnen Samantha Besson und Astrid Epiney hat als Kompetenzzentrum der rechtswissenschaftlichen Fakultäten der Universitäten Bern, Neuenburg und Freiburg unter anderem die Aufgabe, zu der effizienten Nutzung der auf diesem Gebiet zu Verfügung stehenden Ressourcen beizutragen. Neben den mit der Lehre im Europarecht verbundenen Aufgaben zählen zu seinen Aktivitäten die Führung einer europarechtlichen Bibliothek und eines europäischen Dokumentationszentrums, die Organisation von Weiterbildungen sowie die wissenschaftliche Forschung im Europarecht und das Erstellen von Rechtsgutachten.

Die Freiburger Schriften zum Europarecht beinhalten Texte auf Deutsch, Französisch, Englisch und Italienisch, die aus verschiedenen Gründen nicht für eine kommerzielle Veröffentlichung geeignet sind, wie z.B. Diskussionspapiere von Doktoranden, Rechtsgutachten oder schriftliche Fassungen von an der Universität Freiburg gehaltenen Vorträgen.

Editeur / Herausgeber Institut de droit européen / Institut für Europarecht
Avenue de Beauregard 11
CH-1700 Fribourg

euroinstitut@unifr.ch

www.unifr.ch/ius/euroinstitut

Juli 2015

Pas disponible en librairie / nicht im Buchhandel erhältlich

Inhaltsverzeichnis

A. Einleitung und Problemstellung

In der **Europäischen Union** ist auf der Grundlage der hier einschlägigen Verordnungen eine **Koordination der Systeme sozialer Sicherheit** vorgesehen, dies bereits auf das Ende der Übergangszeit,[1] wobei die Rechtsgrundlagen hier mehrmals geändert und 2004 eine gänzlich neue Verordnung erlassen wurde (die jedoch in grossen Teilen auch die bis dahin ergangene Rechtsprechung aufgriff);[2] mit dem Erlass der diesbezüglichen Durchführungsverordnung ist das neue System nunmehr grundsätzlich anwendbar.[3] Das hier einschlägige EU-Sekundärrecht ist vor dem Hintergrund des Auftrags des Art. 48 AEUV zu sehen, der die Einführung eines Systems vorsieht, das den Wanderarbeitnehmern die Zusammenrechnung der nach den verschiedenen innerstaatlichen Rechtsvorschriften berücksichtigten Sozialversicherungszeiten für den Erwerb des Leistungsanspruchs erlaubt und sie in die Lage versetzt, die Zahlung der Leistungen der sozialen Sicherheit in einem anderen Mitgliedstaat als demjenigen, wo sie gearbeitet haben, zu erhalten. Damit **koordiniert das Unionsrecht die nationalen Rechtsvorschriften**, verschmilzt sie aber nicht zu einem einheitlichen Sozialversicherungssystem.[4] Dies zeigt sich daran, dass dem Leistungsempfänger, der in verschiedenen Mitgliedstaaten gearbeitet hat, kein einheitlicher Anspruch gewährt wird. Er hat vielmehr selbständige Leistungsansprüche gegen die Versicherungsträger der Mitgliedstaaten. Doch müssen die Träger bei der Bestimmung des Grundes und/oder der Höhe des Anspruchs ggf. Unionsrecht neben den innerstaatlichen Rechtsvorschriften anwenden und insbesondere, wenn die in einem Mitgliedstaat zurückgelegten Versicherungszeiten nicht ausreichen, um einen Leistungsanspruch entstehen zu lassen, in Anwendung der Verordnungen auch die in anderen Mitgliedstaaten zurückgelegten Versicherungszeiten berücksichtigen.[5]

Die **Schweiz** ist als Nicht-EU-Mitgliedstaat zwar nicht an das einschlägige EU-Sekundärrecht in diesem Zusammenhang gebunden; jedoch sieht das **Personenfreizügigkeitsabkommen**

---

1 Der 1957 unterzeichnete und 1958 in Kraft getretene damalige Vertrag zur Gründung der Europäischen Wirtschaftsgemeinschaft (EWG) sah eine 12-jährige Übergangszeit vor, bevor zahlreiche vertragliche Bestimmungen vollumfänglich zu beachten bzw. anzuwenden waren und während derselben die für die Verwirklichung des Gemeinsamen Marktes bzw. des Binnenmarktes notwendigen Sekundärrechtsakte erlassen werden sollten.

2 Vgl. den Überblick über die einschlägigen Rechtsgrundlagen und die Entwicklung bei *Epiney*, in: Bieber/Epiney/Haag, EU, § 11, Rn. 108 ff.

3 Nach Art. 91 VO 883/2004 gilt die Verordnung erst ab dem Tag des Inkrafttretens der Durchführungsverordnung.

4 Vgl. die Ausführungen in EuGH, Rs. C-227/89 (Rönfeldt), Slg. 1991, I-323, Rn. 13 ff.; s. in diesem Zusammenhang auch EuGH, Rs. C-33/99 (Fahrni), Slg. 2001, I-2415, wo der EuGH festhält, dass die VO 1408/71 (heute abgelöst durch die VO 883/2004) nur dann zur Anwendung komme, wenn es tatsächlich um die Ausübung der Freizügigkeit geht; im Übrigen stehe es den Mitgliedstaaten frei, ihre Systeme der sozialen Sicherheit nach ihrem Belieben auszugestalten, sofern die unionsrechtlichen Vorgaben eingehalten werden. Ausdrücklich in Bezug auf die VO 883/2004 EuGH, Rs. C-140/12 (Brey), Urt. v. 19.9.2013.

5 Zum Ganzen den Überblick bei *Epiney*, in: Bieber/Epiney/Haag, EU, § 11, Rn. 108 ff.; ausführlich die Kommentierung der VO 883/2004 in *Fuchs*, Europäisches Sozialrecht; s. auch die Erörterung der neuen Verordnungen bei *Schulte*, ZESAR 2010, 143 ff.

Schweiz – EU (FZA)[6] eine eigentliche **Einbindung der Schweiz in das unionsrechtliche System der Koordinierung der sozialen Sicherheit** vor, denn die einschlägigen sekundärrechtlichen Rechtsakte werden als für die Schweiz massgeblich erklärt bzw. die Schweiz muss eine gleichwertige Rechtsetzung sicherstellen. Insofern ist die Situation der Schweiz in Bezug auf die Koordinierung der Systeme sozialer Sicherheit mit derjenigen eines EU-Mitgliedstaats im Wesentlichen vergleichbar.[7]

Das unionsrechtliche Koordinierungsrecht auf dem Gebiet der sozialen Sicherheit sowie dessen „Ausdehnung" auf die Schweiz bringt es mit sich, dass die jeweils zuständigen **Leistungserbringer über die notwendigen Informationen** verfügen müssen, um die jeweiligen Ansprüche berechnen zu können. Dies wiederum impliziert bei den in diesem Zusammenhang in Frage stehenden grenzüberschreitenden Sachverhalten einen (grenzüberschreitenden) **Austausch der relevanten (personenbezogenen) Daten** zwischen den verschiedenen Sozialversicherungseinrichtungen, muss doch jeder Leistungserbringer bei der Berechnung der Ansprüche auch ggf. in anderen Mitgliedstaaten bzw. der Schweiz zurückgelegte Versicherungszeiten berücksichtigen.

Im Hinblick auf einen möglichst effektiven und effizienten Datenaustausch in diesem Zusammenhang soll dieser – wie schon in Art. 78 VO 883/2004 vorgesehen, in Erw. 3 Präambel VO 987/2009 formuliert und sodann in Art. 2 ff. VO 987/2009 im Einzelnen ausgestaltet – über verschiedene **elektronische Informationssysteme** erfolgen, wobei in Abhängigkeit von den Leistungen und den auszutauschenden Daten verschiedene Systeme geplant sind. Aufgeworfen wird damit die Frage nach der **gesetzlichen Grundlage für die Einrichtung dieser neuen Systeme**: Denn die Datenbearbeitung durch öffentliche Organe muss sich grundsätzlich auf eine gesetzliche Grundlage stützen, wobei diese bei besonders sensiblen Personendaten zudem formell-gesetzlicher Natur sein muss. Vor diesem Hintergrund soll im Folgenden der Frage nachgegangen werden, ob für die Einrichtung des europäischen Informationssystems EESSI sowie für die damit im Zusammenhang stehenden nationalen Systeme (beispielhaft wird auf die Bereiche der AHV und IV sowie der Unterstellung Bezug genommen) *de lege lata* eine solche gesetzliche Grundlage (im nationalen oder internationalen Recht) existiert. Der Fokus der Untersuchung liegt dabei auf den **datenschutzrechtlichen Aspekten**; sonstige Fragen nach einer ausreichenden rechtlichen Verankerung der Informationssysteme (z.B. im Hinblick auf die Finanzierung) werden weitgehend ausgespart.

Damit ergibt sich auch der **Aufbau der Untersuchung**: Nach einer Skizzierung der vorgesehenen Informationssysteme (B.) sind die sich weitgehend letztlich schon aus völker- und verfassungsrechtlichen Vorgaben ergebenden Anforderungen in Bezug auf das Erfordernis und

---

6 Abkommen zwischen der Europäischen Gemeinschaft und ihren Mitgliedstaaten einerseits und der Schweizerischen Eidgenossenschaft andererseits über die Freizügigkeit (FZA), SR 0.142.112.681; ABl. 2002 L 114, 6 ff. Vgl. zu diesem Abkommen, m.w.N., *Epiney/Metz/Pirker*, Parallelität der Rechtsentwicklung, 193 ff., 154 ff., 203 ff.; *Amarelle/Nguyen* (Hrsg.), Code annoté, vol. III.

7 Grundlegend und ausführlich zu dieser Einbindung *Cardinaux*, Personenfreizügigkeitsabkommen, insbesondere 9 ff., 67 ff.; s. sodann z.B. *Kahil-Wolff*, in: L'accord sur la libre circulation des personnes, 49 ff.

die Ausgestaltung der gesetzlichen Grundlage für eine Datenbearbeitung zu erörtern (C.), um auf dieser Grundlage der Frage nachzugehen, ob für Einrichtung und Betrieb der hier zu untersuchenden Informationssysteme im nationalen Recht oder im Völkerrecht (genauer gesagt im Personenfreizügigkeitsabkommen) *de lege lata* ausreichende gesetzliche Grundlagen bestehen (D.), bevor – daran anschliessend – danach gefragt wird, wie die gesetzlichen Grundlagen *de lege ferenda* ausgestaltet werden könnten (E.), wobei jedoch eine Beschränkung auf einige grundsätzliche Überlegungen erfolgt. Die Untersuchung schliesst mit einer thesenartigen Zusammenfassung der wichtigsten Erkenntnisse und einer kurzen Schlussbetrachtung (F.).

Die vorliegende Untersuchung geht auf ein durch die Verfasserinnen im Auftrag des Bundesamts für Sozialversicherungen erstelltes Gutachten zurück. Inhaltlich handelt es sich aber um ein unabhängiges Gutachten: Die Verfasserinnen wurden ausdrücklich nicht auf eine vorgefasste Ansicht oder ein vorgegebenes Ergebnis verpflichtet, sondern um eine unabhängige Klärung der sich stellenden Fragen gebeten.
Dem Bundesamt für Sozialversicherungen, insbesondere Herrn *Stephan Cueni*, Herrn *Robert Engel*, Frau *Silvia Pittavini* und Herrn *Xavier Rossmanith*, sei an dieser Stelle für das entgegengebrachte Vertrauen und die sehr angenehme Zusammenarbeit gedankt.

B. Die geplanten Informationssysteme – eine Skizze

Die Frage, ob für die im Hinblick auf die effektive Anwendung der Koordinierung der sozialen Sicherheit geplanten Informationssysteme (ausreichende) gesetzliche Grundlagen bestehen, setzt notwendigerweise die Kenntnis der **Funktionsweise der Systeme** voraus. Zu diesem Zweck soll zunächst das auf europäischer Ebene vorgesehene Informationssystem EESSI erläutert werden (I.). In der Folge geht es darum, die auf schweizerische Ebene geplanten Anpassungen im Hinblick auf die Umsetzung des EESSI (II.) sowohl für den Bereich der AHV und IV (1.) als auch für denjenigen der Unterstellung (2.) aufzuzeigen. Bei der Beschreibung dieser Systeme liegt der Akzent auf denjenigen Aspekten, die aus rechtlicher Sicht für die Beantwortung der hier im Zentrum stehenden Frage (Existenz ausreichender Rechtsgrundlagen für die vorgesehenen Datenaustausche) von Bedeutung sind, so dass es weniger um die technische Funktionsweise, denn um die Frage von Art und Umfang des durch die Systeme vorgesehenen bzw. ermöglichten Datenaustauschs geht.

I. Das europäische Informationssystem EESSI

Mit dem Inkrafttreten der neuen EU-Verordnungen zur Koordinierung der Systeme der sozialen Sicherheit[8] tritt der **elektronische Datenaustausch zwischen den Sozialversicherungseinrichtungen** an die Stelle der bisher in Papierform verwendeten E-Formulare,[9] was sich bereits aus den einschlägigen rechtlichen Grundlagen ergibt.[10] Dies gilt aufgrund der im Personenfreizügigkeitsabkommen enthaltenen Verweisungen auch für die Schweiz.[11]

Vor diesem Hintergrund ist der in der VO 883/2004 und der VO 987/2009 vorgesehene **Elektronische Austausch von Informationen der sozialen Sicherheit (EESSI, *Electronic Exchange of Social Security Information*)** zu sehen (vgl. Art. 2 ff. VO 987/2009, s. den Ausdruck EESSI in Art. 95 und Anhang IV VO 987/2009). Es handelt sich hierbei um eine **elektronische Infrastruktur der Union**, die den elektronischen Austausch von Informationen der sozialen Sicherheit ermöglichen soll. Die Grundidee des EESSI geht dahin, dass der Informationsaustausch über das von der Europäischen Kommission zur Verfügung gestellte

---

8 Verordnung (EG) Nr. 883/2004 des Europäischen Parlaments und des Rates vom 29. April 2004 zur Koordinierung der Systeme der sozialen Sicherheit, ABl. 2004 L 166, 1, geändert durch Verordnung (EG) Nr. 988/2009 des Europäischen Parlaments und des Rates vom 16. September 2009 zur Änderung der Verordnung zur Koordinierung der Systeme der sozialen Sicherheit und zur Festlegung des Inhalts ihrer Anhänge, ABl. 2009 L 284, 43; Verordnung Nr. 987/2009 des Europäischen Parlaments und des Rates vom 16. September 2009 zur Festlegung der Modalitäten für die Durchführung der Verordnung (EG) Nr. 883/2004 über die Koordinierung der Systeme der sozialen Sicherheit, ABl. 2009 L 284, 1.

9 *Rossmanith/Engel*, CHSS 2/2012, 120.

10 Vgl. Art. 78 VO 883/2004, Art. 2 ff. VO 987/2009. S. auch schon oben A.

11 Vgl. Art. 8 FZA, der auf die gemäss Anhang II anzuwendenden Rechtsakte Bezug nimmt. S. auch schon oben A.

Verwaltungsnetzwerk sTESTA[12] erfolgen soll.[13] Über eine (nationale) Zugangsstelle werden die Sozialversicherungseinrichtungen, die an ein nationales Netz angeschlossen sind, mit dem europäischen Netzwerk sTESTA verbunden.[14] Die Sozialdaten werden in vorkonfigurierten Datenflüssen (*Business flows*) mittels strukturierter elektronischer Dokumente (*Structured Electronic Document – SED*)[15] übermittelt. M.a.W. erfolgt der Datenaustausch zwischen den Mitgliedstaaten immer über das europäische System, das seinerseits aber nur als „Datenübermittlungsinfrastruktur" funktioniert und selbst grundsätzlich[16] weder personenbezogene Daten speichert noch solche bearbeiten kann. Die Grundidee des Systems geht somit davon aus, dass die Mitgliedstaaten vollumfänglich für die Daten verantwortlich bleiben. Insofern kann das EESSI auch als eine Art „automatisiertes bzw. elektronisches Amtshilfeverfahren" bezeichnet werden. Denn EESSI stellt letztlich den elektronischen Datenaustausch sicher, wobei sich die Übermittlung auf der Grundlage einer entsprechenden Anfrage im Rahmen des europäischen System „automatisch" vollzieht; sobald die Daten die nationale Zugangsstelle des Sendestaates passiert bzw. verlassen haben, werden sie direkt dem (allenfalls eingerichteten) Knotenpunkt zugeleitet und danach („automatisch") der entsprechenden Zugangsstelle des Empfangsstaates zugewiesen.

Das System ist in den Grundzügen – ausgehend von Art. 78 VO 883/2004 – in der VO 987/2009 vorgesehen. Die Umsetzung auf der Ebene der Informatik erfolgt durch die Kommission und bildet Gegenstand eines entsprechenden Projekts, wobei sich dieses selbstredend an die bestehenden sekundärrechtlichen Vorgaben zu halten hat. Im Einzelnen kann die vorgesehene **Funktionsweise des EESSI** auf der Grundlage der sekundärrechtlichen Vorgaben und nach dem aktuellen Stand des Projekts wie folgt skizziert werden:[17]

- Die Übertragung von Daten setzt den **Austausch einer bestimmten Anzahl von SEDs** voraus. Sobald alle im spezifischen Fall notwendigen SEDs ausgetauscht worden sind, ist die Empfängereinrichtung grundsätzlich im Besitz aller von ihr benötigten Informationen. Nach dem aktuellen Stand des EESSI-Projekts sollen einer sozialen Einrichtung nur diejenigen Datenflüsse zugewiesen werden, auf welche sie zur Erfüllung ihrer gesetzlichen Aufgaben angewiesen ist. Dadurch könnten grundlegende Fehlsendungen verhindert werden, da demgemäss eine soziale Einrichtung nicht im Stande ist, Informationen zu versenden oder zu erhalten, die nicht in ihrem Kompetenzbereich liegen (z.B. könnte so eine Krankenkasse keine Informationen zu Fami-

---

12 sTESTA steht für *Secure Trans-European Services for Telematics between Administrations*.

13 *Rossmanith/Engel*, CHSS 2/2012, 120.

14 *Rossmanith*, CHSS 2/2010, 81 (82).

15 S. die Begriffsbestimmung zu „strukturiertes elektronisches Dokument" in Art. 1 Abs. 2 lit. d VO 987/2009.

16 Unter Umständen können die SEDs zu statistischen Zwecken beim Knotenpunkt oder beim nationalen Teil der Zugangsstelle erfasst werden, vgl. hierzu noch im Text.

17 S. insoweit auch die Beschreibung des Systems in: Europäische Datenschutzbeauftragter, Stellungnahme zu einer Meldung des Datenschutzbeauftragten der Europäischen Kommission für eine Vorabkontrolle des Systems zum Elektronischen Austausch von Sozialversicherungsdaten („EESSI") vom 28.7.2011 (Fall 2011-0016).

lienleistungen an eine andere soziale Einrichtung weiterleiten oder von einer anderen Institution entgegennehmen).[18] Allerdings sieht das EESSI-Projekt auch horizontale Datenflüsse *(horizontal flows)* vor, d.h. Datenflüsse, die nicht einem spezifischen Sektor zugeteilt werden, sondern angesichts gewisser Informationen, die für alle Versicherungszweige von Interesse sein können (wie z.B. die Bestimmung des Wohnsitzes oder die Feststellung des Todes einer Person), allgemein zur Verfügung stehen. Mittels der dazugehörigen SEDs *(horizontal SED)* können bestimmte Daten auch zwischen sozialen Einrichtungen, die nicht demselben Sektor angehören, ausgetauscht werden. Dadurch erhöht sich die Gefahr von Fehlmitteilungen, da auf diese Weise der Datenaustausch auf soziale Einrichtungen unterschiedlicher Versicherungszweige ausgedehnt wird.[19]

- Jedoch werden die SEDs von der **Zugangsstelle des Sendestaats zur Zugangsstelle des Empfängerstaats in verschlüsselter Form** übertragen. Befindet sich eine Nachricht im Bereich des europäischen sTESTA-Netzwerks, so kann sie demnach, insbesondere von einem nicht berechtigten Dritten, nicht entschlüsselt bzw. gelesen werden.[20]
- Im EESSI-System bilden die **Zugangsstellen** (*Access Points – AP*)[21] die Verknüpfung des europäischen Verwaltungsnetzwerks sTESTA mit den jeweiligen nationalen Netzwerken. Diese Kontaktstellen setzen sich aus einem internationalen Teil und einem nationalen Teil zusammen.[22] Als integrierender Bestandteil des EESSI prüft der internationale Teil die ein- und ausgehenden Mitteilungen auf ihre Gültigkeit und Vollständigkeit.[23] Während bei den eingehenden Mitteilungen die digitalen Signaturen kontrolliert und die Inhalte entschlüsselt werden, werden die ausgehenden Mitteilungen (wieder) verschlüsselt und mit einer digitalen Signatur versehen. Zudem besteht hier die Möglichkeit die eingehenden Nachrichten zu fragmentieren bzw. die ausgehenden Mitteilungen zu defragmentieren. Der nationale Teil der Zugangsstelle wird vom betreffenden Staat gemäss den eigenen Bedürfnissen ausgearbeitet.[24] An jeder Zugangsstelle kann eine Archivierung aller durchlaufenden Mitteilungen stattfinden.[25]
- Nach dem gegenwärtigen Stand der Dinge werden die Nachrichten jedoch nicht direkt von einer Zugangsstelle zur anderen fliessen, sondern im Rahmen des europäischen sTESTA-Netzwerkes von einem **Knotenpunkt** der Zugangsstelle des Empfängerstaats zugeleitet. Dieser Knotenpunkt soll das *Monitoring* und *Logging* der Daten

---

18 *Rossmanith/Engel*, CHSS 2/2012, 120 f.

19 Guidelines for the use of Horizontal SEDs and Flows des EESSI, Kreisschreiben des INPS Nr. 167 vom 29.12.2011, Anlage 6, 4, 35.

20 *Rossmanith*, CHSS 2/2010, 81 (82, 85).

21 Siehe die Definition der Zugangsstelle in Art. 1 Abs. 2 lit. a VO 987/2009.

22 *Rossmanith*, CHSS 2/2010, 81 (84).

23 Zu den diesbezüglichen Anforderungen siehe Art. 78 Abs. 4 VO 883/2004.

24 *Rossmanith*, CHSS 2/2010, 81 (84); vgl. Art. 78 Abs. 2 VO 883/2004, wonach jeder Staat seinen Teil der elektronischen Datenverarbeitungsdienste in eigener Verantwortung betreibt.

25 *Rossmanith*, CHSS 2/2010, 81 (84).

übernehmen, indem die Mitteilungen in Form der SEDs *(Source, Destination, Timestamp, usw.)* automatisch erfasst und statistisch festgehalten werden. Dies ermöglicht es, verloren gegangene SEDs und den Grund ihres Verlusts *(rejected, still queued, delivered to destination, usw.)* innerhalb des Systems zu ermitteln. Zudem könnten die Anwender so die Module, Protokolle, Applikationen usw. rasch aus der Informationsbibliothek entnehmen. Der Knotenpunkt soll aber keinen Zugriff auf den Inhalt der SEDs haben. Nur die betreffenden Zugangsstellen (Sender und Empfänger) wären erkennbar.[26]

- Für die automatische Zuweisung der Mitteilungen an den Empfängerstaat wird an der Koordinationsstelle ein **elektronisches Hauptverzeichnis *(electronic directory)***[27], das die nationalen Institutionen der sozialen Sicherheit auflistet, angeschlossen. Dadurch ist eine Verteilung der Nachrichten bzw. eine Übermittlung von Daten ohne menschliches Zutun möglich.[28] Gemäss Art. 88 Abs. 4 VO 987/2009 wird dieses Verzeichnis von der Europäischen Kommission aufgebaut und verwaltet.[29] Allerdings obliegt es den Mitgliedstaaten, „ihre" Stellen und Träger der Kommission mitzuteilen und in die Datenbank einzugeben und diese Informationen ständig zu aktualisieren.[30] Das elektronische Hauptverzeichnis ersetzt die Inhalte der Anhänge 1, 2, 3, 4 und 10 der Verordnung (EWG) Nr. 574/72[31] und ist öffentlich zugänglich.[32]
- Zur Umsetzung des EESSI-Systems stellt die Europäische Kommission den Staaten ein **Software-Programm** zur Verfügung, das die **Anschliessung der nationalen Netzwerke an das EESSI-System** sicherstellen soll. Den Staaten steht es jedoch frei, ihre eigene Webapplikation zu entwickeln und zu verwenden, wobei die nationalen Software-Programme dieselben Funktionen wie das europäische Programm beinhalten sollten.[33]

---

26 *Rossmanith*, CHSS 2/2010, 81 (82 f.).

27 Bezeichnung des Hauptverzeichnisses gemäss Ziff. 1 Anhang 4 VO 987/2009; teilweise wird hier auch von *master directory* gesprochen, siehe *Rossmanith*, CHSS 2/2010, 81 (83).

28 *Spiegel*, in: Fuchs, Europäisches Sozialrecht, Art. 78 VO 883/2004, Rn. 7.

29 S. auch die Formulierung bei *Rossmanith*, CHSS 2/2010, 81 (83 f.), der davon spricht, dass das Hauptverzeichnis von der Kommission „kontrolliert und betreut und von den Mitgliedstaaten regelmässig aktualisiert" wird.

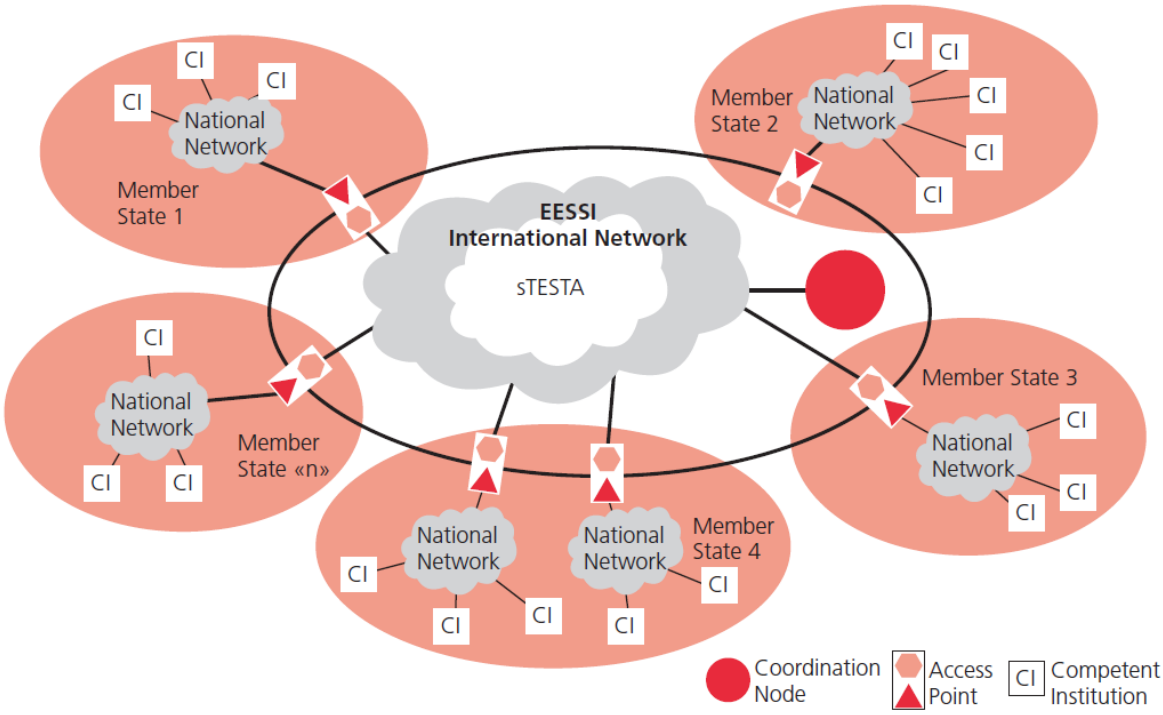
30 Vgl. Art. 88 Abs. 1 VO 987/2009, der die Mitgliedstaaten zur Meldung aller in Betracht kommenden Institutionen verpflichtet sowie Art. 88 Abs. 5 VO 987/2009 bezüglich der ständigen Aktualisierung.

31 Verordnung (EWG) Nr. 574/72 des Rates vom 21. März 1972 über die Durchführung der Verordnung (EWG) Nr. 1408/71 über die Anwendung der Systeme der sozialen Sicherheit auf Arbeitnehmer und Selbständige sowie deren Familienangehörige, die innerhalb der Gemeinschaft zu- und abwandern, ABl. 1972 L 74, 1.

32 Zugang zum Hauptverzeichnis unter <http://ec.europa.eu/social/main.jsp?catId=1028&langId=de>, zuletzt besucht am 30. April 2015.

33 *Rossmanith*, CHSS 2/2010, 81 (84); Guidelines for the use of Applicable Legislation SEDs, Flows and Portable Document A1 des EESSI, Kreisschreiben des INPS Nr. 167 vom 29.12.2011, Anlage 5, 21.

Die abgebildete Darstellung[34] zeigt den beschriebenen Datenaustausch:



Im Rahmen des EESSI-Systems werden gemäss **Art. 2 Abs. 2 VO 987/2009** sämtliche **Daten** ausgetauscht, die zur **Begründung und Feststellung der Rechte und Pflichten der Personen, für welche die VO 883/2004 gilt**, benötigt werden. Demzufolge muss für die Bestimmung der betreffenden Daten auf die VO 883/2004 zurückgegriffen werden, die sich gemäss Art. 3 VO 883/2004 auf Leistungen bei Krankheit, Mutterschaft und Vaterschaft, Invalidität, Alter, Hinterbliebenen, Arbeitsunfällen und Berufskrankheiten, Sterbegeld, Arbeitslosigkeit, Vorruhestandsleistungen und Familienleistungen bezieht.[35] Je nach Versicherungszweig kommen unterschiedliche Kategorien von Daten in Betracht. Die Personalien der in Frage stehenden Person (Name, Vorname, Geburtsdatum, Versichertennummer, Geschlecht, Zivilstand, Staatsangehörigkeit, Adresse) können als sektorübergreifende Daten angesehen werden. Ansonsten muss für jeden Versicherungszweig bzw. jede Anfrage separat untersucht werden, welche Daten im konkreten Fall betroffen sind.

Der Datenaustausch im Rahmen des EESSI-Projekts findet nach Art. 2 Abs. 2 VO 987/2009 zwischen den Mitgliedstaaten entweder **unmittelbar durch die Träger selbst oder über eine Verbindungsstelle** statt. Innerhalb eines Staats sind demnach die Träger von den Verbindungsstellen zu unterscheiden. Die Verbindungsstelle ist jene zentrale nationale Stelle, die Anfragen und Amtshilfeersuchen stellvertretend für die einzelnen Träger in Empfang nimmt und ihnen diese alsdann zur Beantwortung weiterleitet.[36] Sie fungiert somit als Bindeglied

---

34 Ersichtlich in: *Rossmanith/Engel*, CHSS 2/2012, 120 (121).

35 Hierbei gilt es zu beachten, dass gewisse dieser Sozialleistungen in der Schweiz nicht existieren, so etwa Leistungen bei Vaterschaft, Sterbegeld und Vorruhestandsleistungen.

36 *Spiegel*, in: Fuchs, Europäisches Sozialrecht, Art. 78 VO 883/2004, Rn. 7. Vgl. die Definition der Verbindungsstelle in Art. 1 Abs. 2 lit. b VO 987/2009.

zwischen den einzelnen nationalen Trägern eines Versicherungszweigs mit den entsprechenden ausländischen Einrichtungen. Dies führt insofern zu einer erleichterten Rechtsanwendung, als eine Einzelperson so nicht mehr den im Einzelfall zuständigen Träger ausfindig machen muss, sondern ihre Anfrage direkt an die nationale Verbindungsstelle richten kann.[37] Ausserdem liegt es an der Verbindungsstelle, im Fall einer fehlerhaften Kodifizierung einer sozialen Institution im System den dafür zuständigen Träger manuell zu identifizieren.[38] Die das EESSI-System benutzenden Träger und Verbindungsstellen werden gemäss den in Anhang 4 VO 987/2009 festgelegten Vorschriften im Hauptverzeichnis *(electronic directory)* aufgeführt.

In der **Schweiz** betrifft der elektronische Datenaustausch alle **Versicherungszweige, die von der VO 883/2004**[39] und der **VO 987/2009**[40] erfasst werden und somit alle sozialen Einrichtungen, die dem grenzüberschreitenden Datenaustausch gemäss den erwähnten Instrumenten unterliegen. Dazu gehören neben den Verbindungsstellen[41] sämtliche AHV-Ausgleichskassen, IV-Stellen, Familienausgleichskassen, Vorsorgeeinrichtungen, Krankenkassen, Unfallversicherer und Arbeitslosenkassen.[42]

Die zwischen den sozialen Einrichtungen grenzüberschreitend ausgetauschten Daten werden zwar im Rahmen des EESSI-Systems an verschiedenen Stellen – insbesondere an der Zugangsstelle und am Knotenpunkt – in verschlüsselter Form erfasst, jedoch erfolgt diese Erfassung lediglich zum Zweck eines effizienten Datenaustauschs, d.h. dadurch soll beispielsweise der Grund für den Verlust eines SEDs ermittelt werden können.[43]

Das in den sekundärrechtlichen Vorgaben vorgesehene Unionssystem EESSI betrifft lediglich die Frage der **internationalen Architektur** nach dem skizzierten System. Die Ausführungen haben aber auch deutlich gemacht, dass das System darüber hinaus einer **nationalen Durchführung** bedarf, ist doch sicherzustellen, dass die Verbindungsstellen bzw. unter Umständen die Träger[44] über die notwendigen Daten in elektronischer Form verfügen, damit diese übermittelt werden können. Auf welche Weise dies genau geschieht, liegt in der Kompetenz der Mitgliedstaaten bzw. der EWR-Staaten und der Schweiz, wobei jedoch selbstredend den Anforderungen des Unionsrechts an den grenzüberschreitenden elektronischen Datenaustausch Rechnung zu tragen ist.

---

37 *Spiegel*, in: Fuchs, Europäisches Sozialrecht, Art. 78 VO 883/2004, Rn. 7.

38 *Spiegel*, in: Fuchs, Europäisches Sozialrecht, VO 883/2004, Rn. 9.

39 Siehe Fn. 8.

40 Ebd.

41 Diese sind: das BSV, das SECO, die zentrale Ausgleichsstelle der AHV (ZAS), die gemeinsame Einrichtung KVG, die Schweizerische Unfallversicherungsanstalt (SUVA), der Sicherheitsfonds BVG, vgl. Verbindungsstellen Schweiz: Adressen der schweizerischen Verbindungsstellen und zuständigen Träger des BSV, 1 f.

42 S. Verbindungsstellen Schweiz: Adressen der schweizerischen Verbindungsstellen und zuständigen Träger des BSV, 1 ff.

43 Zur Beschreibung der einzelnen Bestandteile des Informationssystems EESSI, siehe oben.

44 S. Art. 2 Abs. 2 VO 987/2009, der vorsieht, dass die Übermittlung entweder unmittelbar durch die Träger oder über die Verbindungsstellen erfolgt.

II. Zum Stand der Umsetzung in der Schweiz – ausgewählte Aspekte

Für die **Umsetzung des EESSI-Projekts auf nationaler Ebene** sowie für die Einführung des elektronischen Datenaustausches wurde in der **Schweiz** das sogenannte **SNAP-EESSI-Programm**[45] gestartet. Aufgrund der Erkenntnis, dass die Entwicklung einer einzigen Applikation für alle schweizerischen sozialen Einrichtungen nicht möglich ist, soll jedem Sektor sein eigenes Projekt gewidmet werden, das den Eigenheiten des jeweiligen Versicherungszweigs Rechnung trägt.[46] In Bezug auf die geplanten Projekte ist die genaue technische Struktur des Datenaustausches noch offen. Um dennoch auf nationale datenschutzrechtliche Fragen eingehen zu können, werden massgebliche Eckpunkte der nationalen Systeme im Rahmen der AHV und IV sowie der Unterstellung in grober Weise umrissen.

1. Im Bereich der Alters-, Hinterlassenen- und Invalidenversicherung

Die strukturellen Anpassungen auf nationaler Ebene sind vor dem Hintergrund des durch das EESSI-Projekt eingeleiteten elektronischen Datenaustausches zu sehen. Im Bereich der AHV und IV fungiert die zentrale Ausgleichsstelle der AHV (ZAS) als Verbindungsstelle und sorgt als einzige schweizerische Kontaktträgerin[47] für die grenzüberschreitende Datenübermittlung.[48] Um dieser Aufgabe gerecht zu werden, ist die ZAS darauf angewiesen, dass ihr die grenzüberschreitend relevanten Daten von den betroffenen Stellen weitergeleitet werden. Demzufolge haben die zuständigen AHV-Ausgleichskassen oder IV-Stellen entsprechende Daten – in welcher Form auch immer – an die ZAS zu übermitteln, damit grenzüberschreitende Gesuche abgeklärt werden können.[49] Damit wird deutlich, dass das europäische System einen schweizinternen Datenaustausch zwischen der ZAS, den AHV-Ausgleichskassen und den IV-Stellen erfordert.

