

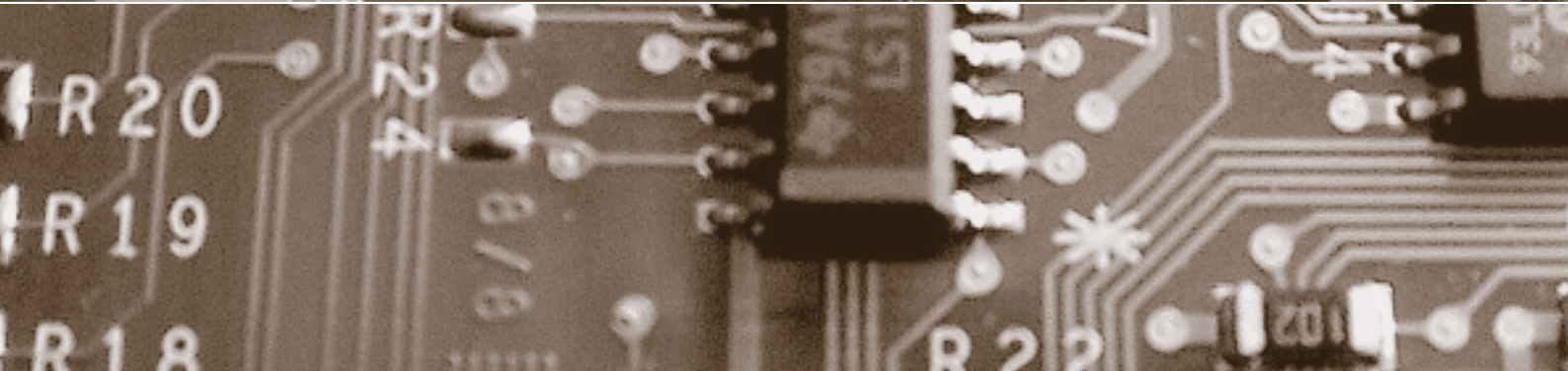
Schwerpunkt:

## Strassenansichten

**fokus:** Verwischte Sicht auf Datenbearbeitungen

**fokus:** Vom Selbstverständnis der Beauftragten

**report:** Das «Wahlcomputer»-Urteil und E-Voting



Herausgegeben von  
**Bruno Baeriswyl**  
**Beat Rudin**  
**Bernhard M. Hämmerli**  
**Rainer J. Schweizer**  
**Günter Karjoth**

## fokus



Schwerpunkt:

### Strassenansichten

auftakt

Das Intime als Freundschaftswährung  
von Kurt Imhof

**Seite 89**

«Strassenansichten» fordern heraus  
von Beat Rudin

**Seite 92**

Verwischte Sicht auf Datenbearbeitungen

von Sven Thomsen, Markus Hansen  
und Marit Hansen

**Seite 94**

Die Anwendbarkeit des Datenschutzgesetzes

von Bruno Baeriswyl

**Seite 98**

Der Fall «Street View» in  
Deutschland

von Thilo Weichert

**Seite 102**

Vom Selbstverständnis der  
Beauftragten

von Bruno Baeriswyl

**Seite 106**

Google betont stets das Prinzip der «Openness» in all ihrem Tun. Aus Datenschutz- und Datensicherheitssicht wäre begrüssenswert, wenn sich Anwender, Betroffene und Aufsichtsbehörden ein exaktes Bild davon machen könnten, wie Google mit personenbezogenen Daten umgeht. Gerade darüber informiert das Unternehmen jedoch allenfalls rudimentär.

**Verwischte Sicht  
auf Daten-  
bearbeitungen**

Wie ist «Street View» nach schweizerischem Datenschutzrecht zu beurteilen? Der Beitrag nimmt insbesondere den Rechtfertigungsgrund des nicht personenbezogenen Bearbeitens und das Konzept der obligatorisch damit verbundenen Anonymisierung der Aufnahmen kritisch unter die Lupe.

**Die Anwendbarkeit  
des Daten-  
schutzgesetzes**

«Street View» in Mitteleuropa: ein unüberwindbarer Konflikt oder bloss der schwierige Beginn einer langen Freundschaft? Der Autor zeichnet den Umgang von Google mit Datenschutzbehörden in Deutschland und Europa nach. Er hat die Hoffnung auf die Einsicht des amerikanischen Informations-Weltkonzerns noch nicht aufgegeben.

