

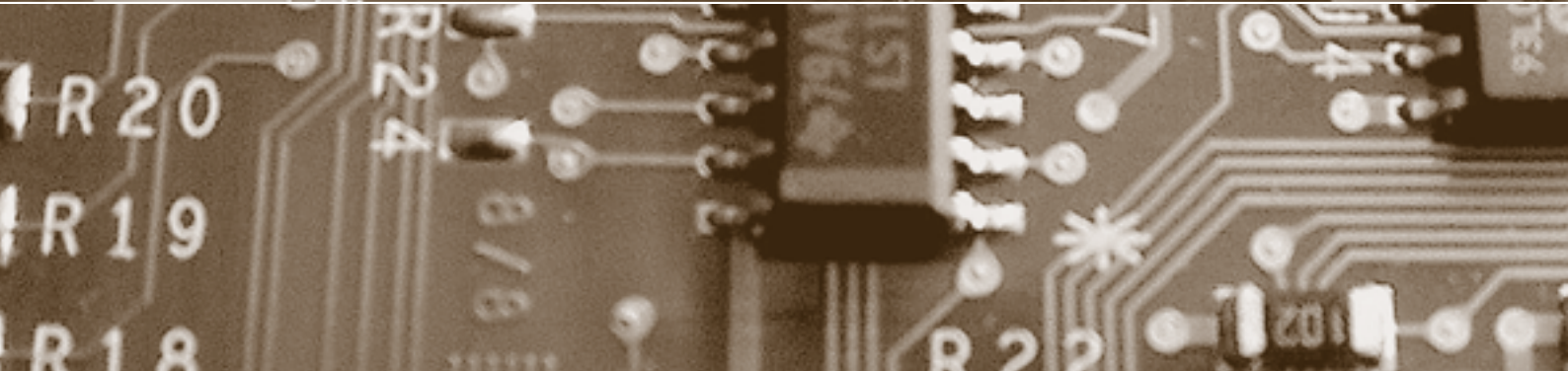
Schwerpunkt:

## Sensor-Actor-Netze

**fokus:** Lagebild für Kritische Infrastrukturen

**fokus:** Privatsphäre trotz intelligenter Zähler

**report:** Sicherheit im Cloud Computing



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

## fokus

Schwerpunkt:

### Sensor-Actor-Netze

auftakt

#### Prima leben ohne Privatsphäre

Roberto Simanowski Seite 1

#### Kritikalität von Sensor-Actor-Netzen

von Bernhard M. Hämmerli Seite 4

#### Lagebild für Kritische Infrastrukturen

von Heiko Borchert/Stefan Brem Seite 6

#### Schutz der Schweiz vor Cyber-Risiken

von Gérald Vernez Seite 10

#### Sicherheit im Energienetz der Zukunft

von Sven Garrels Seite 14

#### PET – ein Konzept harrt der Umsetzung

von Bruno Baeriswyl Seite 18

#### Privatsphäre trotz Intelligenter Zähler

von Markulf Kohlweiss und Lothar Fritsch Seite 22

Für den Schutz Kritischer Infrastrukturen (SKI) ist der regelmässige Austausch von Informationen zwischen Behörden und Unternehmen unerlässlich. Dieser könnte in einem SKI-relevanten Lagebild gebündelt und aufbereitet werden. Darin können Behörden und Betreiber Informationen zum Schutz Kritischer Infrastrukturen bündeln und die Koordination im Hinblick auf Schutzmassnahmen verbessern.

#### Lagebild für Kritische Infrastrukturen

Durch den vermehrten Einsatz von ICT und der damit verbundenen erhöhten Anzahl von Schnittstellen im Energienetz entstehen neue Sicherheitsrisiken in Bezug auf Netzverfügbarkeit, Systemintegrität und Datenschutz. Ein Sicherheitskonzept für das intelligente Stromnetz der Zukunft sollte frühzeitig geplant werden.

#### Sicherheit im Energienetz der Zukunft

Mit «Privacy Enhancing Technology» (PET) sollen neue Anwendungen «datenschutzverträglich» gemacht werden. Die inhärenten Zielkonflikte können nur aufgelöst werden, wenn neben der Technik auch das Datenschutzrecht in die Betrachtung einbezogen wird.

