

Datenschutz und « Bilaterale II »

Zu den Auswirkungen der Schengen-Assoziierung auf das schweizerische Datenschutzrecht –
ausgewählte Aspekte

*Astrid Epiney**

Dieser Beitrag wurde erstmals wie folgt veröffentlicht:

Astrid Epiney, Datenschutz und „Bilaterale II“. Zu den Auswirkungen der Schengen-Assoziierung auf das schweizerische Datenschutzrecht – ausgewählte Aspekte, Schweizerische Juristenzeitung (SJZ) 2006, S. 121-129. Es ist möglich, dass die Druckversion – die allein zitierfähig ist – im Verhältnis zu diesem Manuskript Abweichungen enthält.

I. Einleitung: Schengen und Datenschutz

Mit der Ratifikation der „Bilateralen II“ wird die Schweiz auch datenschutzrechtliche Bestimmungen des Unionsrechts zu übernehmen bzw. anzuwenden haben. Hierzu gehört neben einigen hier nicht weiter zu erörternden sektoriellen Bestimmungen (in erster Linie im Bereich der polizeilichen Zusammenarbeit¹) die Datenschutzrichtlinie der EG aus dem Jahr 1995 (RL 95/46/EG²). Diese ist nach Anhang B des Schengen-Assoziierungsabkommens³ – neben vielen anderen gemeinschaftlichen Rechtsakten – von der Schweiz anzuwenden. Aufgeworfen wird damit die Frage, welchen Anpassungsbedarf diese Richtlinie für das Datenschutzrecht von Bund und Kantonen auslöst. Diese Problematik ist schon insofern sehr vielschichtig, als der Datenschutzrichtlinie eine Reihe von materiellen Vorgaben zu

* Die Autorin ist Professorin für Europa- und Völkerrecht an der Universität Freiburg (Institut für Europarecht) und Dekanin der dortigen Rechtswissenschaftlichen Fakultät.

¹ Vgl. hierzu etwa *Thomas Wahl*, Datenschutz im Rahmen der polizeilichen Zusammenarbeit unter besonderer Berücksichtigung des SIS, in: *Astrid Epiney/Sarah Theuerkauf* (Hrsg.), *Datenschutz und Bilaterale II – zu den Implikationen des europäischen Datenschutzrechts in der Schweiz*, im Erscheinen.

² Richtlinie 95/46/EG des Europäischen Parlaments und des Rates vom 24.10.1995 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr, ABl. L 281 v. 23.11.1995, 31. Zu dieser Richtlinie aus der umfangreichen Literatur etwa *Ulrich Dammann/Spiros Simitis*, EG-Datenschutzrichtlinie, 1997; *Eugen Ehmann/Marcus Helfrich*, EG-Datenschutzrichtlinie, 1999; *Christoph von Burgsdorff*, Die Umsetzung der EG-Datenschutzrichtlinie im nicht öffentlichen Bereich, 2003; *Rudolf Gridl*, Datenschutz in globalen Kommunikationssystemen, 1999, 229 ff.; *Nikolaos Lavranos*, Datenschutz in Europa – Am Beispiel der Datenschutzrichtlinien, des Schengen Information System (SIS) und Europol, *DuD* 1996, 400 (401 ff.); *Hans-Hermann Schild*, Die EG-Datenschutz-Richtlinie, *EuZW* 1996, 549 ff.; *Ulf Brümann*, Europarechtliche Grundlagen, in: *Alexander Roßnagel* (Hrsg.), *Handbuch Datenschutzrecht*, 2003, Kap. 2.4, Rz. 15 ff.

³ Abkommen zwischen der Schweizerischen Eidgenossenschaft, der Europäischen Union und der Europäischen Gemeinschaft über die Assoziierung dieses Staates bei der Umsetzung, Anwendung und Entwicklung des Schengen-Besitzstandes, BBl. 2004, 6447 ff.; s. auch Botschaft zur Genehmigung der bilateralen Abkommen zwischen der Schweiz und der Europäischen Union, einschliesslich der Erlasse zur Umsetzung der Abkommen („Bilaterale II“) vom 1.10.2004, BBl. 2004, 5965 ff.

entnehmen ist, die hier selbstredend nicht alle erörtert werden können⁴. Vielmehr erfolgt im Folgenden eine Beschränkung (zunächst) auf einen im Zusammenhang mit den „Bilateralen II“ bzw. der Schengen-Assoziierung besonders relevanten Aspekt, nämlich die Frage, für welche Bereiche in der Schweiz im Ergebnis eine Beachtung der RL 95/46 sicherzustellen ist (II.). Weiter soll auf die insbesondere (aber nicht nur) für die Kantone relevante Verpflichtung zur Einrichtung einer unabhängigen Kontrollstelle eingegangen werden (III.). Die Ausführungen schliessen mit einer kurzen Schlussbetrachtung (IV.).

II. Zum Anwendungsbereich der Datenschutzrichtlinie in der Schweiz

Nach Anhang B Schengen-Assoziierung „wendet (die Schweiz) den Inhalt der nachstehend aufgeführten Rechtsakte“, zu denen eben auch die RL 95/46 gehört, an. Durch diese allgemeine Formulierung wird die Frage aufgeworfen, ob die Schweiz die Beachtung der RL 95/46 „flächendeckend“ – letztlich ebenso wie die Mitgliedstaaten – sicherzustellen hat oder ob sie deren Anwendung auf die von der Schengen-Assoziierung erfassten Bereiche beschränken kann (2.). Die Bedeutung dieser Fragestellung erschliesst sich vor dem Hintergrund des (grundsätzlichen) sachlichen Anwendungsbereichs der RL 95/46 (1.).

1. Der Anwendungsbereich der RL 95/46 – Grundsätze

In Bezug auf den sachlichen Anwendungsbereich der RL 95/46/EG ist Art. 3 RL 95/46/EG zentral, der für die Eröffnung des Anwendungsbereichs der RL 95/46/EG zwischen zwei „Konstellationen“ unterscheidet:

- Im Falle automatisierter Verarbeitung personenbezogener Daten⁵ ist die Richtlinie jedenfalls anwendbar; sobald auch nur Teile einer Verarbeitungsreihe automatisiert erfolgen, unterliegt die gesamte Verarbeitungsreihe der Richtlinie⁶.