**Der Fall  
«Street View» in  
Deutschland**

Im Vordergrund bei den Aufgaben der Datenschutzbeauftragten stehen die Grundrechte oder das Mandat der Bürgerinnen und Bürger.

**Vom Selbst-  
verständnis der  
Beauftragten**

## impresum

**digma:** Zeitschrift für Datenrecht und Informationssicherheit, ISSN: 1424-9944, Website: [www.digma.info](http://www.digma.info)

**Herausgeber:** Dr. iur. Bruno Baeriswyl, Dr. iur. Beat Rudin, Prof. Dr. Bernhard M. Hämmerli, Prof. Dr. iur. Rainer J. Schweizer, Dr. Günter Karjoth

**Redaktion:** Dr. iur. Bruno Baeriswyl und Dr. iur. Beat Rudin

**Zustelladresse:** Redaktion digma, per Adr. Datenschutzbeauftragter des Kantons Basel-Stadt, Postfach 205, CH-4010 Basel  
Tel. +41 (0)61 201 16 42, Fax +41 (0)61 201 16 41, [redaktion@digma.info](mailto:redaktion@digma.info)

**Erscheinungsplan:** jeweils im März, Juni, September und Dezember

**Abonnementspreise:** Jahresabo Schweiz: CHF 158.00, Jahresabo Ausland: Euro 99.00 (inkl. Versandkosten), Einzelheft: CHF 42.00

**Anzeigenmarketing:** Publicitas Publimag AG, Mürtchenstrasse 39, Postfach, CH-8010 Zürich  
Tel. +41 (0)44 250 31 31, Fax +41 (0)44 250 31 32, [www.publimag.ch](http://www.publimag.ch), [service.zh@publimag.ch](mailto:service.zh@publimag.ch)

**Herstellung:** Schulthess Juristische Medien AG, Arbenzstrasse 20, Postfach, CH-8034 Zürich

**Verlag und Abonnementsverwaltung:** Schulthess Juristische Medien AG, Zwingliplatz 2, Postfach, CH-8022 Zürich  
Tel. +41 (0)44 200 29 99, Fax +41 (0)44 200 29 98, [www.schulthess.com](http://www.schulthess.com), [zs.verlag@schulthess.com](mailto:zs.verlag@schulthess.com)

**Das  
«Wahlcomputer»-  
Urteil und E-Voting**

Das deutsche Bundesverfassungsgericht hatte sich mit der Zulässigkeit von Wahlcomputern zu befassen. Seine Erwägungen sind nicht tel quel auf die Schweiz umsetzbar – der Beitrag regt aber an, sich auch in der Schweiz Gedanken zu machen, ob und in welchem Mass beim E-Voting das nötige Vertrauen sichergestellt werden kann.

**SIS: Quo vadis  
Datenschutz?**

Internationale Informationssysteme wie das Schengener Informationssystem (SIS) lassen den Ruf nach «einheitlichem Recht» laut werden. Die Autorin einer Dissertation zu SIS und Datenschutz postuliert, dass das materielle Datenschutzrecht auf nationaler Ebene sorgfältig(er) ausgearbeitet und wo immer möglich vereinheitlicht werden sollte.

**Organisations-  
übergreifende  
Info-Prozesse**

Die Integration verschiedener IT-Applikationen über direkte Datenschnittstellen hat in den letzten Jahren stark zugenommen. Sobald aber die Grenze der Organisation überschritten wird, kommen Uraltmethoden zum Zuge. Der Autor ortet Defizite bei der Standardisierung, bei der Kommunikationsarchitektur und bei der Sicherheit.

**Die Crux mit dem  
Vertrauen**

Das Bundesamt für Statistik will bestimmte Befragungen für die Bundesstatistik künftig durch ein Meinungsforschungsinstitut durchführen lassen – telefonisch und mit der Androhung einer Busse für «Verweigerer». Der schlusstakt-Autor stellt die Vertrauensfrage.