Die im Rahmen dieses Austausches zirkulierenden Daten lassen sich aus den Angaben erschliessen, die für die Abklärung des konkreten Einzelfalls erforderlich sind. Abzustellen ist demnach auf die im Antrag der Einzelperson enthaltenen Daten, die sich gemäss Art. 46 Abs. 1 VO 987/2009 massgeblich nach dem nationalen Recht des zuständigen Trägers bestimmen. Stellt eine Einzelperson in der Schweiz bei der für ihr Anliegen zuständigen AHV-Ausgleichskasse oder IV-Stelle einen Leistungsantrag, so sind gemäss Art. 29 Abs. 2 ATSG

---

45 SNAP-EESSI bedeutet *Swiss National Action Plan for Electronic Exchange of Social Security Information.*

46 *Rossmanith/Engel*, CHSS 2/2012, 120 (122).

47 Vgl. Art. 47 Abs. 1 VO 987/2009.

48 *Rossmanith/Engel*, CHSS 2/2012, 120 (123).

49 Vgl. Art. 45 Abs. 4 VO 987/2009, wonach der Antrag auf Alters-, Invaliden- oder Hinterbliebenenrenten entweder beim zuständigen Träger am Wohnort oder beim Träger im Staat, in dem die Gesuch stellende Person zuletzt versichert war, einzureichen ist.

die hierfür zur Verfügung stehenden Formulare auszufüllen. Die bekanntzugebenden Daten variieren somit je nachdem ob der Antragssteller eine Leistung der Alters-, Hinterlassenen- oder Invalidenrente beantragt. Jedenfalls hat die Einzelperson bei der Antragsstellung Angaben zu ihrer Person, zum Wohnsitz, zur Erwerbstätigkeit zu machen, wobei zudem unter Umständen auch besonders schützenswerte Personendaten, wie z.B. Angaben zur gesundheitlichen Beeinträchtigung, betroffen sein können.[50]

2. Im Bereich der Unterstellung

Für die Frage, welchen sozialversicherungsrechtlichen Bestimmungen eine erwerbstätige Person untersteht, bestimmt die VO 883/2004 in Art. 11 Abs. 1, dass die Rechtsvorschriften eines einzigen Staates Anwendung finden, wobei es sich dabei im Grundsatz um die Sozialversicherungsgesetzgebung des Erwerbsorts handelt (sog. Grundsatz *lex loci laboris*).[51] Im Verhältnis Schweiz-EU bedeutet dies, dass eine erwerbstätige Person grundsätzlich in demjenigen Land sozialrechtlich versichert ist, in welchem sie einer Beschäftigung nachgeht. Für den Fall, dass eine Person vorübergehend in einem anderen Staat eine Arbeit verrichtet (sog. Entsendung), können aber unter gewissen Voraussetzungen die Rechtsvorschriften des Ursprungsstaats anwendbar bleiben.[52] Im Übrigen enthält die VO 883/2004 auch eine Spezialregelung zur Festlegung der anwendbaren Bestimmungen im Fall der Mehrfachtätigkeit eines Arbeitnehmers bzw. ein Selbstständigerwerbenden in verschiedenen Staaten.[53]
Für die Beurteilung der sozialversicherungsrechtlichen Unterstellung sind in der Schweiz die AHV-Ausgleichskassen oder das BSV zuständig, je nachdem welche Fallkonstellation konkret vorliegt.[54] Denn während die AHV-Ausgleichskassen beispielsweise Fälle beurteilen, in denen ein Selbständigerwerbender bzw. ein Arbeitnehmer im Sinn von Art. 12 VO 883/2004 für höchstens 24 Monate eine Arbeit im Ausland aufnimmt, liegt es in der Zuständigkeit des BSV, darüber hinausgehende Entsendungen durch eine sog. Ausnahmevereinbarung auf der Grundlage von Art. 16 VO 883/2004 zu bescheinigen. Damit diese Stellen tätig werden, muss die ersuchende Person zunächst einen Antrag auf Entsendung bzw. auf Verlängerung derselben stellen. Wird dem Gesuch stattgegeben, so stellt die zuständige AHV-Ausgleichskasse bzw. das BSV dem Arbeitgeber des Entsandten bzw. dem Selbstständigerwerbenden eine Be-

---

50 Für die Ermittlung der im Einzelfall betroffenen Daten sind die im Internet zur Verfügung stehende Formulare zu konsultieren, s. unter <https://www.ahv-iv.ch/de/Merkbl%C3%A4tter-Formulare/Formulare>, zuletzt besucht am 30. April 2015.

51 Eingehender dazu: *Schreiber*, in: Schreiber/Wunder/Dern, Kommentar zur VO 883/2004, Vor Art. 11, Rn. 9; *Steinmeyer*, in: Fuchs, Europäisches Sozialrecht, Art. 11 VO 883/2004, Rn. 9 ff.

52 S. Art. 12 VO 883/2004, der die weiterführende Anwendung der sozialrechtlichen Bestimmungen an die Erfüllung verschiedener Kriterien knüpft.

53 Vgl. die Bestimmung von Art. 13 VO 883/2004, welche die Unterstellung im Fall der Beschäftigung in zwei oder mehr Staaten regelt.

54 *Rossmanith/Engel*, CHSS 2/2012, 120 (122).

stätigung aus, welche, falls ersteres der Fall ist, anschliessend dem betreffenden Arbeitnehmer übergeben wird.[55]

Die grenzüberschreitende Datenübermittlung im Rahmen des EESSI-Projekts impliziert einen – wie auch immer ausgestatteten – schweizerischen Datenaustausch zwischen den Arbeitgebern bzw. Unternehmen, den AHV-Ausgleichskassen und dem BSV. Denn damit das BSV beispielsweise in der Lage ist, eine Ausnahmevereinbarung entsprechend Art. 16 VO 883/2004 mit dem Ausland zu treffen, muss es von den bereits gestatteten Entsendungen durch die AVH-Ausgleichskassen Kenntnis haben.[56] Umgekehrt müssen auch die AHV-Ausgleichskassen zwecks Erfüllung ihrer Aufgaben die Möglichkeit haben, die durch das BSV getroffenen Vereinbarungen einzusehen.[57] Damit die von den zuständigen Stellen gefällten Entscheidungen den Arbeitnehmenden mitgeteilt werden können, sollten schliesslich auch die Unternehmen in den schweizerischen Datenaustausch miteinbezogen werden.[58]

Die Daten, die im Bereich der Unterstellung zwischen den davon betroffenen Behörden ausgetauscht werden, sind ebenfalls[59] aus den dazu auszufüllenden Formularen zu eruieren. Neben den Personalien der ersuchenden Person geht es dabei in erster Linie um die Beschreibung der Arbeitstätigkeit in der Schweiz und im Ausland.[60]

---

55 Entsendungsmerkblatt CH-EU des BSV, Soziale Sicherheit für Entsandte zwischen der Schweiz und der EU, April 2012, 5 und 7; *Niederer/Meyer*, ST 10/13, 712 (714).

56 Denn zum Abschluss einer solchen Vereinbarung muss das BSV Zugang zu den Daten haben, die Aufschluss darüber geben, ob und wie lange eine Person bereits entsandt wurde.

57 Die Gründe für einen solchen Datenaustausch sind darin zu sehen, dass auch die zuständige AHV-Ausgleichskasse zur Bestimmung des anwendbaren Rechts der Informationen über bereits zurückgelegte Entsendungen bedarf.

58 S. hierzu bereits oben im Text.

59 Vgl. die Beschreibung der implizierten Daten im Rahmen der AHV und der IV unter B.II.1.

60 Für Einzelheiten sind die Formulare unter <https://www.ahv-iv.ch/de/Merkbl%C3%A4tter-Formulare/Formulare>, zuletzt besucht am 30. April 2015, zu konsultieren.

C. Völker-, verfassungs- und datenschutzrechtliche Vorgaben für den Betrieb von Informationssystemen

Wird nach der Existenz **gesetzlicher Grundlagen** für die durch die skizzierten Informationssysteme vorgesehenen Datenbearbeitungen gefragt, so ist grundsätzlich zwischen drei verschiedenen Fragen bzw. Ebenen zu unterscheiden:

- Erstens kann nach den gesetzlichen Grundlagen und Vorgaben für die **Errichtung der „internationalen Architektur" des EESSI**, die ausschliesslich durch die Kommission realisiert wird, gefragt werden. Hier können von vornherein nur die einschlägigen sekundärrechtlichen Regelungen – die ihrerseits die primärrechtlichen Vorgaben zu beachten haben und in ihrem Lichte auszulegen sind – herangezogen werden.[61]
- Zweitens geht es um den Datenaustausch bzw. die Datenbearbeitung durch nationale Organe bzw. die **Einrichtung von Informationssystemen durch nationale Organe im Rahmen des EESSI**.
- Drittens schliesslich steht der Erlass derjenigen nationalen Massnahmen bzw. die Einrichtung derjenigen nationalen Systeme zur Debatte, die im Hinblick auf die **effektive nationale Durchführung der durch das Unionsrecht aufgegebenen Verpflichtungen** notwendig oder auch nur sinnvoll sind.

Die erste Ebene ist nicht Gegenstand dieser Untersuchung, die sich vielmehr auf die nationale Ebene konzentriert, so dass nachfolgend lediglich die beiden zuletzt genannten Ebenen berücksichtigt werden. Da es sich hierbei um **Datenbearbeitungen nationaler Organe** bzw. (genauer) von **Bundesorganen** handelt, kommen hier somit die „üblichen" datenschutzrechtlichen Vorgaben zum Zuge, die Bundesorgane zu beachten haben. Diese sollen – nach einigen Bemerkungen zum anwendbaren Recht (I.) – nachfolgend skizziert werden (II.),[62] wobei der Akzent auf der Frage nach der Reichweite der gesetzlichen Grundlage bzw. den Anforderungen an dieselbe liegt.

I. Zum anwendbaren Recht

Vor dem Hintergrund der beschriebenen Informationssysteme ist grundsätzlich davon auszugehen, dass **Bundesorgane** tätig werden (sollen). Daher findet jedenfalls **nationales Recht**

---

61 Relevant ist hier im Übrigen VO 45/2001 (Verordnung (EG) Nr. 45/2001 des Europäischen Parlaments und des Rates vom 18. Dezember 2000 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die Organe und Einrichtungen der Gemeinschaft und zum freien Datenverkehr, ABl. 2001, L 8, 1).

62 Vgl. allgemein zu diesen Vorgaben insbesondere *Epiney*, in: Belser/Epiney/Waldmann, Datenschutzrecht, § 9; *Epiney/Fasnacht*, in: Belser/Epiney/Waldmann, Datenschutzrecht, § 10; *Waldman/Bickel*, in: Belser/Epiney/Waldmann, Datenschutzrecht, § 12; s. auch den Überblick bei *Epiney/Civitella/Zbinden*, Datenschutzrecht in der Schweiz, 21 ff.

Anwendung (1.). Darüber hinaus ist nach der Massgeblichkeit der Regelungen des **Freizügigkeitsabkommens** bzw. – daraus abgeleitet – gewisser unionsrechtlicher Vorgaben zu fragen (2.), bevor ein kurzes Fazit gezogen wird (3.).

Nicht näher eingegangen werden soll im Folgenden jedoch auf die völkerrechtliche Ebene bzw. sonstige Aspekte derselben (abgesehen vom Freizügigkeitsabkommen):

- Zwar ist hier insbesondere die **Datenschutzkonvention des Europarates** von Bedeutung. Diese im Jahr 1985 in Kraft getretene Konvention – die Mindeststandards im Bereich des Datenschutzes schaffen und den grenzüberschreitenden Datenverkehr regeln soll[63] – enthält nämlich durchaus auch in unserem Zusammenhang rechtlich verbindliche[64] Vorgaben. Da dieser Vertrag jedoch als sog. „*non self-executing treaty*" konzipiert wurde, richtet er sich in erster Linie an die Staaten; eine Einzelperson kann sich somit nicht direkt auf die in der Konvention enthaltenen Rechte berufen.[65] Vielmehr ist davon auszugehen, dass die Vertragsstaaten die in der Konvention formulierten Grundsätze auf nationaler Ebene umzusetzen haben, was in der Schweiz durch das Datenschutzgesetz des Bundes sowie die kantonalen Datenschutzgesetze geschehen ist. Insofern ist die Konvention letztlich im Rahmen der völkerrechtskonformen Auslegung des nationalen Rechts zu berücksichtigen.
- Auch die **EMRK** ist im Zusammenhang mit datenschutzrechtlichen Problemstellungen von (grosser) Bedeutung. Denn Datenschutz bzw. das Recht der Einzelnen darauf, dass sie betreffende Daten nicht gespeichert und verwertet, also nicht bearbeitet, werden, ist nach der ständigen Rechtsprechung des EGMR als spezifischer Ausfluss bzw. Teilbereich des Rechts auf Achtung der Privatsphäre (Art. 8 EMRK) zu sehen.[66] Allerdings sind die spezifischen, im Datenschutzgesetz des Bundes geregelten Anforderungen an die Datenbearbeitung (durch öffentliche Organe) letztlich als sich bereits aus Art. 8 EMRK (sowie Art. 13 BV) ergebende Grundsätze anzusehen, so dass den Vorgaben der EMRK und der Verfassung durch eine entsprechende Auslegung und Anwendung dieser Grundsätze Rechnung zu tragen ist.[67]

1. Nationales Recht

Da es bei den in Frage stehenden Informationssystemen soweit ersichtlich um Datenbearbeitungen durch **Bundesorgane**[68] geht, sind – neben den verfassungs- und völkerrechtlichen Regelungen (insbesondere Art. 13 BV, Art. 8 EMRK) – in jedem Fall die Vorgaben des **Datenschutzgesetzes (DSG)** anwendbar (Art. 2 Abs. 1 DSG).

Die **Anwendbarkeit des nationalen Rechts bei grenzüberschreitenden Datenübermittlungen** ist im Übrigen auch Gegenstand der **Kollisionsregel**[69] **des Art. 77 Abs. 1 VO 883/2004**: Danach ist für die Datenübermittlung von einer nationalen Behörde eines Mitgliedstaats zu einer nationalen Behörde eines anderen Mitgliedstaats das Datenschutzrecht des übermittelnden Staats massgebend. Werden die Daten durch die Behörden des Empfängerstaats weitergegeben, gespeichert, verändert oder gelöscht, so sind die Rechtsvorschriften dieses Staats anwendbar.

---

63 *Epiney/Schleiss*, in: Belser/Epiney/Waldmann, Datenschutzrecht, § 3, Rn. 24, m.w.N.; vgl. auch Art. 1 DSK.

64 Neben der DSK bestehen auf völkerrechtlicher Ebene weitere nicht verbindliche datenschutzrechtliche Regelungen. Auf diese dem soft law angehörende Vorschriften wird hier nicht eingegangen; mehr zu diesen bei *Epiney/Schleiss*, in: Belser/Epiney/Waldmann, Datenschutzrecht, § 3, Rn. 51 ff.

65 *Epiney/Schleiss*, in: Belser/Epiney/Waldmann, Datenschutzrecht, § 3, Rn. 25; *Ellger*, Datenschutz im grenzüberschreitenden Datenverkehr, 463.

66 Zum Ganzen, m.w.N., *Epiney/Schleiss*, in: Belser/Epiney/Waldmann, Datenschutzrecht, § 3, Rn. 9 ff.

67 S. insoweit unten C.II.

68 S. noch sogleich im (Klein-)Text.

69 *Wunder*, in: Schreiber/Wunder/Dern, Kommentar zur VO 883/2004, Art. 77, Rn. 3.

Das schweizerische Datenschutzrecht ist demnach auf alle Fälle anzuwenden, in denen Daten an ausländische Behörden übermittelt werden oder empfangene Daten von Schweizer Behörden weitergegeben, gespeichert, verändert oder gelöscht werden. Angesichts dessen gilt etwa Schweizer Recht, solange einerseits die von der Verbindungsstelle ins Ausland übermittelten Daten nicht im erwähnten Sinn verarbeitet werden und sobald andererseits eine schweizerische Verbindungsstelle die aus dem Ausland erhaltenen Informationen an den zuständigen nationalen Träger weiterleitet oder sonstwie bearbeitet.

Demnach muss beim Betrieb der **nationalen Systeme** in jedem Fall das schweizerische Datenschutzrecht eingehalten werden. Aber auch die im Rahmen des **EESSI** (ggf. auf der Grundlage der Vorgaben der einschlägigen Verordnungen)[70] erfolgenden Datenübermittlungen durch nationale Behörden haben (auch) die nationalen Vorgaben zu beachten, jedenfalls soweit diese nicht aufgrund des Vorrangs des Unionsrechts bzw. (in der Schweiz) des Völkerrechts unanwendbar sind. Bedeutsam ist dies insbesondere für die Pflicht der Träger nach Art. 2 Abs. 2 VO 987/2009, unverzüglich alle Daten, die zur Begründung und Feststellung der Rechte und Pflichten der Personen, für die die Grundverordnung gilt, benötigt werden, zur Verfügung zu stellen oder auszutauschen.

Der **Anwendungsbereich des Datenschutzgesetzes des Bundes (DSG)** erstreckt sich auf alle Bearbeitungen von **Personendaten** von natürlichen und juristischen Personen durch Privatpersonen und **Bundesorgane** (Art. 2 Abs. 1 DSG). Keine Anwendung findet das DSG folglich auf Datenbearbeitungen durch kantonale und kommunale Behörden. Dafür sind aufgrund der Kompetenzverteilung der Bundesverfassung die Kantone zuständig.[71] Es steht den Kantonen demnach frei, selbst Bestimmungen betreffend den Datenschutz zu erlassen, sofern es um die Bearbeitung von Personendaten durch kantonale oder kommunale Behörden geht. Allerdings sind die Kantone dabei an die bundesrechtlichen und völkerrechtlichen Vorgaben gebunden,[72] aus denen sich auch Pflichten zu einer diesbezüglichen gesetzlichen Regelung ergeben (können).

Für die Abgrenzung der **Anwendungsbereiche des Datenschutzgesetzes des Bundes und der kantonalen Datenschutzgesetze** muss demzufolge auf das bearbeitende Organ abgestellt werden. Werden Daten von kantonalen Behörden bearbeitet, so ist kantonales Datenschutzrecht anwendbar. Hingegen kommt Bundesrecht zum Zug, falls die Datenbearbeitung durch ein Bundesorgan erfolgt. Bundesorgane sind nach Art. 3 lit. h DSG alle „Behörden und Dienststellen des Bundes sowie Personen, soweit sie mit öffentlichen Aufgaben des Bundes betraut sind". Zu den Behörden und Dienststellen des Bundes gehören alle Stellen der Bundesverwaltung (insbesondere Departemente, Bundesämter, Bundeskanzlei) sowie eidgenössische Anstalten (wie z.B. die SUVA).[73] Unter den Begriff der Personen, die eine öffentliche Aufgabe des Bundes erfüllen und somit Bundesorgane im Sinne von Art. 3 lit. h DSG darstellen, können nur Privatpersonen fallen. Beispielsweise sind gewisse Versicherungen, die als juristische Personen auf der Grundlage des Privatrechts organisiert sind, als Bundesorgane im Sinne des DSG zu betrachten.[74] Hingegen bleiben kantonale und kommunale Organe – unter Vorbehalt von Art. 37 DSG[75] – auch dann dem kantonalen Datenschutzecht unterstellt, wenn sie zwecks Erfüllung einer Aufgabe des Bundes tätig werden.[76] Kantonales Datenschutzrecht kommt im Fall des Vollzugs von Bundesrecht aller-

---

70 Hierzu noch sogleich C.I.2.

71 Die Bundesverfassung enthält keine Vorschrift, die dem Bund eine umfassende Kompetenz im Bereich des Datenschutzes einräumt. Für den Erlass des DSG stützte sich der Bund auf Art. 95, 122 und 173 Abs. 2 BV; vgl. *Belser*, in: Belser/Epiney/Waldmann, Datenschutzrecht, § 5, Rn. 4 ff.

72 *Belser*, in: Belser/Epiney/Waldmann, Datenschutzrecht, § 5, Rn. 44.

73 Botschaft DSG, BBl 1988 II 445; *Epiney*, in: Verwaltungsorganisationsrecht, 5 (12). Für die Bestimmung der Bundesbehörden im Einzelfall ist das Regierungs- und das Verwaltungsorganisationsgesetz massgeblich.

74 *Meier*, Protection des données, Rn. 601 f.

75 Nach Art. 37 Abs. 1 DSG sind die darin aufgezählten Bestimmungen auch auf kantonale Behörden anwendbar, soweit beim Vollzug von Bundesrecht keine kantonalen Datenschutzvorschriften bestehen, die angemessenen Schutz bieten.

76 Botschaft DSG, BBl 1988 II 445; *Belser*, in: Belser/Epiney/Waldmann, Datenschutzrecht, § 5, Rn. 48.

dings dann nicht zum Zug, wenn auf Bundesebene eine abschliessende bereichsspezifische Datenschutzregelung besteht. Aufgrund der in Art. 32 ATSG geregelten Amts- und Verwaltungshilfe trifft dies auf den Bereich der Sozialversicherungen zu.[77] Somit sind in diesem Bereich auch für die vollziehenden kantonalen Behörden ausschliesslich bundesrechtliche Datenschutzbestimmungen massgeblich.

2. Anwendung der europäischen Rechtsakte im Rahmen des Freizügigkeitsabkommens

Die neuen EU-Verordnungen[78], die die Einführung des EESSI vorsehen, sind in der Schweiz im Rahmen des FZA grundsätzlich **direkt anwendbar**.[79] Damit hat die Schweiz die Vorgaben der Verordnungen sowohl in Bezug auf die Datenübermittlung als auch für den Datenschutz und die Bestimmung des anzuwendenden Datenschutzrechts anzuwenden.

Anzumerken ist hier der Vollständigkeit halber, dass die vorbestehenden bilateralen Abkommen zwischen der Schweiz und den EU-Mitgliedstaaten mit Inkrafttreten des FZA grundsätzlich keine Anwendung mehr finden,[80] wobei sie grundsätzlich wieder „aufleben" würden, sollte das Freizügigkeitsabkommen ausser Kraft treten.

Die **VO 883/2004** bezieht sich nach ihrem Art. 3 Abs. 1, der den persönlichen Anwendungsbereich regelt, allein auf **grenzüberschreitende Sachverhalte**.[81] Auch Art. 77 VO 883/2004 zeigt auf, dass die VO 883/2004 erst relevant ist, wenn Daten von einem Mitgliedstaat zu einem anderen Mitgliedstaat übermittelt werden. Werden folglich **Daten ausschliesslich zwischen den sozialen Einrichtungen ein und desselben Staats** ausgetauscht, so finden die im EU-Sekundärrecht festgehaltenen Regeln über den elektronischen Datenaustausch keine Anwendung. Vielmehr bleibt jedem Staat selbst überlassen, ob er im Sozialbereich auch auf nationaler Ebene eine elektronische Übermittlung der Daten einführt.[82] Zur Umsetzung des EESSI müssen die beteiligten Staaten allerdings dafür sorgen, dass ein elektronischer Datenaustausch über ihre Grenzen hinweg möglich ist, d.h. sie sind dazu angehalten, den nationalen Teil der Zugangsstelle zu entwickeln und Institutionen zu errichten, die die verschiedenen SEDs in Empfang nehmen können und sie in der Folge – in welcher Form auch immer – an die zuständige Sozialversicherungsanstalt weiterleiten.[83]

---

77 *Jöhri*, in: Rosenthal/Jöhri, Handkommentar DSG, Art. 37, Rn. 6; a.A. *Prieur*, in: Passadelis/Rosenthal/Thür, Datenschutzrecht, § 13, Rn. 13.6.

78 Siehe Fn. 8.

79 Siehe die Bezugnahme auf die anzuwendenden Rechtsakte in Anhang II FZA, Abschnitt A. Grundlegend zur Wirkungsweise der Verordnungen in der Schweiz, m.w.N., *Cardinaux*, Personenfreizügigkeitsabkommen, Rn. 29 ff.

80 Art. 20 FZA.

81 *Spiegel*, in: Fuchs, Europäisches Sozialrecht, Art. 2 VO 883/2004, Rn. 6; *Dern*, in: Schreiber/Wunder/Dern, Kommentar zur VO 883/2004, Art. 2, Rn. 8.

82 *Spiegel*, in: Fuchs, Europäisches Sozialrecht, Art. 78 VO 883/2004, Rn. 7.

83 Vgl. dazu Art. 4 Abs. 2 VO 987/2009, der den elektronischen Datenaustausch zwischen den Trägern oder den Verbindungsstellen vorsieht. Es genügt folglich, wenn einzig die Verbindungsstellen in der Lage sind, Nachrichten in Form der SEDs zu empfangen und zu verschicken. Siehe auch *Spiegel*, in: Fuchs, Europäisches Sozialrecht, Art. 78 VO 883/2004, Rn. 7, wo ebenfalls darauf hingewiesen wird, dass die Staaten auf nationaler Ebene nicht zu einer elektronischen Bekanntgabe der Daten verpflichtet sind.

In der Schweiz finden die **VO 883/2004** und die **VO 987/2009** demgemäss erst Anwendung, wenn ein **Sachverhalt mit grenzüberschreitenden Bezügen** vorliegt und demnach Daten von einer Verbindungsstelle oder einem Träger ins sTESTA-Netzwerk übertragen werden bzw. die Daten automatisch von der Zugangsstelle übermittelt werden, dies in (direkter) Anwendung der Vorgaben der genannten Sekundärrechtsakte. Die **nationalen Informationssysteme** ihrerseits sind vor dem Hintergrund zu sehen, den **grenzüberschreitenden Datenaustausch zu ermöglichen**.[84] Demzufolge sollten in diese Systeme nur Informationen eingetragen werden, die grenzüberschreitend relevant sind und als solche über die Verbindungsstellen oder Träger ins Ausland gelangen. Aus diesen Gründen sind die Regeln der VO 883/2004 und der VO 987/2009 auch für die in diesen Systemen erfolgenden Datenbearbeitungen von Relevanz, ist doch davon auszugehen, dass den Anforderungen des EU-Sekundärrechts entsprochen werden soll.

Hinsichtlich des **anwendbaren Datenschutzrechts im Rahmen des EESSI-Systems** verweist **Art. 77 Abs. 2 VO 883/2004** auf das einschlägige **Unionsrecht**. Danach sind bei der Anwendung der VO 883/2004 und der VO 987/2009 die unionsrechtlichen Vorgaben betreffend den Datenschutz zu beachten. Was die Betreibung der elektronischen Datenverarbeitungsdienste durch die einzelnen Mitgliedstaaten im Speziellen anbelangt, nimmt auch Art. 78 Abs. 2 VO 883/2004 auf die Einhaltung der unionsrechtlichen Bestimmungen über den Datenschutz Bezug. Diese Bestimmung bezieht sich nur auf die im **Zuge des EESSI notwendigen Datenverarbeitungen bzw. Informationssysteme**, d.h. die bei den nationalen Trägern, der Verbindungsstelle und beim nationalen Teil der Zugangsstelle erforderlichen Verarbeitungsvorrichtungen. Als anwendbares Unionsrecht betreffend den Datenschutz kommen insbesondere die RL 95/46[85] und die VO 45/2001[86] in Betracht,[87] wobei in unserem Zusammenhang angesichts des persönlichen Anwendungsbereichs der VO 45/2001 lediglich die **RL 95/46** – die im Übrigen in näherer Zukunft durch eine Verordnung (die sog. Datenschutzgrundverordnung) abgelöst werden soll[88] – von Bedeutung sein könnte.

---

84 S.o. B.II.

85 Richtlinie 95/46/EG des europäischen Parlaments und des Rates vom 24. Oktober 1995 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr, ABl. 1995 L 281, 31.

86 Verordnung (EG) Nr. 45/2001 des Europäischen Parlaments und des Rates vom 18. Dezember 2000 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die Organe und Einrichtungen der Gemeinschaft und zum freien Datenverkehr, ABl. 2001, L 8, 1.

87 Die Datenschutzrichtlinie für elektronische Kommunikation (RL 2002/58) ist hier nicht einschlägig, da E. 55 der abgeänderten Rechtsakte (RL 2009/136) klarstellt, dass sich der Anwendungsbereich nicht auf geschlossene Benutzergruppen oder Unternehmensnetze bezieht, sondern davon ausschliesslich öffentlich zugängliche elektronische Kommunikationsdienste in öffentlichen Kommunikationsnetzen erfasst werden. Zur Bedeutung von Art. 77 VO 883/2004 neben den Rechtsvorschriften der RL 95/46 *Spiegel*, in: Fuchs, Europäisches Sozialrecht, Art. 77 VO 883/2004, Rn. 4; *Wunder*, in: Schreiber/Wunder/Dern, Kommentar zur VO 883/2004, Art. 77, Rn. 7.

88 Vorschlag vom 25. Januar 2012 für eine Verordnung des Europäischen Parlaments und des Rates zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr (Datenschutz-Grundverordnung), KOM(2012) 11 endgültig; zu diesem Vorschlag etwa *Hornung*, ZD 2012, 100 ff.; *Kern*, digma 2013/01, 34 ff.; *Sydow/Kring*, ZD 2014, 271 ff.; *Körner*, ZESAR 2013, 99 ff., ZESAR 2013, 153 ff.

Denn die VO 45/2001 betrifft den Schutz der Daten, die durch die Organe und Einrichtungen der EU verarbeitet werden. Die Tatsache, dass die Schweiz diese Verordnung nicht übernommen hat, ist insofern nicht von Bedeutung, als sie für die Organe und Einrichtungen der EU innerhalb des Anwendungsbereiches ohnehin gilt.[89] Demgemäss sind diese Vorschriften bei der Datenverarbeitung im Rahmen des von der Europäischen Kommission betriebenen sTESTA-Netzwerkes, insbesondere bei den Bearbeitungen der Daten am Knotenpunkt, zu beachten, kommen jedoch für die hier im Vordergrund stehende Bearbeitung durch nationale Organe nicht zur Anwendung.[90]

Diese Regelungssystematik wirft die Frage auf, ob und ggf. inwieweit über die genannten sekundärrechtlichen Regelungen und ihre Verbindlichkeit für die Schweiz aufgrund des Personenfreizügigkeitsabkommens auch eine **Bindung der Schweiz** – soweit sie die Vorgaben der **VO 883/2004** und der **VO 987/2009** anwendet bzw. im nationalen Recht Massnahmen ergreift, die der **Durchführung dieser Rechtsakte** dienen (wie dies bei den nationalen Informationssystemen der Fall zu sein scheint) – an die **RL 95/46** und – darüber hinaus – an die hier einschlägigen **Unionsgrundrechte** (insbesondere Art. 8 Abs. 1 Grundrechtecharta) anzunehmen ist. Für einen EU-Mitgliedstaat ist diese Frage zweifellos zu bejahen: Die RL 95/46 ist durch die Mitgliedstaaten sowieso zu beachten, und die Unionsgrundrechte sind für die Mitgliedstaaten bei der Durchführung des Unionsrechts massgeblich (Art. 51 Abs. 1 GRCh), und eine solche Durchführungskonstellation liegt auf der Grundlage der Rechtsprechung des EuGH jedenfalls bei der Anwendung und Durchführung von EU-Recht vor.[91]

Eine entsprechende Bindung der Schweiz an die RL 95/46 sowie die Unionsgrundrechte könnte jedoch auf den ersten Blick fraglich sein: Denn einmal erklärt das FZA die RL 95/46 im Bereich der Sozialversicherungen nicht ausdrücklich für anwendbar bzw. massgeblich.[92] Zum anderen nimmt das Personenfreizügigkeitsabkommen auch keinen Bezug – in welcher Form auch immer – auf die EU-Grundrechte, dies trotz des Umstands, dass das Abkommen durchaus grundrechtsrelevante Bereiche berührt bzw. regelt, so dass die EU-Grundrechte also als solche keinen Anteil an dem unionsrechtlichen Besitzstand, der Eingang in das Abkommen gefunden hat, haben.[93]

Ohne dass diese Problematik hier im Einzelnen vertieft werden könnte, erscheint dieser Schluss jedoch der Tragweite der Übernahme von Teilen des unionsrechtlichen Besitzstands im Personenfreizügigkeitsabkommen und den Zielsetzungen des Abkommens nicht Rechnung zu tragen: Denn das Ziel des Abkommens besteht erklärtermassen (vgl. schon die Präambel)

89 *Epiney/Schleiss*, in: Belser/Epiney/Waldmann, Datenschutzrecht, § 4, Rn. 280.

90 Der Europäische Datenschutzbeauftragte kommt in diesem Zusammenhang zum Schluss, die Anforderungen der VO 45/2001 seien grundsätzlich erfüllt, vgl. Europäische Datenschutzbeauftragter, Stellungnahme zu einer Meldung des Datenschutzbeauftragten der Europäischen Kommission für eine Vorabkontrolle des Systems zum Elektronischen Austausch von Sozialversicherungsdaten („EESSI") vom 28.7.2011 (Fall 2011-0016).

91 Vgl. EuGH, Rs. C-617/10 (Aklagaren/Akerberg Fransson), Urt. v. 26.2.2013; diese Rechtsprechung bestätigend EuGH, Rs. C-176/12 (Association de médiation sociale), Urt. v. 15.1.2014; EuGH, Rs. C-206/13 (Siragusa), Urt. v. 6.3.2014; EuGH, Rs. C-265/13 (Torralbo Marcos), Urt. v. 27.3.2014; EuGH, Rs. C-390/12 (Pfleger), Urt. v. 30.4.2014. Zur Problematik, m.w.N., *Epiney*, CDE 2014, 283 ff.

92 Vgl. Anhang II FZA, Abschnitt A.

93 Vgl. in diesem Zusammenhang die Zusammenstellung der verschiedenen Mechanismen der „Übernahme" von EU-Recht in die Bilateralen Abkommen bei *Epiney/Metz/Pirker*, Parallelität der Rechtsentwicklung, 140 ff.

darin, im Verhältnis zur Schweiz in den durch das Abkommen erfassten Bereichen eine parallele Rechtslage herzustellen. Auch wenn der genaue Umfang des „übernommenen" unionsrechtlichen Besitzstandes damit noch nicht abschliessend geklärt ist, dürfte jedenfalls in denjenigen Bereichen, in denen das Abkommen – wie auf dem Gebiet der Sozialversicherungen – direkt auf EU-Sekundärrecht verweist und dieses für massgeblich erklärt, die Übernahme des unionsrechtlichen Besitzstandes kaum zu bezweifeln sein, so dass die erwähnte Zielsetzung vollumfänglich zum Zuge kommt.[94] Damit sind diese Rechtsakte aber im Rahmen des Abkommens grundsätzlich parallel wie im Unionsrecht auszulegen, kann doch nur auf diese Weise der erwähnten Zielsetzung des Abkommens Rechnung getragen werden, ein Ansatz, für den gerade im Bereich des Personenfreizügigkeitsabkommens noch Art. 16 Abs. 2 sowie die bereits erwähnte Präambel angeführt werden können.[95] Im Übrigen geht auch das Bundesgericht in ständiger Rechtsprechung von einem solchen Grundsatz der parallelen Auslegung aus.[96]

Eine solche Parallelität kann jedoch nur erreicht werden, wenn die unionsrechtlichen Auslegungsgrundsätze als solche (allerdings aus methodischer Sicht aufgrund einer völkerrechtlichen Auslegung des Personenfreizügigkeitsabkommens) auch im Rahmen des Abkommens herangezogen werden, was eine Berücksichtigung der im übernommenen unionsrechtlichen Besitzstand enthaltenen (expliziten oder impliziten) „Verweise" nach sich zieht bzw. ziehen muss. Denn die genaue Tragweite der relevanten unionsrechtlichen Vorgaben bzw. Begriffe und Konzepte ist im Unionsrecht eben auch – nach den einschlägigen unionsrechtlichen Grundsätzen – unter Berücksichtigung der EU-Grundrechte sowie sonstiger Verweise (hier auf die RL 95/46) zu bestimmen, so dass diese insoweit Teil der unionsrechtlichen Begriffe sind, auf die im Abkommen zurückgegriffen wird. Dann führt der Grundsatz der parallelen Auslegung zum Schluss, dass auch die für die Auslegung des übernommenen Besitzstands relevanten Aspekte des Unionsrechts zu berücksichtigen sind. Es ist kein Grund ersichtlich, hiervon insoweit eine Ausnahme zu machen, als die RL 95/46 und die EU-Grundrechte betroffen sind. Insbesondere sind die hier im Vordergrund stehenden Erwägungen der Zielsetzung des Abkommens (Sicherstellung einer parallelen Rechtslage in Bezug zur Schweiz wie innerhalb der EU) allgemein einschlägig und implizieren auch und gerade die Relevanz der EU-Grundrechte sowie – im vorliegenden Zusammenhang – der RL 95/46, könnte eine solche Parallelität doch ansonsten nicht sichergestellt werden.[97]

---

94 Vgl. ausführlich insoweit bereits *Epiney/Metz/Pirker*, Parallelität der Rechtsentwicklung, 142 ff., 157 ff., m.w.N.

95 Im Einzelnen, mit ausführlicher Begründung und Herleitung, *Epiney/Metz/Pirker*, Parallelität der Rechtsentwicklung, 191 ff.

96 Grundlegend BGE 136 II 5; s. sodann insbesondere BGE 140 II 112.

97 Vgl. im Einzelnem zu diesem Ansatz in Bezug auf die EU-Grundrechte *Epiney*, FS Europarat, 141 ff.; *Oesch*, ZBl 2014, 171 ff.