Die Wiedergabe von Informationen auf einer Internetseite ist jedenfalls automatisiert, da es nach dem gegenwärtigen technischen Verfahren eines Hochladens der jeweiligen Seite auf einen Server sowie der erforderlichen Vorgänge bedarf, um diese Seite den mit

⁴ Vgl. in diesem Zusammenhang die Beiträge in: *Astrid Epiney/Sarah Theuerkauf* (Hrsg.), *Datenschutz und Bilaterale II – zu den Implikationen des europäischen Datenschutzrechts in der Schweiz*, im Erscheinen.

⁵ Vgl. auch die Legaldefinition der personenbezogenen Daten in Art. 2 lit. a RL 95/46, wonach hierunter „alle Informationen über eine bestimmte oder bestimmbar natürliche Person“ zu verstehen sind. Personenbezogene Daten sind also alle Informationen über eine natürliche Person unabhängig davon, welchen Aspekt der Person – zum Beispiel den beruflichen oder privaten Bereich, Eigenschaften, Kenntnisse, physiologische Merkmale, wirtschaftliche Verhältnisse oder Elemente der persönlichen Lebensgeschichte – sie betreffen. Bei der Bestimmbarkeit der Person wird der direkten Identifizierung (etwa durch eine Kennnummer) die Möglichkeit der indirekten Identifizierung (über die Zuordnung zu einem oder mehreren spezifischen Elementen, die Ausdruck der Identität der Person sind) gleichgestellt.

⁶ Vgl. *Ferdinand Kopp*, *Tendenzen der Harmonisierung des Datenschutzrechts in Europa*, DuD 1995, 204 (207).

dem Internet verbundenen Personen zugänglich zu machen, Vorgänge, die zumindest teilweise in automatisierter Form erfolgen⁷. Daraus folgt, dass das Aufladen einer Internetseite, die auf verschiedene Personen hinweist und diese durch die Namensnennung oder auf andere Weise identifiziert, in den Anwendungsbereich der RL 95/46/EG fällt.

- Bei manueller Verarbeitung von personenbezogenen Daten ist hingegen Voraussetzung, dass die Daten in Dateien gespeichert sind oder gespeichert werden sollen⁸.

Klassische Akten, die keine strukturierten personenbezogenen Datensammlungen enthalten, fallen daher grundsätzlich nicht in den Anwendungsbereich der Richtlinie⁹. Hingegen sind „strukturierte Akten“ – also solche, die aufgrund von Aktenzeichen, Schlüsseln oder sonstigen Verfahren einen strukturierten und damit leichten Zugriff auf Daten ermöglichen – auf der Grundlage der Definition des Begriffs der Dateien in Art. 2 RL 95/46/EG erfasst¹⁰. Die Grenze des (Nicht-) Einbezugs von Akten und Aktensammlungen verläuft damit zwischen (wenn auch nur minimal) strukturierten und unstrukturierten Sammlungen, so dass Akten, die etwa nach Name oder Beruf geordnet sind, in den Anwendungsbereich der RL 95/46/EG fallen, während dies bei aufeinander gestapelten Klarsichthüllen über bestimmte Themen, in die Dokumente einfach „hineingesteckt“ werden, nicht der Fall ist¹¹.

Der Schutz beginnt nicht erst mit der physischen Einfügung personenbezogener Daten in eine Datei, sondern bereits mit der Erhebung, wenn vorgesehen ist, dass die Daten später in eine Datei aufgenommen werden sollen. Steht noch nicht fest, ob dies erfolgen soll, reicht es aus, wenn nach dem Zuschnitt der erfolgten oder beabsichtigten Verarbeitung und den bei dieser Verarbeitung bestehenden Gepflogenheiten objektiv eine dateiförmige Verarbeitung zu erwarten ist¹².

Insgesamt spielt damit die Unterscheidung zwischen manueller und automatischer Datenverarbeitung im Rahmen der RL 95/46/EG kaum noch eine Rolle; vielmehr dürfte sie auf der Grundlage der skizzierten Kriterien auch auf die meisten manuellen Verarbeitungen Anwendung finden¹³.

Weiter ist darauf hinzuweisen, dass die Anwendbarkeit der RL 95/46/EG nicht von der Existenz eines irgendwie gearteten grenzüberschreitenden Bezugs abhängt: Zwar wurde die Richtlinie auch zur Verwirklichung des Binnenmarktes erlassen, und es ist sicherlich kaum zu

⁷ EuGH, Rs. C-101/01, *Lindqvist*, Slg. 2003, I-12971, Rz. 26. Zustimmend etwa *Ludovic Coudray*, Case Law, CMLRev. 2004, 1361 (1370 ff.).

⁸ *Ehmann/Helfrich*, EG-Datenschutzrichtlinie (Fn. 2), Art. 3, Rz. 8; *Alexander Viethen*, Datenschutz als Aufgabe der EG, 2003, 39; *Dammann/Simitis*, EG-Datenschutzrichtlinie (Fn. 2), Art. 3, Rz. 5.

⁹ *Lavranos*, DuD 1996 (Fn. 2), 400 (402), m.w.N. Näher dazu auch *Ehmann/Helfrich*, EG-Datenschutzrichtlinie (Fn. 2), Art. 3, Rz. 12 ff., Art. 2, Rz. 32 f.; *Dammann/Simitis*, EG-Datenschutzrichtlinie (Fn. 2), Art. 2, Rz. 8.

¹⁰ *Ehmann/Helfrich*, EG-Datenschutzrichtlinie (Fn. 2), Art. 1, Rz. 16, Art. 2, Rz. 33 ff.

¹¹ *Dammann/Simitis*, EG-Datenschutzrichtlinie (Fn. 2), Einleitung, Rz. 48.

¹² Ebenso *Dammann/Simitis*, EG-Datenschutzrichtlinie (Fn. 2), Art. 3, Rz. 5.