report



RECHTSPRECHUNG

Das «Wahlcomputer»-Urteil und E-Voting  
von Herbert Burkert **Seite 112**

SCHENGEN

SIS: Quo vadis Datenschutz?  
von Sandra Stämpfli **Seite 118**

PRAXIS

Internes Kontrollsystem  
von Ivan Allemann **Seite 122**

TRANSFER

Organisationsübergreifende Info-Prozesse  
von Roland Portmann **Seite 124**

forum



SAFE HARBOR

Personendaten-Transfer in die USA  
von Jürg Schneider **Seite 126**

agenda

**Seite 106**

schlussakt

Die Crux mit dem Vertrauen  
von Günter Karjoth **Seite 128**

cartoon

von Hanspeter Wyss

## Schengen

# SIS: Quo vadis Datenschutz?



Sandra Stämpfli,  
Dr. iur., Juristische  
Mitarbeiterin beim  
Datenschutz-  
beauftragten des  
Kantons Basel-  
Stadt, Basel  
sandra.staempfli@  
dsb.bs.ch

Die Euphorie im Dezember 2008 war deutlich spürbar, als die Schweiz rund vier Jahre nach der Unterzeichnung der Bilateralen II<sup>1</sup> an das Schengener Informationssystem (SIS) angeschlossen wurde. Das SIS ist das Personen- und Sachfahndungssystem der Schengen-Staaten, auf welches neben den Polizei- und Grenzwach- auch andere Behörden zugreifen können, um Personenkontrollen durchzuführen oder aber gesuchte Personen zur europaweiten Fahndung auszuschreiben. Es stellt die wesentlichste Ausgleichsmassnahme dar, welche den Abbau der Binnen-Grenzkontrollen in Europa kompensieren und die Sicherheit der jeweiligen Staaten garantieren soll.

Als Rechtsgrundlage für den Betrieb des SIS dient das Schengener Durchführungsübereinkommen (SDÜ) aus dem Jahre 1990<sup>2</sup>. Das SDÜ versucht, als Kompromisslösung den unterschiedlichen Bedürfnissen und Auffassungen der Schengen-Staaten gerecht zu werden, und enthält neben den eher technischen Regelungen zum Betrieb des SIS auch datenschutzrechtliche Bestimmungen. Zusätzlich zu diesen Normen gelangen zahlreiche weitere Regelungen unterschiedlicher Natur zur Anwendung:

### Normenschungel

Die EMRK<sup>3</sup> enthält nach wie vor keinen expliziten Schutz der personenbezogenen Daten. Immerhin wurde jedoch

der durch die höchstrichterliche Rechtsprechung geschaffene Anspruch auf Schutz der persönlichen Daten aufgrund von Art. 8 EMRK im Laufe der Zeit erweitert.

Die Europäische Charta der Grundrechte (EGRC)<sup>4</sup> enthält in Art. 8 Abs. 1 das explizite Recht auf Schutz der persönlichen Daten. Inwieweit sich diese Bestimmung auf das SIS auswirken wird, muss sich noch zeigen.

Dagegen statuiert das SDÜ in den Art. 102 ff. besondere, für den Betrieb des SIS anwendbare Datenschutzbestimmungen. Zusätzlich zu diesen Normen erklärt das SDÜ in Art. 117 die Datenschutzkonvention des Europarates<sup>5</sup> sowie dessen Empfehlung R(87) 15<sup>6</sup> auf Datenbearbeitungen im SIS-Kontext für anwendbar. Daneben zählt seit dem Inkrafttreten des SDÜ im Jahre 1990 nicht nur die EU-Richtlinie 95/46<sup>7</sup> zum datenschutzrechtlichen Rahmen des SIS: Seit dem 28. November 2008 gilt der Rahmenbeschluss über den Schutz personenbezogener Daten, die im Rahmen der polizeilichen und justiziel- len Zusammenarbeit in Strafsachen<sup>8</sup> bearbeitet werden. Die Richtlinie gelangt dabei zwar nicht unmittelbar auf SIS-Datenbearbeitungen zur Anwendung, hat aber das nationale Recht der EU-Staaten massgeblich geprägt. Der Rahmenbeschluss vom 28. November 2008 ist für die dritte Säule der EU – und damit auch auf das SIS – anwendbar und von den

Mitgliedstaaten entsprechend umzusetzen.

Das SDÜ enthält neben der Anwendbarkeitsregelung in Bezug auf die Datenschutzkonvention und die Empfehlung R(87) 15 zahlreiche Verweise auf das nationale Recht der Schengen-Staaten. Dieser Rückgriff auf das nationale (Datenschutz-) Recht beruht im Wesentlichen auf dem Bedürfnis, einen möglichst grossen Kreis an Staaten zur Mitwirkung an der kontinuierlichen Aufhebung der Binnengrenzen zu bewegen und gleichzeitig deren Autonomie zu wahren.