Damit kommt es letztlich auch nicht darauf an, wie der Verweis auf die RL 95/46 in der Schengen/Dublin-Assoziierung[98] zu verstehen ist, ist hier doch einiges streitig, wobei in erster Linie auf die Frage nach der genauen Reichweite der Bindungswirkung der RL 95/46 für die Schweiz (lediglich für die von der Schengen-/Dublin-Assoziierung erfasste Bereiche oder allgemeine Verbindlichkeit, ähnlich wie für einen EU-Mitgliedstaat)[99] und die Frage, ob auch die geplante Datenschutzgrundverordnung[100] Teil des Schengen- und Dublinbesitzstands sein soll (was auf EU-Ebene offenbar noch nicht abschliessend geklärt ist), hinzuweisen ist.

3. Fazit

Im Ergebnis ist damit festzuhalten, dass sowohl für die **innerstaatliche Durchführung der Vorgaben der VO 883/2004 und der VO 987/2009** (im Rahmen der Verwirklichung des EESSI) als auch in Bezug auf (rein) **nationale Massnahmen im Hinblick auf die Durchführung dieser Verordnungen** ein **doppelter Standard** anzuwenden ist:

- Erstens ist umfassend das **nationale Recht** heranzuziehen, wobei es im vorliegenden Zusammenhang in erster Linie um die datenschutzrechtlichen Vorgaben geht; hinzu kommt der verfassungsrechtlich und menschenrechtlich verankerte Persönlichkeitsschutz, wobei diese Vorgaben aber durch das Datenschutzgesetz des Bundes (das allein, da Bundesorgane im Sinne des Gesetzes tätig werden, massgeblich ist) konkretisiert werden.
- Zweitens sind im Rahmen der **Anwendung der VO 883/2004 und der VO 987/2009** durch die Schweiz und deren Durchführungen nicht nur die „direkt" in diesen Rechtsakten verankerten, sondern auch diejenigen Vorgaben, auf die diese (explizit oder implizit) verweisen, zu beachten, was insbesondere für die **datenschutzrechtlichen Vorgaben** sowie die **Unionsgrundrechte** relevant ist.

Bei Einrichtung und Betrieb der für den elektronischen Datenaustausch im Rahmen der Anwendung des Koordinationsrechts im Bereich der Sozialversicherung notwendigen Informationssysteme ist somit – soweit die nationale Ebene betroffen ist – einerseits die **Effektivität der unionsrechtlichen Vorgaben** zu beachten, so dass die Informationssysteme so auszugestalten sind, dass der Austausch gemäss der Vorgaben des Sekundärrechts erfolgen kann. Andererseits sind hierbei aber auch die **datenschutzrechtlichen Vorgaben** (auf nationaler und unionsrechtlicher Ebene) zu beachten, so dass das „Wie" dieser Durchführung im Rahmen der durch diese gezogenen Grenzen erfolgen muss.

Auch wenn diese „Doppelspurigkeit" (durch die Massgeblichkeit sowohl des nationalen Rechts als auch des EU-Rechts in Bezug auf die datenschutzrechtlichen Vorgaben) auf den

---

98 Abkommen vom 26. Oktober 2004 zwischen der Schweizerischen Eidgenossenschaft, der Europäischen Union und der Europäischen Gemeinschaft über die Assoziierung dieses Staates bei der Umsetzung, Anwendung und Entwicklung des Schengen-Besitzstands (SAA), SR 0.362.31.

99 Vgl. für die zuletzt genannte Ansicht *Epiney*, SJZ 2006, 121 (122 ff.); a.A. *Brunner*, in: Revision des Datenschutzgesetzes, 139 (140 ff.); *Rudin/Baeriswyl*, in: Datenschutz in Europa und die Schweiz, 169 (175 f.); s. auch Botschaft zur Genehmigung der bilateralen Abkommen zwischen der Schweiz und der Europäischen Union, einschliesslich der Erlasse zur Umsetzung der Abkommen („Bilaterale II"), BBl 2004 5965, 6175; *Epiney/Schleiss*, in: Belser/Epiney/Waldmann, Datenschutzrecht, § 4, Rn. 279.

100 Vgl. Fn. 88.

ersten Blick die Gefahr mit sich bringen könnte, dass die im **nationalen Recht und im EU-Recht verankerten datenschutzrechtlichen Vorgaben** differieren, ist gleichwohl festzuhalten, dass die hier **massgeblichen Grundsätze letztlich parallel** ausgestaltet sind, so dass jedenfalls im Rahmen ihrer Anwendung und Auslegung im hier relevanten Bereich von einer Konvergenz dieser Anforderungen auszugehen ist: Denn sowohl das Unionsrecht als auch das schweizerische Recht im Bereich des Datenschutzes haben als Ausgangspunkt das sich bereits aus Art. 8 EMRK ergebende Recht auf Achtung der Persönlichkeit, und jedenfalls die datenschutzrechtlichen Grundsätze im Allgemeinen sowie das Erfordernis der gesetzlichen Grundlage im Besonderen dürften sich insoweit bereits aus diesen Vorgaben ergeben.[101] Insoweit besteht also eine weitgehende Konvergenz zwischen den Anforderungen des Unionsrechts und des nationalen Rechts, zumal diese im Sinn einer völkerrechtskonformen Auslegung auch beide im Lichte der EMRK auszulegen sind.

Aber auch darüber hinaus sind weitgehende Konvergenzen zwischen der RL 95/46 und dem Datenschutzgesetz des Bundes zu verzeichnen, so dass dieses im Wesentlichen unionsrechtskonform sein dürfte, auch wenn in einzelnen Punkten durchaus gewisse Divergenzen bestehen.[102] Allerdings könnten sich im Zuge des Erlasses der Datenschutzgrundverordnung weitere Divergenzen ergeben.[103]

II. Allgemeine datenschutzrechtliche Grundsätze

Im Folgenden sollen – als Grundlage für die weiteren Ausführungen – die bei jeder Datenbearbeitung durch öffentliche Organe des Bundes zu beachtenden (allgemeinen) **datenschutzrechtlichen Grundsätze** skizziert werden. Dies erfolgt in Anknüpfung an die entsprechenden Regelungen im **Datenschutzgesetz** des Bundes, wobei nach dem Gesagten[104] dem **Unionsrecht im Ergebnis parallele Anforderungen** zu entnehmen sind.

Im Übrigen ist daran zu erinnern, dass diese Grundsätze auch der Datenschutzkonvention des Europarats zu entnehmen sind und sich (jedenfalls weitgehend) auch aus Art. 8 EMRK ergeben.[105]

Dabei sollen im Folgenden diejenigen Grundsätze heraus gegriffen werden, die im Zusammenhang mit dem Betrieb von Informationssystemen (besonders) relevant sind, und im Übrigen wird dem Erfordernis der **gesetzlichen Grundlage** besondere Beachtung geschenkt.

Dabei ergeben sich diese allgemeinen datenschutzrechtlichen Grundsätze letztlich bereits aus den völker- und verfassungsrechtlichen Vorgaben, so dass sie durch spezialgesetzliche Vorgaben lediglich präzisiert und weiterentwickelt, jedoch nicht relativiert, werden dürfen. Insofern sind die allgemeinen bereichsübergreifenden daten-

101 S. insoweit im Einzelnen *Epiney/Schleiss*, in: Belser/Epiney/Waldmann, Datenschutzrecht, § 4, Rn. 9 ff.

102 Vgl. hierzu schon *Epiney/Hofstötter/Meier/Theuerkauf*, Schweizerisches Danteschutzrecht vor europa- und völkerrechtliche Herausforderungen, insbesondere 276 ff.

103 Hierzu *Kern*, digma 2013/01, 34 ff.; s. auch *Kern/Epiney*, in: Durchsetzung der Rechte der Betroffenen im Bereich des Datenschutzes, 19 ff.

104 Vgl. C.I., insbesondere C.I.3.

105 Vgl. schon oben C.I., am Anfang. S. sodann *Epiney/Schleiss*, in: Belser/Epiney/Waldmann, Datenschutzrecht, § 3, Rn. 9 ff., Rn. 20 ff.

schutzrechtlichen Grundsätze grundsätzlich subsidiär heranzuziehen.[106] Darüber hinaus sind die allgemeinen datenschutzrechtlichen Grundsätze auch bei der Auslegung und Anwendung der jeweils zu beachtenden besonderen Vorgaben – insbesondere der gesetzlichen Grundlagen – zu beachten.

1. Zum Grundsatz der Rechtmässigkeit und dem Erfordernis der gesetzlichen Grundlage

Im Sinne des **Grundsatzes der Rechtmässigkeit**, wie er in **Art. 4 Abs. 1 DSG** verankert ist,[107] dürfen Personendaten nur in rechtmässiger Weise bearbeitet werden. Eine rechtswidrige Datenbearbeitung liegt dabei immer vor, wenn sie einer in der Schweiz rechtlich verbindlichen Norm widerspricht.[108]

Art. 17 DSG präzisiert den in Art. 4 Abs. 1 DSG enthaltenen Grundsatz der Rechtmässigkeit für **Bundesorgane** dergestalt, dass sie Personendaten – unabhängig von Verfahren und eingesetzten Mitteln (Art. 3 lit. e DSG) und unabhängig von der Art der bearbeiteten Daten (Art. 3 lit. a-d DSG) – nur dann bearbeiten dürfen, wenn hierfür eine **gesetzliche Grundlage** besteht.[109] M.a.W. genügt es für die Rechtmässigkeit einer solchen Bearbeitung gerade nicht, dass ihr keine Rechtsnormen entgegenstehen, sondern die Bearbeitung muss vielmehr (grundsätzlich) ausdrücklich in einem Gesetz vorgesehen sein. Damit darf eine Datenbearbeitung durch Bundesorgane in der Regel nur erfolgen, wenn sie auf einer bereichsspezifischen gesetzlichen Grundlage beruht (Prinzip der Spezialermächtigung).[110] Daher können sich Bundesorgane grundsätzlich nicht auf das Datenschutzgesetz als Rechtsgrundlage für eine Datenbearbeitung stützen, sondern für das Bearbeiten von Personendaten bedarf es einer bereichsspezifischen Rechtsgrundlage. Nur ausnahmsweise können sich Bundesorgane direkt auf das DSG berufen (vgl. Art. 17a, Art. 19, Art. 22 DSG). Fehlt eine solche Rechtsgrundlage und ist keine Ausnahmeregelung des DSG anwendbar, ist das Bearbeiten von Personendaten widerrechtlich,[111] so dass grundsätzlich sämtliche Formen und Phasen der Datenbearbeitung auf einer Rechtsgrundlage beruhen müssen.[112]

Insofern unterscheiden sich die Anforderungen an die Rechtmässigkeit je nachdem, ob es sich beim Datenbearbeiter um ein öffentliches Organ oder um eine **Privatperson** handelt: Während Privatpersonen zu sämtlichen Bearbeitungen befugt sind, solange sie nicht gegen eine verbindliche Rechtsnorm – insbesondere Art. 28 ZGB –

106 S. schon *Epiney/Schleiss*, in: Belser/Epiney/Waldmann, Datenschutzrecht, § 9, Rn. 7 ff., mit weiteren Hinweisen (insbesondere auch auf die hier nicht ganz klare Judikatur).

107 Siehe auch den entsprechenden Art. 5 lit. a DSK, wonach personenbezogene Daten hinsichtlich automatisierter Bearbeitungen, auf rechtmässige Weise beschafft sein und bearbeitet werden müssen.

108 *Epiney*, in: Belser/Epiney/Waldmann, Datenschutzrecht, § 9, Rn. 11 ff.

109 Ausführlich zum Erfordernis einer gesetzlichen Grundlage für Bundesorgane *Waldmann/Bickel*, in: Belser/Epiney/Waldmann, Datenschutzrecht, § 12, Rn. 40 ff.; s. auch schon *Epiney/Civitella/Zbinden*, Datenschutzrecht in der Schweiz, 39 ff. (worauf die folgenden Ausführungen teilweise beruhen).

110 *Jöhri*, in: Rosenthal/Jöhri, Handkommentar DSG, Art. 17, Rn. 4.

111 *Epiney/Civitella/Zbinden*, Datenschutzrecht in der Schweiz, 40.

112 *Jöhri*, in: Rosenthal/Jöhri, Handkommentar DSG, Art. 17, Rn. 2.

verstossen (wobei darüber hinaus die Vorgaben der Art. 12 ff. DSG zu beachten sind), dürfen Bundesorgane Daten grundsätzlich nur dann bearbeiten, wenn eine gesetzliche Norm sie dazu ermächtigt.[113]

Auch die **Beschaffung von Personendaten** – nach Art. 3 lit. e DSG ein Unterfall der Bearbeitung – durch Bundesorgane setzt eine gesetzliche Grundlage voraus. Liegt eine systematische Erhebung von Personendaten vor – d.h. werden Daten methodisch, organisiert und strukturiert erfasst – so ist die betroffene Person gemäss **Art. 18 DSG** zudem über den Bearbeitungszweck, die gesetzliche Grundlage und die Kategorien der an der Datensammlung Beteiligten und der Datenempfänger zu informieren. Davon zu unterscheiden ist die **Bekanntgabe**[114] von Personendaten, die gemäss Art. 3 lit. f DSG das Zugänglichmachen von Personendaten wie das Einsichtgewähren, Weitergeben oder Veröffentlichen umfasst. Nach Art. 19 Abs. 1 DSG setzt auch die Bekanntgabe durch Bundesorgane eine bereichsspezifische Rechtsgrundlage voraus, wobei die gesetzliche Grundlage explizit und spezifisch die Datenbekanntgabe betreffen muss.[115]

Mit **gesetzlicher Grundlage i.S.v. Art. 17 Abs. 1 DSG** ist ein **Gesetz im materiellen Sinn** gemeint. Vorausgesetzt ist demnach eine generell-abstrakte Norm, sei es eine Verfassungsbestimmung, eine Gesetzes- oder eine Verordnungsnorm.[116] Aber auch völkerrechtliche Bestimmungen können – im Zuge der von der Bundesverfassung zugrunde gelegten monistischen Konzeption des Verhältnisses von Völkerrecht und Landesrecht[117] – gesetzliche Grundlagen darstellen. Daher kann eine Datenbearbeitung durch Bundesorgane auch auf Bestimmungen der VO 883/2004 und der VO 987/2009 gestützt werden, wobei selbstredend jeweils zu ermitteln ist, ob die in Betracht kommende Vorschrift die geplante Datenbearbeitung auch wirklich erfasst.[118]

Normen, die als gesetzliche Grundlage dienen sollen, müssen nicht nur hinsichtlich der **Form**, sondern auch hinsichtlich ihrer **Normdichte** gewissen Anforderungen genügen. So ist die gesetzliche Grundlage hinreichend klar, bestimmt und umfassend zu fassen.[119] Daher müssen in der gesetzlichen Grundlage zumindest folgende Aspekte hinreichend klar und genügend detailliert geregelt sein:[120]

- Bearbeitungszweck;
- Art und Ausmass der Datenbearbeitung;
- beteiligte Behörden bzw. Personen (datenbearbeitende Stellen, zugangsberechtigte Stellen u.a.m.);
- betroffene Datenkategorien.

---

113 *Epiney*, in: Belser/Epiney/Waldmann, Datenschutzrecht, § 9, Rn. 11.

114 Gemäss Art. 3 lit. e DSG wird aber auch die Bekanntgabe unter die Bearbeitung subsumiert.

115 *Waldmann/Bickel*, in: Belser/Epiney/Waldmann, Datenschutzrecht, § 12, Rn. 89; *Epiney/Civitella/Zbinden*, Datenschutzrecht in der Schweiz, 47.

116 Botschaft DSG, BBl 1988 II 467; *Epiney/Civitella/Zbinden*, Datenschutzrecht in der Schweiz, 40.

117 Vgl. aus der Rechtsprechung aus jüngerer Zeit, m.w.N., BGE 139 I 16 E. 4.3.

118 S. in diesem Zusammenhang noch die Ausführungen unten D.

119 *Belser*, in: Belser/Epiney/Waldmann, Datenschutzrecht, § 6, Rn. 125.

120 11. Tätigkeitsbericht des EDSB, 13; *Epiney/Civitella/Zbinden*, Datenschutzrecht in der Schweiz, 40; *Epiney/Fasnacht*, Jusletter v. 24.2.2014, Rn. 26.

Zudem kann aus dem Rechtsmässigkeitsprinzip abgeleitet werden, dass die **Anforderungen an die Bestimmtheit einer Rechtsgrundlage** mit der Intensität der Datenbearbeitung und einer **erhöhten Gefahr für Persönlichkeitsverletzungen steigen**. Demzufolge ist eine gesetzliche Grundlage für breit zugängliche Daten, die in einem hohen Ausmass bearbeitet werden, sehr präzise und bestimmt zu formulieren.[121] Im Einzelfall hängt der Grad der Bestimmtheit einer Norm von den konkreten Umständen und damit vom Ausmass der Grundrechtseinschränkung, der Art der bearbeiteten Daten, dem Kreis der betroffenen Personen und Organe sowie der Komplexität der zu treffenden Entscheidung ab.[122]

Darüber hinaus verlangt **Art. 36 Abs. 1 S. 2 BV**, dass **schwerwiegende Einschränkungen von Grundrechten** – wie beispielsweise des Rechts auf informationelle Selbstbestimmung i.S.v. Art. 13 BV – in einem **Gesetz im formellen Sinn** vorgesehen werden müssen.[123] Diese Vorgabe wird auf bundesrechtlicher Ebene durch **Art. 17 Abs. 2 DSG** präzisiert. Gemäss dieser Bestimmung dürfen besonders schützenswerte Personendaten sowie Persönlichkeitsprofile durch Bundesorgane grundsätzlich nur bearbeitet werden, wenn sie dazu durch ein Gesetz im formellen Sinn ausdrücklich ermächtigt werden. Ferner setzt das DSG auch für die Bekanntgabe von besonders schützenswerten Personendaten sowie Persönlichkeitsprofilen durch Bundesorgane eine formell-gesetzliche Grundlage voraus (Art. 19 Abs. 1 i.V.m. Art. 17 Abs. 2 DSG); werden besonders schützenswerte Daten über ein **Abrufverfahren** zugänglich gemacht, ist auch dies ausdrücklich gesetzlich vorzusehen (Art. 19 Abs. 3 DSG).

Dass je nach Art des Eingriffes unterschiedlich hohe Anforderungen an die Qualität der gesetzlichen Grundlage zu stellen sind, ergibt sich im Übrigen auch aus **Art. 8 EMRK**, so wie diese Bestimmung in ständiger Rechtsprechung ausgelegt wird.[124] Dies impliziert auch, dass an die normative Dichte der gesetzlichen Grundlage gerade bei besonders schützenswerten Personendaten höhere Anforderungen zu stellen sind.

Im Übrigen und ergänzend ist darauf hinzuweisen, dass **Art. 36 Abs. 1 S. 2 BV** insofern weiter als das Datenschutzgesetz geht, als davon jede schwerwiegende Grundrechtseinschränkung erfasst wird, wohingegen sich Art. 17 Abs. 2 DSG nur auf besonders schützenswerte Personendaten sowie Persönlichkeitsprofile bezieht. So setzt Art. 36 Abs. 1 S. 2 BV eine Rechtsgrundlage in einem Gesetz im formellen Sinn auch dann voraus, wenn beispielsweise die Form der Datenbeschaffung – und nicht die Kategorie der Daten – in einem besonders schweren Eingriff in die Persönlichkeitsrechte resultiert (z.B. bei einer geheimen Überwachung).[125]

Vor diesem Hintergrund sind die im **Datenschutzgesetz formulierten qualifizierten Anforderungen an die gesetzliche Grundlage** bei bestimmten Datenbearbeitungen im Ergebnis **verfassungsrechtlicher Natur**; sie präzisieren m.a.W. die sich bereits aus Art. 13, 36 BV sowie Art. 8 EMRK ergebenden Vorgaben. Insofern kann gegen ihre Massgeblichkeit im Rahmen des Erlasses anderer Bundesgesetze auch nicht geltend gemacht werden, das Datenschutzgesetz sei kein „Supergesetz", dem Vorrang gegenüber anderen Gesetzen zukomme;[126] vielmehr geht es in diesem Zusammenhang um die Beachtung verfassungs- und menschenrechtlicher Anforderungen.

Wie bereits erwähnt, kennt das Datenschutzgesetz für durch Bundesorgane erfolgende Datenbearbeitungen **Ausnahmen vom Prinzip des Erfordernisses einer gesetzlichen Grundlage**:

---

121 *Epiney/Fasnacht*, Jusletter v. 24.2.2014, Rn. 22, 23, 26, 27.

122 Botschaft DSG, BBl 1988 II 467; *Epiney/Civitella/Zbinden*, Datenschutzrecht in der Schweiz, 40; *Waldmann/Bickel*, in: Belser/Epiney/Waldmann, Datenschutzrecht, § 12, Rn. 45.

123 *Epiney/Civitella/Zbinden*, Datenschutzrecht in der Schweiz, 40.

124 Vgl. zur angesprochenen EGMR-Rechtsprechung *Epiney/Schleiss*, in: Belser/Epiney/Waldmann, Datenschutzrecht, § 3, Rn. 17, m.w.N.

125 *Epiney/Civitella/Zbinden*, Datenschutzrecht in der Schweiz, 40.

126 Missverständlich insoweit *Gächter/Egli*, Jusletter v. 6.9.2010, Rn. 270 ff. S. hierzu bereits schon *Epiney*, in: Belser/Epiney/Waldmann, Datenschutzrecht, § 9, Rn. 7 ff., m.w.N.

- Neben der Vorgabe einer formell-gesetzlichen Grundlage enthält **Art. 17 Abs. 2 DSG** gleichzeitig eine **abschliessende Aufzählung** von Fallgestaltungen, in denen Daten auch ohne gesetzliche Grundlage bearbeitet werden dürfen.[127] Von besonderer Bedeutung sind hier Fälle, in denen die Datenbearbeitung zur Erfüllung einer in einem Gesetz im formellen Sinn klar umschriebenen Aufgabe „unentbehrlich" ist (lit. a) oder in denen die betroffene Person im Einzelfall in die Datenbearbeitung eingewilligt hat (lit. c).
- Indem **Art. 17a DSG** dem Bundesrat ermöglicht, automatisierte Bearbeitungen von besonders schützenswerten Personendaten oder Persönlichkeitsprofilen unter gewissen Voraussetzungen vor Inkrafttreten einer formell-gesetzlichen Rechtsgrundlage zu bewilligen, stellt auch dieser Artikel eine Ausnahme vom Erfordernis einer gesetzlichen Grundlage dar. Art. 17a DSG kommt insbesondere dann zum Zug, wenn neue Informatiksysteme, worunter auch die hier im Vordergrund stehenden Informationssysteme fallen, in **Pilotversuchen** geprüft werden.[128]

  Art. 17a Abs. 1 DSG nennt in diesem Zusammenhang die Voraussetzungen, die für die automatisierte Datenbearbeitung im Rahmen von Pilotversuchen gegeben sein müssen, damit (vorübergehend) auf eine gesetzliche Grundlage verzichtet werden kann:
  - Die Aufgaben, die die Datenbearbeitung erforderlich machen, müssen in einem Gesetz im formellen Sinn geregelt sein.
  - Es müssen ausreichende Massnahmen zur Verhinderung von Persönlichkeitsverletzungen getroffen werden.
  - Die praktische Umsetzung einer Datenbearbeitung muss eine Testphase vor dem Inkrafttreten des Gesetzes im formellen Sinn zwingend erfordern. Dieser Punkt wird in Art. 17a Abs. 2 DSG durch eine beispielhafte Aufzählung präzisiert. So kann eine derartige zwingende Erforderlichkeit einer solchen Testphase gegeben sein, wenn die Erfüllung der Aufgabe technische Neuerungen oder bedeutende organisatorische oder technische Massnahmen erfordert, deren Auswirkungen zunächst evaluiert werden müssen.

  Die Modalitäten der automatisierten Datenbearbeitung sind diesfalls in einer Verordnung des Bundesrates zu regeln (Art. 17a Abs. 3 DSG), wobei der Bundesrat vor Erteilung der Bewilligung eine Stellungnahme des Datenschutzbeauftragten einholen muss (Art. 17a Abs. 1 DSG). Nach zwei Jahren ist ein Evaluationsbericht vorzulegen (Art. 17a Abs. 4 DSG), und die automatisierte Datenbearbeitung muss in jedem Fall abgebrochen werden, wenn innert fünf Jahren keine ausreichende Rechtsgrundlage in Kraft getreten ist (Art. 17a Abs. 5 DSG).
  Ohne an dieser Stelle im Detail zu prüfen, ob die Voraussetzungen des Art. 17a DSG in Bezug auf die hier im Vordergrund stehenden Informationssysteme vorliegen, könnte dies *a priori* grundsätzlich durchaus zu bejahen sein. In jedem Fall ist bzw. wäre aber eine bundesrätliche Verordnung notwendig.

- Bezüglich der (eine spezifische Form der Datenbearbeitung darstellenden) **Datenbekanntgabe** durch Bundesorgane enthält **Art. 19 Abs. 1 DSG** eine spezifische Regelung, der angesichts des im Vergleich zu einer rein „amtsinternen" Datenbearbeitung grundsätzlich gesteigerten Risikopotentials der Datenbekanntgabe teilweise – im Verhältnis zu Art. 17 DSG – **höhere Anforderungen an die gesetzliche Grundlage** bzw. die zulässigen Ausnahmekonstellationen zu entnehmen sind. Der Anwendungsbereich

---

127 *Jöhri*, in: Rosenthal/Jöhri, Handkommentar DSG, Art. 17, Rn. 75. Im Sinne des Grundsatzes *ad maiore minus* bezieht sich Art. 17 Abs. 2 DSG nicht nur auf die Bearbeitung besonders schützenswerter Personendaten oder von Persönlichkeitsprofilen, sondern auch auf die Bearbeitung „normaler" Personendaten.

128 BBl 2003 2142; *Jöhri*, in: Rosenthal/Jöhri, Handkommentar DSG, Art.17a, Rn. 4.

der Vorschrift erstreckt sich sowohl auf den Datenaustausch zwischen Bundesorganen untereinander als auch auf die Weitergabe an kantonale oder ausländische Behörden sowie an Private.[129] In unserem Zusammenhang ist von besonderer Bedeutung, dass sich die gesetzliche Grundlage ausdrücklich auf die Datenbekanntgabe beziehen muss und das **Surrogat** für eine gesetzliche Grundlage in Art. 19 Abs. 1 lit. a DSG von vornherein nur dann zu greifen vermag, wenn die Datenbekanntgabe im **Einzelfall** zur Erfüllung einer gesetzlichen Aufgabe unentbehrlich ist.[130]

Art. 19 Abs. 1 lit. a DSG (die bekannt zu gebenden Daten sind für den Empfänger im Einzelfall zur Erfüllung einer gesetzlichen Aufgabe unentbehrlich) betrifft die Konstellation, dass der Empfänger seine gesetzliche Aufgabe ohne die Datenbekanntgabe letztlich nicht erfüllen könnte. Umfassende bzw. systematische Datenbekanntgaben bei Vorliegen typisierter und nach allgemein-abstrakten Kriterien bestimmten Voraussetzungen können angesichts des Abstellens dieser Vorschrift auf den „Einzelfall" von vornherein nicht von diesem Surrogat erfasst werden und sind damit nur gestützt auf eine ausdrückliche gesetzliche Grundlage zulässig.

- Werden **Personendaten für nicht personenbezogene Zwecke**, wie Forschung, Planung und Statistik bearbeitet, so gelten gemäss **Art. 22 DSG** ebenfalls erleichterte Anforderungen an die gesetzliche Grundlage.

Abgesehen vom erwähnten Pilotversuch ist vor diesem Hintergrund davon auszugehen, dass die **Inbetriebnahme von Informationssystemen wie die in Frage stehenden grundsätzlich einer gesetzlichen Grundlage** bedarf. Die möglicherweise in Betracht kommenden Ausnahmen vermögen nämlich im Ergebnis in aller Regel nicht zu greifen:

- Eine möglicherweise vorliegende **Einwilligung** (Art. 17 Abs. 2 lit. c, Art. 19 Abs. 1 lit. b DSG) kann eine gesetzliche Grundlage jedenfalls nicht ersetzen, da nicht davon auszugehen ist, dass die Einwilligung „im Einzelfall" erfolgt: Denn die Einwilligung müsste – insbesondere soweit es um automatisierte Übermittlungen ins Ausland über das EESSI geht – im Voraus erfolgen, so dass sie sich von vornherein gar nicht auf alle, möglicherweise in Zukunft zu erwartenden Datenbearbeitungen beziehen kann. Eine Einwilligung im Einzelfall dürfte nämlich nur anzunehmen sein, wenn sich die Einwilligung auf eine bestimmte Datenbearbeitung in einer bestimmten Konstellation zu einem bestimmten Zeitpunkt bezieht. Damit erscheint eine Einwilligung im Einzelfall bei der Einrichtung von Informationssystemen grundsätzlich ausgeschlossen, implizieren diese doch eine systematische Datenbearbeitung (z.B. durch einen regelmässigen Rückgriff auf die Daten durch die Berechtigten).[131] Im Übrigen wird gerade bei Informationssystemen in der Regel schon eine ausreichende Information – eine Einwilligung ist von vornherein nur auf der Grundlage einer angemessenen Information gültig – zu verneinen sein, denn die Betroffenen dürften in den wenigsten Fällen um-

129 *Epiney/Civitella/Zbinden*, Datenschutzrecht, 47.

130 Im Übrigen unterscheidet Art. 19 DSG nicht zwischen verschiedenen Kategorien von Daten, vgl. in diesem Zusammenhang *Waldmann/Bickel*, in: Belser/Epiney/Waldmann, Datenschutzrecht, § 12, Rn. 90; *Jöhri*, in: Rosenthal/Jöhri, Handkommentar DSG, Art. 19, Rn. 19.

131 Vgl. schon, m.w.N., *Epiney/Schleiss*, Jusletter v. 7.11.2011, insb. Rn. 26.

fassend über die Art der Datenbank, die genau dort enthaltenen Daten, die Art und Weise der Datenflüsse sowie die Zugriffsberechtigten informiert sein. Zudem erscheint es in all denjenigen Konstellationen, in denen kontextunabhängig durch die Berechtigten auf die Daten zugegriffen werden kann, grundsätzlich nicht möglich, im Vorfeld „ausdrücklich" jedem Zugriff zuzustimmen, sind diese Zugriffe doch mitunter nicht vorhersehbar. Eine angemessene Information erscheint also bei Informationssystemen in aller Regel schwierig bis unmöglich, so dass auch eine Zustimmung zu den entsprechenden Datenbearbeitungen nicht möglich ist. Weiter könnte gerade im Zusammenhang mit Datenbearbeitungen, die im Hinblick auf die Zusprechung staatlicher Sozialversicherungsleistungen erfolgen, auch zweifelhaft sein, ob eine allfällige Einwilligung wirklich aus freiem Willen erfolgt, dies zumindest dann, wenn die Leistungsgewährung erst im Anschluss an eine derartige Datenbearbeitung erfolgt oder erfolgen kann.[132]

- Aber auch die **„Unentbehrlichkeit" der Datenbearbeitung zur Erfüllung einer in einem Gesetz klar umschriebenen Aufgabe** dürfte im Fall der Einrichtung von Informationssystemen als solchen grundsätzlich nicht zum Zuge kommen können bzw. wird häufig zweifelhaft sein: Zwar könnte im vorliegenden Zusammenhang eine Datenbearbeitung im Hinblick auf die Sicherstellung der Koordinierung der Systeme sozialer Sicherheit auf den ersten Blick möglicherweise durch dieses Surrogat einer gesetzlichen Grundlage erfasst sein. Es ist jedoch zu beachten, dass es für die Bejahung der Unentbehrlichkeit der Datenbearbeitung für die Erfüllung einer gesetzlich umschriebenen Aufgabe jedenfalls nicht ausreichend ist, dass die Datenbearbeitung im Hinblick auf die Erfüllung der gesetzlichen Aufgabe hilfreich ist oder dieser (nur) dient, sondern die Erfüllung der gesetzlichen Aufgabe darf ohne die Bearbeitung der besonders schützenswerten Personendaten nicht möglich sein. M.a.W. würde die Erfüllung der Aufgabe ohne die fragliche Datenbearbeitung geradezu vereitelt,[133] so dass es nicht genügt, dass die Datenbearbeitung die Wahrnehmung der gesetzlichen Aufgabe erleichterte oder effizienter gestaltete.[134] Insofern dürfte diese Anforderung über die „normalen" Vorgaben der Verhältnismässigkeit und Zweckmässigkeit hinausgehen.[135] Selbst wenn man diese Voraussetzung in Bezug auf bestimmte Datenbearbeitungen im Hinblick auf die Sicherstellung der Koordinierung der Systeme sozialer Sicherheit bejahen könnte, ist doch darüber hinaus zu beachten, dass sich die skizzierte Anforderung nicht nur auf den Grundsatz der Bearbeitung der betroffenen, möglicherweise gar besonders schützenswerten Personendaten, sondern auch auf die genaue Ausgestaltung derselben (Umfang der Datenbearbeitung, Ausgestaltung des Zugangs

132 Vgl. zum Ganzen schon *Epiney*, FS Steinauer, 97 (102 ff.).

133 Vgl. *Jöhri*, in: Rosenthal/Jöhri, Handkommentar DSG, Art. 17, Rn. 77; *Waldmann/Bickel*, in: Belser/Epiney/Waldmann, Datenschutzrecht, § 12, Rn. 53; Botschaft DSG, BBl 1988 II 468.

134 Vgl. zum Ganzen – mit Bezug zur Bearbeitung besonders schützenswerter Daten – schon *Epiney*, FS Steinauer, 97 (105 ff.).

135 S. schon *Epiney*, FS Steinauer, 97 (105 ff.); *Epiney/Fasnacht*, Jusletter v. 24.2.2014, Rn. 32.

u.a.m.) bezieht. Denn es widerspräche Sinn und Zweck dieses Surrogats einer gesetzlichen Grundlage, die zwingende Erforderlichkeit nur auf den Grundsatz, nicht aber die Modalitäten der Datenbearbeitung zu beziehen: Die Vorschrift will nämlich offenbar sicherstellen, dass in dieser Konstellation (besonders schützenswerte) Personendaten nur unter der Voraussetzung bearbeitet werden, dass dies zwingend zur Wahrnehmung einer gesetzlichen Aufgabe notwendig ist, dies im Hinblick auf den verfassungsrechtlich gebotenen Schutz der Persönlichkeit. Unterschiede man nun zwischen Grundsatz und Modalitäten, würde diese Zielsetzung unterlaufen, implizierte ein derartiger Ansatz doch, dass gewisse Bearbeitungen erfolgten, die gerade nicht zwingend für die Wahrnehmung der gesetzlichen Aufgabe notwendig sind (z.B. eine Aufbewahrung besonders schützenswerter Personendaten, ohne dass dies für die Erfüllung der gesetzlichen Aufgabe zwingend erforderlich wäre, sondern dieser nur dient, ihre Wahrnehmung also erleichtert wird). Es kann jedoch kaum angenommen werden, dass bei allen Modalitäten einer Datenbearbeitung im Rahmen von Informationssystemen die skizzierten hohen Anforderungen an die Unentbehrlichkeit erfüllt sind.

- Schliesslich ist zu beachten, dass – wie im Text erwähnt – im Falle der **Datenbekanntgabe** höhere Anforderungen zum Zuge kommen (Art. 19 Abs. 1 DSG); soweit eine solche in „systematischer“ Weise erfolgt (was jedenfalls im Zusammenhang mit der grenzüberschreitenden Datenübermittlung im Rahmen des EESSI zu bejahen ist), muss grundsätzlich eine ausdrückliche gesetzliche Grundlage vorliegen, und es reicht insbesondere nicht aus, dass die bekannt gegebenen Daten zur Erfüllung einer gesetzlichen Aufgabe unentbehrlich sind, da dieses Surrogat (Art. 19 Abs. 1 lit. a DSG) nur bei einer Datenbekanntgabe „im Einzelfall“ zu greifen vermag.

Die **gesetzliche Grundlage für Informationssysteme** muss zudem in gewissen Konstellationen in einem **formellen Gesetz** verankert werden, so (grundsätzlich) wenn es um die **Bearbeitung von besonders schützenswerten Personendaten** geht (Art. 17 Abs. 2 DSG). Wenn ein **Abrufverfahren** eingerichtet wird, ist dies in der gesetzlichen Grundlage ausdrücklich vorzusehen (Art. 19 Abs. 3 S. 1 DSG). In diesen Fällen hat die gesetzliche Grundlage im Übrigen auch den gesteigerten Anforderungen an die Normdichte, also die inhaltliche Bestimmtheit und die Detailliertheit, zu genügen. Die soeben erwähnten allgemeinen Anforderungen an den **Inhalt der gesetzlichen Grundlage** können daher für Informationssysteme, die solche Charakteristika aufweisen, wie folgt präzisiert werden:

- Der **Bearbeitungszweck** ist abschliessend und genau zu umschreiben bzw. durch entsprechende Verweise klarzustellen.
- Die genügende Präzisierung von **Art und Ausmass der Datenbearbeitung** impliziert die Verankerung, grundsätzlich in einem Gesetz im formellen Sinn, der grundlegenden Architektur des Systems, so dass aus dem Gesetz erkennbar sein muss, welche Datenbearbeitungen genau erfolgen und auf welche Weise sie durchgeführt werden (eben über ein Informationssystem). Zwar können gewisse, insbesondere technische Präzi-

sierungen auch auf Verordnungsstufe erfolgen; jedoch müssen die Grundstruktur und die Anlage des vorgesehenen Informationssystems bereits in einem formellen Gesetz geregelt sein.[136] Nur unter dieser Voraussetzung kann angesichts der mit einem solchen System einhergehenden Gefährdung der Persönlichkeitsrechte davon ausgegangen werden, dass die gesetzliche Grundlage hinreichend klar und präzise formuliert ist. Denn diese Anforderung impliziert auch und gerade, dass in solchen Konstellationen die für die Datenbearbeitung verwendeten Mittel mit hinreichender Genauigkeit aus der gesetzlichen Grundlage hervorgehen müssen, sind diese doch für die Intensität der Beeinträchtigung der Persönlichkeitsrechte von entscheidender Bedeutung.