¹³ Ähnlich *Herbert Burkert*, Internationale Grundlagen, in: Alexander Roßnagel, Handbuch Datenschutzrecht, 2003, Kap. 2.3, B, V, Rz. 44.

bestreiten, dass sie die Bedingungen für Funktionieren und Errichtung des Binnenmarktes verbessert, führt sie doch zu einer Angleichung des Datenschutzniveaus in den Mitgliedstaaten mit der Folge der Erleichterung des grenzüberschreitenden Kommunikationsflusses. Dies bedeutet jedoch nicht, dass die Richtlinie nur im Falle des Bestehens eines grenzüberschreitenden Bezugs anwendbar wäre. Dies würde zu Ungewissheiten und letztlich Zufälligkeiten hinsichtlich der Anwendbarkeit der Richtlinie führen. Im Übrigen sind auch Art. 3 Abs. 1 RL 95/46/EG keinerlei Anhaltspunkte darüber zu entnehmen, dass ein grenzüberschreitender Bezug eine Voraussetzung für die Anwendbarkeit der Richtlinie wäre und dass ein solches Erfordernis die Verwirklichung eines Teils der Zielsetzungen der RL 95/46/EG in Frage stellte¹⁴.

2. Zur Relevanz der RL 95/46 für die Schweiz im Rahmen der „Bilateralen II“

Die Datenschutzrichtlinie (RL 95/46) ist nach Anhang B der Schengenassoziiierung – neben vielen anderen gemeinschaftlichen Rechtsakten – von der Schweiz anzuwenden. Es ist bemerkenswert, dass weder dieser Anhang B des Abkommens noch der Abkommenstext selbst ausdrücklich¹⁵ Hinweise darauf enthalten, dass die RL 95/46 nur in den von der Schengen/Dublin-Assoziierung erfassten Bereichen anzuwenden ist. Daher fragt es sich, ob die Vorgaben der Richtlinie nicht nur in von der Schengen/Dublin-Assoziierung betroffenen Bereichen, sondern darüber hinaus in allen von ihrem Anwendungsbereich erfassten Gebieten massgeblich sind, mit der Folge, dass die Schweiz die RL 95/46 im Ergebnis letztlich wie ein EU-Mitgliedstaat anzuwenden hätte. Die Auswirkungen im Falle der Bejahung dieser Frage sind nicht zu unterschätzen, implizierte eine allgemeine Anwendung der Datenschutzrichtlinie doch auch deren Relevanz etwa im Gesundheitsbereich (Spitäler) oder im Schulsektor. Aus gemeinschaftsrechtlicher Sicht ist der Anwendungsbereich der Datenschutzrichtlinie nämlich – wie erörtert¹⁶ – denkbar weit, findet sie doch allgemein im Falle automatisierter Verarbeitung personenbezogener Daten und bei manueller Verarbeitung personenbezogener Daten, die in Dateien gespeichert werden, Anwendung; weiter ist sie unabhängig vom Vorliegen eines grenzüberschreitenden Bezugs heranzuziehen. Hinzuweisen ist allerdings auf darauf, dass die polizeiliche Zusammenarbeit jedenfalls nicht in ihren Geltungsbereich fällt, da hier spezifische Regelungen zum Zuge kommen¹⁷.

¹⁴ Vgl. EuGH, verb. Rs. C-465/00, C-138/01, C-139/01, *Rechnungshof/Österreichischer Rundfunk* (Fn. 5), Rz. 39 ff. Diese Rechtsprechung bestätigend EuGH, Rs. C-101/01, *Lindqvist*, Slg. 2003, I-12971, Rz. 40 ff., wonach auch der Klausel in Art. 3 Abs. 2 erster Spiegelstrich RL 95/46/EG, nach der die Richtlinie keine Anwendung auf Tätigkeiten findet, die nicht in den Anwendungsbereich des Gemeinschaftsrechts fallen, nichts anderes zu entnehmen sei. Zustimmend etwa *Coudray*, CMLRev. 2004 (Fn. 7), 1361 (1368 ff.).

¹⁵ Zu Art. 2 Abs. 2 Schengenassoziiierung noch sogleich im Text.

¹⁶ S.o. II.1.

¹⁷ Vgl. hierzu *Wahl*, in: *Datenschutz und Bilaterale II* (Fn. 1). S. im Übrigen auch den Vorschlag der Kommission vom 4.10.2005 für einen Rahmenbeschluss des Rates über den Schutz personenbezogener Daten, die im Rahmen der polizeilichen und justiziellen Zusammenarbeit in Strafsachen verarbeitet

Die Frage der Reichweite der Verpflichtung der Schweiz, u.a. die RL 95/46 mit der Ratifizierung des Abkommens über die Schengen-Assoziierung anzuwenden, wurde bemerkenswerterweise in der Botschaft des Bundesrates zu den Bilateralen II nicht eigens erörtert; vielmehr beschränkt sich der Bundesrat in dem allgemeinen Abschnitt über Datenschutz darauf festzuhalten, dass die RL 95/46 „mithin auch für alle Aspekte der Schengener Zusammenarbeit“ gelte¹⁸; daran anschliessend werden die inhaltlichen Vorgaben der RL 95/46 skizziert. Allerdings deuten andere Teile der Botschaft und die vorgenommenen bzw. in Aussicht gestellten Gesetzgebungsvorhaben darauf hin, dass der Bundesrat lediglich von einer „sektoriellen Massgeblichkeit“ der RL 95/46 (in den Bereichen, die von Schengen / Dublin abgedeckt sind) ausgeht, so wenn er in verschiedene bereichsspezifische Gesetze eigens datenschutzrechtliche Bestimmungen einführen will, die den datenschutzrechtlichen Anforderungen der RL 95/46 Rechnung tragen¹⁹. Was die derzeit laufende Revision des Datenschutzgesetzes angeht²⁰, so hält der Bundesrat fest, dass nur punktuellen Mängeln Abhilfe geschaffen und den Anliegen der diesbezüglichen Motionen²¹ Rechnung getragen werden solle; hingegen gehe es gerade nicht um eine umfassende Revision des Datenschutzgesetzes, um es allgemein mit den Anforderungen der RL 95/46 in Einklang zu bringen. Eine solche werde aber notwendig, wenn sich die Schweiz im Rahmen einer Assoziierung an Schengen/Dublin zu einer Anwendung der RL 95/46 verpflichte²². Wenn man auch in diese Formulierung sicherlich nicht bereits eine eigentliche Stellungnahme zu den Folgen der ja erst später tatsächlich unterzeichneten Schengen-Assoziierung hineinlesen kann, so deutet sie doch darauf hin, dass im Falle einer Assoziierung an Schengen und der damit verbundenen „Anwendung“ der RL 95/46 in der Schweiz eine umfassende Anpassung des Datenschutzgesetzes für notwendig erachtet wurde, dies offenbar auf der Grundlage des umfassenden Anwendungsbereichs der RL 95/46 auch für nicht durch die Schengen-Assoziierung erfasste Bereiche. Umsomehr erstaunt es, dass in der Botschaft zu den Bilateralen II ohne nähere Begründung offenbar eine andere Sicht zugrunde gelegt wird. Betrachtet man nun die rechtlichen Vorgaben in der Schengen-Assoziierung, so könnte die sachliche Beschränkung des Abkommens auf den Schengen-Besitzstand tatsächlich auf den ersten Blick die Annahme nahe legen, die Vorgaben der RL 95/46 seien lediglich für die von der Assoziierung erfassten Bereiche – also den Schengen-Besitzstand (sowie für den Dublin-