### Und in der Schweiz?

Die Schweizer Gesetzgebung tut sich mit der rechtlichen Umsetzung des SIS bis heute schwer. Zum Zeitpunkt der probeweisen Inbetriebnahme des SIS am 1. Juli 2008 waren lediglich das StGB angepasst und die N-SIS-Verordnung<sup>9</sup> gestützt auf die neuen StGB-Bestimmungen erlassen worden. In den Kantonen waren zahlreiche Gesetzgebungsprojekte erst im Entstehen begriffen, nur wenige Kantone verfügten über die notwendigen Bestimmungen in den jeweiligen Gesetzen – obschon das SIS in der Testphase von Juli bis Dezember 2008 intensiv genutzt wurde<sup>10</sup>.

Mittlerweile wurde Art. 355d StGB durch den äquivalenten Art. 16 des Bundesgesetzes über die polizeilichen Informationssysteme des Bundes (BPI)<sup>11</sup> ersetzt. Mit der Delegation der Regelung des Betriebs

des N-SIS an den Bundesrat mittels Art. 16 und 19 BPI basiert die Verordnung auf formell-gesetzlichen Bestimmungen. Dennoch stellt sich, in Anbetracht des Umstandes, dass auch Fingerabdrücke, Lichtbilder sowie besondere Körpermerkmale mit dem SIS bearbeitet werden können, die Frage, ob diese Regelung tatsächlich den verfassungsrechtlichen Grundsätzen entspricht: Um einen Eingriff in die informationelle Selbstbestimmung der Betroffenen zu legitimieren (Art. 36 Abs. 1 BV), bedarf es zur Bearbeitung dieser sensiblen Daten einer konkreten Grundlage in einem Gesetz im formellen Sinne. Die Delegation weckt damit Bedenken in Bezug auf den Grundrechtsschutz bei Datenbearbeitungen. Im Hinblick auf die voranschreitende Entwicklung des SIS ist eine flexible Regelung des Betriebs wünschenswert, dass dabei jedoch auf die für den Schutz der Betroffenen notwendigen Rechtsgrundlagen verzichtet wird, ist aus rechtsstaatlicher Sicht bedauerlich<sup>12</sup>.

Das Schengen-Informationsaustausch-Gesetz (SlaG)<sup>13</sup>, welches voraussichtlich 2010 in Kraft treten wird, vervollständigt den Kreis der auf Bundesebene anwendbaren Bestimmungen. Zwar bezieht sich das SlaG nicht unmittelbar auf das SIS, der allgemeine Informationsaustausch zwischen den Strafverfolgungsbehörden des Bundes und denjenigen der übrigen Schengen-Staaten wird jedoch immer wieder SIS-Daten mit einbeziehen.

BPI, N-SIS-Verordnung und SlaG beziehen sich ausnahmslos auf Daten, die bereits erhoben wurden. Die eigentliche Datenbeschaffung findet jedoch im Wesentlichen durch kantonale (Polizei-)Behörden statt. Auf diese Datenbearbeitungen gelangen die jeweiligen kantonalen Bestimmungen,

insbesondere die Polizeigesetze und (noch) die Strafprozessordnungen, zur Anwendung. Auch der Informationsaustausch zwischen kantonalen Behörden und anderen Schengen-Staaten ist kantonal geregelt. Obschon Art. 14 SlaG die Anwendbarkeit des Bundesgesetzes vorsieht, wenn keine entsprechenden kantonalen Bestimmungen erlassen werden, ist der Erlass von kantonalen SlaG angezeigt. Nur so kann die schleichende Ausdehnung des Anwendungsbereichs von Bundesrecht eingedämmt werden.

Die Vielfalt der anwendbaren Bestimmungen wird bei näherer Betrachtung einzelner SIS-Ausschreibungen besonders deutlich:

#### **Z.B. Art. 99 SDÜ**

Die verdeckte Registrierung im Sinne von Art. 99 SDÜ ermöglicht die (geheime) polizeiliche Fahndung nach Personen, die im Verdacht stehen, eine aussergewöhnlich schwere Straftat begangen zu haben oder eine Gefahr für die öffentliche Sicherheit und Ordnung darzustellen.