- In diesem Rahmen sind auch die an der **Datenbearbeitung beteiligten Behörden bzw. Personen** (datenbearbeitende Stellen, zugangsberechtigte Stellen u.a.m.) zu präzisieren, so dass erkennbar ist, wer welche Datenbearbeitung vornimmt und wer auf welche Weise Zugang zu den Daten hat.
- Die **betroffenen Datenkategorien** sind möglichst genau zu umschreiben, wobei es hier grundsätzlich denkbar ist, dass im Gesetz im formellen Sinn die erfassten Personendaten in Anknüpfung an den Bearbeitungszweck in eher generischer Form umschrieben werden und eine genauere Präzisierung dann auf Verordnungsstufe erfolgt.
- Die Frage der **Dauer der Aufbewahrung** und der **Löschung** von Personendaten ist zu regeln.
- Die **Rechte der Betroffenen** sind ggf. – im Verhältnis zu den allgemeinen, sich bereits aus dem Datenschutzgesetz des Bundes ergebenden Anforderungen – zu präzisieren.

2. Zum Grundsatz der Zweckbindung

Im Sinne des **Grundsatzes der Zweckbindung**, wie er in **Art. 4 Abs. 3 DSG** formuliert ist,[137] dürfen Personendaten nur zu dem Zweck bearbeitet werden, der bei der Beschaffung angegeben wurde, aus den Umständen ersichtlich oder gesetzlich vorgesehen ist.

Erfolgt die Datenbearbeitung durch **Bundesorgane**, so hat die Bearbeitung dem **gesetzlich vorgesehenen Zweck** zu entsprechen. Hier ist der gesetzlich vorgesehene Zweck deshalb so bedeutsam, weil sich ein Bundesorgan für die Datenbearbeitung in jedem Fall auf eine den Zweck beinhaltende gesetzliche Grundlage zu stützen hat (17 Abs. 1 DSG). Die beiden anderen Alternativvarianten, namentlich der aus den Umständen ersichtliche und der bei der Be-

136 S. insoweit auch *Ballenegger*, in: Maurer-Lambrou/Blechta, BK Datenschutzgesetz, Öffentlichkeitsgesetz, Art. 17, Rn. 23; *Waldmann/Bickel*, in: Belser/Epiney/Waldmann, Datenschutzrecht, § 12, Rn. 50, die mit Verweis auf ein Gutachten des EDSB in VPB 60.77 und den vierten Tätigkeitsbericht des EDSB betonen, der Einsatz eines (weitverzweigten) EDV-Systems müsse explizit im Gesetz vorgesehen sein.

137 Derselbe Grundsatz lässt sich auf internationaler Ebene in Art. 5 lit. b DSK wiederfinden.

schaffung angegebene Zweck, rücken bei einer Bearbeitung durch öffentliche Organe daher in den Hintergrund.[138]

Der Grundsatz der Zweckbindung befasst sich nicht mit dem Zweck selbst, sondern setzt eine Relation voraus, nämlich dass der **Bearbeitungszweck mit dem angegebenen, gesetzlich vorgesehenen oder aus den Umständen ersichtlichen Zweck übereinstimmt**.[139] Eine Zweckänderung der Bearbeitung verstösst somit grundsätzlich gegen das Prinzip der Zweckbindung, wobei eine **Modifikation des Bearbeitungszwecks** allenfalls als eine neue zulässige Datenbearbeitung verstanden werden kann, sofern die dafür notwendigen Voraussetzungen erfüllt sind.[140]

Im Allgemeinen sollte die Erfüllung des Grundsatzes der Zweckbindung in unserem Zusammenhang keine grundsätzlichen grösseren Probleme aufwerfen,[141] geht es doch um die Einrichtung von Informationssystemen, die die Durchführung der Vorschriften über die Koordinierung der Systeme der sozialen Sicherheit der beteiligten Staaten sicherstellen sollen, womit der konkrete Zweck bekannt ist. Soweit ersichtlich,[142] erfolgt die Bearbeitung auch in der Tat zu diesem Zweck.

Im Gegensatz zum Datenschutzgesetz des Bundes, das keine Bearbeitungen von der Einhaltung des Prinzips der Zweckbindung ausnimmt, ermöglicht Art. 13 RL 95/46 eine Relativierung des Grundsatzes der Zweckbindung, worunter z.B. auch Bearbeitungen aus wichtigem finanziellem Interesse der EU oder einer ihrer Mitgliedstaaten fallen.

3. Zum Grundsatz der Verhältnismässigkeit

Der in **Art. 4 Abs. 2 DSG** vorgesehene **Grundsatz der Verhältnismässigkeit** ist ebenfalls auf verfassungsrechtlicher (Art. 5 Abs. 2 BV) und völkerrechtlicher Ebene (Art. 8 Abs. 2 EMRK, Art. 5 lit. c DSK) sowie im Unionsrecht (vgl. allgemein Art. 5 Abs. 1 EUV, s. auch Art. 6 Abs. 1 lit. e RL 95/46) verankert. Im Allgemeinen bedeutet dieser Grundsatz, dass die Massnahme **geeignet** und **erforderlich** ist, um den verfolgten Zweck zu erreichen, und dass die von öffentlichen Interessen getragene Datenbearbeitung mit den betroffenen sonstigen (privaten oder auch öffentlichen) Interessen in einem **angemessenen Verhältnis** steht (Verhältnismässigkeit i.e.S.).[143] Die Beachtung des Verhältnismässigkeitsgrundsatzes wird in einer konkreten Prüfung des Einzelfalls und anhand objektiver Kriterien beurteilt.[144] Aufgrund

138 Vgl. *Epiney*, in: Belser/Epiney/Waldmann, Datenschutzrecht, § 9, Rn. 32, insbesondere Fn. 100.

139 *Epiney*, in: Belser/Epiney/Waldmann, Datenschutzrecht, § 9, Rn. 31; *Rosenthal*, in: Rosenthal/Jöhri, Handkommentar DSG, Art. 4, Rn. 32.

140 *Epiney*, in: Belser/Epiney/Waldmann, Datenschutzrecht, § 9, Rn. 35.

141 Zur Einhaltung des Grundsatzes der Zweckbindung bei Informationssystemen bereits *Epiney/Fasnacht*, Jusletter v. 24.2.2014, Rn. 51 f.

142 S. die Beschreibung der Systeme oben B.

143 *Epiney*, in: Belser/Epiney/Waldmann, Datenschutzrecht, § 9, Rn. 23.

144 *Epiney*, in: Belser/Epiney/Waldmann, Datenschutzrecht, § 9, Rn. 24; *Rosenthal*, in: Rosenthal/Jöhri, Handkommentar DSG, Art. 4, Rn. 22.

des verfassungsrechtlichen Rangs und der kantonalrechtlichen Konkretisierungen ist dieser Grundsatz auch bei der behördeninternen Weitergabe von Personendaten zu beachten.[145]

Dem Erfordernis der Geeignetheit und der Erforderlichkeit wird dann entsprochen, wenn die Datenbearbeitung für einen bestimmten Zweck **objektiv geeignet** und **tatsächlich erforderlich** ist.[146] Ob die Datenbearbeitung objektiv geeignet ist, um den verfolgten Zweck zu erreichen, misst sich in erster Linie an der Genauigkeit, mit der die Datenbearbeitung das verfolgte Ziel herbeiführen wird bzw. soll. Je besser die Datenbearbeitung auf den zu erreichenden Zweck abgestimmt ist, desto geeigneter zeigt sich die Massnahme.[147] Steht für die Erreichung des erstrebten Zwecks kein milderes Mittel zur Verfügung, so ist die Massnahme zudem als erforderlich anzusehen. Hinsichtlich ihres Umfangs und ihrer Intensität ist die Datenbearbeitung insoweit erforderlich, als die betreffenden Daten zur Erfüllung des zu erreichenden Zwecks benötigt werden.[148] In diesem Sinn kommt der Verhältnismässigkeitsgrundsatz auch in Art. 2 Abs. 2 VO 987/2009 zum Ausdruck, der den Informationsaustausch auf die zur Begründung und zur Feststellung von Rechten und Pflichten benötigten Daten beschränkt. Darüber hinausgehende Datenbearbeitungen verstossen gegen das Prinzip der Verhältnismässigkeit. Als unproblematisch erweist sich die Einhaltung der Voraussetzungen der Geeignetheit und der Erforderlichkeit im Fall einer Bearbeitung, die zur Erfüllung einer formell-gesetzlich umschriebenen Aufgabe unentbehrlich ist (Art. 17 Abs. 2 lit. a DSG). Liegt eine in diesem Sinn unentbehrliche Bearbeitung vor, so ist sie in jedem Fall als geeignet und erforderlich anzusehen.[149]

Die **Verhältnismässigkeit i.e.S.** bzw. Angemessenheit verlangt, dass der Zweck der Bearbeitung mit der Persönlichkeitsbeeinträchtigung des Betroffenen in einem **vernünftigen Verhältnis** steht, so dass der betroffenen Person die Datenbearbeitung hinsichtlich ihres Zweckes sowie der dazugehörigen Mittel **zugemutet** werden kann.[150] Bei der Abwägung der involvierten Interessen müssen insbesondere die Intensität der Persönlichkeitsbeeinträchtigung des Betroffenen, der Datenschutz als öffentliches Interesse und das entgegenstehende öffentliche Interesse an einer Datenbearbeitung zwecks Erfüllung einer gesetzlichen Aufgabe mit einbezogen werden.[151]

In unserem Zusammenhang spielt der Verhältnismässigkeitsgrundsatz insbesondere in Bezug auf die Erforderlichkeit eine Rolle: So sind nur solche Daten in die Informationssysteme aufzunehmen, die tatsächlich der Koordinierung der Systeme der sozialen Sicherheit zwischen den beteiligten Staaten dienen. Weiter ist die Zugangsberechtigung entsprechend auszugestal-

---

145 Siehe auch *Epiney/Fasnacht*, Jusletter v. 24.2.2014, Rn. 53; zur Beachtung des Verhältnismässigkeitsgrundsatzes durch öffentlich-rechtliche Krankenhäuser vgl. *Baeriswyl*, in: Datenschutz im Gesundheitswesen, 49 (60).

146 Botschaft DSG, BBl 1988 II 450; *Rosenthal*, in: Rosenthal/Jöhri, Handkommentar DSG, Art. 4, Rn. 20.

147 *Epiney*, in: Belser/Epiney/Waldmann, Datenschutzrecht, § 9, Rn. 27.

148 *Epiney*, in: Belser/Epiney/Waldmann, Datenschutzrecht, § 9, Rn. 27, m.w.N.

149 *Epiney/Fasnacht*, Jusletter v. 24.2.2014, Rn. 56.

150 Botschaft DSG, BBl 1988 II 450; *Epiney*, in: Belser/Epiney/Waldmann, Datenschutzrecht, § 9, Rn. 27 mit Beispielfällen.

151 Vgl. mit weiteren Ausführungen *Epiney/Fasnacht*, Jusletter v. 24.2.2014, Rn. 57.

ten, so dass die Trägereinrichtungen nur zu solchen Daten Zugang haben dürfen, die sie tatsächlich für die Erfüllung ihrer gesetzlichen Aufgabe benötigen.

4. Zum Grundsatz der Transparenz und zur Informationspflicht der Betroffenen

Der **Grundsatz der Transparenz** im Sinne von **Art. 4 Abs. 4 DSG** besagt, dass die Beschaffung von Personendaten und insbesondere der Zweck ihrer Bearbeitung für die betroffene Person erkennbar sein muss. Ziel dieses Grundsatzes ist es, die **Transparenz für die Betroffenen** zu erhöhen, d.h. die betroffenen Personen sollen selbst entscheiden können, ob sie sich gegen eine bevorstehende Bearbeitung wehren wollen.[152] Zwar bezieht sich Art. 4 Abs. 4 DSG lediglich auf die Beschaffung von Personendaten und den Zweck ihrer Bearbeitung, so dass aus diesem Grundsatz keine generelle Informationspflicht seitens der bearbeitenden Personen abgeleitet werden kann. Allerdings kann sich eine solche Pflicht aus anderen Grundsätzen – wie insbesondere dem Grundsatz von Treu und Glauben[153] – ergeben.[154]
Die über den in Art. 4 Abs. 4 DSG verankerten Grundsatz der Transparenz hinausgehenden Informationspflichten sind in **Art. 14 DSG (für Privatpersonen)** sowie **Art. 18a (für Bundesorgane)** geregelt. Die beiden Regelungen stimmen weitgehend überein.[155] Zu erwähnen ist jedoch, dass sich die Informationspflicht im Fall einer Datenbearbeitung durch Privatpersonen auf besonders schützenswerte Personendaten und Persönlichkeitsprofile beschränkt, während Bundesorgane den betroffenen Personen die Beschaffung jeder Art von Personendaten mitzuteilen haben. Die Informationspflicht der Bundesorgane und der Privatpersonen kann unter den in Art. 9 DSG erwähnten Voraussetzungen eingeschränkt werden.[156] Zudem entfällt eine solche Pflicht von Bundesorganen unter den in Art. 18a Abs. 4 DSG genannten Umständen.
In engem Zusammenhang mit dem Grundsatz der Transparenz und den Informationspflichten steht **Art. 3 Abs. 3 VO 987/2009**. Gemäss dieser Bestimmung haben die Mitgliedstaaten dafür zu sorgen, dass die betroffenen Personen die Rechte zum Schutz ihrer Daten umfassend wahrnehmen können. Eine effektive Durchsetzung der zustehenden Rechte setzt voraus, dass die betroffenen Personen von einer Datenbearbeitung Kenntnis erhalten. Die Kenntnisnahme einer bevorstehenden Datenbearbeitung kann angenommen werden, wenn diese entweder bei

152 *Rosenthal*, in: Rosenthal/Jöhri, Handkommentar DSG, Art. 4, Rn. 51.
153 *Epiney*, in: Belser/Epiney/Waldmann, Datenschutzrecht, § 9, Rn. 22, 38; *Meier*, Protection des données, Rn. 658.
154 *Rosenthal*, in: Rosenthal/Jöhri, Handkommentar DSG, Art. 4, Rn. 51; *Epiney*, in: Belser/Epiney/Waldmann, Datenschutzrecht, § 9, Rn. 38 ff.
155 Zur Parallelität der Regelungsinhalte siehe *Epiney/Fasnacht*, in: Belser/Epiney/Waldmann, Datenschutzrecht, § 11, Rn. 16.
156 Ausführlich zu den möglichen Einschränkungsgründen *Epiney/Fasnacht*, in: Belser/Epiney/Waldmann, Datenschutzrecht, § 11, Rn. 51 ff.

der Datenbeschaffung erkennbar ist (Grundsatz der Transparenz) oder wenn die betroffenen Personen spezifisch darüber informiert wurden.

5. Zum Grundsatz der Datensicherheit

Nach dem in **Art. 7 DSG**[157] geregelten **Grundsatz der Datensicherheit** sind Personendaten gegen unbefugtes Bearbeiten durch angemessene technische und organisatorische Massnahmen zu schützen. Damit wird sowohl dem Dateninhaber als auch dem Datenbearbeiter eine Dauerpflicht zur Gewährleistung der Datensicherheit auferlegt.[158] Auf der Grundlage von Art. 7 Abs. 2 DSG hat der Bundesrat die Mindestanforderungen an die Datensicherheit in der Verordnung zum Datenschutzgesetz näher präzisiert, was in **Art. 8-12 VDSG für Privatpersonen** und in **Art. 20-23 VDSG für Bundesorgane** erfolgt ist, wobei Art. 8-10 VDSG aufgrund des Verweises in Art. 20 VDSG auch auf Bundesorgane Anwendung finden. Die im spezifischen Fall angemessene Massnahme hängt jedenfalls von den konkreten Umständen des Einzelfalls ab und muss dem Verhältnismässigkeitsgrundsatz entsprechen.[159]
Ganz allgemein wird in **Art. 8 Abs. 1 VDSG** zunächst festgelegt, vor welchen **Risiken** – darunter z.B. die unbefugte Vernichtung, der Verlust, technische Fehler, die Fälschung, usw. – Datenkommunikationsnetze Schutz zu bieten haben. Darauf folgen in Art. 9 VDSG acht Schutzziele, welche die Datenkommunikationsnetze mittels angemessener organisatorischer und technischer Massnahmen erfüllen sollten, wobei deren Einhaltung nicht zwingend eine ausreichende Datensicherheit im Sinne von Art. 7 Abs. 1 DSG zur Folge hat.[160]
Für die **automatisierte Datenbearbeitung** im Rahmen des EESSI-Systems ist insbesondere die in Art. 9 Abs. 1 lit. g VDSG reglementierte **Zugriffskontrolle** von Bedeutung. Demgemäss soll der Zugriff der berechtigten Personen auf diejenigen Personendaten beschränkt werden, die sie zur Erfüllung ihrer Aufgabe benötigen. Damit ist auch gesagt, dass die im Einzelfall berechtigten Personen durch das System als solche erkannt werden müssen, so dass der Zugriff Nicht-Berechtigter verhindert werden kann.[161] Diese Bestimmung gilt nicht nur für behördeninterne, sondern auch für behördenexterne Datenkommunikationsnetze.[162] Durch die Zugriffsbegrenzung des Kommunikationsnetzes soll der Gefahr einer unbewussten oder bewussten Fehlbearbeitung und dem Datenmissbrauch vorgebeugt werden.[163] Zur Umsetzung dieses Kontrollziels kommen unterschiedliche **Sicherheitsmassnahmen** (die auch kombiniert

157 Entspricht Art. 7 DSK.
158 *Rosenthal*, in: Rosenthal/Jöhri, Handkommentar DSG, Art. 7, Rn. 5 f.
159 *Epiney*, in: Belser/Epiney/Waldmann, Datenschutzrecht, § 9, Rn. 53; vgl. dazu die in Art. 8 Abs. 2 VDSG aufgeführte Liste von Kriterien, die bei der Wahl der Massnahme zu beachten sind.
160 *Rosenthal*, in: Rosenthal/Jöhri, Handkommentar DSG, Art. 7 Rn. 18; *Stamm-Pfister*, in: Maurer-Lambrou/Blechta, BK Datenschutzgesetz, Öffentlichkeitsgesetz, Art. 7, Rn. 24.
161 Zur Verweigerung des Zugriffs von nicht Berechtigten siehe auch die Benutzerkontrolle gemäss Art. 9 Abs. 1 lit. f VDSG sowie die Bekanntgabekontrolle im Sinne von Art. 9 Abs. 1 lit. d VDSG.
162 *Epiney/Fasnacht*, Jusletter v. 24.2.2014, Rn. 63.
163 Leitfaden des EDÖB zu technischen und organisatorischen Massnahmen, 12.

werden können) in Betracht, deren Verhältnismässigkeit im konkreten Einzelfall geprüft werden muss:[164]

- spezifizierte Zugangsrechte für jeden Mitarbeiter, welche die möglichen Bearbeitungen, die zeitliche Begrenzung, usw. festlegen;
- Erarbeitung einer Zugangsrechtematrix;
- Authentifizierung beim Zugang zum Informationssystem mit genügender Sicherheit (insbesondere bei besonders schützenswerten Personendaten);
- Protokollierung der Zugriffe auf das System.

Gemäss **Art. 10 VDSG** hat bei einer automatisierten **Bearbeitung von besonders schützenswerten Personendaten oder Persönlichkeitsprofilen** eine **Protokollierung** stattzufinden. Zur Erstellung eines Protokolls ist die verantwortliche Behörde im Sinne des Verhältnismässigkeitsgrundsatzes aber nur dann verpflichtet, wenn der Datenschutz nicht durch präventive Massnahmen gewährleistet werden kann (Art. 10 Abs. 1 S. 1 VDSG).[165] Dies ist insbesondere dann der Fall, wenn ansonsten nachträglich nicht festgestellt werden kann, ob die Daten für diejenigen Zwecke bearbeitet wurden, für die sie erhoben oder bekannt gegeben wurden (Art. 10 Abs. 1 S. 2 VDSG). Zudem sind diese Protokolle revisionsgerecht aufzubewahren und nur für diejenigen Personen zugänglich, denen die Überwachung der Datenschutzvorschriften obliegt (Art. 10 Abs. 2 VDSG). In der Protokollierung sind unter anderem sämtliche Zugriffe der zur Bearbeitung berechtigten Personen in sog. „log files" aufzunehmen, um so die soeben erwähnte Zugriffskontrolle zu gewährleisten.[166]

In der Lehre wird die im Bundesrecht verankerte Protokollpflicht stark kritisiert. Von mehreren Autoren wird sie insbesondere wegen des „enormen Aufwandes" als praxisfremd bezeichnet. Zudem werde der Protokollpflicht in der Realität kaum Genüge getan und auch die rechtlichen Konsequenzen einer ungenügenden Protokollierung seien in der Praxis als vernachlässigbar befunden worden.[167]

Die Verordnung zum DSG sieht sowohl für den privaten Bereich (Art. 11 VDSG) als auch bei Bearbeitungen durch Bundesorgane (Art. 21 VDSG) die Erstellung eines **Bearbeitungsreglements** vor. Die Pflicht des verantwortlichen Bundesorgans, ein Bearbeitungsreglement zu verfassen, erstreckt sich gemäss Art. 21 VDSG auf alle automatisierten Datensammlungen, die besonders schützenswerte Daten oder Persönlichkeitsprofile beinhalten (lit. a), durch mehrere Bundesorgane benutzt werden (lit. b), Kantonen, ausländischen Behörden, internationalen Organisationen oder privaten Personen zugänglich gemacht werden (lit. c) oder mit anderen Datensammlungen verknüpft sind (lit. d). Dieses Reglement stellt eine Art Dokumentation oder Handbuch dar, das Auskunft über die interne Organisation des verantwortlichen Bundesorgan sowie die Datenbearbeitungs- und Kontrollverfahren gibt.[168] Inhaltlich umfasst ein sol-

164 Siehe Leitfaden des EDÖB zu technischen und organisatorischen Massnahmen, 13; *Rosenthal*, in: Rosenthal/Jöhri, Handkommentar DSG, Art. 7, Rn. 19.

165 *Epiney/Fasnacht*, Jusletter v. 24.2.2014, Rn. 69.

166 *Epiney/Fasnacht*, Jusletter v. 24.2.2014, Rn. 70.

167 Eingehender zur Kritik der Protokollierung *Rosenthal*, in: Rosenthal/Jöhri, Handkommentar DSG, Art. 7, Rn. 20 sowie *Meier*, Protection des données, Rn. 814.

168 *Meier*, Protection des données, Rn. 815.

ches Reglement gemäss Art. 21 Abs. 2 VDSG Angaben zum verantwortlichen Organ und den gesammelten Daten (lit. a-c), die technischen und organisatorischen Massnahmen zur Gewährleistung der Datensicherheit (lit. d), die Beschreibung der Datenfelder und die Organisationseinheiten, die Zugriff darauf haben (lit. e), Art und Umfang der Benutzerzugriffe (lit. f), das Datenbearbeitungs- und das Auskunftsverfahren (lit. g und i) und die Konfiguration der Informatikmittel (lit. h).[169]

6. Besondere Grundsätze für den grenzüberschreitenden Datenaustausch

Im Rahmen des EESSI-Projekts werden die erfassten personenbezogenen (Sozial-) Daten von einer sozialen Einrichtung eines beteiligten Staates an eine soziale Institution eines anderen Mitgliedstaates übermittelt. Vor diesem Hintergrund sind auch die **Anforderungen an den grenzüberschreitenden Datenaustausch** zu beachten.

Angesichts der besonderen Risiken, die mit grenzüberschreitenden Datenübermittlungen einhergehen,[170] formuliert **Art. 6 DSG spezifische Anforderungen** für diese Art der Datenbearbeitung. Die Bestimmung – deren Vorgaben kumulativ zu den allgemeinen datenschutzrechtlichen Grundsätzen und Bestimmungen zu beachten sind[171] – wurde im Zuge der Revision des DSG im Jahr 2008 an das Zusatzprotokoll zur DSK angepasst.

Deutlich wird damit, dass die Regelung des Datenschutzgesetzes vor dem Hintergrund der **Datenschutzkonvention des Europarates** zu sehen ist, soll Art. 6 DSG diese doch in das nationale Recht umsetzen. Der grenzüberschreitende Datenverkehr ist in Art. 12 DSK geregelt, wobei diese Bestimmung auf dem Grundsatz der Freiheit des Datenverkehrs zwischen den Mitgliedstaaten beruht:[172] In der Annahme, dass die Vertragsstaaten der DSK ein gleichwertiges Datenschutzniveau bieten,[173] ist es den Staaten gemäss Art. 12 Abs. 2 DSK grundsätzlich verwehrt, den grenzüberschreitenden Datenverkehr in Richtung eines anderen Vertragsstaates unter alleiniger Begründung, die Privatsphäre schützen zu wollen, zu verbieten oder einer Genehmigungspflicht zu unterstellen.[174] Die gewählte Formulierung ist jedoch missverständlich, da daraus abgeleitet werden könnte, dass eine Einschränkung des freien Datenverkehrs nur zulässig ist, sofern damit auch anderen, nicht datenschutzrechtlichen Zwecken gedient ist. Entsprechend dem Sinn dieser Bestimmung, der die Errichtung nicht-tarifärer Handelshemmnisse unter einem datenschutzrechtlichen Vorwand verhindern will, sind im Rahmen von Art. 12 DSK jedoch auch allgemein geltende Anforderungen an den Datenschutz zu berücksichtigen.[175] Die Regelung von

169 Zum Inhalt eines Bearbeitungsreglements siehe auch den Leitfaden des EDÖB zu technischen und organisatorischen Massnahmen, 31.

170 Vgl. zusammenfassend *Epiney/Fasnacht*, in: Belser/Epiney/Waldmann, Datenschutzrecht, § 10, Rn. 2.

171 *Rosenthal*, in: Rosenthal/Jöhri, Handkommentar DSG, Art. 7, Rn. 2; *Walter*, in: Révision de la Loi sur la protection des données, 99 (121); *Epiney/Fasnacht*, in: Belser/Epiney/Waldmann, Datenschutzrecht, § 10, Rn. 4.

172 *Epiney/Schleiss*, in: Belser/Epiney/Waldmann, Datenschutzrecht, § 3, Rn. 39; *Ellger*, Datenschutz im grenzüberschreitenden Datenverkehr, 472.

173 *Walter*, in: La protection des données en Suisse et en Europe, 83 (100).

174 *Epiney/Schleiss*, in: Belser/Epiney/Waldmann, Datenschutzrecht, § 3, Rn. 39.

175 *Epiney/Schleiss*, in: Belser/Epiney/Waldmann, Datenschutzrecht, § 3, Rn. 39; *Ellger*, Datenschutz im grenzüberschreitenden Datenverkehr, 472 f.

Art. 12 DSK betrifft nur den Export personenbezogener Daten; der Import unterliegt hingegen dem nationalen Datenschutzrecht des Empfängerstaats.[176]
Art. 12 Abs. 3 DSK sieht zwei Ausnahmen vom Prinzip des freien Datenverkehrs vor: Nach Art. 12 Abs. 3 lit. a DSK kann ein Staat, der für bestimmte Arten von Personendaten einen besonderen Schutz vorsieht, den Datenexport in einen anderen Vertragsstaat einschränken, sofern dieser Staat nicht über einen gleichwertigen Schutz verfügt. Gegenstand dieser Vorschrift sind insbesondere sensible Daten, die nicht bereits von Art. 6 DSK erfasst werden.[177] Da aber die Bestimmung nicht festlegt, was als gleichwertiger Schutz anzusehen ist, kommt den Staaten diesbezüglich ein weiter Gestaltungsspielraum zu.[178] Die zweite Ausnahme, die in Art. 12 Abs. 3 lit. b DSK festgehalten ist, betrifft die Übermittlung von Daten in einen Vertragsstaat, der die Daten seinerseits an einen Nicht-Vertragsstaat weiterleitet, ohne dass der letztere ein genügendes Datenschutzniveau gewährleistet.[179] Diese zweite Ausnahme soll verhindern, dass das Datenschutzrecht des Sendestaats umgangen wird.[180]
Die Regelung bezüglich der grenzüberschreitenden Datenübermittlung in Drittstaaten findet sich im **Zusatzprotokoll** (ZP) Nr. 181 zur DSK. Nach Art. 2 Abs. 1 ZP ist ein solcher Datenexport nur erlaubt, sofern der Empfängerstaat über ein genügendes Datenschutzniveau verfügt. Ausnahmen zu diesem Grundsatz sind aber nach Art. 2 Abs. 2 ZP in zwei Konstellationen möglich, namentlich wenn das nationale Recht eine solche Übermittlung angesichts spezifischer Interessen des Betroffenen oder berechtigter überwiegender Interessen vorsieht (lit. a), oder wenn der für die Weitergabe Verantwortliche Garantien übernimmt, die durch die zuständige Behörde in Übereinstimmung mit dem internationalen Recht als hinreichend erachtet werden (lit. b).

Nach dem in **Art. 6 Abs. 1 DSG** verankerten Grundsatz darf eine Bekanntgabe von Personendaten ins Ausland nicht erfolgen, wenn dadurch die **Persönlichkeit der betroffenen Person schwerwiegend gefährdet** wird, und jedenfalls wenn im **Empfängerstaat keine Gesetzgebung besteht, die angemessenen Schutz** gewährleistet. Entscheidend ist, ob der Versender der Personendaten aufgrund des konkreten Einzelfalles auf eine schwerwiegende Gefährdung bzw. auf ein unangemessenes Schutzniveau schliessen kann.[181]
Wann der Schutz als angemessen anzusehen ist, wird im Gesetz nicht näher präzisiert. Allerdings nimmt die Botschaft zum revidierten Datenschutzgesetz dann ein angemessenes Schutzniveau an, wenn die **Gesetzgebung des Drittstaats den Anforderungen der Datenschutzkonvention des Europarates** gerecht wird und diese auch in der Praxis umgesetzt und angewandt wird.[182] Auch die **Einhaltung der RL 95/46** spricht für die Anerkennung eines angemessenen Schutzes.[183] Als Hilfsmittel bei der Prüfung des angemessenen Schutzes dient die vom EDÖB erstellte Liste, welche alle Staaten aufführt, die ein angemessenes Datenschutzniveau aufweisen (Art. 7 DSG). Diese Liste ist nicht verbindlicher Natur, sondern gibt lediglich Anhaltspunkte dafür, dass ein Staat datenschutzrechtlich einen angemessenen Schutz bietet.[184] Allerdings wird der Inhaber der Datensammlung, der sich bei seiner Datenbekannt-

176 Erläuternder Bericht des Europarats zum Übereinkommen zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten, Ziff. 66; *Ellger*, Datenschutz im grenzüberschreitenden Datenverkehr, 471.
177 Auch andere Daten können davon betroffen sein, vgl. *Walter*, in: La protection des données en Suisse et en Europe, 83 (101); *Ellger*, Datenschutz im grenzüberschreitenden Datenverkehr, 476.
178 Ansätze einer Begriffsbestimmung bestehen aber in den Richtlinien der OECD; *Epiney/Schleiss*, in: Belser/Epiney/Waldmann, Datenschutzrecht, § 3, Rn. 40.
179 *Epiney/Schleiss*, in: Belser/Epiney/Waldmann, Datenschutzrecht, § 3, Rn. 40; *Walter*, in: La révision de la Loi sur la protection des données, 99 (109).
180 *Walter*, in: La Protection des données en Suisse et en Europe, 83 (101).
181 *Epiney/Fasnacht*, in: Belser/Epiney/Waldmann, Datenschutzrecht, § 10, Rn.10.
182 BBl 2003 2128; s. *Walter*, in: La révision de la Loi sur la protection des données, 99 (122 f.).
183 *Rosenthal*, in: Rosenthal/Jöhri, Handkommentar DSG, Art. 6, Rn. 32.
184 *Walter*, in: La révision de la Loi sur la protection des données, 99 (123); *Epiney/Fasnacht*, in: Belser/Epiney/Waldmann, Datenschutzrecht, § 10, Rn. 11.

gabe ins Ausland auf diese Liste beruft, als gutgläubig erachtet, solange nicht das Gegenteil bewiesen wurde.[185]

Eine Verletzung von Art. 6 DSG kann aber auch vorliegen, wenn der in Frage stehende Empfängerstaat zwar ein angemessenes Schutzniveau bietet, jedoch auf andere Weise die Persönlichkeit der betroffenen Person in schwerwiegender Weise gefährdet. Folglich muss das Vorhandensein einer **schwerwiegenden Gefährdung der Persönlichkeit grundsätzlich für jeden Einzelfall** nachgeprüft werden.[186]

Art. 6 Abs. 2 DSG listet einen **abschliessenden**[187] **Ausnahmekatalog** von Tatbeständen auf, die eine Datenbekanntgabe ins Ausland zulassen, obwohl im entsprechenden Empfängerstaat ein angemessenes Schutzniveau fehlt.

Im Zusammenhang mit dem EESSI-Projekt ist zu beachten, dass alle beteiligten Staaten nicht nur Vertragsstaaten der EMRK sind, sondern (im Ergebnis) auch die datenschutzrechtlichen Vorgaben des Unionsrechts, insbesondere die RL 95/46, zu beachten haben. Damit ist davon auszugehen, dass in diesen Staaten ein angemessener Schutz besteht. Angesichts der in den EU-Mitgliedstaaten sowie in den EWR-Staaten geltenden rechtsstaatlichen Grundsätzen ist weiter anzunehmen, dass dieser gesetzliche Schutz grundsätzlich auch in der Praxis gewährleistet ist, so dass – trotz möglicher Lücken im Einzelfall – grundsätzlich nicht davon auszugehen ist, dass die im vorliegenden Zusammenhang zur Debatte stehende Datenübermittlung eine schwerwiegende Persönlichkeitsverletzung mit sich bringt. Daher dürfte sie den Anforderungen des Art. 6 Abs. 1 DSG entsprechen.

185 *Epiney/Fasnacht*, in: Belser/Epiney/Waldmann, Datenschutzrecht, § 10, Rn. 11.

186 *Epiney/Fasnacht*, in: Belser/Epiney/Waldmann, Datenschutzrecht, § 10, Rn. 13.

187 Boschaft 2003, BBl 2003 2128f.; *Walter*, in: La révision de la Loi sur la protection des données, 99 (128); *Meier*, Protection des données, Rn. 1309.

D. Reichweite der gesetzlichen Grundlagen *de lege lata*

Für die Datenbearbeitung durch öffentliche Organe spielt – wie dargelegt[188] – die Existenz einer (ausreichenden) **gesetzlichen Grundlage** eine zentrale Rolle. Diese hat sich ihrerseits an den (letztlich auf verfassungsrechtlichen Grundlagen beruhenden) allgemeinen datenschutzrechtlichen Grundsätzen (insbesondere die Prinzipien der Zweckbindung, der Verhältnismässigkeit und der Transparenz) zu orientieren, Grundsätze, die daher auch bei der Auslegung und Anwendung bestehender gesetzlicher Grundlagen zu berücksichtigen sind, ebenso wie bei der Beantwortung der Frage, ob eine bestimmte gesetzliche Regelung eine ausreichende gesetzliche Grundlage für die vorgesehene Datenbearbeitung darstellt.
Vor diesem Hintergrund konzentrieren sich die weiteren Ausführungen auf die Frage, ob sich im nationalen oder internationalen Recht bereits **gesetzliche Grundlagen für die geplanten Informationssysteme, namentlich für das europäische Informationssystem EESSI** (I.) **sowie für die damit im Zusammenhang stehenden nationalen Systeme** (II.) finden lassen bzw. wo es diesbezüglich allenfalls noch Lücken gibt.

Einer gesetzlichen Grundlage bedarf es jedenfalls, da – wie dargelegt[189] – die Voraussetzungen für eine Ausnahme von der gesetzlichen Grundlage vorliegend kaum erfüllt sein dürften, insbesondere, weil es nicht um eine Datenbearbeitung lediglich im Einzelfall geht (so dass auch eine Einwilligung der Betroffenen grundsätzlich die gesetzliche Grundlage nicht ersetzen kann) und auch das Surrogat der zwingenden Notwendigkeit der Bearbeitung zur Erfüllung einer gesetzlich klar umschriebenen Aufgabe in Bezug auf Informationssysteme grundsätzlich nicht zu greifen vermag.