werden, KOM (2005) 475 endg., der die derzeitigen eher zersplitterten und sektoriellen Regelungen für die verschiedenen Bereiche zusammenfassen soll, wobei jedoch Europol und Eurojust nach wie vor ausgenommen werden sollen; hier sollen auch weiterhin eigene datenschutzrechtliche Standards zum Zuge kommen.

¹⁸ Vgl. Botschaft zur Genehmigung der bilateralen Abkommen zwischen der Schweiz und der Europäischen Union, einschliesslich der Erlasse zur Umsetzung der Abkommen („Bilaterale II“) vom 1.10.2004, BBl. 2004, 5965 (6108).

¹⁹ Vgl. Botschaft „Bilaterale II“, BBl. 2004, 5965 (6236 ff., 6250 ff., 6260 ff., 6282) in Bezug auf das ANAG, das Asylgesetz, das Waffenrecht und das Betäubungsmittelrecht.

²⁰ Vgl. die Botschaft in BBl. 2003, 2101.

²¹ Motion 2000 M 00.3000 zur erhöhten Transparenz bei der Erhebung von Personendaten; 1999 M 98.3529 zum erhöhten Schutz von Personendaten bei Online-Verbindungen.

²² Vgl. Botschaft zur Änderung des DSG, BBl. 2003, 2101 (2107).

Besitzstand) – zu beachten. Denn der sachliche Anwendungsbereich des Assoziierungsabkommens erstreckt sich nur (aber immerhin) auf den im Einzelnen im Anhang A umschriebenen Schengen-Besitzstand.

Eine nähere Analyse von Struktur und Zielsetzungen des Abkommens vor dem Hintergrund der Charakteristika des Gemeinschaftsrechts legt jedoch eine andere Sicht nahe: Zunächst finden sich in dem Abkommen selbst keinerlei Hinweise darauf, dass die RL 95/46 lediglich „sektoriell“ anzuwenden wäre, im Gegenteil: Im hier relevanten Anhang B wird die Schweiz im ersten Satz allgemein verpflichtet, „den Inhalt der nachstehend aufgeführten Rechtsakte“ – zu denen auch die RL 95/46 gehört – anzuwenden, was darauf schliessen lässt, dass die im Anhang B genannten Rechtsakte als solche vollumfänglich massgeblich und damit anzuwenden sind. Dieser Schluss wird durch Art. 1 Schengen-Assoziierung bestätigt, wonach die Schweiz allgemein „in den Bereichen, die Gegenstand der in den Anhängen A und B genannten Bestimmungen sind, sowie bei der Weiterentwicklung dieser Bestimmungen assoziiert“ wird. Hieran vermag auch Art. 2 Abs. 2 Schengen-Assoziierung – wonach die in Anhang B aufgeführten Bestimmungen insoweit von der Schweiz umgesetzt und angewandt werden, als sie Bestimmungen des Schengen-Besitzstandes ersetzen bzw. weiterentwickeln oder aufgrund des Schengener Abkommens angenommen worden sind – nichts zu ändern: Denn der in Bezug auf die RL 95/46 allein in Betracht kommende zweite Variante kann wohl nur entnommen werden, dass der „Rechtsgrund“ der Annahme des jeweiligen Rechtsakts – wobei in Bezug auf den Begriff der Annahme unklar bleibt, ob dieser sich auf den Erlass des jeweiligen Rechtsakts oder auf dessen Einbezug in die Schengen-Assoziierung bezieht²³ – im Zusammenhang mit dem Schengen-Besitzstand stehen muss, während der Geltungsbereich selbst der im Anhang B genannten Rechtsakte hingegen nicht eingeschränkt wird. Eine Beschränkung des materiellen Anwendungsbereichs der in Anhang B genannten Rechtsakte könnte auch nicht durch eine solche „Generalklausel“ vorgenommen werden, da sich die Frage der genauen Fassung des Anwendungsbereichs dieser Rechtsakte jeweils anders stellt oder zumindest stellen kann. Vor diesem Hintergrund dürfte sich die Tragweite dieser Klausel in Art. 2 Abs. 2 Schengen-Assoziierung darauf beschränken, dass der Zusammenhang der genannten Rechtsakte mit dem Schengen-Besitzstand hergestellt wird bzw. (für die erste Alternative) dass nur die Weiterentwicklungen des Schengen-Besitzstandes einbezogen werden.

Darüber hinaus und vor allem ist spezifisch in Bezug auf die RL 95/46 von Bedeutung, dass die mit „Schengen/Dublin“ einhergehende enge Zusammenarbeit der Behörden in zahlreichen Bereichen ein Mindestmass an Datenschutz in den teilnehmenden Staaten impliziert; eine Art sektorielle Abgrenzung je nach Relevanz für den Schengen/Dublin-Besitzstand ist schon insofern nicht überzeugend, als gerade im Bereich der Datenverarbeitung vielfältige Verbindungen und Interdependenzen bestehen, so dass sich Mängel in einem bestimmten

²³ Wobei sicherlich letzterer Aspekt gemeint sein dürfte, denn weder die RL 95/46 noch viele andere Rechtsakte wurden „aufgrund des Schengener Abkommens“ angenommen.

Bereich auf andere Bereiche auswirken können, ganz abgesehen davon, dass die Abgrenzung zwischen „schengen- oder dublinrelevant“ oder nicht ggf. recht schwierig sein kann. Man denke etwa an das Beispiel eines sich in Spitalbehandlung befindlichen Asylbewerbers, dessen Krankendaten nicht angemessen geschützt werden. Vor diesem Hintergrund spricht die Zielsetzung des Einbezugs der RL 95/46 in die durch die Schweiz i.Erg. anzuwendenden Rechtsakte – nämlich die Sicherstellung eines Mindestniveaus an Datenschutz angesichts der durch die Schengenassoziiierung vereinbarten engen Zusammenarbeit in zahlreichen Bereichen mit den damit implizierten Datenaustausch – für eine Verpflichtung der Schweiz, die RL 95/46 als solche vollumfänglich anzuwenden.