#### *Allgemeine Risiken*

Art. 99 SDÜ ist bedenklich weit gefasst: Wie konkret die besagten Anhaltspunkte für ein Verbrechen sein sollten, wird nicht näher festgehalten. Eine «Einschränkung» erfährt Art. 99 SDÜ nur durch den Begriff der «aussergewöhnlich schweren Straftaten». Das SDÜ selbst enthält keinerlei Konkretisierungen, so dass die genauere Bestimmung der aussergewöhnlich schweren Straftaten resp. der Gesamtbeurteilung des Täters ausschliesslich dem jeweiligen nationalen Recht überlassen wird.

In der Schweiz darf eine Ausschreibung zur verdeckten Registrierung nur vorgenommen werden, wenn eine schwere Straftat im Sinne des

Art. 4 Abs. 2 des Bundesgesetzes über die verdeckte Ermittlung (BVE)<sup>14</sup> befürchtet wird (Art. 33 Abs. 4 N-SIS-Verordnung). Während das SDÜ die Planung von «in erheblichem Umfang aussergewöhnlich schwere(n) Straftaten» voraussetzt, begnügt sich die N-SIS-Verordnung mit lediglich «schweren Straftaten». Der Ermessensspielraum ist hier offensichtlich weit und lässt erahnen, wie unterschiedlich die jeweiligen Entscheide der Behörden ausfallen werden. Im Sinne des Grundsatzes der Verhältnismässigkeit ist bei dem Entscheid, ob es sich um eine in erheblichem Umfang aussergewöhnlich schwere Straftat handelt und damit eine Ausschreibung im Sinne von Art. 99 SDÜ notwendig wird, grosse Sorgfalt geboten.

Gemäss Art. 99 Abs. 3 SDÜ soll es ferner den für die Staatssicherheit zuständigen Stellen möglich sein, eine Ausschreibung zur Abwehr einer erheblichen Gefährdung der inneren und äusseren Sicherheit des Staates vorzunehmen. Diese Ausweitung der ausschreibebefugten Stellen ist problematisch:

■ Geheimdienste sind in ihrer Arbeit grundsätzlich nicht in die Aktivitäten der Zoll- und Polizeibehörden eingebunden, können sich nun jedoch durch Art. 99 Abs. 3 SDÜ der polizeilichen Fahndungsmassnahmen bedienen und auch von

#### **Kurz & bündig**

Informationssysteme internationalen Charakters lassen immer wieder den Ruf nach «einheitlichem Recht» laut werden. Handlungsbedarf besteht jedoch nicht in Bezug auf das «formelle» Datenschutzrecht – hier besteht weitestgehend Einigkeit. Es ist das «materielle», das auf die konkreten Abläufe und Behörden bezogene Recht, welches insbesondere auf nationaler Ebene sorgfältig(er) ausgearbeitet und wo immer möglich vereinheitlicht werden sollte.

ausländischer Polizeiarbeit direkt profitieren. Auf diese Weise besteht die Gefahr, dass die Polizei- und Grenzbehörden zu Erfüllungshilfen der Geheimdienste werden.

■ Je mehr Behörden Zugriff auf ein Datenverarbeitungssystem gewährt wird, umso grösser wird das Risiko einer Persönlichkeitsverletzung. Im Sinne des Verhältnismässigkeitsgrundsatzes sollte der Kreis der Zugriffsberechtigten möglichst klein gehalten werden.

#### *Risiken für Betroffene*

Für die möglicherweise von einer Ausschreibung im Sinne von Art. 99 SDÜ betroffenen Personen zeigt sich eine vielschichtige datenschutzrechtliche Problematik:

■ Sofern eine Person sich über eine allfällige Ausschreibung im SIS zur verdeckten

Registrierung informieren will, ist ein schriftliches Gesuch an das fedpol zu richten (Art. 49 Abs. 1 N-SIS-Verordnung).

Grundsätzlich beurteilt sich das Auskunftsrecht nach dem Recht desjenigen Staates, in welchem das Gesuch um Auskunft gestellt wurde (Art. 109 Abs. 1 SDÜ). Im Sinne von Art. 109 Abs. 2 SDÜ hat die Auskunftserteilung jedoch zwingend immer dann zu unterbleiben, wenn der Gesuchsteller zur verdeckten Registrierung ausgeschrieben ist. Es wird also keine Auskunft darüber erteilt, ob tatsächlich eine Speicherung im SIS vorhanden ist.