Bei der Erörterung der möglicherweise in Frage kommenden gesetzlichen Grundlagen wird soweit möglich und sachdienlich zwischen den **verschiedenen vorgesehenen Datenbearbeitungen im Rahmen der erwähnten Informationssysteme** unterschieden. Dabei geht es im Wesentlichen um die Datenbekanntgabe von einer schweizerischen Verbindungsstelle oder einem Träger über die nationale Zugangsstelle zu einem ausländischen Träger sowie um den Datenaustausch zwischen schweizerischen sozialversicherungsrechtlichen Behörden. Da angesichts des derzeitigen Stands der Arbeiten an den Informationssystemen die konkret vorgesehenen Datenbekanntgaben im Rahmen der nationalen Systeme nicht eruiert werden können bzw. (möglicherweise) auch noch nicht abschliessend determiniert sind, wird hinsichtlich dieser Systeme auf eine separate Beurteilung der einzelnen Datenbearbeitungen verzichtet und eine abstrakte Betrachtungsweise angelegt, die jedoch gleichwohl den bestehenden Rahmen aufzuzeigen vermag.

188 Oben C.II.1.
189 C.II.1.

I. Zum grenzüberschreitenden Datenaustausch im Rahmen des EESSI

Nach dem Gesagten werden im Rahmen des (komplexen) Systems des EESSI verschiedenste Daten zwischen einer grossen Anzahl sozialer Einrichtungen ausgetauscht. Im Allgemeinen geht es um die **Übermittlung** all derjenigen **Daten**, deren Kenntnis für die **Begründung und Feststellung der sich aus der VO 883/2004 ergebenden Rechte und Pflichten** für die vom persönlichen Anwendungsbereich der Verordnung erfassten Personen **notwendig** ist, was den Einbezug der davon betroffenen sozialen Einrichtungen impliziert.[190] Die einzelnen Sozialversicherungszweige werden in der Schweiz durch spezifische, ihren Bedürfnissen angepasste Projekte dem EESSI-System angeschlossen.

Gemäss der in Art. 2 Abs. 2 VO 987/2009 enthaltenen Regelung vollzieht sich der grenzüberschreitende Datenaustausch entweder unmittelbar durch die Träger selbst oder mittelbar über die Verbindungsstellen. Hinsichtlich jedes Versicherungszweiges muss dementsprechend separat untersucht werden, wie die Daten grenzüberschreitend ausgetauscht werden. Denn während beispielsweise im Bereich der AHV und IV davon ausgegangen werden kann, dass die Verbindungsstelle – d.h. die zentrale Ausgleichsstelle der AHV (ZAS) – für die grenzüberschreitende Datenvermittlung auf der Grundlage der VO 883/2004 und der VO 987/2009 sorgen wird[191], zeichnet sich im Rahmen der Krankenversicherung eine gesonderte Anschliessung der einzelnen, in der obligatorischen Krankenversicherung tätigen Krankenkasse ab.[192] Davon ausgehend beschäftigt sich das folgende Kapitel in erster Linie mit der Frage, ob und inwieweit für diese **grenzüberschreitende Datenübermittlung von einer Verbindungsstelle bzw. einem Träger zu einer ausländischen Behörde über die nationale Zugangsstelle eine (ausreichende) gesetzliche Grundlage** besteht. Dabei ist auf die möglichen Grundlagen im Personenfreizügigkeitsabkommen bzw. in den durch dieses „übernommenen" Sekundärrechtsakten einzugehen (1.), bevor in diesem Zusammenhang ebenfalls in Betracht kommende Bestimmungen des schweizerischen (Sozialversicherungs-) Rechts erörtert werden (2.).

Ausgangspunkt ist dabei, dass im Rahmen des EESSI-Systems **besonders schützenswerte Personendaten** betroffen sein können: In der abschliessenden Liste von Art. 3 lit. c DSG sind nicht nur Angaben über die Gesundheit (Ziff. 2), sondern auch Daten bezüglich Massnahmen der sozialen Hilfe (Ziff. 3) relevant. Gesundheitliche Daten sind allerdings erst dann als besonders schützenswert zu betrachten, wenn anhand der Informationen auf den physischen oder psychischen Gesundheitszustand einer Person geschlossen werden kann. Entscheidend ist, ob die Informationen über die Gesundheit einer Person einen medizinischen Befund zulas-

190 S. insoweit auch Art. 2 Abs. 2 VO 987/2009.
191 S. dazu bereits oben B.II.1.
192 *Rossmanith/Engel*, CHSS 2/2012, 120 (123).

sen.[193] Besonders schützenswerte Personendaten liegen demnach insbesondere dann vor, wenn Leistungen der Invalidenversicherung, der Krankenversicherung oder der Unfallversicherung in Frage stehen.[194] In aller Regel stellen Leistungen der Sozialversicherungen zwar keine Massnahmen der sozialen Hilfe im Sinn von Art. 3 lit. c Ziff. 3 DSG dar.[195] Allerdings sind gemäss Botschaft zum DSG Sozialversicherungsleistungen dann als Massnahmen der sozialen Hilfe zu qualifizieren, wenn sie in Zusammenhang mit einer Krankheit oder einem Unfall stehen.[196] Denn in diesen Fällen können den Sozialversicherungsdaten Anhaltspunkte über den Gesundheitszustand einer Person entnommen werden.[197] Deshalb sind, zumindest für solche Fälle, die damit einhergehenden strengeren Anforderungen zu berücksichtigen. Da die vorgesehenen Informationssysteme „ein Ganzes" darstellen, in zahlreichen Bereichen besonders schützenswerte Daten nach dem Gesagten betroffen sein können und es wohl kaum praktikabel erscheint (und auch nicht vorgesehen ist), im Einzelfall eine Unterscheidung zu treffen, ist davon auszugehen, dass die qualifizierten Vorgaben für die Bearbeitung besonders schützenswerter Daten zum Zuge kommen, was einerseits eine formell-gesetzliche Grundlage, andererseits erhöhte Anforderungen an die Bestimmtheit der gesetzlichen Grundlage impliziert.[198] Dies gilt jedenfalls, soweit die eigentliche grenzüberschreitende Übermittlung über die Zugangsstellen über eine einzige Verbindungsstelle erfolgen sollte. Sobald jedoch – wie dies offenbar in der Schweiz vorgesehen ist – je nach den betroffenen Bereichen verschiedene Verbindungsstellen eingerichtet werden, wäre jeweils im Einzelnen zu prüfen, ob besonders schützenswerte Daten bearbeitet werden.[199]

Im Übrigen handelt es sich bei der grenzüberschreitenden Datenübermittlung jedenfalls um eine **Datenbekanntgabe** im Sinne des Art. 19 Abs. 1 DSG, womit die strengeren Voraussetzungen dieser Bestimmung zu beachten sind.[200] Besonders hervorzuheben ist in diesem Zusammenhang, dass die gesetzliche Grundlage auch den genauen Umfang der Datenbekanntgabe sowie die Grundzüge der Art und Weise der Bekanntgabe regeln muss, um den Anforderungen an die Bestimmtheit einer gesetzlichen Grundlage gerecht zu werden.

---

193 Botschaft DSG, BBl 1988 II 446; *Blechta*, in: Maurer-Lambrou/Blechta, BK Datenschutzgesetz, Öffentlichkeitsgesetz, Art. 3, Rn. 33.

194 *Blechta*, in: Maurer-Lambrou/Blechta, BK Datenschutzgesetz, Öffentlichkeitsgesetz, Art. 3, Rn. 38.

195 BGE 124 III 170, E. 3b betreffend der Auskunftspflicht der Sozialversicherungen gegenüber den Betreibungsämtern; *Jöhri*, in: Rosenthal/Jöhri, Handkommentar DSG, Art. 3, Rn. 52; *Blechta*, in: Maurer-Lambrou/Blechta, BK Datenschutzgesetz, Öffentlichkeitsgesetz, Art. 3, Rn. 38.

196 Botschaft DSG, BBl 1988 II 446.

197 *Jöhri*, in: Rosenthal/Jöhri, Handkommentar DSG, Art. 3 Rn. 52; *Blechta*, in: Maurer-Lambrou/Blechta, BK Datenschutzgesetz, Öffentlichkeitsgesetz, Art. 3 Rn. 38.

198 Vgl. im Einzelnen zu diesen erhöhten Anforderungen *Waldmann/Bickel*, in: Belser/Epiney/Waldmann, Datenschutzrecht, § 12, Rn. 47 ff.; s. auch schon oben C.II.1.

199 Vgl. insoweit unten D.II., in Bezug auf die Bereiche der AHV und IV sowie der Unterstellung.

200 Zu diesen oben C.II.1.

1. Zu den möglichen gesetzlichen Grundlagen im Personenfreizügigkeitsabkommen

Eine gesetzliche Grundlage für eine Datenbearbeitung kann sich nicht nur im nationalen Recht, sondern auch im **internationalen Recht** finden lassen, wobei in unserem Zusammenhang in erster Linie das **Personenfreizügigkeitsabkommen** in Betracht kommt.[201] So ist denn auch – wie skizziert – die **Einrichtung des EESSI** zumindest im Grundsatz bereits durch die **VO 883/2004** und die **VO 987/2009** vorgesehen. Diese Verordnungen sind als **Teil des Anhangs II FZA** auch für die Schweiz relevant und durch diese zu beachten, so dass im Folgenden danach zu fragen ist, ob und ggf. inwieweit diese (auch)[202] die grenzüberschreitende Datenübermittlung zulassen bzw. vorsehen.[203] Denn sowohl die VO 883/2004 als auch die VO 987/2009 enthalten diverse, die Einrichtung des EESSI betreffende Bestimmungen, die auch Fragen des Datenaustauschs betreffen.
Dabei sind die VO 883/2004 und die VO 987/2009 als **„Gesetze im formellen Sinn"** im Sinn des Art. 17 Abs. 2 DSG anzusehen (Art. 3 lit. j DSG),[204] so dass sie auch eine genügende gesetzliche Grundlage für die Bearbeitung besonders schützenswerter Personendaten darstellen können.

a) Zur VO 883/2004

Bereits die **VO 883/2004** enthält diverse Bestimmungen, die einerseits den **Datenaustausch** zwischen den beteiligten Staaten und den **Grundsatz der Einrichtung eines Informationssystems** wie das EESSI, andererseits gewisse **Pflichten der betroffenen Personen** vorsehen.
Im Einzelnen ist auf folgende Bestimmungen hinzuweisen:

- **Art. 76 VO 883/2004** regelt die **Grundsätze der Zusammenarbeit zwischen den nationalen Sozialversicherungseinrichtungen zur Erfüllung der ihnen zugewiesenen Aufgaben**.[205] Von Bedeutung ist dabei insbesondere **Art. 76 Abs. 2 VO 883/2004**, wonach sich die Behörden und Träger der Mitgliedstaaten für die Zwecke der VO 883/2004 zu unterstützen haben und zwar so, als handle es sich um die Anwendung ihrer eigenen Rechtsordnung. Art. 76 Abs. 2 VO 883/2004 beschreibt damit die mitgliedstaatliche Amtshilfe unter den nationalen Behörden und Trägern, wobei die ausländischen Anfragen von den nationalen Institutionen so zu behandeln sind, als

201 S. insoweit schon oben C.I.2., C.II.1.
202 Nicht eingegangen wird hingegen auf den „internationalen" bzw. europäischen Teil des EESSI, für den die Union und hier die Kommission verantwortlich ist.
203 Vgl. auch schon oben C.I.2.
204 Vgl. im Übrigen auch *Biaggini*, BV Kommentar, Art. 36, Rn. 13, der explizit darauf hinweist, dass auch völkerrechtliche Verträge als Gesetze im formellen Sinn angesehen werden können.
205 *Wunder*, in: Schreiber/Wunder/Dern, Kommentar zur VO 883/2004, Art. 76, Rn. 1.

handle es sich um eine innerstaatliche Angelegenheit. Das konkrete Ausmass der Amtshilfepflicht ist demnach dem nationalen Recht zu entnehmen, welches das Verfahren der innerstaatlichen Amtshilfe regelt.[206] Abgesehen von der grundsätzlichen Kostenfreiheit der Amtshilfe enthält Art. 76 Abs. 2 VO 883/2004 keine weiteren Angaben zur Art und zum Umfang der gegenseitigen Amtshilfe.[207]

- Nach **Art. 76 Abs. 3 VO 883/2004** können die Behörden und Träger der Mitgliedstaaten für die Zwecke der VO 883/2004 miteinander sowie mit den betroffenen Personen oder deren Vertretern direkt in Kontakt treten. Demnach soll zwischen den einzelnen Sozialversicherungsträgern der Mitgliedstaaten ein unmittelbarer Informationsaustausch stattfinden können, ohne dass in jedem Einzelfall eine Mitteilung die Verbindungsstelle passieren muss.

  Ein solches Vorgehen ist allerdings dann nicht möglich, wenn im Sinn von Art. 66 Abs. 2 VO 987/2009 Kosten zu erstatten sind. Dafür muss in jedem Fall die entsprechende Verbindungsstelle kontaktiert werden.[208] Ermöglicht wird der direkte Kontakt durch die elektronische Datenbank, die die Kontaktadressen aller nationalen Sozialversicherungsträger enthält.[209] Aus der Systematik der Regelung kann zudem abgeleitet werden, dass ein solch direkter Kontakt nicht zwingend im Rahmen des EESSI zu erfolgen hat. Denn die diesbezügliche Vorschrift befindet sich ausserhalb des Artikels 78 VO 883/2004, der die Einführung des EESSI begründet. Der direkte Kontakt kann somit auch auf andere Art und Weise, wie z.B. per Telefon, hergestellt werden. Gemäss Art. 76 Abs. 3 VO 883/2004 sollen die betroffenen Personen oder ihre Vertreter ebenfalls durch die nationalen Sozialversicherungseinrichtungen direkt benachrichtigt werden können.[210]

- Um eine ordnungsgemässe Anwendung der VO 883/2004 sicherzustellen, wird in **Art. 76 Abs. 4 VO 883/2004** die **gegenseitige Pflicht zur Information und Zusammenarbeit der Träger und der Personen, die der VO 883/2004 unterliegen**, normiert. Die Pflichten der Träger und der betroffenen Personen werden je in einem Untersatz konkretisiert. Während die Träger jede Anfrage innert einer angemessenen Frist zu beantworten und die betroffenen Personen zwecks Wahrnehmung ihrer Rechte ausreichend zu informieren haben, werden die betroffenen Personen dazu verpflichtet, den Trägern des zuständigen Mitgliedstaats jede relevante Änderung ihrer persönlichen oder familiären Situation so bald wie möglich mitzuteilen.
- **Art. 77 VO 883/2004 verweist** in Bezug auf die von den Behörden oder den Trägern der beteiligten Staaten vorgenommenen Datenübermittlungen auf das **Datenschutzrecht des übermittelnden Mitgliedstaats**.

---

206 Vgl. *Spiegel*, in: Fuchs, Europäisches Sozialrecht, Art. 76 VO 883/2004, Rn. 8 f. mit einem Beispiel zum österreichischen Recht, wonach Daten zur Einkommensfeststellung nicht direkt von den Steuerbehörden herausgegeben werden können und sich somit der ausländische Träger an die dafür zuständige, österreichische Sozialversicherungsanstalt richten muss, gegenüber welchem die Steuerbehörde auskunftspflichtig ist.

207 *Wunder*, in: Schreiber/Wunder/Dern, Kommentar zur VO 883/2004, Art. 76, Rn. 6.

208 *Spiegel*, in: Fuchs, Europäisches Sozialrecht, Art. 76 VO 883/2004, Rn. 12.

209 Hierzu bereits oben B.I.

210 *Wunder*, in: Schreiber/Wunder/Dern, Kommentar zur VO 883/2004, Art. 76, Rn. 8 f.; *Spiegel*, in: Fuchs, Europäisches Sozialrecht, Art. 76 VO 883/2004, Rn. 15 f.

- Schliesslich ist auf **Art. 78 VO 883/2004** hinzuweisen, dem zu entnehmen ist, dass die **Datenübermittlung in elektronischer Form** zu erfolgen hat. Die Einführung des EESSI beruht also letztlich auf dieser Bestimmung.

b) Zur VO 987/2009

Die **VO 987/2009** enthält insbesondere in **Art. 2 ff. Präzisierungen zum Datenaustausch** sowie zur **Einrichtung des elektronischen Verzeichnisses an der Koordinationsstelle**. Im Einzelnen geht es im Wesentlichen um folgende Bestimmungen:

- Ganz allgemein wird in **Art. 2 Abs. 1 VO 987/2009** zunächst festgehalten, dass der **Informationsaustausch** den Grundsätzen der öffentlichen Dienstleistungen, der Effizienz, der aktiven Unterstützung, der raschen Bereitstellung und Zugänglichkeit zu entsprechen hat.
- In **Art. 2 Abs. 2 VO 987/2009** werden die Träger sodann dazu angehalten, alle **notwendigen Daten unverzüglich zur Verfügung zu stellen** oder **ohne Verzug auszutauschen**.

  Die Daten können nach dieser Vorschrift entweder unmittelbar durch die Träger selbst oder auf dem Wege der Verbindungsstellen übermittelt werden. Aus Gründen der Verfahrensökonomie könnte ein Austausch über die Verbindungsstellen vorzuziehen sein, da es sich für die einzelnen Träger als schwieriger erweist, den im Einzelfall zuständigen, ausländischen Träger ausfindig zu machen.[211]

- Die **Grundzüge zum Datenaustausch zwischen den betroffenen Personen und den Trägern** sind in **Art. 3 VO 987/2009** geregelt. Nach Art. 3 Abs. 2 VO 987/2009 müssen die Personen, die der VO 883/2004 unterliegen, den zuständigen Trägern alle massgeblichen Informationen, Dokumente oder Belege übergeben. Auf der anderen Seite haben die Träger gemäss Art. 3 Abs. 4 VO 987/2009 den betroffenen Personen alle zur Anwendung der VO 883/2004 und der VO 987/2009 erforderlichen Informationen und Dokumente auszustellen.
- Die **Datenübermittlung zwischen den Trägern oder Verbindungsstellen** hat **elektronisch** zu erfolgen, entweder unmittelbar oder mittelbar über die Zugangsstellen (wobei die letztere Option – soweit ersichtlich – derzeit im Vordergrund steht)[212]; dabei ist die Datensicherheit zu gewährleisten (**Art. 4 Abs. 2 VO 987/2009**).
- **Art. 14 ff. VO 987/2009** enthalten **weitere präzisierende bzw. spezifische Bestimmungen**, u.a. zur grenzüberschreitenden Zusammenarbeit und zum Datenaustausch, dies in Bezug auf bestimmte Sozialversicherungszweige. Diese Vorgaben präzisieren (teilweise) die erwähnten allgemeinen Bestimmungen.

---

211 *Spiegel*, in: Fuchs, Europäisches Sozialrecht, Art. 76 VO 883/2004, Rn. 13.

212 Ibid., Art. 78 VO 883/2004, Rn. 4. S. insoweit bereits oben B.I.

Beispielhaft werden hier die relevanten Bestimmungen für die Informationssysteme im Rahmen der AHV und der IV sowie der Unterstellung erwähnt:

- Soll das **anwendbare Recht** bestimmt werden, so müssen die ausländischen Sozialversicherungsanstalten gemäss **Art. 20 VO 987/2009** dem zuständigen Träger alle Auskünfte erteilen, die für die Festsetzung des Anwendungszeitpunkts und der Beiträge erforderlich sind. Des Weiteren wird in Art. 15-18 VO 987/2009 festgelegt, wie das Verfahren zur Bestimmung des anwendbaren Rechts ablaufen soll. Auch diese Bestimmungen beinhalten einige Hinweise zu den im Rahmen des EESSI zu erfolgenden Datenbearbeitungen, wobei es jedoch im Wesentlichen darum geht, den Verfahrensablauf festzulegen.
- Die **Datenbearbeitungen**, die im Rahmen der **Alters-, Invaliden- oder Hinterbliebenenrenten** erfolgen, werden in **Art. 47 VO 987/2009** umschrieben. Mit „Kontakt-Träger" im Sinne von Art. 47 Abs. 1 VO 987/2009 ist derjenige Träger gemeint, dem ein Antrag zugestellt bzw. weitergeleitet wird. Dieser Träger „fördert" nach Art. 47 Abs. 1 VO 987/2009 den Datenaustausch und sorgt dafür, dass die betroffenen Personen über den Stand der Bearbeitung ihres Antrags informiert sind. Mit Ausnahme der Fälle, die nach Art. 44 VO 883/2004 zu beurteilen sind[213], werden die Bearbeitungsvorgänge in Art. 47 Abs. 4-6 VO 987/2009 näher erläutert. Nach Abs. 4 stellt der zuständige Träger den beteiligten ausländischen Trägern alle ihm zur Verfügung stehenden Dokumente sowie allenfalls die von der antragsstellenden Person übergebenen relevanten Unterlagen zu, so dass diese Träger gleichzeitig mit der Bearbeitung des Gesuchs beginnen können. Zusätzlich werden den ausländischen sozialen Einrichtungen die Versicherungs- oder Wohnzeiten, die nach den Rechtsbestimmungen des Kontakt-Trägers zurückgelegt wurden, mitgeteilt (Abs. 4). Die beteiligten Träger haben ihrerseits dem Kontakt-Träger sowie den anderen beteiligten Trägern ihre Versicherungs- oder Wohnzeiten mitzuteilen (Abs. 5). Schliesslich muss jeder beteiligte Träger dem Kontakt-Träger und den anderen betroffenen Trägern seine Entscheidung, den Leistungsbetrag und weitere erforderliche Angaben übermitteln (Abs. 6). Ferner regelt Art. 48 VO 987/2009, wie die antragsstellende Person über die verschiedenen Entscheidungen der Träger zu benachrichtigen ist.

- Schliesslich ist die Einrichtung des ***electronic directory***, das die nationalen Institutionen der sozialen Sicherheit auflistet,[214] in **Art. 88 i.V.m. Anhang 4 VO 987/2009** vorgesehen. Geregelt ist hier auch die Pflicht der Mitgliedstaaten zur ständigen Aktualisierung (Art. 88 Abs. 5 VO 987/2009) sowie der genaue Inhalt der im Verzeichnis figurierenden Daten.

Im *electronic directory* sind die zuständigen Behörden der Mitgliedstaaten (Art. 1 lit. m VO 883/2004), die zuständigen Träger (Art. 1 lit. q VO 883/2004), die Träger des Wohn- und Aufenthaltsorts (Art. 1 lit. r VO 883/2004), die Zugangsstellen (Art. 1 Abs. 2 lit. a VO 987/2009) und die Verbindungsstellen (Art. 1 Abs. 2 lit. b VO 987/2009) aufzuführen (Art. 88 Abs. 1 VO 987/2009), wobei die Mitgliedstaaten ihre eigenen nationalen Kontaktstellen angeben müssen und die ständige Aktualisierung zu gewährleisten haben (Art. 88 Abs. 4, 5 VO 987/2009). Dabei sind alle Einrichtungen über Identifizierungscodes abzubilden; eine Auswahl oder pauschale Verweise sind nicht zulässig,[215] eine Vorgabe, die letztlich vor dem Hintergrund der Ermöglichung automatisierter Übermittlungen über die Zugangsstellen zu sehen ist.

---

213 Art. 44 VO 883/2004 kommt nur zur Anwendung, wenn für eine Person ausschliesslich die Rechtsvorschriften des Typs A galten, was bedeutet, dass diese Person Rechtsbestimmungen unterstellt war, wonach die Höhe der Leistungen bei Invalidität nicht von der Dauer der Versicherungs- und Wohnzeiten abhängt. Da dies bei der schweizerischen Gesetzgebung nicht der Fall ist, sind diese Koordinierungsvorschriften und die damit zusammenhängenden Spezialbestimmungen für die Schweiz nicht von Bedeutung.

214 S.o. B.I.

215 *Spiegel*, in: Fuchs, Europäisches Sozialrecht, Art. 78 VO 883/2004, Rn. 9.

c) Fazit

Im Ergebnis ist festzustellen, dass die VO 883/2004 und die VO 987/2009 zahlreiche Bestimmungen enthalten, die die Einrichtung des EESSI, den Datenaustausch und die Pflichten von Mitgliedstaaten, Trägern und in den Anwendungsbereich der Verordnung fallenden Personen betreffen. Fragt man danach, ob diese Bestimmungen die oben[216] erläuterten Vorgaben an eine **gesetzliche Grundlage** für einen grenzüberschreitenden Datenaustausch der erfassten Daten erfüllen, so erscheinen folgende Aspekte von besonderer Bedeutung zu sein:

- Der **Bearbeitungszweck** ergibt sich aus einer Zusammenschau der als Rechtsgrundlagen in Betracht kommenden Bestimmungen und den sonstigen Vorgaben der Verordnungen, geht es doch um den Datenaustausch im Hinblick auf die effektive Durchführung der Koordinierung der von den Verordnungen erfassten Systeme bzw. Leistungen der sozialen Sicherheit. Zwar ist anzumerken, dass die Präzisierung des Bearbeitungszwecks im Einzelnen auf dieser Grundlage einen gewissen Interpretations- und Rechercheaufwand impliziert, ist doch zunächst der sachliche Anwendungsbereich auf der Grundlage der Rechtsprechung des Gerichtshofs zu klären, bevor noch zu spezifizieren ist, was genau unter die Koordinierung zu fassen ist. Damit könnten an der hinreichenden Präzision der Regelung des Bearbeitungszwecks gewisse Zweifel bestehen. Im Ergebnis erscheint es aber vertretbar anzunehmen, dass mittels eines gewissen Aufwands der Bearbeitungszweck angesichts der Regelungen der EU-Verordnungen in Verbindung mit der einschlägigen Rechtsprechung durchaus ermittelt werden kann, so dass eine genügend klare Umschreibung des Bearbeitungszwecks in den Verordnungen bejaht werden kann.
- Die an der Datenbearbeitung **Beteiligten** (in erster Linie die Träger und die Verbindungsstellen) ergeben sich einerseits aus dem Zweck der Verordnungen und werden andererseits im *electronic directory* aufgeführt, so dass die Datenbearbeiter durchaus aus den Rechtsgrundlagen (i.V.m. dem *electronic directory*) ersichtlich sind. Allerdings ist jedenfalls zu beachten, dass es an den **Mitgliedstaaten** ist, die Verbindungsstellen sowie die Zugangsstellen zu definieren, so dass hierfür jedenfalls keine Grundlage in den Verordnungen besteht. Allerdings könnte vertreten werden, durch die Mitteilung an die Kommission bzw. das Einfügen in die Datenbank (das *electronic directory*) – die ja die Anhänge der bisherigen Durchführungsverordnung ersetzt – würden diese Stellen als Datenbearbeiter gesetzlich verankert, so dass ein eigenständiges Aufführen in einem nationalen Rechtsakt überflüssig sei (auch angesichts des Umstands, dass das *electronic directory* ständig aktualisiert wird).

  Gewisse Zweifel bleiben hier jedoch: Denn dieser Ansatz implizierte, dass diejenige Bundesstelle, welche diese Information bzw. Aktualisierung vornimmt, letztlich „autonom“ (d.h. ohne gesetzliche Grundlage) entscheiden könnte, wer die Datenbearbeitung bzw. die Datenbekanntgabe vornimmt, so dass

[216] C.II.1.

hierfür im Ergebnis eben doch keine gesetzliche Grundlage besteht. An dieser Einschätzung vermag auch der Umstand nichts zu ändern, dass es aus pragmatischer Sicht naheliegend sein könnte, allein auf das *electronic directory* abzustellen. Immerhin bleibt aber anzumerken, dass die Modifikationen des Verzeichnisses jedenfalls auf EU-Ebene genehmigt werden müssen.

- In Bezug auf die hinreichend präzise **Umschreibung von Umfang und Art der Datenbearbeitung bzw. der Datenbekanntgabe** ist daran zu erinnern,[217] dass sich die Datenbearbeitung bzw. die Datenübermittlung nach den erörterten Vorgaben immer nur auf diejenigen Daten bezieht, die zur Durchführung der Koordinierung der erfassten Systeme sozialer Sicherheit notwendig sind, was eine Eingrenzung der betroffenen Daten impliziert. Allerdings kann es durchaus gewissen Unsicherheiten unterworfen sein, welche Daten denn nun genau durch diese doch eher generische Umschreibung erfasst werden. Angesichts des Umstands, dass es hier (auch) um die Bearbeitung besonders schützenswerter Daten geht, könnte daher ein derartiges eher generelles Abstellen auf den Zweck der Datenbearbeitung den **Anforderungen an eine hinreichende Bestimmtheit** nicht Rechnung tragen. Hinzu kommt, dass es jedenfalls um eine Datenbekanntgabe im Sinne des Art. 19 Abs. 1 DSG geht, bei der ebenfalls erhöhte Anforderungen an die Bestimmtheit der gesetzlichen Grundlage zum Zuge kommen.

Im Einzelnen ist in Bezug auf die **Normdichte** der untersuchten Bestimmungen insbesondere auf folgende Punkte hinzuweisen:

- Beim **Amtshilfeverfahren (Art. 76 VO 883/2004)** wird zum einen explizit auf innerstaatliches Recht Bezug genommen. Im Rahmen der Umsetzung des EESSI in der Schweiz sind somit die entsprechenden Bestimmungen der schweizerischen Sozialversicherungsgesetzgebung zu beachten.[218] Zum anderen werden hier zwar die Grundlagen der Zusammenarbeit geregelt, jedoch fehlen wesentliche Aspekte, wie insbesondere die genau erfassten Daten.
- **Art. 2 Abs. 2 VO 987/2009** verpflichtet die Träger (und ggf. die Verbindungsstellen) dazu, alle notwendigen Daten zur Verfügung zu stellen bzw. auszutauschen. Dabei sind eine grosse Anzahl beteiligter Träger, Behörden und betroffener Personen in Verbindung mit dem grossen Fluss unterschiedlicher Arten von Daten erfasst.
- **Art. 78 VO 883/2004** und **Art. 4 VO 987/2009** können als gesetzliche Grundlage für die Einführung des elektronischen Datenaustausches und die Pflicht der Träger sowie der Verbindungsstellen zur Verwendung elektronischer Mittel herangezogen werden. Allerdings können diesen Bestimmungen keine Einzelheiten zu den Datenbearbeitungsvorgängen entnommen werden.
- **Art. 15 ff. VO 987/2009** beinhalten einige Hinweise zu den im Rahmen des EESSI zu erfolgenden Datenbearbeitungen, wobei es jedoch im Wesentlichen darum geht, den Verfahrensablauf festzulegen. Was spezifisch Art. 20 VO 987/2009 anbelangt, so ergibt sich aus dieser Bestimmung, welche Daten zwischen den verschiedenen Trägern ausgetauscht werden, namentlich alle Informationen, die für die Bestimmung des Anwendungszeitpunktes und der Beiträge benötigt werden. Allerdings fehlt eine eigentliche Umschreibung der erfassten Datenkategorien sowie des Ausmasses und der Art der Datenbearbeitung. Ebensowenig ergibt sich aus dieser Bestimmung, wer konkret Empfänger dieser Daten ist (dies kann aber anhand der elektronischen Datenbank ergründet werden und hängt jedenfalls vom im Mitgliedstaat geltenden System der Sozialversicherungen ab).
- Ähnliche Erwägungen können in Bezug auf **Art. 47 VO 987/2009** angestellt werden. Im Übrigen weist Art. 47 VO 987/2009 eher den Charakter einer Verfahrensnorm auf, die trotz der nur schwer fassbaren Komplexität des Systems die Art und das Ausmass der zu erwartenden Datenbearbeitungen wenig genau darlegt. Dazu kommt, dass insbesondere im Bereich der Invalidenversicherung in besonderem Mass auch besonders schützenswerte Personendaten betroffen sein könnten, auf deren Bearbeitung in der gesetzlichen Grundlage explizit hinzuweisen ist.[219] Aus Art. 47 VO 987/2009 ist nicht zu erkennen, welche Kategorien von Daten konkret bearbeitet werden.

---

217 Oben D.I.1.a), b).

218 Dazu weiter unten D.I.2.

219 11. Tätigkeitsbericht des EDSB, 13.

Auch wenn sich somit aus den erwähnten Bestimmungen der genaue Umfang der Datenbearbeitung bzw. der Datenbekanntgabe nur in groben Zügen ergibt, so dass es zweifelhaft sein könnte, ob den Anforderungen an eine hinreichende Bestimmtheit der gesetzlichen Grundlage im vorliegenden Zusammenhang entsprochen wird, ist aber jedenfalls zu beachten, dass Art und Umfang der zu übermittelnden Daten durch Auslegung ermittelt werden können und durch ergänzende Beschlüsse (insbesondere der Kommission bzw. der Verwaltungskommission) im Einzelnen präzisiert werden, ein Vorgehen, das bereits in den Verordnungen selbst vorgesehen ist. So werden in den sog. SEDs die betroffenen Daten im Einzelnen aufgeführt, so dass auf dieser Grundlage eine hohe Präzision anzunehmen ist. Insofern erscheint es vertretbar, die (zugegebenermassen selbst nicht sehr präzisen) Vorgaben der **Verordnungen als ausreichende formell-gesetzliche Grundlagen** anzusehen, die jedoch der Präzisierung bedürfen, die insbesondere durch die SEDs erfolgt ist.[220]

Wenn die VO 883/2004 und 987/2009 nicht als ausreichende gesetzliche Grundlage für die grenzüberschreitende Datenbekanntgabe im Rahmen des EESSI durch schweizerische Behörden bzw. Bundesorgane anzusehen wären, dürfte die Datenbekanntgabe nur gestützt auf eine gesetzliche Grundlage im **nationalen Recht** erfolgen. Dies stellt auch keinen Widerspruch zu der sich aus den genannten Verordnungen bzw. dem Personenfreizügigkeitsabkommen ergebenden Pflicht der Schweiz dar, für eine derartige Datenübermittlung (auf elektronischem Weg) zu sorgen, wobei im Einzelnen die Vorgaben der Verordnungen zu beachten sind. Denn auch wenn Verordnungen unmittelbar anwendbar sind, gibt es doch häufig **Verordnungsbestimmungen, die einer nationalen Durchführung** bedürfen, und es bleibt den Mitgliedstaaten bzw. den beteiligten Staaten unbenommen, hier die nationalen Vorgaben zu beachten (unter der Voraussetzung, dass die effektive Beachtung des Unionsrechts bzw. des Personenfreizügigkeitsabkommens nicht beeinträchtigt wird). Für diese Sicht spricht auch, dass sich aus den Verordnungen ergibt, dass für die Datenbearbeitung durch nationale Behörden oder Träger eben das nationale Datenschutzrecht Anwendung findet (vgl. insbesondere Art. 77 VO 883/2004).[221]

Im Übrigen stellen die Verordnungen eine **genügende gesetzliche Grundlage für weitere Pflichten bzw. Vorhaben** dar. Dies gilt insbesondere für die Einrichtung des *electronic directory* (vgl. Art. 88 i.V.m. Anhang 4 VO 987/2009) sowie für gewisse (Auskunfts-) Pflichten der in den persönlichen Anwendungsbereich der Verordnungen fallenden Versicherten. In Bezug auf das *electronic directory* bzw. die Rechtsgrundlagen für seine Einrichtung ist noch

---

220 Zu beachten gilt es allerdings, dass der EuGH die Beschlüsse der Verwaltungskommission in seiner ständigen Rechtsprechung nicht als rechtsverbindlich erachtet, sondern diese lediglich als Hilfsmittel qualifiziert. S. EuGH, Rs. 89/80 (Romano), Slg. 1981, 1241, Rn. 20; EuGH, Rs. C-102/91 (Knoch), Slg. 1992, I-4341, Rn. 52; EuGH, Rs. C-202/97 (Fitzwilliam), Slg. 2000, I-883, Rn. 32. Diesem Argument könnte jedoch entgegengehalten werden, dass diese Rechtsprechung nicht auf Grundlage der neuen Verordnungen 883/2004 und 987/2009 ergangen ist und dass die Verwaltungskommission durch Art. 4 Abs. 1 VO 987/2009 gesetzlich explizit ermächtigt wird, die Struktur, den Inhalt, das Format und die Verfahren im Einzelnen festzulegen.

221 An dieser Stelle ist noch anzufügen, dass der deutsche Bundesbeauftragte für den Datenschutz und die Informationsfreiheit in seinem Tätigkeitsbericht zum Schluss kam, dass die in der VO 883/2004 und VO 987/2009 verankerten Bestimmungen den datenschutzrechtlichen Anforderung nicht genügten. Deshalb wurde in Deutschland das „Gesetz zur Koordinierung der Systeme der sozialen Sicherheit in Europa“ erlassen, welches die entsprechenden konkretisierenden Bestimmungen enthält. S. dazu den 24. Tätigkeitsbericht zum Datenschutz für die Jahre 2011 und 2012 des Bundesbeauftragten für den Datenschutz und die Informationsfreiheit, 33. In anderen Mitgliedstaaten hingegen wurden offenbar keine solchen nationalen Durchführungsvorschriften erlassen, sondern die unionsrechtlichen Bestimmungen werden als ausreichende gesetzliche Grundlagen für die grenzüberschreitende Datenbekanntgabe angesehen.

hinzuzufügen, dass es hier nur – aber immerhin – um dieses Verzeichnis als solches geht, das letztlich eine Liste von Kontaktadressen darstellt, dessen konkrete (elektronische) Gestaltung eine effiziente (automatisierte) Übermittlung der relevanten Daten erlauben soll. Hingegen stellen weder das *electronic directory* selbst noch die für seine Einrichtung massgeblichen Rechtsgrundlagen eine gesetzliche Grundlage für einen irgendwie gearteten Datenaustausch dar, geht es hier doch nur um die Verpflichtung, eine derartige Liste nach den Vorgaben der Verordnung zu erstellen und für deren Aktualität zu sorgen. Ebensowenig vermag die Aufnahme einer bestimmten Institution in das *electronic directory* Zuständigkeiten der betreffenden Institution zu begründen; hierfür ist vielmehr das nationale Recht einschlägig.
Somit kann abschliessend zu den in unserem Zusammenhang möglicherweise relevanten Bestimmungen in den **VO 883/2004 und 987/2009** festgehalten werden, dass diese die **Zusammenarbeit zwischen den Behörden und Trägern in grundlegender Weise regeln** sowie einige **Rechtspflichten der betroffenen Personen** vorsehen. Darüber hinaus umschreiben sie den Bearbeitungszweck und lassen die an der Bearbeitung beteiligten Stellen erkennen. Der **Umfang der Datenbearbeitung bzw. der Datenbekanntgabe** wird in groben Zügen umschrieben, und die diesbezüglichen Präzisierungen finden sich im Durchführungsrecht. Insofern könnten zwar Zweifel daran bestehen, ob die gesetzlichen Grundlagen die geforderte Präzision für den vorgesehenen grenzüberschreitenden Datenaustausch aufweisen; dies erscheint jedoch vertretbar.