Insgesamt ergibt sich damit aus dem Abkommen über die Schengen-Assoziierung – entgegen mancher anderslautender Äusserungen – nach der hier vertretenen Ansicht eine Pflicht der Schweiz, die RL 95/46 allgemein, und nicht nur in den vom Schengen-Besitzstand erfassten Bereichen, anzuwenden, womit ein Mindeststandard an datenschutzrechtlichen Garantien sichergestellt werden soll, dies letztlich mit dem Ziel, in diesem Bereich einen mit der Rechtslage in der EU vergleichbaren Standard zu gewährleisten.

Nur am Rande sei in diesem Zusammenhang noch bemerkt, dass eine Differenzierung der „Umsetzung“ der RL 95/46 je nach vom Schengen- und/oder Dublinbesitzstand erfassten Materien auch nicht aus der Sicht des nationalen Rechts nicht sinnvoll wäre, ist doch nur schwer einsehbar, warum in bestimmten („schengenrelevanten“) Bereichen ein verstärkter Datenschutzstandard oder weitergehende Kontrollmöglichkeiten unabhängiger Datenschutzkontrollstellen zum Zuge kommen sollen, in anderen vergleichbaren Bereichen jedoch nicht. Jedenfalls bleibt es gerade den Kantonen unbenommen, im Rahmen der in jedem Fall notwendigen Anpassung der kantonalen Gesetzgebung sich auch allgemein an die Vorgaben der RL 95/46 anzulehnen.

III. Zum Handlungsbedarf in der Schweiz: die Verpflichtung zur Einrichtung einer unabhängigen Kontrollstelle

Damit müsste also die Schweiz die Datenschutzrichtlinie vollumfänglich beachten. Der sich hieraus ergebende Handlungsbedarf sollte aber – soweit die materiellen datenschutzrechtlichen Grundsätze betroffen sind – nicht überschätzt werden: Ohne dies hier im Einzelnen ausführen zu können, dürfte nämlich den Grundanforderungen der Datenschutzrichtlinie an die Datenverarbeitung – Stichworte sind hier das Zweckbestimmungsprinzip, die Verhältnismässigkeit, die grundsätzliche Notwendigkeit einer gesetzlichen Grundlage oder der Einwilligung der Betroffenen für eine Datenverarbeitung sowie besondere Vorkehrungen für sensible Daten (wie etwa solche über den Gesundheitszustand oder religiöse Überzeugungen) – in der schweizerischen

Datenschutzgesetzgebung auf Bundes- und Kantonsebene entsprochen werden²⁴; dies gilt jedoch nur insoweit, als tatsächlich eine Datenschutzgesetzgebung existiert, was nicht in allen Kantonen der Fall ist. Insoweit besteht also auf kantonaler Ebene jedenfalls (teilweise) Handlungsbedarf.

Von Bedeutung insbesondere für die kantonale Ebene ist aber die auch in einem Zusatzprotokoll zur Datenschutzkonvention des Europarates²⁵ enthaltene Vorgabe der Datenschutzrichtlinie, „völlig unabhängige Kontrollstellen“ einzurichten, die die Einhaltung der Anforderungen der in Umsetzung der Datenschutzrichtlinie ergangenen mitgliedstaatlichen Gesetzgebung überwachen sollen. So haben die Kontrollstellen die „ihnen zugewiesenen Aufgaben in völliger Unabhängigkeit“ wahrzunehmen. (Art. 28 Abs. 1 RL 95/46). Da der Eidgenössische Datenschutzbeauftragte nicht für die Überwachung der datenschutzrelevanten Tätigkeiten kantonaler Behörden zuständig ist, müssen ausgehend von dieser Anforderung auch die Kantone solche Kontrollstellen schaffen. Im Einzelnen verpflichtet Art. 28 RL 95/46 dazu, zur Überwachung der Anwendungen der Richtlinie in den Mitgliedstaaten eine oder mehrere²⁶ „völlig unabhängige“ Kontrollstelle(n) zu schaffen; diese sind für die Kontrolle aller Verarbeitungen zuständig, die auf dem Hoheitsgebiet ihres Mitgliedstaates stattfinden, unabhängig vom einzelstaatlichen Recht, das auf die jeweilige Verarbeitung anzuwenden ist (Art. 28 Abs. 6 RL 95/46/EG).

Die genaue rechtliche Tragweite dieser Bestimmung wirft einige Fragen auf, wobei diejenige nach der Ausgestaltung der Unabhängigkeit der Kontrollstelle(n) (1.) und diejenige nach den den Kontrollstellen einzuräumenden Befugnissen (2.) von besonderer Bedeutung sind.

1. Unabhängigkeit der Kontrollstelle

Art. 28 Abs. 1 RL 95/46 verpflichtet nur (aber immerhin) dazu, völlig unabhängige Kontrollstellen einzurichten, womit lediglich das Ergebnis vorgegeben wird. Die genaue Ausgestaltung der Unabhängigkeit bleibt damit den Mitgliedstaaten überlassen²⁷, so dass insbesondere nicht eine irgendwie geartete institutionelle Ausgestaltung (etwa die Schaffung einer juristischen Person) gefordert ist (Unabhängigkeit nicht als Organisationsmerkmal,

²⁴ Vgl. zu den Anforderungen der RL 95/46 im Einzelnen in diesem Zusammenhang *Epiney/Theuerkauf*, in: Datenschutz und Bilaterale II (Fn. 4).

²⁵ Die Texte sind unter www.conventions.coe.int/ im Internet abrufbar. Die Revision des Datenschutzgesetzes auf Bundesebene trägt den Anforderungen dieses Protokolls bereits Rechnung. Vgl. Botschaft zur Änderung des DSG, BBl. 2003, 2101 ff.

²⁶ Die Richtlinie nimmt damit Rücksicht auf die föderalistische Struktur mancher Mitgliedstaaten, wie zum Beispiel Deutschland, wo es neben dem Bundesdatenschutzbeauftragten auch Datenschutzbeauftragte der einzelnen Bundesländer gibt, vgl. *Ehmann/Helfrich*, EG-Datenschutzrichtlinie (Fn. 2), Art. 28, Rz. 1; *Gridl* (Fn.), 256; *Dammann/Simitis*, EG-Datenschutzrichtlinie (Fn. 2), Art. 28, Rz. 4.