Im Sinne von Art. 49 Abs. 4 N-SIS-Verordnung muss das fedpol ein Gesuch innert maximal 60 Tagen beantworten. Weder das SDÜ noch die N-SIS-Verordnung oder aber das SIRENE-Handbuch enthalten

Vorschriften, wie in einem solchen Fall vorgegangen werden muss. Art. 16 Abs. 9 BPI – als gesetzliche Grundlage für den Betrieb des N-SIS – verweist jedoch auf Art. 18 des Bundesgesetzes über Massnahmen zur Wahrung der Inneren Sicherheit (BWIS)<sup>15</sup>. Der Antragsteller wird damit an den EDÖB verwiesen, womit das indirekte Auskunftsrecht zur Anwendung gelangt. Die Unzulänglichkeiten dieser «Auskunftserteilung» sind hinreichend bekannt – die betroffene Person wird sich auch nach Erhalt dieser «Auskunft» nicht im Klaren darüber sein können, ob sie im SIS vermerkt ist oder nicht.

■ Auch der EDÖB sieht sich, möchte er die Rechtmässigkeit eines Eintrages nach Art. 99 SDÜ im SIS überprüfen, vor Problemen: Ob die Ausschreibung korrekt vorgenommen

### Literatur, weiterführende Links

- STEPHAN BREITENMOSER/SABINE GLESS/OTTO LAGODNY (Hrsg.), Schengen in der Praxis – Erfahrungen und Ausblicke, Zürich/Lachen 2009.
- BEAT RUDIN, Verfassungswidrige Anwendbarkeit des Bundesdatenschutzgesetzes, SJZ 105 (2009), 1 ff.
- SANDRA STÄMPFLI, Das Schengener Informationssystem und das Recht der informationellen Selbstbestimmung, Diss. Basel, Bern 2009.

### Fussnoten

- <sup>1</sup> Botschaft des Bundesrates vom 1. Oktober 2004 zur Genehmigung der sektoriellen Abkommen zwischen der Schweiz und der Europäischen Union, einschliesslich der Erlasse zur Umsetzung der Abkommen, BBl 2004, 5965 ff.
- <sup>2</sup> Übereinkommen zur Durchführung des Übereinkommens von Schengen vom 14. Juni 1985 zwischen den Regierungen der Staaten der Benelux-Wirtschaftsunion, der Bundesrepublik Deutschland und der Französischen Republik betreffend den schrittweisen Abbau der Kontrollen an den gemeinsamen Grenzen (SDÜ), ABi. L 239/2000, 19 ff.
- <sup>3</sup> SR 0.101.
- <sup>4</sup> ABi. L 303/2007, 1 ff.
- <sup>5</sup> <<http://conventions.coe.int/Treaty/GER/Treaties/Html/108.htm>> (besucht am 20.7.2009).
- <sup>6</sup> <[http://www.coe.int/T/DG1/LegalCooperation/Economiccrime/organisedcrime/Rec\\_1987\\_15.pdf](http://www.coe.int/T/DG1/LegalCooperation/Economiccrime/organisedcrime/Rec_1987_15.pdf)> (besucht am 20.7.2009).
- <sup>7</sup> ABi. L 281/1995, 31 ff.
- <sup>8</sup> ABi. L 350/2008, 60 ff.
- <sup>9</sup> Verordnung über den nationalen Teil des Schengener Informationssystems, SR 362.0.
- <sup>10</sup> SANDRA STÄMPFLI, Das Schengener Informationssystem und das Recht der informationellen Selbstbestimmung, Diss. Basel, Bern 2009, 76 f.
- <sup>11</sup> SR 361.
- <sup>12</sup> RAINER SCHWEIZER, St. Galler Kommentar zu Art. 36 BV, Rz. 10 ff.
- <sup>13</sup> Entwurf für ein Bundesgesetz über den Informationsaustausch zwischen den Strafverfolgungsbehörden des Bundes und denjenigen der anderen Schengen-Staaten (Schengen-Informationsaustausch-Gesetz) in Ausführung des RB 2006/960/JI, BBl 2008, 9062.
- <sup>14</sup> SR 312.8.
- <sup>15</sup> SR 120.

wurde resp. ob die zugrunde liegenden Daten rechtmässig erhoben und bearbeitet wurden, beurteilt sich entweder nach Bundes- oder nach kantonalem Recht. Handelt es sich um eine ausländische Ausschreibung, ist das Recht des jeweiligen ausschreibenden Staates zu Rate zu ziehen.