2. Zu den möglichen gesetzlichen Grundlagen im geltenden schweizerischen Recht

Die im EESSI vorgesehene grenzüberschreitende Datenübermittlung von einer Verbindungsstelle bzw. einem Träger zu einer ausländischen Behörde über die nationale Zugangsstelle könnte darüber hinaus möglicherweise auf eine Rechtsgrundlage im geltenden schweizerischen Recht gestützt werden. In der Tat enthält die **schweizerische Gesetzgebung zum Sozialversicherungsrecht** an verschiedenen Orten Bestimmungen zum Informationsaustausch zwischen sozialen Einrichtungen bzw. Sozialversicherungsträgern. Neben den im ATSG verankerten allgemeinen Bestimmungen (a) sind insbesondere die in den verschiedenen Spezialgesetzen figurierenden Regelungen (b) auf ihre Geeignetheit als gesetzliche Grundlagen zu überprüfen, bevor ein kurzes Fazit gezogen wird (c); bei den in Betracht kommenden Rechtsgrundlagen handelt es sich jeweils um Bundesgesetze, so dass das Erfordernis der formellgesetzlichen Grundlage erfüllt ist bzw. wäre.

a) Allgemeine Bestimmungen im ATSG

Das **Bundesgesetz über den allgemeinen Teil des Sozialversicherungsrechts (ATSG)** koordiniert das Sozialversicherungsrecht des Bundes und ist gemäss Art. 2 ATSG auf alle bundesgesetzlich geregelten Sozialversicherungen anwendbar, sofern dies in den einzelnen Spezialgesetzen vorgesehen ist. Die für den grenzüberschreitenden Datenaustausch (möglicherweise) relevanten Bestimmungen des ATSG sind somit nur dann von Bedeutung, wenn im entsprechenden Bundesgesetz auf das ATSG verwiesen wird. Im Rahmen der AHV und der IV sowie der Unterstellung ist das ATSG auf der Grundlage von Art. 1 Abs. 1 AHVG grundsätzlich anwendbar, soweit das AHVG keine abweichenden Bestimmungen enthält. Das ATSG enthält denn auch verschiedene Bestimmungen, die *a priori* als gesetzliche Grundlagen für einen grenzüberschreitenden Datenaustausch, so wie er im Rahmen des EESSI vorgesehen ist, in Betracht kommen könnten.

Fraglich könnte jedoch sein, ob diese angesichts der in **Art. 33 ATSG** verankerten **Schweigepflicht** zum Zuge kommen können. Denn nach dieser Vorschrift werden die an der Durchführung sowie der Kontrolle oder der Beaufsichtigung der Durchführung der Sozialversicherungsgesetze beteiligten Personen dazu verpflichtet, gegenüber Dritten Verschwiegenheit zu bewahren. Als einer der Zwecke dieser Bestimmung ist der Persönlichkeitsschutz der versicherten Person zu nennen. Die betroffene Person soll darauf vertrauen können, dass die sie betreffenden Informationen nicht weitergegeben werden.[222] Strafrechtlich werden diese Personen alsdann durch Art. 320 StGB geschützt, der die Verletzung eines Amtsgeheimnisses unter Strafe stellt.[223] Gemäss Art. 19 Abs. 4 lit. b DSG steht eine solche Schweigepflicht grundsätzlich der Bekanntgabe von Personendaten entgegen; Ausnahmen davon sind allerdings möglich, wenn das betreffende Einzelgesetz dies vorsieht.[224] Da Art. 33 ATSG jedoch nicht selbst Ausnahmen von der Schweigepflicht vorsieht, ist umstritten, in welchem Verhältnis die Bestimmungen des ATSG – insbesondere Art. 32 ATSG betreffend die Amts- und Verwaltungshilfe – zur Schweigepflicht stehen.[225] U.E. sprechen im Ergebnis die besseren Gründe dafür, dass **Ausnahmen von der in Art. 33 ATSG verankerten Schweigepflicht** nicht nur aufgrund von Bestimmungen in einzelnen **Spezialgesetzen**, sondern auch aufgrund der im **ATSG** selbst enthaltenen Vorschriften zum Zuge kommen könnten.[226] Denn auch wenn in einem solchen Fall der Grundsatz *lex specialis derogat legi generali* nicht (zwin-

---

222 *Kieser*, ATSG-Kommentar, Art. 33, Rn. 3, 5.

223 *Pärli*, Gutachten IIZ, 22.

224 BBl 2000 261; *Kieser*, ATSG-Kommentar, Art. 33, Rn. 13; *Jöhri*, in: Rosenthal/Jöhri, Handkommentar DSG, Art. 19, Rn. 102 f.; *Ehrensperger/Moser*, in: Maurer-Lambrou/Blechta, BK Datenschutzgesetz, Öffentlichkeitsgesetz, Art. 19, Rn. 67.

225 Siehe *Kieser*, ATSG-Kommentar, Art. 33 Rn. 5 und Art. 32 Rn. 3, der die in Art. 32 geregelte Amts- und Verwaltungshilfe als Ausnahme von der Schweigepflicht ansieht. *Weibel* vertritt dagegen die Ansicht, dass die Voraussetzungen von Art. 32 und 33 ATSG in jedem Fall kumulativ zu prüfen sind, siehe dazu *Weibel*, Plädoyer 4/2011, 34 (39).

226 So auch *Kieser*, ATSG-Kommentar, Art. 31, Rn. 5; Art. 33, Rn. 15 ff.; ebenso *Prieur*, in: Passadelis/Rosenthal/Thür, Datenschutzrecht, § 13, Rn. 13.50; vgl. dazu auch BBl 2000 260, 262.

gend) greift, ist nicht ersichtlich, weshalb die in den Spezialgesetzen verankerten Rechtsvorschriften zur Datenbekanntgabe eine Ausnahme darstellen können, ohne dass dies für die zugrunde liegenden, allgemeinen Rechtsbestimmungen des ATSG gälte.[227] Durch die Ausnahmeregelungen in den Spezialgesetzen soll es vielmehr möglich sein, eine über die allgemeinen Bestimmungen des ATSG hinausgehende Datenbekanntgabe zu erlauben.[228]

Damit sind im Folgenden diejenigen Bestimmungen des **ATSG** auf ihre Eignung als gesetzliche Grundlage für die grenzüberschreitende Datenbekanntgabe im Rahmen des EESSI zu überprüfen, die (auch) als **Ausnahme zur allgemeinen Schweigepflicht** in Betracht kommen. Dies sind in erster Linie Art. 28 Abs. 3 ATSG (Ermächtigung zur Auskunftserteilung), Art. 31 Abs. 2 ATSG (Meldepflicht bei geänderten Verhältnissen), Art. 47 ATSG (Akteneinsicht) und Art. 32 ATSG (Amts- und Verwaltungshilfe):

- Gemäss **Art. 28 Abs. 3 ATSG** sind alle Personen und Stellen, namentlich Arbeitgeber, Ärztinnen und Ärzte, Versicherungen sowie Amtsstellen, im Einzelfall von der die Leistung beanspruchenden Person zu ermächtigen, die für die **Abklärung von Leistungsansprüchen erforderlichen Auskünfte** zu erteilen. Anwendbar ist Art. 28 Abs. 3 ATSG demnach nur im Fall eines Leistungsverfahrens, nicht aber beispielsweise im Rahmen der Verfahren betreffend die Unterstellung.[229] Zudem betrifft Art. 28 Abs. 3 ATSG nur die Auskunftserteilung; andere Mitwirkungsarten, wie die Herausgabe von Akten, sind davon nicht erfasst.[230] Massgeblich ist hier ferner, dass sich die Ermächtigung nur auf die im Einzelfall erforderlichen Auskünfte bezieht. Eine generelle Auskunftsermächtigung kann daher nicht auf diese Vorschrift gestützt werden.[231]
- Nach **Art. 31 Abs. 2 ATSG** hat die an der Durchführung der Sozialversicherung beteiligte Person oder Stelle den **Versicherungsträgern Änderungen der für die Leistung massgebenden Verhältnisse zu melden**, wenn sie hiervon Kenntnis erhalten. Damit wird allerdings lediglich der Informationsaustausch im Fall von geänderten Verhältnissen, die Auswirkungen auf den Leistungsanspruch haben, geregelt.[232] Ist eine Weitergabe von Daten in anderen Konstellationen geboten, so kann Art. 31 Abs. 2 ATSG nicht als Rechtsgrundlage herangezogen werden.

  Ergänzend ist aber in diesem Zusammenhang darauf hinzuweisen, dass der Informationsaustausch nach Art. 31 Abs. 2 ATSG – im Gegensatz zur allgemeinen Verwaltungshilfe i.S.v. Art. 32 ATSG – kein Ersuchen des Versicherungsträgers voraussetzt. Vielmehr haben alle an der Durchführung der Sozialversicherung beteiligten Personen und Stellen die geänderten Verhältnisse dem Versicherungsträger mitzuteilen, sobald sie davon Kenntnis erhalten haben. So kann beispielsweise eine IV-Stelle dazu angehalten

227 S. auch *Belser/Noureddine*, in: Belser/Epiney/Waldmann, Datenschutzrecht, § 7, Rn. 84, wo für die Begründung einer Ausnahme zur Schweigepflicht eine gesetzliche Grundlage verlangt wird.

228 BBl 2000 260; s. auch *Belser/Noureddine*, in: Belser/Epiney/Waldmann, Datenschutzrecht, § 7, Rn. 84.

229 *Kieser*, ATSG-Kommentar, Art. 28, Rn. 6.

230 *Kieser*, ATSG-Kommentar, Art. 28, Rn. 34.

231 BBl 1999 4584; BGer, Urteil 9C_250/2009 vom 29.09.2009 E.3.3; *Kieser*, ATSG-Kommentar, Art. 28, Rn. 36 f.; *Gächter/Siki*, Sozialversicherungsrecht, 90.

232 S. dazu *Kieser*, ATSG-Kommentar, Art. 31, Rn. 6.

sein, die beteiligte Unfallversicherung über die Änderungen des Gesundheitszustands, welcher einen Einfluss auf die Beurteilung des Invaliditätsgrades hat, zu informieren.[233]

- Nach **Art. 47 ATSG** steht gewissen Behörden und Personen, unter der Voraussetzung, dass überwiegende Privatinteressen gewahrt bleiben, ein **Recht auf Akteneinsicht** zu. Von Bedeutung ist dabei insbesondere Art. 47 lit. b ATSG, der den Parteien zur Wahrung oder Erfüllung eines Anspruches oder einer Pflicht bzw. zur Ergreifung eines Rechtsmittels Einsicht in die dafür benötigten Daten gewährt. Vorausgesetzt ist allerdings, dass die um Akteneinsicht ersuchende Sozialversicherungsanstalt als **Partei im Sinne von Art. 34 ATSG** angesehen werden kann.[234] Ausserdem muss sich das Gesuch um Akteneinsicht auf ein noch nicht abgeschlossenes Verfahren beziehen.[235]

  Gemäss Art. 34 ATSG gilt eine Sozialversicherungseinrichtung dann als Partei, wenn ihr ein Rechtsmittel gegen die Verfügung eines Versicherungsträgers oder eines ihm gleichgestellten Durchführungsorgans zusteht.[236] Zur Bestimmung der im Einzelfall in Frage kommenden sozialen Einrichtungen muss demnach auf die in Art. 59 ATSG und Art. 89 BGG geregelte Beschwerdebefugnis zurückgegriffen werden.[237] Zu nennen ist hier auch Art. 49 Abs. 4 ATSG, der dem durch eine Verfügung eines anderen Versicherungsträgers berührten Träger dasselbe Rechtsmittel einräumt wie der versicherten Person. Mit dieser Regelung wird jedoch lediglich auf Art. 59 ATSG Bezug genommen; eine Einschränkung oder Ausweitung der Beschwerdebefugnis kann sich daraus nicht ergeben.[238] Art. 59 ATSG setzt voraus, dass der um Akteneinsicht ersuchende Träger durch die Verfügung des anderen Trägers berührt wird und ein schutzwürdiges Interesse an der Änderung oder Aufhebung der Verfügung hat. Berührtsein bedeutet, dass der Träger im Bereich der Leistungskoordination durch die Verfügung des anderen Versicherungsträgers in seinen rechtlichen oder tatsächlichen Interessen spürbar betroffen ist. Dass die Verfügung bei der eigenen Entscheidung lediglich mitzuberücksichtigen ist, ohne dass der betreffende Träger daran gebunden wäre, reicht dafür nicht aus. Ein Berührtsein kann jedoch dann angenommen werden, wenn der Träger von Gesetzes wegen bzw. aufgrund der Gerichtspraxis an die Entscheidung des anderen Versicherungsträgers gebunden ist, wie dies in Bezug auf eine Vorsorgeeinrichtung beispielsweise bei der Feststellung des Invaliditätsgrades durch die zuständige IV-Stelle der Fall ist.[239]
  Die Gewährung der Akteneinsicht ist aber nur insofern zulässig, als die Daten für die Erfüllung einer Verpflichtung nach dem Sozialversicherungsgesetz erforderlich sind und die überwiegende Privatinteressen gewahrt bleiben.[240] Bei der Interessenabwägung ist namentlich das private Interesse des Versicherten, dass ihn betreffende heikle Informationen nicht weitergegeben werden, miteinzubeziehen.[241]

- Im Vergleich zu den bisher erwähnten Rechtsbestimmungen, die sich allesamt mit spezifischen Fällen der Auskunftserteilung befassen, sieht **Art. 32 ATSG** eine **allgemeine Amts- und Verwaltungshilfe** vor. Die grenzüberschreitende Datenübermittlung von einer schweizerischen Verbindungsstelle oder einem Träger an eine ausländische Behörde betrifft die in Art. 32 Abs. 2 ATSG verankerte Verwaltungshilfe, die

233 *Kieser*, ATSG-Kommentar, Art. 31, Rn. 25, Art. 32, Rn. 7.
234 *Kieser*, ATSG-Kommentar, Art. 47, Rn. 17.
235 *Weibel*, Plädoyer 4/2011, 34 (39); *Kieser*, ATSG-Kommentar, Art. 28, Rn. 15.
236 Vgl. auch *Kieser*, ATSG-Kommentar, Art. 28, Rn. 13.
237 *Kieser*, ATSG-Kommentar, Art. 34, Rn. 12; auch für die Legitimation zur Einsprache ist Art. 59 ATSG massgebend, fehlt doch die entsprechende Regelung in Art. 52 ATSG, siehe *Kieser*, ATSG-Kommentar, Art. 49, Rn. 63.
238 Vgl. *Kieser*, ATSG-Kommentar, Art. 49, Rn. 63.
239 *Kieser*, ATSG-Kommentar, Art. 49, Rn. 49 f. Zum Beispiel der Bindung einer Vorsorgeeinrichtung an die Bestimmung des Invaliditätsgrades durch die zuständige IV-Stelle siehe BGE 123 V 269 E. 2.a). Abzulehnen ist gemäss bundesgerichtlicher Rechtsprechung hingegen die Bindung eines Unfallversicherers an die zuletzt genannte Entscheidung einer IV-Stelle, vgl. BGE 132 V 1 E. 3.1.
240 BBl 2000 264; siehe dazu auch weiter unten D.II.3.a)aa).
241 *Kieser*, ATSG-Kommentar, Art. 47, Rn. 15.

unter den gleichen Voraussetzungen wie die Amtshilfe nach Abs. 1 zu gewähren ist.[242] Demgemäss geben die Organe der einzelnen Sozialversicherungen einander auf schriftliche und begründete Anfrage im Einzelfall kostenlos diejenigen Daten bekannt, die für die Erfüllung der in lit. a-d genannten Aufgaben erforderlich sind. In einer abschliessenden[243] Liste enthält Art. 32 Abs. 1 ATSG die Zwecke, zu deren Erfüllung die Daten notwendig sein müssen. Dazu gehören gemäss Gesetz die Festsetzung, Änderung oder Rückforderung von Leistungen (lit. a), die Verhinderung ungerechtfertigter Bezüge (lit. b), die Festsetzung und den Bezug der Beiträge (lit. c) und der Rückgriff auf haftpflichtige Dritte (lit. d). In persönlicher Hinsicht bezieht Art. 32 Abs. 2 ATSG mit dem Begriff der Organe der einzelnen Sozialversicherungen – ein eher weit gefasster Ausdruck[244] – nicht nur die schweizerischen Verbindungsstellen und Träger, sondern auch die ausländischen Versicherungsträger als Empfänger mit ein.[245] Einschränkend darf aber eine Datenbekanntgabe nur stattfinden, falls sie auf einer schriftlichen und begründeten Anfrage beruht. Eine Auskunftserteilung ohne vorangehendes Gesuch wird damit ausgeschlossen.[246] Mit der Begründung soll sichergestellt werden, dass die Anfrage für den ersuchten Träger nachvollziehbar ist, weshalb damit wohl keine besonders hohen Anforderungen einhergehen.[247] Da die Verwaltungshilfe gemäss Art. 32 Abs. 1 ATSG nur im konkreten Einzelfall erfolgen darf, ist der Austausch einer unbestimmten Anzahl von Daten davon ausgenommen. Eine zulässige Verwaltungshilfe im Sinn von Art. 32 ATSG setzt zudem voraus, dass nur diejenigen Daten bekannt gegeben werden, die für die Erfüllung einer in Art. 32 Abs. 1 ATSG genannten Aufgaben benötigt werden. Dies bedeutet, dass die Informationen nur insoweit an andere Träger zu übermitteln sind, als sich diese Stellen diese Daten ohne die Übermittlung nur unter erheblichem Mehraufwand beschaffen könnten.[248] Deshalb ist vorgängig der Zugang zu den betreffenden Informationen im Rahmen der Mitwirkungspflichten zu untersuchen.[249] Ob die Datenbekanntgabe in diesem Sinn tatsächlich erforderlich ist, wird – wie auch der Grundsatz der Verhältnismässigkeit im Allgemeinen – in einer Interessensabwägung geprüft.[250]

---

242 *Kieser*, ATSG-Kommentar, Art. 32, Rn. 8.

243 S. unter Anführung eines Beispiels für die weit gefasste Bedeutung der aufgezählten Zwecke *Prieur*, in: Passadelis/Rosenthal/Thür, Datenschutzrecht, § 13, Rn. 13.41, dazu auch weiter unten im Text.

244 Vgl. *Kieser*, ATSG-Kommentar, Art. 32, Rn. 13, der jeden Versicherungsträger und jedes Organ in der Durchführung der Sozialversicherung darunter subsumiert.

245 Für den Miteinbezug ausländischer Institutionen spricht im konkreten Fall auch Art. 76 Abs. 2 VO 883/2004, wonach Anfragen ausländischer Institutionen so zu behandeln sind, als handle es sich um eine innerstaatliche Angelegenheit. S. insoweit bereits oben D.I.1.a).

246 Zur weitergehenden rechtlichen Tragweite von Art. 31 Abs. 2 ATSG s. bereits oben im Text.

247 BBl 2000 262; *Kieser*, ATSG-Kommentar, Art. 32, Rn. 14; *Weibel*, Plädoyer 4/2011, 34 (37).

248 *Prieur*, in: Passadelis/Rosenthal/Thür, Datenschutzrecht, § 13, Rn. 13.40.

249 *Eugster/Luginbühl*, in: Datenschutz im Gesundheitswesen, 73 (129); *Kieser*, ATSG-Kommentar, Art. 32, Rn. 16; *Weibel*, Plädoyer 4/2011, 34 (37).

250 *Kieser*, ATSG-Kommentar, Art. 32, Rn. 16. In Bezug auf die Erforderlichkeit einer Datenbekanntgabe kam das Bundesgericht im BGE 136 V 2 zum Schluss, dass die den Fall betreffenden Daten der IV-Stelle für die Unfallversicherung zwecks Verhinderung ungerechtfertigter Bezüge (Art. 32 Abs. 1 lit. b

Für den **grenzüberschreitenden Datenaustausch** von einer schweizerischen Verbindungsstelle oder einem Träger an eine ausländische Sozialversicherungsstelle sind die im ATSG verankerten Bestimmungen als gesetzliche Grundlagen durchaus **in Betracht zu ziehen**, wobei die Tragweite der einzelnen Regelungen jedoch unterschiedlich ausfällt. Die Einrichtung eines eigentlichen **Informationssystems zum grenzüberschreitenden Austausch von Personendaten** im Hinblick auf die Koordinierung der Systeme der sozialen Sicherheit – so wie es im Rahmen des EESSI stattfinden soll – ist jedoch nicht erwähnt bzw. vorgesehen. Sie dürfte denn auch im Ergebnis durch die angeführten Bestimmungen nicht gedeckt sein bzw. diese stellen hierfür wohl **keine genügenden gesetzlichen Grundlagen** dar:

- Der **Anwendungsbereich des Art. 28 Abs. 3 ATSG** ist insofern **beschränkt**, als nur Leistungsverfahren erfasst werden. Der grenzüberschreitende Informationsaustausch im Rahmen der Unterstellung ist davon ausgeschlossen. Dazu kommt, dass unter Umständen im Rahmen des EESSI nicht nur Auskünfte erteilt werden, sondern auch Unterlagen zirkulieren, was nicht in den Anwendungsbereich von Art. 28 Abs. 3 ATSG fällt. Ausserdem scheint zweifelhaft, ob angesichts des Ausmasses des zu erfolgenden Datenaustauschs mit dem Ausland eine Einzelermächtigung i.S.v. Art. 28 Abs. 3 ATSG überhaupt auszureichen vermag. Datenschutzrechtlich handelt es sich bei einer solchen Einzelermächtigung jedenfalls um eine Einwilligung,[251] die jedoch nur im Einzelfall eine gesetzliche Grundlage zu ersetzen vermag.[252]
- Erhält eine Verbindungsstelle oder ein Träger Kenntnis von einer geänderten Sachlage, so haben sie dies aufgrund von **Art. 31 Abs. 2 ATSG** den davon betroffenen ausländischen Versicherungsträgern mitzuteilen. Da diesbezüglich keine spezialgesetzlichen Normierungen bestehen, spricht Vieles dafür, dass sich die betreffende Verbindungsstelle oder der Träger für die Datenbekanntgabe ins Ausland auf Art. 31 Abs. 2 ATSG stützen kann.[253] Allerdings ist die Norm **nicht genügend präzise und bestimmt**, um als gesetzliche Grundlage im Sinne von Art. 19 i.V.m. Art. 17 DSG für die Einrichtung eines Informationssystems wie das EESSI angesehen werden zu können. Aus Art. 31 Abs. 2 ATSG ist zwar der Zweck der zu erfolgenden Datenbearbeitung bzw. ihr grober Anwendungsbereich ersichtlich. Hingegen geht aus der Norm nicht hervor, dass bei der grenzüberschreitenden Datenübermittlung durchaus auch besonders schützenswerte Personendaten übermittelt werden könnten. Überdies und vor allem ist die Bestimmtheit von Art. 31 Abs. 2 ATSG auch deshalb als ungenügend zu betrachten, weil die Art und das Ausmass der Datenbearbeitungen zu wenig genau dargelegt werden. Dass auch grenzüberschreitende Datenübermittlungen stattfinden

---

ATSG) erforderlich waren. Der Grund dafür war, dass die IV-Akten relevante Informationen hätten enthalten können, die darüber Aufschluss geben, ob jemals eine Verletzung im Sinn des Unfallversicherungsrechts diagnostiziert wurde.

251 Siehe auch *Weibel*, Plädoyer 4/2011, 34 (41).

252 S. insoweit schon oben C.II.1.

253 *Kieser*, ATSG-Kommentar, Art. 31, Rn. 28.

und eine grosse Anzahl ausländischer Versicherungsträger in elektronischer Form informiert werden könnten, lässt sich aus dem Wortlaut von Art. 31 Abs. 2 ATSG nicht ableiten. Grundsätzlich kann nämlich eine derart allgemein und generisch gefasste Bestimmung keinesfalls eine gesetzliche Grundlage für ein doch sehr ausdifferenziertes Informationssystem, innerhalb desselben eine Vielzahl von Daten grenzüberschreitend übermittelt werden (unter Einschluss besonders schützenswerter Personendaten), darstellen; hierfür ist vielmehr eine spezifische gesetzliche Grundlage erforderlich.

Schliesslich gilt es noch anzufügen, dass im Rahmen des EESSI-Systems eine Meldung aufgrund veränderter Verhältnisse ohnehin kaum von Bedeutung sein dürfte, da gemäss dem europäischen System zur Koordinierung der sozialen Sicherheit eine Einzelperson einer nationalen Gesetzgebung in Bezug auf sämtliche Sozialversicherungen unterstellt ist.[254] Die Meldepflicht aufgrund von veränderten Verhältnissen dürfte demnach grundsätzlich nur dann grenzüberschreitend relevant sein, wenn sie sich einerseits auf für die Bestimmung des Anwendungszeitpunkts relevante Tatsachen bezieht oder aber wenn andererseits für die Beurteilung eines Leistungsanspruches mehrere verschiedene Rechtsordnungen anwendbar sind und sich deren Entscheidungen gegenseitig beeinflussen.

- Das **Akteneinsichtsrecht** nach **Art. 47 lit. b ATSG** kann nur dann als rechtliche Grundlage für die grenzüberschreitende Datenübermittlung herangezogen werden, wenn die ausländischen Versicherungsträger unter den Begriff der **Partei i.S.v. Art. 34 ATSG** fallen. Dafür muss der ausländische Träger gemäss Art. 49 Abs. 4 ATSG durch die Verfügung des inländischen Trägers in seinen rechtlichen oder tatsächlichen Interessen betroffen sein. Entscheidend ist, ob der ausländische Träger die schweizerische Verfügung lediglich zu berücksichtigen hat oder ob er aufgrund einer Gesetzesnorm oder der Rechtsprechung an diese gebunden ist. Eine solche Bindung dürfte hier wohl zu verneinen sein, da das europäische Koordinierungssystem keine Harmonisierung der verschiedenen Gesetzgebungen beinhaltet. Vielmehr können die Mitgliedstaaten beispielsweise frei entscheiden, welcher Betrag auf der Grundlage ihrer nationalen Sozialversicherungsgesetzgebung zuzusprechen ist. Folglich kann Art. 47 lit. b ATSG grundsätzlich keine gesetzliche Grundlage für die grenzüberschreitende Datenübermittlung darstellen.
- Die **allgemeine Verwaltungshilfe** nach **Art. 32 ATSG** ist einzig zur Erfüllung der in Abs. 1 genannten Zwecke zulässig. Der grenzüberschreitende Datenaustausch des EESSI-Systems betrifft wohl hauptsächlich die Festsetzung der Beträge im Sinn von Art. 32 Abs. 1 lit. a ATSG. Doch kommt im Fall einer Datenübermittlung im Rahmen eines Verfahrens betreffend die Unterstellung keiner der erwähnten Zwecke in Betracht. Auch wenn man den Begriff der „Festsetzung von Leistungen“ weit auslegt,[255] kann dieser Informationsaustausch nicht mehr unter Art. 32 Abs. 1 lit. a ATSG fallen. Im Übrigen ist fraglich, ob der grenzüberschreitende Datenaustausch des EESSI-Systems auf einem schriftlichen und begründeten Gesuch beruht. Werden die elektro-

254 Art. 11 Abs. 1 VO 883/2004.

255 Vgl. *Kieser*, ATSG-Kommentar, Art. 32, Rn. 17, der eine enge Auslegung der in Art. 32 Abs.1 ATSG erwähnten Zwecke ablehnt.

nischen Dokumente, wie bisher geplant,[256] nur in einer bestimmten Abfolge ausgetauscht, so kann grundsätzlich davon ausgegangen werden, dass jeder Informationsmitteilung eine Anfrage (*request*) des ersuchenden Trägers vorangeht.[257] Jedoch richtet der ersuchende Träger seine Anfrage im Rahmen des EESSI in elektronischer Form an den Empfänger. Ein nach Art. 32 ATSG gefordertes schriftliches und begründetes Gesuch dürfte demzufolge nicht vorliegen. Zudem erscheint Art. 32 ATSG vor dem Hintergrund, dass unter Umständen besonders schützenswerte Personendaten über die Grenze hinweg ins Ausland übertragen werden, als zu wenig bestimmt. Denn auch hier gilt (wie schon in Bezug auf Art. 31 Abs. 2 ATSG), dass eine solche allgemein gefasste Bestimmung keinesfalls eine gesetzliche Grundlage für ein doch sehr ausdifferenziertes Informationssystem, innerhalb desselben eine Vielzahl von Daten grenzüberschreitend übermittelt werden (unter Einschluss besonders schützenswerter Personendaten), darstellen kann.

b) Spezialgesetzliche Bestimmungen

Neben den erörterten allgemeinen, im ATSG enthaltenen Bestimmungen könnten auch die in diversen **Spezialgesetzen** (im Bereich der Sozialversicherungen) verankerten Regelungen als Ausnahmen in Bezug auf die in Art. 33 ATSG vorgesehene Schweigepflicht und – daran anschliessend – als gesetzliche Grundlagen für einen grenzüberschreitenden Datenaustausch im Rahmen des EESSI in Betracht kommen, wobei es im vorliegenden Rahmen um die Alters-, Hinterlassenen- und Invalidenversicherung sowie die Feststellung des anwendbaren Rechts im Rahmen der Entsendung bzw. der Beschäftigung in mehreren Staaten geht.

Da der Fokus auf der AHV/IV sowie auf der Unterstellung liegt, werden die Rechtsgrundlagen nur insoweit beleuchtet, als der grenzüberschreitende Datenaustausch in den erwähnten Bereichen betroffen ist. Ausser Acht gelassen werden hingegen die gesetzlichen Grundlagen in den schweizerischen Sozialversicherungsgesetzen betreffend den Datenaustausch im Bereich anderer Sozialversicherungszweige.

Im Bereich der **Alters-, Hinterlassenen- und Invalidenversicherung** nimmt die **zentrale Ausgleichsstelle der AHV (ZAS) als Verbindungsstelle die grenzüberschreitende Datenübermittlung** vor und hat sich als solche auf eine gesetzliche Grundlage zu stützen. Je nachdem, welches Verfahren durch das Gesuch der Einzelperson eingeleitet wurde, handelt die ZAS in **Anwendung des AHVG oder des IVG**. Für die Datenbekanntgabe bezieht sich der massgebliche **Art. 66a Abs. 2 IVG** bezüglich der nicht in Abs. 1 geregelten Datenübermitt-

256 S.o. B.I.

257 Vgl. das in den Guidelines beschriebene Verfahren des Datenaustausches, Guidelines for the use of Horizontal SEDs and Flows des EESSI, Kreisschreiben des INPS Nr. 167 vom 29.12.2011, Anlage 6; Guidelines for the use of Pension SEDs, Flows and Portable Document P1 des EESSI, Kreisschreiben des INPS Nr. 156 vom 15.12.2011, Anlage 5; Guidelines for the use of Applicable Legislation SEDs, Flows and Portable Document A1 des EESSI, Kreisschreiben des INPS Nr. 167 vom 29.12.2011, Anlage 5.

lungen auf die **sinngemässe Anwendung von Art. 50a AHVG**, der die Datenbekanntgabe im Rahmen der AHV normiert. Deshalb ist, unabhängig davon, ob es sich um ein IV- oder ein AHV-Verfahren handelt, auf alle Fälle Art. 50a AHVG zu beachten.

Hingegen ist die konkrete Ausgestaltung der grenzüberschreitenden Datenübermittlung im Bereich der Unterstellung weitgehend ungewiss. An dieser Stelle kann deshalb lediglich darauf hingewiesen werden, dass diese Bekanntgabe wohl durch die für die Beurteilung solcher Fälle zuständigen Stellen – d.h. durch das BSV und/oder die AHV-Ausgleichskassen – vollzogen wird. Jedenfalls kann auch hier auf Art. 50a AHVG zurückgegriffen werden, da sowohl das BSV auch die AHV-Ausgleichskassen dabei in Anwendung des AHVG tätig werden.

Art. 50a AHVG sieht verschiedene Konstellationen vor, bei deren Vorliegen eine Datenbekanntgabe durch Organe, die mit der Durchführung, der Kontrolle oder der Beaufsichtigung der Durchführung des AHV-Gesetzes betraut sind, erfolgen darf. Diese Vorschriften stellen somit nicht nur Ausnahmen von der Schweigepflicht nach Art. 33 ATSG, sondern auch **gesetzliche Grundlagen für die erfasste Datenbekanntgabe** dar, wobei in unserem Zusammenhang folgende Fallgestaltungen (*a priori*) einschlägig sein könnten:

- **Art. 50a Abs. 1 lit. a AHVG** bezieht sich auf eine **Datenbekanntgabe von einem mit der Durchführung des AHVG beauftragten Organs** an ein **anderes mit der Durchführung sowie der Kontrolle oder der Beaufsichtigung der Durchführung dieses Gesetzes betrautes Organ**.[258] Die ausländischen sozialen Institutionen sind nach Massgabe von Art. 49 AHVG jedoch nicht als Organe anzusehen, die für die Durchführung, die Kontrolle oder die Beaufsichtigung des AHVG zuständig sind.[259] Folglich kann Art. 50a Abs. 1 lit. a AHVG im vorliegenden Fall nicht zur Anwendung gelangen.
- Erfolgt die grenzüberschreitende Datenübermittlung an ein **Organ „einer anderen Sozialversicherung"** im Sinn von **Art. 50a Abs. 1 lit. b AHVG**, so könnte diese letztgenannte Rechtsbestimmung als gesetzliche Grundlage dienen. Abzugrenzen sind die Organe „einer anderen Sozialversicherung" von dem in Art. 32 Abs. 2 ATSG verwendeten Begriff der „Organe der einzelnen Sozialversicherungen". Während Art. 32 Abs. 2 ATSG sehr allgemein abgefasst wurde und deshalb unseres Erachtens durchaus auch ausländische Sozialversicherungseinrichtungen miteinbeziehen könnte,[260] ist Art. 50a Abs. 1 lit. b AHVG unter Berücksichtigung der in Art. 50a Abs. 1 lit. a

---

258 Vgl. Art. 49 AHVG, wonach die Durchführung der AHV unter Aufsicht des Bundes durch die Arbeitgeber und Arbeitnehmer, Verbandsausgleichskassen, kantonalen Ausgleichskassen, Ausgleichskassen des Bundes und eine zentrale Ausgleichsstelle erfolgt.

259 Es könnte höchstens argumentiert werden, dass diese Institutionen aufgrund des in Art. 153a AHVG enthaltenen Verweises auf den Anhang II des FZA, worin die VO 883/2004 und die VO 987/2009 für anwendbar erklärt werden, als Ausführungsorgane des AHVG fungieren, da diese Verordnungen durch die Bezugnahme in Art. 153a AHVG als integrierender Bestandteil dieses Gesetzes zu betrachten sein könnten. Dieses Argumentationsweise geht allerdings zu weit und ist im Ergebnis nicht überzeugend, sind doch die Verordnungen als Völkerrecht vom schweizerischen Bundesrecht zu unterscheidende Rechtsakte, die durch ihre Bezugnahme im FZA nicht Bestandteil eines bundesrechtlich geltenden Spezialversicherungsgesetzes werden.

260 S.o. D.I.2.a).

AHVG verankerten Konstellation enger auszulegen. Denn da sich Art. 50a Abs. 1 lit. a AHVG auf die Ausführungsorgane des AHVG bezieht, spricht der systematische Zusammenhang dafür, dass mit „Organe einer anderen Sozialversicherung“ in lit. b lediglich diejenigen sozialen Einrichtungen, die in Anwendung eines anderen schweizerischen Bundesgesetzes handeln, gemeint sind. Zudem soll Art. 50a Abs. 1 lit. b AHVG nicht als Auffangtatbestand für alle nicht unter lit. a subsumierbaren Datenaustausche dienen, ist doch in Art. 50a Abs. 4 AHVG eine Regelung für die übrigen – d.h. die nicht von Art. 50a Abs. 1-3 AHVG erfassten – Fälle vorgesehen. Aus diesen Gründen kann u.E. die Datenbekanntgabe von einer schweizerischen Verbindungsstelle oder einem Träger an eine ausländische Sozialversicherungseinrichtung nicht unter Art. 50a Abs. 1 lit. b AHVG subsumiert werden.