#### PET – ein Konzept harrt der Umsetzung

Intelligente Zähler versprechen eine bessere Ausnutzung vorhandener Infrastruktur für Netzbetreiber und erhöhte Transparenz für Konsumenten. Kann die Privatsphäre im eigenen Heim bedingungslos geschützt werden, oder folgt auf den gläsernen Mobilfunkkunden nun der gläserne Stromkunde?

#### Privatsphäre trotz Intelligenter Zähler

## 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 131.00 (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 19, Fax +41 (0)44 200 29 08, [www.schulthess.com](http://www.schulthess.com), [zs.verlag@schulthess.com](mailto:zs.verlag@schulthess.com)

## Sicherheit im Cloud Computing

Obwohl in den Medien intensiv über Cloud Computing und entsprechende ökonomische Vorteile berichtet wird, werden die latent vorhandenen Sicherheitsprobleme meist verschwiegen bzw. ignoriert. Muss man den Cloud-Anbietern einfach vertrauen?

## E-Learning: Kryptografie und -analyse

Das Open-Source-Projekt CrypTool (CT) hat sich die Aufgabe gestellt, Kryptografie und Kryptoanalyse mit Beispielen und Visualisierungen so darzustellen, dass man ein gutes Verständnis und Awareness für IT-Sicherheit erreicht.

## Familie und Arbeitsplatz: heikle Ortung

Location Based Services sind heikel oder unzulässig, wenn sie der Überwachung von Kindern und Arbeitnehmenden dienen. Die gesetzliche Vertretung ist bei älteren Kindern meist nicht befugt, an deren Stelle die Einwilligung zur Datenbearbeitung zu erteilen. Das Arbeitsrecht schränkt die Überwachung von Arbeitnehmenden erheblich ein.

## EU: Zu neuen Ufern lockt ein neuer Tag?

Die EU-Kommission hat Entwürfe für eine «Regulation» und eine «Directive» zur Vereinheitlichung des Datenschutzrechts vorgelegt. Mit dem darin enthaltenen «right to be forgotten» und dem Strafenkatalog würde ein bedeutender Schritt in Richtung Harmonisierung des Datenschutzrechts getan. Es ist zu hoffen, dass der Gedanke der Entwürfe in der definitiven Fassung immer noch zu erkennen sein wird.

## Aus den Datenschutzbehörden

Wer ist neu zur Datenschutzbeauftragten gewählt worden? Welche Themen haben Datenschutzbehörden im letzten Quartal bearbeitet? Die Unterrubrik berichtet über Personelles und Aktuelles aus der Datenschutzzsene.

## report



Sicherheit

### Sicherheit im Cloud Computing

von Rolf Oppliger

Seite 28

Lernen

### E-Learning:

#### Kryptografie und -analyse

von Bernhard Esslinger/Sibylle Hick Seite 32

Follow-up: Location Based Services

### Familie und Arbeitsplatz: heikle Ortung

von Daniel Kettiger

Seite 36

Rechtsentwicklung

### EU: Zu neuen Ufern lockt ein neuer Tag?

von Sandra Husi-Stämpfli

Seite 38

Transfer

### Private Smartphones im Geschäftsumfeld

von Roland Portmann

Seite 42

## forum



privatim

### Aus den Datenschutzbehörden

von Sandra Husi-Stämpfli

Seite 44

ISSS

### Jahresprogramm ISSS 2012

von Ursula Widmer

Seite 45

ISSS

### Wie sicher sind «sichere» IT-Systeme?

von Sonja Hof

Seite 46

agenda

Seite 47

schlussstakt

### In der Gratis-Falle

von Bruno Baeriswyl

Seite 48

cartoon

von Reto Fontana

## Rechtsentwicklung

# EU: Zu neuen Ufern lockt ein neuer Tag?<sup>1</sup>



Dr. iur. Sandra Husi-Stämpfli, Juristische Mitarbeiterin beim Datenschutzbeauftragten des Kantons Basel-Stadt, Basel  
sandra.husi@dsb.bs.ch

Mit dem Inkrafttreten der Verträge von Lissabon<sup>2</sup> im Jahr 2009 erfuhr die Europäische Union eine grundlegende Umstrukturierung. Aufbruchstimmung setzte ein. Die bisherige Säulenstruktur wurde aufgehoben, die einzelnen Bereiche wurden in den mehr (Art. 3 AEUV) oder weniger (Art. 4 Abs. 2 AEUV) umfassenden Zuständigkeitsbereich der Union überführt. Ziel dieser Auflösung war es unter anderem, die Harmonisierung der einzelnen Rechtsgebiete zu verbessern bzw. überhaupt zu ermöglichen<sup>3</sup>.