²⁷ Zum Kriterium der Unabhängigkeit ausführlich *Brühmann*, in: Handbuch Datenschutzrecht (Fn. 2), Kap. 2.4, Rz. 42 f.; *Georgios Gounalakis/Elmar Mand*, Die neue EG-Datenschutzrichtlinie – Grundlagen einer Umsetzung in nationales Recht, CR 1997, 497, 501 f., mit Hinweisen auf hier im Einzelnen bestehende Meinungsstreitigkeiten.

sondern als Tätigkeitsqualifikation²⁸). Diese Sicht ergibt sich bereits aus der Entstehungsgeschichte der Vorschrift, wurde doch das Erfordernis der Unabhängigkeit als Organisationsmerkmal der Stelle zugunsten der Unabhängigkeit als Qualifikation der Tätigkeit ersetzt²⁹. Vor diesem Hintergrund schließen eine organisatorische „Einbettung“ in die staatliche Behördenstruktur und eine gerichtliche oder parlamentarische Kontrolle durch staatliche Organe die Unabhängigkeit nicht a priori aus; dies ergibt sich im Übrigen schon daraus, dass nach Art. 28 Abs. 3 am Ende RL 95/46/EG gegen beschwerende Entscheidungen der Kontrollstelle der Rechtsweg eröffnet ist und ihre Tätigkeiten damit der gerichtlichen Kontrolle unterliegen.

Soll die Kontrollstelle – was jedenfalls von Art. 28 RL 95/46 gefordert wird – ihre Aufgaben in „völliger Unabhängigkeit“ wahrnehmen können, so muss allgemein in funktionaler Hinsicht sichergestellt sein, dass die Kontrollstellen frei von jedem Einfluss ihre Entscheidungen vorbereiten und umsetzen können³⁰. Jede Einflussnahme von außen muss daher ausgeschlossen sein, und die Wahrnehmung der personellen und finanziellen Angelegenheiten der Kontrollstelle muss so ausgestaltet sein, dass ihre Unabhängigkeit nicht in Frage gestellt wird³¹. Die Unabhängigkeit ist damit nicht nur gegenüber den „Kontrollierten“, sondern gegenüber allen hoheitlichen und privaten Akteuren zu gewährleisten³².

Diese allgemein formulierten Anforderungen an die Unabhängigkeit der Kontrollstelle entfalten auf verschiedenen Ebenen Implikationen, womit die für die geforderte Unabhängigkeit notwendigen (Mindest-) Kriterien formuliert werden können:

- Die Kontrollstelle muss völlig weisungsfrei handeln. Eine irgendwie geartete staatliche Aufsicht, auch wenn sie auf die Rechtmäßigkeit beschränkt ist, dürfte mit der Unabhängigkeit der Kontrollstelle nicht vereinbar sein³³, da die Frage der Rechtmäßigkeit des Handelns der Kontrollstelle sehr häufig eng mit der Art und Weise der Ausübung der Kontrollstelle verbunden sein wird. Denkbar ist damit – neben der gerichtlichen Kontrolle – im Falle der Einbindung der Kontrollstelle in die Verwaltung lediglich eine „verwaltungsmäßige“ Kontrolle insbesondere durch das Parlament, ähnlich wie sie häufig für die Gerichte vorgesehen ist. Dabei müssen derartige Kontrollmechanismen so ausgestaltet sein, dass sie von vornherein keine Implikationen

²⁸ Vgl. *Brühann*, in: Handbuch Datenschutzrecht (Fn. 2), Kap. 2.4, Rz. 42; *Dammann/Simitis*, EG-Datenschutzrichtlinie (Fn. 2), Art. 28, Rz. 5.

²⁹ Vgl. *Brühann*, in: Handbuch Datenschutzrecht (Fn. 2), Kap. 2.4, Rz. 42.

³⁰ Ebenso *Burkert*, in: Handbuch Datenschutzrecht (Fn. 13), Kap. 2.3, B, V, Rz. 55; *Dammann/Simitis*, EG-Datenschutzrichtlinie (Fn. 2), Art. 28, Rz. 5 f.; *Johanna Kübler*, Die Säulen der EU, 2002, 93 f.; *von Burgsdorff*, Umsetzung der EG-Datenschutzrichtlinie (Fn. 2), 91.

³¹ S. in diesem Zusammenhang auch *Ehmann/Helfrich*, EG-Datenschutzrichtlinie (Fn. 2), Art. 28, Rz. 3 ff., die davon ausgehen, dass die „völlige Unabhängigkeit“ nur bei kumulativem Vorliegen der institutionellen, funktionellen und materiellen Unabhängigkeit gegeben sei, was i.Erg. der hier vertretenen Ansicht entspricht.

³² Unklar insofern *Kopp*, DuD 1995 (Fn. 6), 204 (211).

³³ Wie hier *Ehmann/Helfrich*, EG-Datenschutzrichtlinie (Fn. 2), Art. 28, Rz. 6; wohl auch *Dammann/Simitis*, EG-Datenschutzrichtlinie (Fn. 2), Art. 28, Rz. 5 f.; a.A. ohne nähere Begründung *Brühann*, in: Handbuch Datenschutzrecht (Fn. 2), Kap. 2.4, Rz. 44.

für die Wahrnehmung der Aufgaben durch die Kontrollstelle entfalten können. Dies dürfte insbesondere implizieren, dass Art und Inhalt der Kontrolle klar im Voraus festgelegt sind und jedenfalls keinen Zusammenhang mit der Wahrnehmung der eigentlichen Aufgaben der Kontrollstelle (Kontrolle der Einhaltung der datenschutzrechtlichen Vorgaben) aufweisen dürfen. In Betracht kommen damit etwa Rechnungsführungskontrollen oder auch gewisse disziplinarische Massnahmen.