- Eine solche Datenbekanntgabe könnte damit lediglich aufgrund des **Art. 50a Abs. 4 lit. b AHVG** erfolgen. Danach ist eine Datenbekanntgabe jedoch nur dann zulässig, wenn die **betroffene Person im Einzelfall schriftlich eingewilligt** hat oder, wenn das Einholen der Einwilligung nicht möglich ist, diese aber nach den Umständen als im Interesse des Versicherten vorausgesetzt werden darf. Bei der grenzüberschreitenden Datenübermittlung durch die schweizerischen Sozialversicherungsträger handelt es sich nicht um eine Fallgestaltung, die das Einholen einer Einwilligung grundsätzlich verunmöglicht. Vorausgesetzt ist somit, dass die betroffene Person im Einzelfall schriftlich eingewilligt hat, was jedoch bei Informationssystemen wie dem EESSI grundsätzlich ausgeschlossen erscheint,[261] so dass auch diese Bestimmung vorliegend nicht einschlägig sein kann.

c) Fazit

Im Ergebnis besteht damit im **nationalen Recht keine ausreichende gesetzliche Grundlage zur grenzüberschreitenden Datenübermittlung**, so wie sie im Rahmen des EESSI vorgesehen ist. Die in Frage kommenden Rechtsgrundlagen sind entweder bereits tatbestandlich zumindest teilweise nicht einschlägig oder aber dann jedenfalls zu unbestimmt, um als gesetzliche Grundlage für ein derart umfassendes Informationssystem, in dessen Rahmen auch besonders schützenswerte Daten übermittelt werden können, fungieren zu können.

Während Art. 31 Abs. 2 ATSG lediglich einen spezifischen Fall einer Datenbekanntgabe erfasst und ohnehin als zu unbestimmt zu qualifizieren ist, kann Art. 47 Abs. 1 lit. b ATSG im Fall einer grenzüberschreitenden Datenübermittlung im Rahmen des EESSI wohl gar nicht zur Anwendung gelangen. Auch Art. 32 Abs. 2 ATSG, der die allgemeine Verwaltungshilfe zwischen den Sozialversicherungseinrichtungen regelt, kann aufgrund seiner Unbestimmtheit nicht als gesetzliche Grundlage taugen. Darüber hinaus können dem AHVG keine Spezialbestimmungen entnommen werden, die es erlaubten, Personendaten an ausländische Verbindungsstellen oder Träger zu übermitteln.

[261] S.o. C.II.1.

II. Zum sozialversicherungsrechtlichen Datenaustausch innerhalb der Schweiz

Für die Umsetzung des elektronischen Datenaustausches zwischen den an der Koordinierung der Systeme sozialer Sicherheit beteiligten europäischen Staaten sind auch auf nationaler Ebene strukturelle Anpassungen notwendig, die über die reine Durchführung des EESSI hinausgehen. In der Schweiz werden daher verschiedene, auf den jeweiligen Sozialversicherungszweig angepasste Informationssysteme entwickelt.[262] Beispielhaft für die Bereiche der AHV und IV sowie der Unterstellung soll deshalb im folgenden Kapitel untersucht werden, ob sich für den Betrieb von Informationssystemen bereits gesetzliche Grundlagen im schweizerischen Recht finden lassen, welche die damit einhergehenden Datenbearbeitungen zulassen.

Da die zu erwartenden Datenbearbeitungen im Rahmen der nationalen Informationssysteme zu diesem Zeitpunkt nicht im Einzelnen eruiert werden können, werden die möglichen Rechtsgrundlagen lediglich einer abstrakten Prüfung unterzogen. Hierbei werden zunächst die spezifischen Anforderungen, die sich an die gesetzlichen Grundlagen für die nationalen Informationssysteme im Rahmen der AHV und IV sowie der Unterstellung stellen, zusammenfassend erörtert (1.) und die möglichen Rechtsgrundlagen für die beiden Sozialversicherungsbereiche im Einzelnen dargelegt (2.). Nachfolgend werden die Anwendungsvoraussetzungen des massgeblichen Art. 50a AHVG besprochen (3.), und schliesslich ein Fazit gezogen (4.).

1. Spezifische Anforderungen an die Ausgestaltung der Rechtsgrundlagen

Die sich an die gesetzlichen Grundlagen stellenden Anforderungen hängen massgeblich davon ab, wie der Datenaustausch im Rahmen der nationalen Informationssysteme vonstatten gehen soll.[263] Denn werden die nationalen Informationssysteme so konzipiert, dass Daten mittels **Abrufverfahren** i.S.v. Art. 19 Abs. 3 DSG zugänglich gemacht werden, so sind die damit einhergehenden erhöhten Anforderungen zu beachten. Beim Abrufverfahren handelt es sich um ein automatisiertes Verfahren, das dem Datenempfänger ermöglicht, sich die gesuchte Information in einem vorhandenen Datenbestand selbst zu beschaffen bzw. „abzurufen“, ohne dass die die Daten eigentlich bekanntgebende Stelle mitwirken muss bzw. die Abrufung überhaupt bemerkt. Insofern beinhaltet das Abrufverfahren ein „Selbstbedienungselement“ durch den Datenempfänger, und das wesentliche Kennzeichen eines Abrufverfahrens ist der Übergang der Verfügungsmacht über die Datenbekanntgabe vom Datenherrn auf den Daten-

262 S. im Einzelnen oben B.II.

263 Zu den datenschutzrechtlichen Anforderungen im Einzelnen C.II.

empfänger.[264] M.a.W. haben Dritte in einem Abrufverfahren ohne vorangehendes Gesuch – gerichtet an den eigentlichen Datenbearbeiter bzw. denjenigen, der die Daten bekannt gegeben hat – Zugang zu den gewünschten Daten. Dies ist insbesondere auch dann der Fall, wenn Informationen über das Internet entweder mit verschlüsseltem oder einem sonstwie geschütztem Zugang zugänglich gemacht werden.[265] Da die Frage des Vorliegens eines Abrufverfahrens in Bezug auf die nationalen Informationssysteme nicht abschliessend beantwortet werden kann, sei lediglich darauf hingewiesen, dass im Fall ihrer Bejahung die in **Art. 19 Abs. 3 DSG festgelegten Erfordernisse**, die auf das erhöhte Gefährdungspotential für die Rechte der Betroffenen zurückzuführen sind,[266] berücksichtigt werden müssen. Verlangt wird in Art. 19 Abs. 3 DSG, dass die Datenbekanntgabe mittels Abrufverfahren **ausdrücklich vorgesehen** wird, wobei sich die Rechtsgrundlage bei besonders schützenswerten Personendaten oder Persönlichkeitsprofilen in einem Gesetz im formellen Sinn befinden muss.

Ferner sind für den Fall, dass in den nationalen Informationssystemen **besonders schützenswerte Personendaten** bearbeitet werden, die damit einhergehenden erhöhten Vorgaben von Art. 17 Abs. 2 DSG (i.V.m. Art. 19 Abs. 1 und 3 DSG) zu beachten. Demgemäss dürfen besonders schützenswerte Personendaten und Persönlichkeitsprofile grundsätzlich nur bearbeitet bzw. bekannt gegeben werden, wenn dies in einem **Gesetz im formellen Sinn** ausdrücklich vorgesehen wird. Diesem Erfordernis liegt zugrunde, dass mit den erhöhten Gefahren für die Persönlichkeitsrechte allgemein auch die Anforderungen an die Ausgestaltung der Rechtsgrundlage steigen.[267]

Wie bereits in Bezug auf das EESSI-System im Allgemeinen,[268] sind auch hinsichtlich des Datenaustausches im **Bereich der AHV und IV** die erhöhten Vorgaben in Bezug auf die Zulässigkeit der Bearbeitung besonders schützenswerter Personendaten in Betracht zu ziehen. Für den konkreten Einzelfall muss dies mittels der abschliessenden Aufzählung von Art. 3 lit. c DSG ermittelt werden. Bezüglich des in Frage stehenden Sozialversicherungszweigs kann aber angenommen werden, dass durchaus auch besonders schützenswerte Personendaten i.S.v. Art. 3 lit. c DSG bearbeitet werden.[269] Damit ist für den Betrieb eines solchen Informationssystems im Grundsatz eine formell-gesetzliche Grundlage erforderlich, welche hinreichend präzise zu formulieren ist. Was den **Bereich der Unterstellung** betrifft, so könnte es sich unter Umständen ebenfalls um besonders schützenswerte Personendaten handeln. Obwohl bei den entsprechenden Daten nicht grundsätzlich davon ausgegangen werden kann, dass es sich um religiöse, weltanschauliche, politische oder gewerkschaftliche Ansichten handelt, wäre es denkbar, dass solche Daten im Einzelfall möglicherweise vorliegen. Davon ist

---

264 *Epiney/Schleiss*, Jusletter v. 7.11.2011, Rn. 15; *Jöhri*, in: Rosenthal/Jöhri, Handkommentar DSG, Art. 19, Rn. 74; *Ehrensperger*, in: Maurer-Lambrou/Blechta, BK Datenschutzgesetz, Öffentlichkeitsgesetz, Art. 19, Rn. 50; *Waldmann/Bickel*, in: Belser/Epiney/Waldmann, Datenschutzrecht, § 12, Rn. 95.

265 BBl 2000 259; *Epiney/Schleiss*, Jusletter v. 7.11.2011, Rn. 12 ff.; *Jöhri*, in: Rosenthal/Jöhri, Handkommentar DSG, Art. 19, Rn. 76.

266 *Epiney/Schleiss*, Jusletter v. 7.11.2011, Rn. 18, 21; BBl 2000 259.

267 S. insoweit bereits oben C.II.1.

268 S.o. D.I., am Anfang.

269 Zur Begründung s.o. D.I., am Anfang.

auszugehen, wenn die gemachten Angaben, wie z.B. die berufliche Tätigkeit, Aufschluss über religiöse, weltanschauliche, politische oder gewerkschaftliche Ansichten der Person geben. Damit kann jedoch nicht ganz generell auf das Vorliegen besonders schützenswerte Personendaten geschlossen werden. Wenn auch im Einzelfall nicht auszuschliessen ist, dass gewisse Daten besonders schützenswerte Personendaten darstellen können, ist doch vor dem Hintergrund des Gesagten grundsätzlich davon auszugehen, dass ein Informationssystem im Rahmen des letztgenannten Bereichs keine besonders schützenswerten Personendaten enthält.
Zusammenfassend kann somit festgehalten werden, dass bis auf Weiteres ungewiss ist, ob die nationalen Informationssysteme eine Datenbekanntgabe mittels Abrufverfahren implizieren, welche gemäss Art. 19 Abs. 3 DSG ausdrücklich in der gesetzlichen Grundlage vorzusehen ist. Hingegen kann bereits zu diesem Zeitpunkt darauf hingewiesen werden, dass zumindest für den Bereich der AHV und IV aufgrund der Bearbeitung besonders schützenswerter Personendaten eine formell-gesetzliche Grundlage erforderlich ist. Ausgehend davon und aufgrund des beschränkten Umfangs dieser Untersuchung wird im Folgenden ausschliesslich geprüft, ob formell-gesetzliche Grundlagen den Betrieb von Informationssystemen in den beiden Bereichen zulassen. Die Untersuchung gesetzlicher Grundlagen im materiellen Sinn wird hingegen weitgehend ausgespart.

2. Zu den möglichen gesetzlichen Grundlagen

Da im Rahmen der geplanten nationalen Informationssysteme ein Austausch grenzüberschreitend relevanter Daten stattfinden wird, kommen grundsätzlich auch die in **der VO 883/2004 und der VO 987/2009 verankerten Bestimmungen als gesetzliche Grundlagen** in Frage. Allerdings beziehen sich diese Rechtsakte im Wesentlichen auf den (grenzüberschreitenden) Datenaustausch im Rahmen des Informationssystems EESSI, während die innerstaatliche Durchführung den Mitgliedstaaten bzw. den assoziierten Staaten überlassen ist. Aus diesem Grund scheiden diese Rechtsakte als mögliche gesetzliche Grundlagen von vornherein aus.[270]
Vor diesem Hintergrund konzentrieren sich die weiteren Ausführungen auf die Frage, ob im **schweizerischen Recht** ausreichende (d.h. den soeben erwähnten Vorgaben genügende) gesetzliche Grundlagen für die verschiedenen Datenbearbeitungen zu finden sind.
Im Rahmen des Informationssystems für den Bereich der AHV und IV werden grenzüberschreitend relevante Daten zwischen den AHV-Ausgleichskassen, den IV-Stellen und der ZAS ausgetauscht. Diese drei zuständigen Stellen werden hierbei in Anwendung des AHVG oder des IVG tätig, je nachdem wie sich der konkrete Einzelfall präsentiert. Neben den im ATSG enthaltenen Bestimmungen, die in Anlehnung an das oben Gesagte hier wohl ebenfalls

[270] Im Übrigen ist darauf hinzuweisen, dass für den Fall, dass ein Abrufverfahren vorliegt, dies in diesen Vorschriften überdies nicht explizit vorgesehen wird, was aufgrund von Art. 19 Abs. 3 DSG erforderlich wäre.

nicht als genügende Gesetzesgrundlagen herangezogen werden können,[271] sind die massgeblichen Bestimmungen demnach insbesondere in den Spezialgesetzen des AHVG und des IVG zu finden. Auch im Bereich der Unterstellung ist das AHVG als massgebliche Rechtsgrundlage zu betrachten, da sowohl die AHV-Ausgleichskassen als auch das BSV und die Arbeitgeber als Durchsetzungsorgane dieses Gesetzes handeln. Aus diesem Grund wird die Analyse der möglichen Rechtsgrundlagen für die Bereiche der AHV und IV sowie der Unterstellung auf die **im AHVG und im IVG verankerten Bestimmungen** eingeschränkt.
Die Zulässigkeit einer Datenbearbeitung im Rahmen der Invalidenversicherung wird in Art. 66 ff. IVG geregelt, wobei Art. 66 IVG lediglich den Grundsatz festlegt, wonach das AHVG auf den in dieser Vorschrift erwähnten Regelungsbereich sinngemäss anwendbar ist. Für die Datenbekanntgabe im Speziellen ist auf Art. 66a IVG abzustellen, welcher die Voraussetzungen für die Datenbekanntgabe der das IVG anwendenden Behörden regelt. Während Art. 66a Abs. 1 IVG lediglich die Datenbekanntgabe an die in lit. a-c erwähnten Behörden erfasst, ist entsprechend Abs. 2 derselben Bestimmung für übrige Datenbekanntgaben Art. 50a AHVG sinngemäss anwendbar. Angesichts dessen, dass die im Rahmen des geplanten Informationssystems zu erfolgenden Datenbekanntgaben Art. 66a Abs. 2 IVG betreffen, konzentriert sich die folgende Untersuchung sowohl hinsichtlich des Datenaustausches im Rahmen der AHV und IV als auch bezüglich der Unterstellung auf **die massgebliche Bestimmung des AHVG, namentlich Art. 50a AHVG**.

3. Zur Anwendung von Art. 50a AHVG

Da, wie soeben aufgezeigt,[272] der Rahmen der zulässigen Datenbekanntgabe in den Bereichen der AHV und IV sowie der Unterstellung im Wesentlichen durch Art. 50a AHVG bestimmt ist, gilt es diese Vorschrift im Folgenden etwas genauer zu untersuchen, um dadurch den Rechtsrahmen für die darauf basierenden Datenbekanntgaben zu erfassen. Dazu werden in einem ersten Schritt die Tatbestandsvoraussetzungen des relevanten Art. 50a Abs. 1 lit. a AHVG analysiert (a) und in einem weiteren Schritt die in Art. 50 Abs. 5-7 AHVG verankerten Modalitäten der Bekanntgabe beleuchtet (b), woraufhin in einem letzten Abschnitt ein Fazit gezogen wird (c).

271 Für die Begründung s.o. D.I.2.a).
272 D.II.2.

a) Zulässigkeit der Datenbekanntgabe

Art. 50a AHVG regelt eine Vielzahl von Fallkonstellationen, welche die Datenbekanntgaben unter jeweils verschiedenen Voraussetzungen zulassen.[273] Für die geplanten nationalen Informationssysteme scheint insbesondere die in Art. 50a Abs. 1 lit. a AHVG festgehaltene Regelung von Bedeutung zu sein. Denn diese Vorschrift betrifft die Datenbekanntgabe an eine andere mit der Durchführung, der Kontrolle oder der Beaufsichtigung der Durchführung des Gesetzes betrauten Organs, wobei alle an den beiden Informationssysteme beteiligten Stellen als solche Organe anzusehen sind.[274] Entsprechend dieser Vorschrift ist eine Datenbekanntgabe in Abweichung von der Schweigepflicht nach Art. 33 ATSG[275] zwischen den genannten Stellen immer dann als zulässig zu erachten, wenn keine überwiegenden Privatinteressen entgegenstehen (aa) und die Daten zur Erfüllung der nach dem AHVG bzw. IVG übertragenen Aufgaben erforderlich sind (bb).

aa) Keine entgegenstehenden Privatinteressen

Einer Datenbekanntgabe auf der Grundlage von Art. 50a Abs. 1 lit. a AHVG dürfen **keine überwiegenden privaten Interessen** entgegenstehen. Damit bringt das Gesetz zum Ausdruck, dass in jedem Einzelfall eine Interessenabwägung – wie dies im Übrigen auch das Verhältnismässigkeitsprinzip fordert[276] – vorzunehmen ist.[277] Bei dieser Interessenabwägung sollen insbesondere die Interessen derjenigen Person berücksichtigt werden, über welche Personendaten bekannt gegebenen werden.[278] Nicht jedes subjektive Interesse kann hier von Bedeutung sein; vielmehr ist für die Beurteilung, ob das in Frage stehende Privatinteresse als

---

273 S. dazu bereits oben D.I.2.b).

274 Vgl. dazu Art. 49 AHVG, wonach die Durchführung der AHV u.a. durch die Aufsicht des Bundes, die Arbeitgeber und Arbeitnehmer, die kantonalen Ausgleichskassen und die zentrale Ausgleichsstelle erfolgt. Damit werden die AHV-Ausgleichskassen, die ZAS und die Arbeitgeber ausdrücklich als Durchführungsorgane bestimmt. Daneben ist auch das BSV als mit der Durchführung des Gesetzes betraut anzusehen: Denn es nimmt die Aufsicht über die Durchführung der AHV wahr, da das Eidgenössische Departement des Innern nach der Ausführungsbestimmung des Art. 176 AHVV gewisse Aufgaben an das BSV weiter delegieren kann, womit dem BSV Teilaufgaben in der Aufsicht des Gesetzes zukommen, siehe dazu *Houstek*, CHSS 5/2000, 238 ff.; *Prieur*, in: Passadelis/Rosenthal/Thür, Datenschutzrecht, § 13, Rn. 13.77. Werden Daten durch IV-Stellen bekannt gegeben, so fallen auch diese Stellen unter die Regelung von Art. 50a Abs. 1 lit. a AHVG, dies weil die IV-Stellen als Durchführungsorgane der Invalidenversicherung im Sinn von Art. 53 IVG gelten und diese Bestimmung aufgrund der sinngemässen Anwendung von Art. 50a Abs. 1 lit. a AHVG im Rahmen einer solchen Bekanntgabe analog zur Anwendung gelangt.

275 Dazu schon oben D.I.2.a).

276 Zum Prinzip der Verhältnismässigkeit allgemein schon oben C.II.3.

277 *Kieser*, ATSG-Kommentar, Art. 32, Rn. 16.

278 Zur Voraussetzung der Wahrung überwiegender Privatinteressen in Art. 84a KVG, vgl. *Eugster/Luginbühl*, in: Datenschutz im Gesundheitswesen, 73 (132); bezüglich der Datenbekanntgabe i.S.v. Art. 86a Abs. 2 BVG siehe BGer, Urteil 2A.96/2000 vom 25. Juli 2001, E. 5, wo das Bundesgericht spezifisch auf das Interesse des Versicherten hinweist.

überwiegend anzusehen ist, eine objektive Betrachtungsweise anzulegen.[279] Ein überwiegendes Privatinteresse könnte demnach dann bestehen, wenn besonders heikle Gesundheitsdaten einer Behörde mitgeteilt werden, bei welcher sich Sachbearbeiter aus dem Bekanntenkreis der betroffenen Person mit dem Fall befassen.[280] Hinsichtlich der geplanten nationalen Informationssysteme steht dem Interesse des Betroffenen an der Geheimhaltung seiner Daten in erster Linie das allgemeine Interesse an der Durchsetzung der Rechtsbestimmungen und damit auch an der Abklärung des Leistungsanspruches bzw. der Unterstellungsfrage entgegen. Werden nur die für die Beurteilung des Gesuches benötigten Daten einzig an die dafür zuständigen Institutionen weitergeleitet, so kann u.E. zwar grundsätzlich davon ausgegangen werden, dass kein überwiegendes Privatinteresse besteht. Dennoch ist zu beachten, dass es im Fall einer „automatischen" Datenbekanntgabe – d.h. ohne eine **Prüfung des Einzelfalls** – nicht möglich bzw. nicht vorgesehen ist zu prüfen, ob einer Datenbekanntgabe im Einzelfall überwiegende Privatinteressen entgegenstehen, so dass die Einschlägigkeit dieser Vorschrift unter diesen Umständen zu verneinen ist. Damit ist gleichzeitig auch gesagt, dass die Erfüllung dieses Kriteriums letztlich nicht nur von der individuell vorliegenden Interessenslage, sondern zugleich auch von der – bis auf Weiteres unbekannten – konkreten Durchführung der Datenbekanntgaben abhängt.

bb) Erforderlichkeit zur Erfüllung einer gesetzlichen Aufgabe

Zusätzlich zur Wahrung privater Interessen verlangt Art. 50a Abs. 1 lit. a AHVG, dass die Bekanntgabe nur erfolgen darf, sofern die Daten für die Erfüllung der nach dem Gesetz übertragenen Aufgaben erforderlich sind. Für die Prüfung dieses Merkmals muss zunächst eine im Gesetz verankerte Aufgabe ermittelt werden. Ausgehend davon ist danach zu fragen, ob die Datenbekanntgabe tatsächlich auch erforderlich ist, um diese gesetzliche Aufgabe zu erfüllen. Sowohl das **AHVG** als auch das **IVG** legen die Aufgaben der anwendenden Behörden gesetzlich in einzelnen Bestimmungen fest.[281] Im Wesentlichen geht es dabei um die im vierten Abschnitt zur Organisation enthaltenen Vorschriften, namentlich Art. 51 AHVG (Arbeitgeber), Art. 63 AHVG (Ausgleichskassen), Art. 71 AHVG (Zentrale Ausgleichsstelle) und Art. 57 IVG (IV-Stellen) sowie Art. 60 IVG (Ausgleichkassen). Diese Aufgaben sind allerdings im Zusammenhang mit den schweizerischen Rechtsverhältnissen zu sehen. Für Datenbekanntgaben im Rahmen der nationalen Informationssysteme, die im Wesentlichen zum Zweck der grenzüberschreitenden Datenübermittlung erfolgen, können diese Gesetzesbestimmungen

279 *Eugster/Luginbühl*, in: Datenschutz im Gesundheitswesen, 73 (132); *Pärli*, Gutachten IIZ, 38.

280 *Eugster/Luginbühl*, in: Datenschutz im Gesundheitswesen, 73 (132).

281 Darüber hinaus regeln auch die Verordnungen des AHVG und des IVG den Aufgabenbereich dieser Stellen, wobei diese Bestimmungen hier ausser Acht gelassen werden können, da Art. 50a Abs. 1 lit. a AHVG explizit eine gesetzliche Verankerung der Aufgabe vorschreibt.

deshalb kaum herangezogen werden. Dementsprechend sind die zu erfüllenden Aufgaben letztlich auf die europäischen Verordnungen zurückzuführen.
Angesichts der direkten Anwendbarkeit der **VO 883/2004** und der **VO 987/2009** kann ebenfalls auf die in diesen Verordnungen geregelten Aufgaben der beteiligten Träger zurückgegriffen werden.[282] So statuiert z.B. Art. 47 Abs. 5 VO 987/2009 für den Bereich der AHV und IV, dass die beteiligten Träger dem Kontakt-Träger und den andere beteiligten Trägern so bald wie möglich die Versicherungs- oder Wohnzeiten mitzuteilen haben, die nach den von ihnen anzuwendenden Rechtsvorschriften zurückgelegt worden sind. Des Weiteren sind sie gemäss Art. 47 Abs. 6 VO 987/2009 verpflichtet, den Kontakt-Träger und die anderen betroffenen Träger über ihre Entscheidung, den Leistungsbetrag und alle nach Art. 53-55 VO 883/2004 notwendigen Angaben zu informieren. Für den Bereich der Unterstellung sei beispielshaft auf Art. 15 VO 987/2009 hingewiesen, der dem Arbeitgeber ein Informationspflicht gegenüber dem zuständigen Träger auferlegt. Zudem befasst sich Art. 16 VO 388/2004 mit den Ausnahmevereinbarungen, die durch das BSV vorzunehmen sind, und zur Abwicklung dieser Abkommen das BSV Zugang zu gewissen Daten haben muss. Sektorübergreifend ist zudem auf **Art. 2 Abs. 2 VO 987/2009** hinzuweisen, der die Gesamtheit der Träger ausdrücklich dazu verpflichtet, all jene Daten auszutauschen, die zur Begründung und Feststellung der Rechte und Pflichten nach der VO 883/2004 benötigt werden. Insbesondere unter diese letztgenannte Bestimmung könnte eine Reihe von Aufgaben gefasst werden. Denn auf der Grundlage von Art. 2 Abs. 2 VO 987/2009 können die Träger die auf der Grundlage der VO 883/2004 benötigten Daten gegenseitig einfordern, woraus eine Vielzahl von Datenübermittlungen an diese Träger resultieren dürfte. Angesichts dessen dürfte die Erforderlichkeit im Grundsatz wohl keine grossen Schwierigkeiten aufwerfen, insbesondere auch weil die nationalen Systeme im Grunde entwickelt worden sind, um die Umsetzung der gesetzlichen Aufgaben wirkungsvoller zu gestalten.

b) Modalitäten der Datenbekanntgabe

Neben den bereits erwähnten Tatbestandsvoraussetzungen gilt es zudem die in **Art. 50a Abs. 5-7 AHVG** verankerten Anforderungen an die **Modalitäten der Datenbekanntgabe** zu beachten.[283] Zunächst wird in Art. 50a Abs. 5 AHVG festgehalten, dass lediglich diejenigen Daten bekanntgegeben werden dürfen, die für den in Frage stehenden Zweck erforderlich sind, womit das in Art. 4 Abs. 3 DSG verankerte Prinzip der Zweckbindung sowie das Verhältnismässigkeitsprinzip nach Art. 4 Abs. 2 DSG zum Ausdruck kommen. Für die Datenbe-

[282] Ausserdem kann hier noch angemerkt werden, dass Art. 80a Abs. 1 lit. a IVG und Art. 153a Abs. 1 lit. a AHVG explizit auf das FZA im Allgemeinen und dessen Anhang II sowie die VO Nr. 1408/71 und Nr. 574/72 verweist; zur direkten Anwendbarkeit s. bereits oben C.I.2.

[283] Art. 66 Abs. 2 IVG verweist auf Art. 50a AHVG im Allgemeinen, weshalb die Absätze 5-7 auch auf eine Datenbekanntgabe im Rahmen eines IV-Verfahrens anwendbar sind.

kanntgabe im Rahmen der nationalen Informationssysteme bedeutet dies, dass nur diejenigen Daten übermittelt werden dürfen, die mit der gesetzlich vorgesehenen Aufgabe derart in Zusammenhang stehen, dass sie für deren Erfüllung tatsächlich benötigt werden. Die davon betroffenen Daten können den einzelnen Spezialbestimmungen bzw. ganz allgemein Art. 2 Abs. 2 VO 987/2009 entnommen werden. Die Beschränkung auf die zur Erfüllung der Aufgaben erforderlichen Daten dürfte im Rahmen der nationalen Informationssysteme kein grundsätzliches Problem darstellen, wurde doch ein derartiger Informationsaustausch entwickelt, um die gesetzlichen Aufgaben effizienter erfüllen zu können. Zudem wird die Erforderlichkeit bereits bei der Prüfung der Tatbestandsvoraussetzungen von Art. 50a Abs. 1 lit. a AHVG mitberücksichtigt, da danach verlangt wird, dass die Daten zur Erfüllung der gesetzlichen Aufgaben erforderlich sein müssen.[284]

Nach **Art. 50a Abs. 7 AHVG** sollen die Daten in der Regel **schriftlich** und kostenlos bekannt gegeben werden. Bei besonders aufwendigen Arbeiten kann der Bundesrat jedoch eine Gebühr vorsehen.[285] Die in Art. 50a Abs. 6 AHVG erwähnten und vom Bundesrat geregelten weiteren Modalitäten haben ihren Niederschlag in Art. 209bis und 209ter AHVV gefunden, wobei gleichzeitig angefügt sei, dass diese weiterführenden Bestimmungen für die vorliegende Untersuchung nicht von Relevanz sind.[286] In rechtlicher Hinsicht könnte hingegen problematisch sein, dass Art. 50a Abs. 7 AHVG vorschreibt, dass die Datenbekanntgabe in der Regel schriftlich zu erfolgen hat.[287] Der Ausdruck „in der Regel" macht allerdings deutlich, dass ein elektronisch zu erfolgender Datenaustausch nicht gänzlich ausgeschlossen ist. Diesbezüglich bleibt aber immerhin fraglich, ob die Einrichtung eines nationalen Informationssystems, welches ausschliesslich eine Bearbeitung elektronischer Daten beinhaltet, noch mit Art. 50a Abs. 7 AHVG zu vereinbaren ist. Ungeachtet dessen ist es vor dem Hintergrund, dass für eine ausreichend bestimmte Gesetzesgrundlage verlangt wird, dass Art und Ausmass der zu erfolgenden Datenbearbeitungen in der Rechtsgrundlage offengelegt werden,[288] angezeigt, die elektronische Datenbearbeitung im konkreten Fall vorzusehen.

4. Fazit

Im Hinblick auf die Errichtung nationaler Informationssysteme ist eine hinreichende gesetzliche Grundlage erforderlich, die den Gefahren der Persönlichkeitsrechte der Betroffenen genü-

284 Eingehender dazu bereits oben D.II.3.a)bb).

285 Vgl. Art. 209ter AHVV.

286 Denn diese Rechtsbestimmungen betreffen die Rechtsmittelinstanz bei Streitigkeiten über Datenbekanntgaben (Art. 209bis AHVV) und die Kosten der Bekanntgabe i.S.v. Art. 50a Abs. 4 AHVG sowie die Publikation i.S.v. Art. 50a Abs. 3 AHVG (Art. 209ter AHVV).

287 In Abweichung von Art. 32 ATSG wird nur vorausgesetzt, dass die Datenbekanntgabe in der Regel schriftlich zu erfolgen hat; ein schriftlich begründetes Gesuch um Datenherausgabe ist jedoch nicht erforderlich; s. auch *Pärli*, Gutachten IIZ, 26.

288 C.II.1.

gend Rechnung trägt. In diesem Sinn sind für den Fall, dass Daten mittels Abrufverfahren bekannt gegebenen werden und besonders schützenswerte Personendaten betroffen sind, die entsprechenden erhöhten Vorgaben zu beachten. Werden Daten über ein **Abrufverfahren** zugänglich gemacht, so ist dies in der gesetzlichen Grundlage explizit vorzusehen. In Zusammenhang mit Art. 50a AHVG ist eine solche Datenübermittlung jedenfalls nicht als zulässig zu erachten, denn zum einen geht aus letzterer Vorschrift das Abrufverfahren nicht ausdrücklich hervor und zum anderen erscheint die Bestimmung angesichts der damit einhergehenden Anforderungen als zu unbestimmt. Denn grundlegende datenschutzrechtliche Aspekte – wie die Funktionsweise des Abrufverfahrens, die zugangsberechtigten Stellen, die Rechte der Betroffen, die Kategorien der zu bearbeitenden Daten sowie die Aufbewahrungs- und Löschungsbedingungen – werden nicht geregelt. Darüber hinaus sind zumindest teilweise **besonders schützenswerte Personendaten** betroffen, deren Bearbeitung eine formellgesetzliche Grundlage erfordern. Angesichts dessen, dass eine solche Rechtsgrundlage genügend präzise auszuformulieren ist, scheint fraglich, ob Art. 50a AHVG den damit einhergehenden Anforderungen gerecht wird, da es hinsichtlich einiger Aspekte, namentlich Art und Ausmass der Datenbearbeitung, der beteiligten Behörden sowie der genauen Datenkategorien, wohl an der Bestimmtheit dieser Vorschrift mangelt.

Daneben wirft auch die Erfüllung der **Tatbestandsvoraussetzungen von Art. 50a Abs. 1 lit. a AHVG** einige Schwierigkeiten auf. Erstens bringt die Einrichtung eines Informationssystems die Gefahr mit sich, dass Daten automatisch und damit ohne Einzelfallprüfung weitergeleitet werden. Diesfalls kann Art. 50a AHVG nicht herangezogen werden, setzt diese Vorschrift doch eine Interessenabwägung im Einzelfall voraus. Vor dem Hintergrund, dass die Datenbekanntgaben zwecks Abklärung eines konkreten Gesuches an die dafür zuständigen Institutionen erfolgen, dürfte die Wahrung überwiegender Privatinteressen im Übrigen grundsätzlich nicht weiter problematisch sein. Zweitens muss die Datenbekanntgabe zur Erfüllung einer gesetzlichen Aufgabe erforderlich sein. Da die nationalen Informationssysteme letztlich auf die in der VO 883/2004 und der VO 987/2009 festgelegten Aufgaben zurückzuführen sind, sind vor allem die darin enthaltenen Aufgaben zu berücksichtigen. Schon der allgemeine Art. 2 Abs. 2 VO 987/2009 weist auf die Notwendigkeit der Datenbekanntgaben hin und legt damit nahe, dass sich eine Vielzahl von Datenbekanntgaben aus dieser Vorschrift ergeben können und damit das Kriterium der Erforderlichkeit letztlich als erfüllt zu betrachten ist. Ferner hat aber die Datenbekanntgabe gemäss Art. 50a Abs. 7 AHVG in der Regel schriftlich zu erfolgen. Es scheint vertretbar, eine ausnahmsweise elektronische Datenbekanntgabe zuzulassen, doch ist es zweckmässig, bei systematischen Bekanntgaben – wie dies im Rahmen von Informationssystemen wohl der Fall ist – die elektronische Übermittlung gesetzlich vorzusehen, insbesondere weil damit auch höhere Risiken für die Persönlichkeitsrechte der Betroffenen verbunden sind.

E. Zur Ausgestaltung der gesetzlichen Grundlagen *de lege ferenda*

Insgesamt hat eine Analyse der bestehenden gesetzlichen Grundlagen ergeben, dass die einschlägigen Regelungen in den VO 883/2004 und 987/2009 unter Umständen als ausreichende gesetzliche Grundlagen für die **grenzüberschreitenden Datenbekanntgaben** betrachtet werden können. Hingegen bereitet das Auffinden von gesetzlichen Grundlagen für die **Datenbearbeitungen im Rahmen der im Hinblick darauf geplanten nationalen Systeme** grössere Schwierigkeiten: Der massgebliche Art. 50a AHVG scheint zwar generell geeignet zu sein, gewisse Datenbearbeitungen zu rechtfertigen. Doch scheint diese Vorschrift bei systematischen Datenbearbeitungen im Rahmen von Informationssystemen aufgrund der damit einhergehenden grösseren Gefährdung für die Persönlichkeitsrechte des Betroffenen – insbesondere im Fall der Bearbeitung besonders schützenswerter Personendaten und der Einrichtung eines Abrufverfahrens – als zu wenig spezifisch und bestimmt.

Nach der hier vertretenen Ansicht wäre somit eine Inbetriebnahme der geplanten nationalen Systeme grundsätzlich nur zulässig, wenn hierfür die **erforderlichen gesetzlichen Grundlagen geschaffen** werden. Hierfür kommen grundsätzlich zwei unterschiedliche Ansätze in Betracht:

- Erstens könnte in Betracht gezogen werden, die anwendbaren Rechtsgrundlagen jeweils **punktuell und damit bereichsspezifisch** um ausreichende gesetzliche Grundlagen zu ergänzen. Dies implizierte, dass für die jeweils geregelte Datenbearbeitung der Bezug auf die geplanten Systeme in das Gesetz eingefügt werden müsste und die wesentlichen Aspekte des Informationssystems geregelt werden müssten.
- Zweitens könnte eine **eigene Rechtsgrundlage** für die Einrichtung und den Betrieb der im Rahmen der Koordinierung der Systeme sozialer Sicherheit in Aussicht genommenen Informationssysteme geschaffen werden. Dies implizierte ein eigenes, horizontales Bundesgesetz, in dem die verschiedenen Systeme geregelt werden, wobei ggf. auch gewisse gemeinsame Bestimmungen formuliert werden könnten.