### **Handlungsbedarf**

Das Beispiel der verdeckten Registrierungen verdeutlicht das allgemeine datenschutzrechtliche Problem, welches SIS-Datenbearbeitungen mit sich bringen: Das «formelle» Datenschutzrecht, welches die Grundsätze der Gesetzmässigkeit, der Verhältnismässigkeit sowie des Handels nach Treu und Glauben umfasst, ist auf internationaler Ebene zwar über zahlreiche Erlasse unterschiedlicher Natur verteilt. Gleichwohl sind diese verschiedenen Normen in ihrem Kern identisch und halten die Voraussetzungen einer rechtsstaatlichen Datenbearbeitung sowie die Rechte der betroffenen Personen in allgemeiner Form fest. Die zahlreichen nationalen Auffassungen bei der Auslegung

der unbestimmten Rechtsbegriffe führen zu unterschiedlichen Vorgehensweisen der jeweiligen Behörden. Dies ist im Zusammenhang mit ausgesprochen sensiblen Bereichen wie Datenbearbeitungen im SIS problematisch.

Dennoch erscheint eine Vereinheitlichung der internationalen Datenschutz-Bestimmungen, wie sie im Zusammenhang mit dem SIS immer wieder thematisiert wird, wenig sinnvoll. Eine nähere Konkretisierung der Bestimmungen und eine Verringerung des Auslegungsspielraums der nationalen Behörden wäre wohl nur schwer konsensfähig. Hier ist eine verstärkte Zusammenarbeit der nationalen sowie der europäischen Kontrollinstanzen angezeigt, um möglichst einheitliche und allgemein umzusetzende Auslegungsmassstäbe zu erarbeiten.

Das «materielle» Datenschutzrecht, die in den jeweiligen nationalen Sachgesetzen verankerten Regelungen, die das Datenbearbeiten konkret und meist behördenspezifisch regeln, divergiert hingegen nicht nur international – was durchaus

nachvollziehbar ist –, sondern auch auf nationaler Ebene.

Mit dem BPI und der N-SIS-Verordnung wurde dieser Problematik zumindest so weit Rechnung getragen, als für den Betrieb und die Nutzung des Schengener Informationssystems eine einheitliche Grundlage geschaffen wurde, welche auch für die kantonalen Benutzer verbindlich ist. Insbesondere die N-SIS-Verordnung lässt aber die notwendige Bestimmtheit vermissen, die für ein angemessenes Datenschutzniveau notwendig gewesen wäre. Zudem wurden die Spielräume, welche durch das SDÜ und die übrigen internationalen (Rahmen-)Bestimmungen gewährt werden, nur zurückhaltend ausgenutzt. Im Interesse der betroffenen Personen muss bei der Ausarbeitung des «materiellen» Datenschutzrechts grössere Sorgfalt angewandt werden. Es ist nicht die Quantität der Datenschutzbestimmungen, welche das SIS zum Risiko für die betroffenen Personen werden lässt, sondern die Qualität der Bestimmungen. ■

## Meine Bestellung

- 1 Jahresabonnement digma (4 Hefte des laufenden Jahrgangs)  
à **CHF 158.00** bzw. bei Zustellung ins Ausland **EUR 123.00** (inkl. Versandkosten)

Name \_\_\_\_\_ Vorname \_\_\_\_\_

Firma \_\_\_\_\_

Strasse \_\_\_\_\_

PLZ \_\_\_\_\_ Ort \_\_\_\_\_ Land \_\_\_\_\_

Datum \_\_\_\_\_ Unterschrift \_\_\_\_\_

### Bitte senden Sie Ihre Bestellung an:

Schulthess Juristische Medien AG, Zwingliplatz 2, CH-8022 Zürich

Telefon +41 44 200 29 19

Telefax +41 44 200 29 18

E-Mail: [zs.verlag@schulthess.com](mailto:zs.verlag@schulthess.com)

Homepage: [www.schulthess.com](http://www.schulthess.com)

Schulthess 