- Die (erstmalige) Bestellung der leitenden Organe oder des Leiters / der Leiterin der Kontrollstelle darf nicht einzig durch die Exekutive erfolgen, könnte diese doch auf diese Weise Einfluss auf die Ausübung der Tätigkeit der Behörde nehmen. Ein Einbezug des Parlaments³⁴ oder auch von Gerichten ist daher notwendig; dieser kann unterschiedlich ausgestaltet sein. Weiter dürfen Leitung und / oder Mitglieder des leitenden Gremiums nur in genau bestimmten Ausnahmefällen entlassen werden bzw. ihr Mandat darf nur in solchen Ausnahmefällen nicht wieder erneuert werden, könnte doch ansonsten über die Drohung der Nichtwiederwahl oder der Nichtwiederernennung die Unabhängigkeit der Behörde in Frage gestellt werden.
- Interessenskonflikte der Kontrollstelle – etwa aufgrund anderer Aufgaben – müssen ausgeschlossen sein. Vor diesem Hintergrund wird eine Kontrollstelle in der Regel nur dann die Voraussetzung der Unabhängigkeit erfüllen, wenn sie neben den Aufgaben als Kontrollstelle für Datenschutz keine weiteren Aufgaben (z.B. im Zusammenhang mit der Überwachung eines Gewerbes oder der Überwachung bestimmter Behörden) wahrnimmt.
- Die Kontrollstelle muss über genügend Personal- und Finanzmittel verfügen, um ihre Aufgaben wahrnehmen zu können, und ihr muss im Rahmen des vorgesehenen Budgets eine gewisse Budgethoheit zustehen. Nur durch diese Voraussetzung kann – im Sinne der Effektivität der Errichtung der unabhängigen Kontrollstelle – gewährleistet werden, dass die Stelle ihre Aufgaben auch tatsächlich wahrnehmen kann.

2. Befugnisse

Die Kontrollstellen haben ganz allgemein die „Anwendung der von den Mitgliedstaaten zur Umsetzung dieser Richtlinie erlassenen einzelstaatlichen Vorschriften in ihrem Hoheitsgebiet zu überwachen“ (Art. 28 Abs. 1 RL 95/46). Im Einzelnen ist ihnen jedenfalls die Möglichkeit einzuräumen, zu gesetzgeberischen Entwürfen mit datenschutzrechtlicher Relevanz Stellungnahmen abzugeben (Art. 28 Abs. 2 RL 95/46/EG). Darüber hinaus wird man aus der allgemeinen Aufgabenbeschreibung der Kontrollstellen in Art. 28 Abs. 1 RL 95/46 ableiten können, dass sie mit Bezug auf die Wahrnehmung der Kontrollbefugnisse mit den zur

³⁴ Wie auch die vielfach übliche Ernennung von Richtern durch die Legislative zeigt. Allerdings muss diese ihre Aufgabe auch unter Beachtung der Unabhängigkeit der Kontrollstelle ausüben.

Erfüllung dieser Aufgaben notwendigen Befugnissen auszustatten sind. Art. 28 Abs. 3 RL 95/46 führt – ohne dass er in allgemeiner Form die den Kontrollstellen einzuräumenden Befugnisse umschreibt – nicht abschliessend einige Befugnisse auf, die den Kontrollstellen jedenfalls zustehen müssen:

- Erstens müssen sie über Untersuchungsbefugnisse verfügen (Art. 28 Abs. 3 erster Spiegelstrich), wobei diese Befugnisse im Einzelnen so auszugestalten sind, dass die Kontrollstelle alle für die Erfüllung ihres Auftrags erforderlichen Informationen einholen können müssen. Damit sind den Kontrollstellen also umfassende Zugangs- und Untersuchungsbefugnisse einzuräumen, und ihnen muss die Kompetenz zukommen, letztlich alle Daten, die Gegenstand von Verarbeitungen sind, sowie die Verarbeitungsvorgänge einzusehen, dies jederzeit, nicht nur bei Vorliegen besonderer Verdachtsmomente oder Anlässe. Materiell müssen sich diese Befugnisse auf die Untersuchungen erstrecken können, die für die Wahrnehmung der Kontrollaufgaben notwendig sind. Diese Zuständigkeiten implizieren auch, dass den Kontrollstellen keine Amts- oder Berufsgeheimnisse entgegengesetzt werden können³⁵.
- Zweitens müssen den Kontrollstellen „wirksame Einwirkungsbefugnisse“ eingeräumt werden, wobei Art. 28 Abs. 3 zweiter Spiegelstrich RL 95/46/EG u.a. die Befugnis erwähnt, gewisse verbindliche Anordnungen zu treffen. Allerdings werden diese nur „beispielsweise“ aufgeführt. Hieraus kann man sicherlich ableiten, dass die Mitgliedstaaten nicht zwingend alle genannten Einwirkungsbefugnisse kumulativ vorsehen müssen. Jedenfalls aber müssen die Einwirkungsbefugnisse wirksam sein, m.a.W. die effektive Beachtung der datenschutzrechtlichen Vorgaben auf der jeweiligen Ebene sicherstellen können. Nur auf diese Weise kann auch gewährleistet werden, dass die Kontrollstellen tatsächlich die Einhaltung der mitgliedstaatlichen Umsetzungsgesetzgebung zur RL 95/46 sicherstellen können, so dass auch die Effektivität der Befugnisse der Kontrollstellen hier eine Rolle spielt. Diese effektive Wirksamkeit der Einwirkungsbefugnisse dürfte in Bezug auf die (Nicht-) Beachtung bestehender gesetzlicher Vorgaben implizieren, dass jedenfalls bei Privaten eine direkte Anordnungsbefugnis vorzusehen ist, ist doch nicht ersichtlich, wie sie sonst angehalten werden könnten, die „Empfehlungen“ der Kontrollstelle zu befolgen. Aber auch gegenüber Stellen der öffentlichen Verwaltung dürfte in aller Regel nur eine Anordnungsbefugnis – ggf. insofern indirekter Natur, indem „weiche“ Einwirkungen vorzuschalten sind, so dass ein gewisses Verfahren zu beachten ist – gewährleisten, dass die (mögliche) Verletzung datenschutzrechtlicher Grundsätze tatsächlich durchgesetzt werden kann³⁶. Es ist nämlich nicht ersichtlich, auf welche Weise ansonsten die

³⁵ Umgekehrt sind aber auch die Mitglieder und Bediensteten der Kontrollstellen dem Berufsgeheimnis umfassend (also auch nach Ausscheiden aus dem Dienst) zu unterwerfen (Art. 28 Abs. 7 RL 95/46/EG).