Versucht man eine grundsätzliche Bewertung dieser Optionen, so sprechen die besseren Gründe für den zuletzt genannten Ansatz: Eine sektorielle Vorgehensweise wäre nicht nur sehr viel komplizierter, müssten doch entsprechende Modifikationen in verschiedenen Gesetzen bzw. Rechtsgrundlagen vorgesehen werden, sondern brächte auch eine gewisse Rechtszersplitterung mit sich, da ähnliche Aspekte in verschiedenen Gesetzen geregelt wären. Damit einher ginge eine gewisse Unübersichtlichkeit und eine Einbusse an Rechtsklarheit, was gerade in einem Bereich, in dem es auch um die Bearbeitung besonders schützenswerter Personendaten geht, nicht erstrebenswert erscheint. Auch sprechen der Regelungszusammenhang bzw. die gemeinsamen Bezüge der vorgesehenen Informationssysteme zur Koordinierung der Systeme sozialer Sicherheit für eine derartige **horizontale Regelung**, und schliess-

lich erlaubte eine solche eine spezifische Ausgestaltung der gesetzlichen Grundlagen, die in jeder Beziehung den Besonderheiten der vorgesehenen Datenbearbeitungen Rechnung tragen könnte.

In einem solchen **horizontalen Gesetz** müssten **die einzelnen Informationssysteme** als solche vorgesehen sein, wobei insbesondere folgende Aspekte bereits auf formell-gesetzlicher Ebene in den Grundzügen festgelegt werden müssten (während Präzisierungen durchaus auch auf dem Verordnungsweg erfolgen können):

- Der **Bearbeitungszweck** ist jeweils zu spezifizieren, ggf. unter Bezugnahme bzw. Verweis auf bestehende gesetzliche Bestimmungen.
- Die **betroffenen Datenkategorien** sind zu bezeichnen, auch hier ggf. unter Bezugnahme bzw. Verweis auf bestehende gesetzliche Bestimmungen.
- **Art und Ausmass der Datenbearbeitung** sind zu umschreiben. Hierzu gehören insbesondere die verschiedenen vorgesehenen Datenbearbeitungen sowie die grundsätzliche Funktionsweise der Informationssysteme (unter Einschluss des genauen Bearbeitungsverfahrens, wobei ein Abrufverfahren ausdrücklich vorzusehen ist).
- Die **Dauer der Datenbearbeitungen** und die **Löschung** sind vorzusehen.
- Die **beteiligten Behörden bzw. Personen** sind im Einzelnen aufzuführen (datenbearbeitende Stellen, zugangsberechtigte Stellen u.a.m.).
- Die **Rechte der Betroffenen** sind ggf. zu spezifizieren (Informationsrechte, Zugangsrechte, Recht auf Berichtigung).

Bei der genauen Ausgestaltung dieser Punkte ist den allgemeinen datenschutzrechtlichen Grundsätzen (insbesondere den Grundsätzen der Zweckbindung, der Verhältnismässigkeit und der Transparenz) Rechnung zu tragen. Im Übrigen sind auch die sonstigen allgemeinen Anforderungen – insbesondere Datensicherheit – zu beachten.[289]

[289] Hierzu im Zusammenhang mit kantonalen Informationssystemen *Epiney/Fasnacht*, Jusletter v. 24.2.2014, Rn. 61 ff.; allgemein *Epiney*, in: Belser/Epiney/Waldmann, Datenschutzrecht, § 9, Rn. 44 ff.

F. Zusammenfassung und Schlussbetrachtung

I. Zusammenfassung

Die wesentlichen Erkenntnisse der vorliegenden Untersuchung können wie folgt – thesenartig – zusammengefasst werden:

- Bei der Einrichtung und dem Betrieb der für den elektronischen Datenaustausch im Rahmen der Anwendung des Koordinationsrechts im Bereich der Sozialversicherung notwendigen Informationssysteme ist – soweit die nationale Ebene betroffen ist – einerseits die Effektivität der **unionsrechtlichen Vorgaben bzw. derjenigen des Freizügigkeitsrechts** zu beachten, so dass die Informationssysteme so auszugestalten sind, dass der Austausch gemäss der Vorgaben des Sekundärrechts bzw. des Personenfreizügigkeitsabkommens erfolgen kann. Andererseits sind hierbei aber auch die **datenschutzrechtlichen Vorgaben** (auf nationaler und unionsrechtlicher Ebene) zu beachten, so dass das „Wie" dieser Durchführung im Rahmen der durch diese gezogenen Grenzen erfolgen muss.
- Für eine Datenbearbeitung im Rahmen der vorgesehenen Informationssysteme ist grundsätzlich eine **gesetzliche Grundlage** erforderlich; soweit besonders schützenswerte Personendaten bearbeitet werden, muss es sich dabei um ein Gesetz im formellen Sinn handeln. Jedenfalls muss die gesetzliche Grundlage hinreichend bestimmt sein, also insbesondere Art und Ausmass der Datenbearbeitung, die beteiligten Behörden sowie die genauen Datenkategorien angesichts des hohen Gefährdungspotentials der geplanten Bearbeitungen präzise umschreiben. Ist ein Abrufverfahren vorgesehen, muss auch dieses explizit in der gesetzlichen Grundlage verankert sein.
- Die **grenzüberschreitende Datenübermittlung**, so wie sie im Rahmen des **EESSI** vorgesehen ist, ist Gegenstand verschiedener völkerrechtlicher Bestimmungen (Personenfreizügigkeitsabkommen bzw. die VO 883/2004 und die VO 987/2009). Obwohl die hier einschlägigen Regelungen auf Verordnungsstufe nicht durchgehend sehr präzise sind (insbesondere soweit der Umfang der Datenbekanntgaben betroffen ist), erscheint es vertretbar, sie als gesetzliche Grundlagen anzusehen, da sich die weiteren Präzisierungen – wie schon in den Verordnungen selbst angelegt – aus dem Durchführungsrecht ergeben.
- Für die **geplanten nationalen Informationssysteme** ist vor allem Art. 50a Abs. 1 lit. a AHVG als gesetzliche Grundlage von Bedeutung. Entsprechend dieser Bestimmung sind die Daten, die zwischen den daran beteiligten Stellen ausgetauscht werden, in aller Regel als erforderlich für die Erfüllung einer gesetzlichen Aufgabe zu betrachten. Damit sind die Tatbestandsvoraussetzungen von Art. 50a Abs. 1 lit. a AHVG zumeist als erfüllt anzusehen. Abhängig von der konkreten Ausgestaltung der Datenbe-

kanntgabe ist aber unter Umständen problematisch, dass das in Art. 50a Abs. 1 AHVG aufgeführte Erfordernis der Wahrung überwiegender privater Interessen eine Einzelfallprüfung impliziert, was der Einrichtung eines Informationssystems zumindest teilweise entgegenstehen könnte. Zudem ist in Bezug auf alle zu erfolgenden Datenbekanntgaben zu beachten, dass das Vorliegen eines Abrufverfahrens sowie die Bearbeitung besonders schützenswerter Personendaten entsprechend höhere Anforderungen an die Ausgestaltung der gesetzlichen Grundlagen nach sich ziehen: Diese müssen nicht nur in einem Gesetz im formellen Sinn figurieren, sondern auch hinreichend bestimmt sein (insbesondere in Bezug auf Art und Ausmass der Datenbearbeitung, die beteiligten Behörden sowie die genauen Datenkategorien), und das Abrufverfahren muss als solches in der gesetzlichen Grundlage vorgesehen sein. In Zusammenhang mit Art. 50a AHVG ist die Einrichtung eines Abrufverfahrens jedenfalls nicht als zulässig zu erachten, denn zum einen geht aus letzterer Vorschrift das Abrufverfahren nicht ausdrücklich hervor, und zum anderen erscheint die Bestimmung angesichts der damit einhergehenden Anforderungen als zu unbestimmt. Denn grundlegende datenschutzrechtliche Aspekte – wie die Funktionsweise des Abrufverfahrens, die zugangsberechtigten Stellen, die Rechte der Betroffen, die Kategorien der zu bearbeitenden Daten sowie die Aufbewahrungs- und Löschungsbedingungen – werden darin nicht geregelt. Soweit zudem besonders schützenswerte Personendaten betroffen sind, scheint es ebenfalls an der ausreichenden Bestimmtheit dieser Regelung zu mangeln, dies insbesondere in Bezug auf Art und Ausmass der Datenbearbeitung, die Umschreibung der beteiligten Behörden sowie der genauen Datenkategorien.

- Die notwendigen Rechtsgrundlagen für den Betrieb der nationalen Systeme sollten über den Erlass eines **„horizontalen" Bundesgesetzes** geschaffen werden, das eine eigene Rechtsgrundlage für die Einrichtung und den Betrieb der im Rahmen der Koordinierung der Systeme sozialer Sicherheit in Aussicht genommenen Informationssysteme darstellte.
- Vor dem Erlass einer solchen gesetzlichen Grundlage dürfen solche Informationssysteme nur als **Pilotversuche** im Sinne des **Art. 17a DSG** betrieben werden.

II. Schlussbetrachtung

Im Ergebnis dürfen somit die im Rahmen der Koordinierung der Systeme sozialer Sicherheit notwendigen Datenbearbeitungen auf nationaler Ebene nur dann im Rahmen der vorgesehenen Informationssysteme erfolgen, wenn die hierfür **erforderlichen gesetzlichen Grundlagen geschaffen** werden, wobei im Hinblick auf die Rechtsklarheit und die Rechtssicherheit eine eigene, **horizontale Rechtsgrundlage in einem Bundesgesetz die u.E. beste Lösung** wäre. Dieses mag zwar auf den ersten Blick erstaunen, sind doch die vorgesehenen Datenbe-

arbeitungen – soweit ersichtlich – als erforderlich zur Erfüllung der bereits gesetzlich festgelegten Aufgaben anzusehen, so dass man versucht sein könnte, „dem Datenschutz“ eine Verhinderung der effizienten Wahrnehmung gesetzlicher Aufgaben vorzuwerfen.

Ein solches Vorbringen greift jedoch zu kurz: Der Umstand, dass eine gewisse Datenbearbeitung sinnvoll ist oder sein kann, bedeutet eben gerade noch nicht, dass sie zulässig ist. Der Persönlichkeitsschutz und damit letztlich grund- und menschenrechtliche Vorgaben verlangen hier vielmehr auch gewisse „formelle“ bzw. „formale“ Vorkehrungen. Soweit besonders schützenswerte Personendaten betroffen sind und/oder Informationssysteme geplant sind, in deren Rahmen möglicherweise auch noch ein eigentliches Abrufverfahren vorgesehen ist, geht es dabei in erster Linie um hinreichend klare und hinreichend umfassende Rechtsgrundlagen, damit den datenschutzrechtlichen Grundsätzen auch tatsächlich entsprochen werden kann (verlangen diese doch jeweils nach einer Präzisierung für die jeweils betroffenen Bereiche) und die vorgesehene Datenbearbeitung auch in jeder Hinsicht und für die Betroffenen klar erkennbar geregelt ist. Im Hinblick auf die mit solchen Systemen einhergehenden **Gefährdungen für die Persönlichkeitsrechte der Betroffenen** erscheint dies ebenso sinnvoll wie notwendig, auch wenn hiermit Effizienzverluste einhergehen mögen, darf doch in einem Rechtsstaat Effizienz grundsätzlich kein Grund für die Nichtbeachtung grundlegender rechtsstaatlicher Errungenschaften sein.[290]

[290] Zu diesem Aspekt bereits *Epiney/Fasnacht*, Jusletter v. 24.2.2014, Rn. 78.

G. Verzeichnis der Rechtsakte und Materialien

I. Völkerrecht

DSK	Übereinkommen zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten vom 28. Januar 1981 (Europarats-Konvention Nr. 108), SR 0.235.1
	Erläuternder Bericht des Europarats zum Übereinkommen zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten, Strasbourg 1981 (verfügbar unter <http://conventions.coe.int/Treaty/Commun/QueVoulezVous.asp?CL=GER&NT=108>, zuletzt besucht am 30. April 2015)
EMRK	Konvention zum Schutze der Menschenrechte und Grundfreiheiten (EMRK) vom 4. November 1950, SR 0.101
FZA	Abkommen zwischen der Europäischen Gemeinschaft und ihren Mitgliedstaaten einerseits und der Schweizerischen Eidgenossenschaft andererseits über die Freizügigkeit vom 21. Juni 1999, SR 0.142.112.681
ZP DSK	Zusatzprotokoll zum Übereinkommen zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten bezüglich Aufsichtsbehörden und grenzüberschreitende Datenübermittlung vom 8. November 2001 (Europarats-Konvention Nr. 181), SR 0.235.11

II. Unionsrecht

Primärrecht

AEUV	Konsolidierte Fassung des Vertrags über die Arbeitsweise der Europäischen Union, ABl. 2012 C 326, 47
Grundrechtecharta	Charta der Grundrechte der Europäischen Union, ABl. 2010 C 83, 389

Sekundärrecht

VO 988/2009 Verordnung (EG) Nr. 988/2009 des Europäischen Parlaments und des Rates vom 16. September 2009 zur Änderung der Verordnung zur Koordinierung der Systeme der sozialen Sicherheit und zur Festlegung des Inhalts ihrer Anhänge, ABl. 2009 L 284, 43

VO 987/2009 Verordnung (EG) Nr. 987/2009 des Europäischen Parlaments und des Rates vom 16. September 2009 zur Festlegung der Modalitäten für die Durchführung der Verordnung (EG) Nr. 883/2004 über die Koordinierung der Systeme der sozialen Sicherheit, ABl. 2009 L 284, 1

VO 883/2004 Verordnung (EG) Nr. 883/2004 des Europäischen Parlaments und des Rates vom 29. April 2004 zur Koordinierung der Systeme der sozialen Sicherheit, ABl. 2004 L 166, 1

VO 45/2001 Verordnung (EG) Nr. 45/2001 des Europäischen Parlaments und des Rates vom 18. Dezember 2000 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die Organe und Einrichtungen der Gemeinschaft und zum freien Datenverkehr, ABl. 2001 L 8, 1

VO 574/72 Verordnung (EWG) Nr. 574/72 des Rates vom 21. März 1972 über die Durchführung der Verordnung (EWG) Nr. 1408/71 über die Anwendung der Systeme der sozialen Sicherheit auf Arbeitnehmer und Selbständige sowie deren Familienangehörige, die innerhalb der Gemeinschaft zu- und abwandern, ABl. 1972 L 74, 1

VO 1408/71 Verordnung (EWG) Nr. 1408/71 des Rates vom 14. Juni 1971 zur Anwendung der Systeme der sozialen Sicherheit auf Arbeitnehmer und deren Familien, die innerhalb der Gemeinschaft zu- und abwandern, ABl. 1971 L 149, 2

RL 2009/136 Richtlinie 2009/136/EG des Europäischen Parlaments und des Rates vom 25. November 2009 zur Änderung der Richtlinie 2002/22/EG über den Universaldienst und Nutzerrechte bei elektronischen Kommunikationsnetzen und -diensten, der Richtlinie 2002/58/EG über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre in der elektronischen Kommunikation und der Verordnung (EG) Nr. 2006/2004 über die Zusammenarbeit im Verbraucherschutz (Text von Bedeutung für den EWR), ABl. 2009 L 337, 11

RL 2002/58 Richtlinie 2002/58/EG des Europäischen Parlaments und des Rates vom 12. Juli 2002 über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre in der elektronischen Kommunikation (Datenschutzrichtlinie für elektronische Kommunikation), ABl. 2002 L 201, 37

RL 95/46/EG Richtlinie 95/46/EG des Europäischen Parlaments und des Rates vom 24. Oktober 1995 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr, ABl. 1995 L 281, 31

Materialien

EESSI, Guidelines for the use of Applicable Legislation SEDs, Flows and Portable Document A1, Kreisschreiben des INPS Nr. 167 vom 29.12.2011, Anlage 5 (verfügbar unter <http://www.inps.it/search122/ricerca.aspx?sTrova=circolare+n.+167+del+29-12-2011>, zuletzt besucht am 30. April 2015)

EESSI, Guidelines for the use of Horizontal SEDs and Flows, Kreisschreiben Nr. 167 des INPS vom 29.12.2011, Anlage 6 (verfügbar unter <http://www.inps.it/search122/ricerca.aspx?sTrova=circolare+n.+167+del+29-12-2011>, zuletzt besucht am 30. April 2015)

EESSI, Guidelines for the use of Pension SEDs, Flows and Portable Document P1 d, Kreisschreiben des INPS Nr. 156 vom 15.12.2011, Anlage 5 (verfügbar unter <http://www.inps.it/search122/ricerca.aspx?sTrova=circolare+n.+156+15-12-2011>, zuletzt besucht am 30. April 2015)

Europäische Kommission, Vorschlag vom 25. Januar 2012 für eine Verordnung des Europäischen Parlaments und des Rates zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr (Datenschutz-Grundverordnung), KOM(2012) 11 endg.

III. Schweizerisches Recht

Rechtsakte

AHVG Bundesgesetz über die Alters und Hinterlassenenversicherung (AHVG) vom 20. Dezember 1946, SR 831.10

AHVV Verordnung über die Alters- und Hinterlassenenversicherung (AHVV) vom 31. Oktober 1947, SR 831.101

ATSG Bundesgesetz über den Allgemeinen Teil des Sozialversicherungsrechts (ATSG) vom 6. Oktober 2000, SR 830.1

BGG Bundesgesetz über das Bundesgericht (Bundesgerichtsgesetz, BGG) vom 17. Juni 2005, SR 173.110

BV Bundesverfassung der Schweizerischen Eidgenossenschaft vom 18. April 1999, SR 101

BVG Bundesgesetz über die berufliche Alters-, Hinterlassenen- und Invalidenvorsorge (BVG) vom 25. Juni 1982, SR 831.40

DSG Bundesgesetz über den Datenschutz (DSG) vom 19. Juni 1992, SR 235.1

IVG Bundesgesetz über die Invalidenversicherung (IVG) vom 19. Juni 1959, SR 831.20

KVG Bundesgesetz über die Krankenversicherung (KVG) vom 18. März 1994, SR 832.10

STGB Schweizerisches Strafgesetzbuch vom 21. Dezember 1937, SR 311.0

VDSG Verordnung zum Bundesgesetz über den Datenschutz (VDSG) vom 14. Juni 1993, SR 235.11

Materialien

Bundesamt für Sozialversicherungen (BSV), Entsendungsmerkblatt CH-EU, Soziale Sicherheit für Entsandte zwischen der Schweiz und der EU, April 2012 (verfügbar unter <http://www.bsv.admin.ch/vollzug/documents/index/category:130/lang:deu>, zuletzt besucht am 30. April 2015)

Bundesamt für Sozialversicherungen (BSV), Verbindungsstellen Schweiz: Adressen der schweizerischen Verbindungsstellen und zuständigen Träger (verfügbar unter <http://www.bsv.admin.ch/vollzug/documents/index/category:133/lang:deu>, zuletzt besucht am 30. April 2015)

Bundesrat, Botschaft über die Anpassung und Harmonisierung der gesetzlichen Grundlagen für die Bearbeitung von Personendaten in den Sozialversicherungen vom 24. November 1999, BBl 2000 255

Bundesrat, Botschaft zum Bundesgesetz über den Datenschutz (DSG) vom 23. März 1988, BBl 1988 II 413 (zit.: Botschaft DSG)

Bundesrat, Botschaft zur Änderung des Bundesgesetzes über den Datenschutz (DSG) und zum Bundesbeschluss betreffend den Beitritt der Schweiz zum Zusatzprotokoll vom 8. November 2001 zum Übereinkommen zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten bezüglich Aufsichtsbehörden und grenzüberschreitende Datenübermittlung vom 19. Februar 2003, BBl 2003 2101

Bundesrat, Botschaft zur Genehmigung der bilateralen Abkommen zwischen der Schweiz und der Europäischen Union, einschliesslich der Erlasse zur Umsetzung der Abkommen („Bilaterale II“) vom 1. Oktober 2004, BBl 2004 5965

Eidgenössischer Datenschutz- und Öffentlichkeitsbeauftragter (EDÖB), Leitfaden zu den technischen und organisatorischen Massnahmen des Datenschutzes, Eidgenössischer Datenschutz- und Öffentlichkeitsbeauftragter, September 2011 (verfügbar unter <http://www.edoeb.admin.ch/datenschutz/00628/00629/00636/index.html?lang=de>, zuletzt besucht am 30. April 2015)

Eidgenössischer Datenschutzbeauftragter (EDSB), 11. Tätigkeitsbericht 2003/2004 (verfügbar unter <http://www.edoeb.admin.ch/dokumentation/00153/01027/index.html?lang=de>, zuletzt besucht am 30. April 2015)

Eidgenössischer Datenschutzbeauftragter (EDSB), 4. Tätigkeitsbericht 1996/1997 (verfügbar unter <http://www.edoeb.admin.ch/dokumentation/00153/01027/index.html?lang=de>, zuletzt besucht am 30. April 2015)

Eidgenössischer Datenschutzbeauftragter (EDSB), Gutachten vom 25.04.1996, VPB 60.77

H. Literatur

Amarelle, Cesla/Nguyen, Minh Son (Hrsg.): Code annoté de droit des migrations. Volume III: Accord sur la libre circulation des personnes (ALCP), Bern 2014 (zit.: *Verfasser*, in: Amarelle/Nguyen, Code annoté).

Baeriswyl, Bruno: Entwicklungen und Perspektiven des Datenschutzes in öffentlich-rechtlichen Krankenhäusern – Erfahrungen aus dem Kanton Zürich, in: Hürlimann, Barbara/Jacobs, Reto/Poledna, Thomas (Hrsg.), Datenschutz im Gesundheitswesen, Zürich 2001, 49 ff.

Belser, Eva-Maria/Epiney, Astrid/Waldmann, Bernhard: Datenschutzrecht. Grundlagen und öffentliches Recht, Bern 2011 (zit.: *Verfasser*, in: Belser/Epiney/Waldmann, Datenschutzrecht).

Biaggini, Giovanni: BV Kommentar. Bundesverfassung der Schweizerischen Eidgenossenschaft und Auszüge aus der EMRK, den Uno-Pakten sowie dem BGG, Zürich 2007.

Bieber, Roland/Epiney, Astrid/Haag, Marcel: Die Europäische Union. Europarecht und Politik, 11. Aufl., Baden-Baden 2015 (zit.: *Verfasser*, in: Bieber/Epiney/Haag, EU).

Brunner, Stephan C.: Zur Umsetzung von „Schengen" und „Dublin" im Bereich des Datenschutzes: Drei Thesen, in: Astrid Epiney/Patrick Hobi (Hrsg.), Die Revision des Datenschutzgesetzes / La révision de la Loi fédérale sur la protection des données, Zürich/Basel/Genf 2009, 139 ff.

Cardinaux, Basile: Das Personenfreizügigkeitsabkommen und die schweizerische berufliche Vorsorge, Diss. Freiburg i.Ue.,Zürich/Basel/Genf 2008.

Ellger, Reinhard: Der Datenschutz im grenzüberschreitenden Datenverkehr, Baden-Baden 1990.

Epiney, Astrid: Datenschutz und „Bilaterale II", SJZ 2006, 121 ff.

Epiney, Astrid: Datenschutzrechtliche Rahmenbedingungen. Zu den datenschutzrechtlichen Vorgaben für öffentliche Organe des Bundes und der Kantone, in: Schweizerische Vereinigung für Verwaltungsorganisationsrecht (Hrsg.), Verwaltungsorganisationsrecht – Staatshaftungsrecht – öffentliches Dienstrecht. Jahrbuch 2010, Bern 2011, 5 ff.

Epiney, Astrid: Zur Verbindlichkeit der EU-Grundrechte in der und für die Schweiz, in: Bernhard Altermatt/Gilbert Casasus (Hrsg.), 50 Jahre Engagement der Schweiz im Europarat 1963-2013, Zürich 2013, 141 ff.

Epiney, Astrid: Besonders schützenswerte Personendaten – Zu den Anforderungen an die Rechtmässigkeit der Bearbeitung durch öffentliche Organe im Falle des Fehlens einer gesetzlichen Grundlage, FS Paul-Henri Steinauer, Bern 2013, 97 ff.

Epiney, Astrid: Le champ d'application de la Charte des droits fondamentaux : l'arrêt *Fransson* et ses implications, CDE 2014, 283 ff.

Epiney, Astrid/Civitella, Tamara/Zbinden, Patrizia: Datenschutzrecht in der Schweiz. Eine Einführung in das Datenschutzgesetz des Bundes, mit besonderem Akzent auf den für Bundesorgane relevanten Vorgaben, Freiburger Schriften zum Europarecht Nr. 10, Freiburg 2009.

Epiney, Astrid/Fasnacht, Tobias: Zu den datenschutzrechtlichen Vorgaben für Errichtung und Betrieb von Informationssystemen, Jusletter vom 24. Februar 2014.

Epiney, Astrid/Hofstötter, Bernard/Meier, Annekathrin/Theuerkauf, Sarah: Schweizerisches Datenschutzrecht vor europa- und völkerrechtlichen Herausforderungen. Zur rechtlichen Tragweite der europa- und völkerrechtlichen Vorgaben und ihren Implikationen für die Schweiz, Zürich 2007.

Epiney, Astrid/Metz, Beate/Pirker, Benedikt: Zur Parallelität der Rechtsentwicklung in der EU und in der Schweiz. Ein Beitrag zur rechtlichen Tragweite der „Bilateralen Abkommen", Zürich 2012.

Epiney, Astrid/Schleiss, Yvonne: Ausgewählte Aspekte des Art. 19 Abs. 3 DSG (Abrufverfahren), Jusletter vom 7. November 2011.

Eugster, Gebhard/Luginbühl, Rudolf: Datenschutz in der obligatorischen Krankenpflegeversicherung, in: Hürlimann, Barbara/Jacobs, Reto/Poledna, Thomas (Hrsg.), Datenschutz im Gesundheitswesen, Zürich 2001, 73 ff.

Fuchs, Maximilian (Hrsg.): Europäisches Sozialrecht, 6. Aufl., Baden-Baden/Basel/Wien 2013 (zit.: *Verfasser*, in: Fuchs, Europäisches Sozialrecht).

Gächter, Thomas/Egli, Philipp: Informationsaustausch im Umfeld der Sozialhilfe, Jusletter vom 6. September 2010.

Gächter, Thomas/Siki, Eva: Sozialversicherungsrecht, Allgemeiner Teil. Entwicklungen 2009, Bern 2010.

Hornung, Gerrit: Eine Datenschutz-Grundverordnung für Europa? ZD 2012, 100 ff.

Houstek, Martine: Die Aufsicht über die AHV, CHSS 5/2000, 238 ff.

Kahil-Wolff, Bettina: L'application et l'interprétation de l'ALCP: le cas de la sécurité sociale, in: Astrid Epiney/Beate Metz/Robert Mosters (Hrsg.), Das Personenfreizügigkeitsabkommen Schweiz – EU. Auslegung und Anwendung in der Praxis / L'accord sur la libre circulation des personnes Suisse – UE. Interprétation et application dans la pratique, Zürich 2011, 49 ff.

Kern, Markus: Datenschutzrevision in Europa: Neuer Wein? Neue Schläuche?, digma 2013/01, 34 ff.

Kern, Markus/Epiney, Astrid: Durchsetzungsmechanismen im EU-Recht und ihre Implikationen für die Schweiz, in: Astrid Epiney/Daniela Nüesch (Hrsg.), Durchsetzung der Rechte der Betroffenen im Bereich des Datenschutzes / La mise en œuvre des droits des particuliers dans le domaine de la protection des données, Zürich 2015, 19 ff.

Kieser, Ueli: ATSG-Kommentar, 2. Aufl., Zürich/Basel/Genf 2009.

Körner, Marita: Die Reform des EU-Datenschutzes: Der Entwurf einer EU-Datenschutz-Grundverordnung (DS-GVO), Teil I, ZESAR 2013, 99 ff., Teil II, ZESAR 2013, 153 ff.

Maurer-Lambrou, Urs/Blechta, Gabor P. (Hrsg.): Datenschutzgesetz, Öffentlichkeitsgesetz, Basler Kommentar, 3. Aufl., Basel 2014 (zit.: *Verfasser*, in: Mauer-Lambrou/Blechta, BK Datenschutzgesetz, Öffentlichkeitsgesetz).

Meier, Philippe: Protection des données, Fondements, principes généraux et droit privé, Bern 2011.

Niederer, Christoph/Meyer, Barbara: Grenzüberschreitende Erwerbstätigkeit. Aus sozialversicherungs- und steuerrechtlicher Sicht, ST 10/13, 712 ff.

Oesch, Matthias: Grundrechte als Elemente der Wertegemeinschaft Schweiz – EU. Zur Auslegung der Bilateralen Verträge, ZBl 2014, 171 ff.

Pärli, Kurt: Gutachten „Datenschutz und Datenaustausch in der IIZ" im Auftrag der Nationalen IIZ-Gremien, 2013.

Passadelis, Nicolas/Rosenthal, David/Thür, Hanspeter (Hrsg.): Datenschutzrecht. Beraten in Privatwirtschaft und öffentlicher Verwaltung, Basel 2015 (zit. *Verfasser*, in: Passadelis/Rosenthal/Thür, Datenschutzrecht).

Rosenthal, David/Jöhri, Yvonne: Handkommentar zum Datenschutzgesetz, sowie weiteren, ausgewählten Bestimmungen, Zürich 2008 (zit.: *Verfasser*, in: Rosenthal/Jöhri, Handkommentar DSG).

Rossmanith, Xavier: EESSI – der elektronische Datenaustausch, CHSS 2/2010, 81 ff.

Rossmanith, Xavier/Engel, Robert: Elektronischer Datenaustausch in Europa: Implementierung von EESSI in der Schweiz, CHSS 2/2012, 120 ff.

Rudin, Beat/Baeriswyl, Bruno: „Schengen" und der Datenschutz in den Kantonen: Anforderungen – Beurteilung – Handlungsbedarf, in: Astrid Epiney/Sarah Theuerkauf (Hrsg.), Datenschutz in Europa und die Schweiz / La protection des données en Europe et la Suisse, 2006, 169 ff.

Schreiber, Frank/Wunder, Annett/Dern, Susanne: Kommentar zu VO (EG) Nr. 883/2004. Verordnung zur Koordinierung der Systeme der sozialen Sicherheit, München 2012 (zit.: *Verfasser*, in: Schreiber/Wunder/Dern, Kommentar zur VO 883/2004).

Schulte, Bernd: Die neue europäische Sozialrechtskoordinierung – die Verordnungen (EG) Nr. 883/04 und Nr. 987/09, ZESAR 2010, 143 ff.

Sydow, Gernot/Kring, Markus: Die Datenschutzgrundverordnung zwischen Technikneutralität und Technikbezug. Konkurrierende Leitbilder für den europäischen Rechtsrahmen, ZD 2014, 271 ff.

Walter, Jean-Philippe: La Convention du Conseil de l'Europe pour la protection des personnes à l'égard du traitement automatisé des données, in: Epiney, Astrid/Freiermuth, Marianne (Hrsg.), Datenschutz in der Schweiz und in Europa – La protection des données en Suisse et en Europe, Fribourg 1999, 83 ff.

Walter, Jean-Philippe: Communication des données personnelles à l'étranger, in: Astrid Epiney/Patrick Hobi (Hrsg.), Die Revision des Datenschutzgesetzes – La révsion de la Loi sur la protection des données, Zürich 2009, 99 ff.

Weibel, Rosmarie: Grenzen des Datenaustauschs bei den Sozialversicherungen, Plädoyer 4/2011, 34 ff.

I. Abkürzungen

a.A.	anderer Ansicht
ABl.	Amtsblatt der Europäischen Union
Abs.	Absatz
AHV	Alters- und Hinterlassenenversicherung
AP	Access Point
Art.	Artikel
Aufl.	Auflage
BBl	Bundesblatt der Schweizerischen Eidgenossenschaft
BGE	Amtliche Sammlung der Entscheidungen des Schweizerischen Bundesgerichts
BGer	Bundesgericht
BK	Basler Kommentar
BSV	Bundesamt für Sozialversicherung
bzw.	Beziehungsweise
C	Communications
CDE	Cahiers de droit européen
CHSS	Soziale Sicherheit (Zeitschrift)
d.h.	das heisst
digma	Zeitschrift für Datenrecht und Informationssicherheit
Diss.	Dissertation
Dr.	Doktor
DS-GVO	Datenschutz-Grundverordnung
ebd.	ebenda
EDÖB	Eidgenössischer Datenschutz- und Öffentlichkeitsbeauftragter
EDSB	Eidgenössischer Datenschutzbeauftragter
EDV	Elektronische Datenverarbeitung
EESSI	Electronic Exchange of Social Security Information
EG	Europäische Gemeinschaft
endg.	endgültig
Erw./E.	Erwägung
EU	Europäische Union
EuGH	Gerichtshof der Europäischen Union
EWG	Europäisches Wirtschaftsgemeinschaft
EWR	Europäischer Wirtschaftsraum
f.	folgende
ff.	fortfolgende
Fn.	Fussnote

FS	Festschrift
ggf.	gegebenenfalls
Hrsg.	Herausgeber
i.e.S.	im engeren Sinn
i.S.v.	im Sinne von
i.V.m.	in Verbindung mit
ibid.	ibidem
IIZ	Interinstitutionelle Zusammenarbeit
INPS	Istituto Nazionale della Previdenza Sociale (Italien)
insb.	insbesondere
IV	Invalidenversicherung
KOM	Kommission
L	Législation
lit.	litera
LL.M.	Legum Magister
m.a.W.	mit anderen Worten
m.w.N.	mit weiteren Nachweisen
MLaw	Master of Law
Nr.	Nummer
Prof.	Professorin
RL	Richtlinie
Rn.	Randnote
Rs.	Rechtssache
S.	Satz
s./s.o.	siehe (oben)
SECO	Staatssekretariat für Wirtschaft
SED	Structured electronic Document
SJZ	Schweizerische Juristen-Zeitung (Zeitschrift)
Slg.	Sammlung
SNAP-EESSI	Swiss National Action Plan for Electronic Exchange of Social Security Information
sog.	sogenannt
SR	Systematische Sammlung des Bundesrechts
ST	Der Schweizer Treuhänder (Zeitschrift)
sTESTA	Secure Trans-European Services for Telematics betweeen Administrations
SUVA	Schweizerische Unfallversicherung
u.a.	unter anderem
u.a.m.	und andere(s) mehr
u.E.	unseres Erachtens

Urt.	Urteil
usw.	und so weiter
v.	vom
Vgl.	Vergleiche
VO	Verordnung
vol.	volume
VPB	Verwaltungspraxis der Bundesbehörden
z.B.	zum Beispiel
ZAS	Zentrale Ausgleichsstelle
ZBl	Schweizerisches Zentralblatt für Staats- und Verwaltungsrecht
ZD	Zeitschrift für Datenschutz
ZESAR	Zeitschrift für europäisches Sozial- und Arbeitsrecht
Ziff.	Ziffer
zit.	zitiert

Cahiers fribourgeois de droit européen

Freiburger Schriften zum Europarecht

Publiés sous l'égide de l'Institut de droit européen de l'Université de Fribourg
Herausgegeben vom Institut für Europarecht der Universität Freiburg i. Ü.

Derniers numéros parus / Letzte erschienene Nummern

15 Astrid Epiney
Zur Vereinbarkeit der Einführung einer Alpentransitbörse mit den Vorgaben des EU-Rechts

16 Astrid Epiney / Tobias Fasnacht
Zu den datenschutzrechtlichen Vorgaben für Errichtung und Betrieb von Informationssystemen : unter besonderer Berücksichtigung der Bearbeitung besonders schützenswerter Personendaten und der Zugriffsberechtigung und am Beispiel des Klienten-Informationssystems für Sozialarbeit (KiSS)

17 Astrid Epiney / Emilie M. Praz (traduction)
Zur rechtlichen Tragweite der Art. 121 a, Art. 197 Ziff. 11 BV – ausgewählte Aspekte / La portée juridique des articles 121a et 197 ch. 11 Cst. – aspects choisis

18 Astrid Epiney / Daniela Nüesch
Datenschutzrechtliche Anforderungen für den Betrieb von Informationssystemen im Bereich der Koordinierung der Systeme sozialer Sicherheit zwischen der Schweiz und der EU: aufgezeigt am Beispiel der AHV, der IV und der Unterstellung

Der vorliegende Band geht verschiedenen datenschutzrechtlichen Fragen nach, die sich im Zuge der Einführung der in den VO 883/2009 und der VO 987/2009 (die die Koordinierung der System sozialer Sicherheit betreffen) vorgesehenen elektronischen Informationssysteme stellen. Diese Problematik ist vor dem Hintergrund zu sehen, dass die Schweiz aufgrund der einschlägigen Regelungen des Personenfreizügigkeitsabkommens verpflichtet ist, diese EU-Verordnungen anzuwenden bzw. eine gleichwertige Rechtslage sicherzustellen. Dabei wird in erster Linie untersucht, ob die geltenden Regelungen bereits genügende gesetzliche Grundlagen für den vorgesehenen elektronischen Austausch der Daten enthalten. Diese datenschutzrechtliche Analyse bezieht sich nicht nur auf die europarechtlichen Aspekte und den grenzüberschreitenden Datenaustausch, sondern auch auf die Frage, ob und inwieweit im nationalen (schweizerischen) Recht genügende gesetzliche Grundlagen für den in diesem Zusammenhang notwendigen elektronischen Datenaustausch bestehen.

Astrid Epiney, Rektorin, Prof. Dr. iur., LL.M., Lehrstuhl für Europarecht, Völkerrecht und öffentliches Recht der Universität Freiburg i.Ue., geschäftsführende Direktorin des Instituts für Europarecht.

Daniela Nüesch, MLaw, diplomierte Assistentin, Lehrstuhl für Europarecht, Völkerrecht und öffentliches Recht der Universität Freiburg i.Ue.