## Harmonisierung des Datenschutzrechts

Die angestrebte Vereinheitlichung des Rechts innerhalb der EU macht natürlich auch vor dem Datenschutzrecht nicht halt. Im Gegenteil, aufgrund des Querschnitt-Charakters des Datenschutzrechts ist die Harmonisierung in diesem Rechtsgebiet immer wieder ein Thema. So stellte sich im Zuge Lissabons auch die Frage, wie der bestehende EU-Datenschutzrechtskanon (Richtlinie 95/46/EG für die erste Säule<sup>4</sup>, Rahmenbeschluss 2008/977/JI für die dritte Säule<sup>5</sup>) an die neuen Gegebenheiten angepasst und möglichst im selben Arbeitsschritt aktualisiert werden könnte.

Die Kommission hat vor diesem Hintergrund zwischen Juli 2009 und Januar 2011 eine breit angelegte und medial stark propagierte Konsultation durchgeführt. Themati-

siert wurden dabei nicht nur der neue rechtliche Rahmen für den Schutz von Personendaten innerhalb der EU, sondern, im Interesse einer möglichst praxisorientierten und breit abgestützten Gesetzgebung, auch bereichsspezifische Probleme, welche gezielt mit betroffenen Kreisen diskutiert wurden.

## Grosse Hoffnungen ...

Die Resultate der Konsultation<sup>6</sup> bestärkten die Kommission in ihrer Auffassung, dass es weiterhin sinnvoll (und notwendig) sei, an einem zweigleisigen Regelwerk festzuhalten, um den Schutz von Personendaten bei Datenbearbeitungen innerhalb der EU optimal zu gewährleisten. Zum einen soll dies mit der am 25. Januar 2012 präsentierten «Regulation of the European Parliament and of the Council on the protection of individuals with regards to the processing of personal data and on the free movement of such data»<sup>7</sup>, zum anderen mit der ebenfalls an diesem Tag vorgestellten «Directive of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data by competent authorities for the purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and the free movement of such data»<sup>8</sup> geschehen. Beide Erlasse liegen derzeit als Entwurf vor und lassen,

nicht zuletzt auch aufgrund des Vergleichs mit dem durchgesickerten Vor-Entwurf<sup>9</sup>, erste Beurteilungen und Prognosen zu.

## ... zu Recht?

Der Vertrag von Lissabon hat die Rechtsetzungskompetenz der Union im Bereich des Datenschutzrechts erheblich erweitert: Art. 16 Abs. 2 AEUV legitimiert Parlament und Rat einerseits zum Erlass von Bestimmungen zum Schutze natürlicher Personen bei der Verarbeitung personenbezogener Daten im Rahmen von Tätigkeiten, die in den Anwendungsbereich des Unionsrechts fallen und andererseits zur Regelung des freien Datenverkehrs.

Allerdings muss auch diese Kompetenz im Lichte des dem Unionsrecht anhaftenden Grundsatzes der Subsidiarität verstanden werden. Die Union darf in Bereichen, in welchen sie keine umfassende Rechtsetzungskompetenz inne hat, nur dann tätig werden, wenn «und soweit die Ziele der in Betracht gezogenen Massnahmen von den Mitgliedstaaten weder auf zentraler noch auf regionaler oder lokaler Ebene ausreichend verwirklicht werden können, sondern vielmehr wegen ihres Umfangs oder ihrer Wirkungen auf Unionsebene besser zu verwirklichen sind» (Art. 5 Abs. 3 EUV). Da alle EU-Mitgliedstaaten nicht nur die Datenschutzkonvention des Europarates<sup>10</sup> ratifiziert haben, sondern auch auf