³⁶ I. Erg. wie hier, jedoch ohne nähere Begründung, *Ehmann/Helfrich*, EG-Datenschutzrichtlinie (Fn. 2), Art. 28, Rz. 9. Unklar *Brühmann*, in: *Handbuch Datenschutzrecht* (Fn. 2), Kap. 2.4, Rz. 45, der (lediglich) betont, dass die Eingriffsbefugnisse wirksam sein müssen

Wirksamkeit der Einwirkungsbefugnisse – die ja jedenfalls zu gewährleisten ist – sichergestellt werden soll: Zwar können auch parlamentarische Kontrollfunktionen der Verwaltung durchaus Wirkung entfalten; gleiches gilt für die Wirkung von Presseberichten o.ä.³⁷. Es ist aber nicht zu verkennen, dass solche „Kontrollmechanismen“ häufig eher zufällig greifen und die „Funktionslogik“ hier eine andere ist als im Rahmen einer Kontrollstelle, die ohne Anlass sicherzustellen hat, dass die datenschutzrechtlichen Vorgaben eingehalten werden.

Vor diesem Hintergrund impliziert nach der hier vertretenen Ansicht das Erfordernis der Wirksamkeit der Einwirkungsbefugnisse, dass die Kontrollstelle auch gegenüber Stellen der öffentlichen Verwaltung in die Lage versetzt wird, die Einhaltung der in Umsetzung der Richtlinie erlassenen datenschutzrechtlichen Vorgaben in rechtsverbindlicher Form durchzusetzen. In Bezug auf das Verfahren sind dabei verschiedene Möglichkeiten denkbar: So kann der Kontrollstelle eine umfassende Anordnungsbefugnis in Bezug auf den Umgang mit Daten bzw. deren Verarbeitung im Hinblick auf die Einhaltung der einschlägigen datenschutzrechtlichen Vorgaben eingeräumt werden. Oder aber sie wird dazu legitimiert, jederzeit eine solche verbindliche Anordnung bei einem Gericht zu beantragen.

- Schließlich ist der Kontrollstelle ein Klagerecht oder eine „Anzeigebefugnis“ bei Verstößen gegen die nationalen Vorschriften zur Umsetzung der RL 95/46/EG einzuräumen. Die genaue Bedeutung dieser Anzeigebefugnis bleibt etwas im Dunkeln; der Gegensatz zur Klage dürfte es aber nahe legen, hierunter nur eine Art Informationsbefugnis der (Straf-) Gerichte zu verstehen, denen eine Pflicht zukommt, der Anzeige nachzugehen, wobei die Verfahrensherrschaft aber bei ihnen liegen dürfte³⁸. Im Gegensatz dazu liegt die Verfahrensherrschaft bei einer Klagebefugnis bei der Kontrollbehörde, die damit eine gerichtliche Entscheidung „erzwingen“ kann.

Im Übrigen dürfte sich dieses Klage- oder Anzeigerecht im Wesentlichen auf die von den Mitgliedstaaten nach Art. 24 RL 95/46/EG vorzusehenden Sanktionen beziehen, so dass es in erster Linie in strafrechtlichen oder verwaltungsstrafrechtlichen Verfahren zum Zuge kommen dürfte, nicht hingegen bei zivilrechtlichen Streitigkeiten³⁹. Im Verhältnis zu den wirksamen Einwirkungsbefugnissen stellt die Befassung der Justizbehörden eine Alternative dar, auf die die Kontrollstelle möglicherweise bei besonders komplexen Sachverhalten oder wiederholten Verstößen zurückgreifen wird⁴⁰.

³⁷ Vgl. die entsprechenden Hinweise bei *Dammann/Simitis*, EG-Datenschutzrichtlinie (Fn. 2), Art. 28, Rz. 10, die darauf hinweisen, dass bei öffentlichen Stellen eine Beachtung datenschutzrechtlicher Vorschriften etwa von Verwarnungen aufgrund des öffentlichen Drucks sowie durch parlamentarische Kontrollfunktionen gewährleistet werden könne. Sie wollen daraus ableiten, dass gegenüber öffentlichen Stellen nicht zwingend eine Anordnungsbefugnis vorzusehen ist.

³⁸ Ebenso *Dammann/Simitis*, EG-Datenschutzrichtlinie (Fn. 2), Art. 28, Rz. 11.

³⁹ Vgl. *Dammann/Simitis*, EG-Datenschutzrichtlinie (Fn. 2), Art. 28, Rz. 11.

⁴⁰ Vgl. *Brühann*, in: Handbuch Datenschutzrecht (Fn. 2), Kap. 2.4, Rz. 45.

IV. Zusammenfassende Schlussbetrachtung

Insgesamt konnten die Ausführungen aufzeigen, dass die Anpassung des schweizerischen Rechts an die Anforderungen der Datenschutzrichtlinie zwar sicherlich keine umwälzenden Modifikationen des schweizerischen Datenschutzrechts mit sich bringt. Gleichwohl sind aber die Herausforderungen nicht zu verkennen, wobei nach dem Gesagten zwei Aspekte von besonderer Bedeutung sind: Zum einen ist nach der hier vertretenen Ansicht sicherzustellen, dass die Datenschutzrichtlinie in allen Bereichen – also nicht nur den „schengen- oder dublinrelevanten“ Gebieten – beachtet wird. Zum anderen sind auf kantonaler Ebene nicht nur überall Datenschutzgesetze zu schaffen, sondern es sind unabhängige Kontrollstellen einzurichten, die effektiv die ihnen zustehenden Aufgaben – die auch im Ergebnis Anordnungsbefugnisse gegenüber kantonalen Verwaltungen umfassen müssen – wahrnehmen können. Gerade letzterer Punkt dürfte die Kantone vor nicht zu unterschätzende Herausforderungen stellen, wobei die Potentiale interkantonaler Zusammenarbeit nicht unterschätzt werden sollten. Jedenfalls ist zu beachten, dass der Schengen-Besitzstand in der Schweiz – wie dies auch bei den anderen Schengen-Staaten der Fall war – erst nach einer „Überprüfung“ der Kompatibilität der schweizerischen Gesetzgebung mit den Vorgaben des Abkommens in Kraft gesetzt werden wird, womit die Frage der ausreichenden Datenschutzgesetzgebung auf kantonaler Ebene und auf Bundesebene eine gewisse (zusätzliche) Brisanz erhält.