teilweise langjährige und differenzierte Datenschutztraditionen in verschiedenen Bereichen zurückgreifen können, kann von einem Regelungs«defizit» keine Rede sein. Damit sind der Union die Hände weitgehend gebunden. Die «Harmonisierung» des Datenschutzrechts erfolgt denn auch hauptsächlich durch die Wiedergabe bereits verankerter Grundsätze (Rechtmässigkeit der Datenbearbeitung, Verhältnismässigkeit, Wahrung der Rechte der Betroffenen etc.) und deren Konkretisierung. Allerdings hält sich auch diese «Vereinheitlichung» in Grenzen, so dass den Mitgliedstaaten Möglichkeiten für eigene Interpretationen belassen werden. Dies ist aber, wenn man dem Wortlaut des Explanatory Memorandum Glauben schenken darf, durchaus beabsichtigt, spricht die Kommission doch explizit von einer *Rahmengesetzgebung*, der ein Spielraum für nationale Lösungen inhärent ist.

### Was ist wirklich neu?

Die augenscheinlichste Neuerung findet sich in der gewählten Rechtsform für die beiden Erlasse. Der Inhalt der ehemaligen Richtlinie wird neu in einer «Regulation» enthalten sein, der Rahmenbeschluss wird zur Richtlinie («Directive»). Diese Änderung ist nicht nur durch die neue Erlassstruktur des Lissabonner Vertragswerks bedingt, sondern scheint durchaus weiterreichende Hintergründe zu haben: Wie die Kommission ausführt, kann die direkte Anwendbarkeit der «Regulation» erheblich zur Harmonisierung des Rechts und zu einer gesteigerten Rechtssicherheit führen<sup>11</sup>. Dass die Bestimmungen für den Schutz der Persönlichkeitsrechte bei Datenbearbeitungen im Zusammenhang mit polizeilichen

und justiziellen Verfahren lediglich in einer Richtlinie festgehalten sind, dürfte, obwohl von der Kommission als optimale Grundlage für eine Rahmengesetzgebung gepriesen<sup>12</sup>, andere Hintergründe haben: Die Mitgliedstaaten sind seit jeher ausgesprochen zurückhaltend, wenn es darum geht, ihre Souveränitätsrechte im Bereich des Polizei- und Justizwesens an die EU abzutreten. Diese Skepsis wirkt sich unweigerlich auch auf das bereichsspezifische Datenschutzrecht aus. Als entsprechend utopisch dürfte sich die Konsensfindung für eine «Regulation on Police and Criminal Justice Data Protection» herausgestellt haben, was letztlich zur Wahl einer Richtlinie geführt haben dürfte.

Materiell finden sich die folgenden, teilweise erheblichen, Änderungsvorschläge:

- Erstmals wird in Art. 17 der Regulation ein «right to be forgotten» explizit statuiert. Der Stellungnahme des Europäischen Datenschutzbeauftragten<sup>13</sup> zu diesen Belangen ist beizupflichten – Datensubjekte müssen zwingend das Recht haben, ihre bei Providern etc. vorhandenen Informationen nach einer gewissen Zeit gänzlich (und insbesondere unwiederherstellbar!) löschen zu lassen. Andernfalls laufen die Rechte der Betroffenen leer. Allerdings bleibt die vorgeschlagene Regulation weitere Konkretisierungen schuldig, so dass nicht klar wird, wie das «right to be forgotten» umgesetzt werden soll: Tür und Tor für länderspezifische Interpretationen sind einmal mehr geöffnet.

- Der Entwurf zur Regulation enthält in Art. 79 endlich einen ausgedehnten Strafenkatalog und geht so einen wesentlichen Schritt in Richtung eines einheitlichen Sanktionensystems innerhalb der EU.

Dieser soll bei Verfehlungen von datenbearbeitenden Privatpersonen und Unternehmen zur Anwendung gelangen und basiert auf einem dreistufigen und der Schwere der Verfehlung entsprechenden System: Für Unternehmen werden die Strafen proportional zum Jahresumsatz festgelegt (0,5, 1 oder 2%), Privatpersonen können mit Strafen von 100 € bis sogar 1 000 000 € belegt werden. Die möglichen Straftatbestände sind weit gefasst und eröffnen damit ein ausgedehntes Anwendungsfeld – was im Interesse einer möglichst umfassenden Sanktionierung widerrechtlicher Datenbearbeitungen sein dürfte.

- Eine wesentliche prozessuale Vereinfachung stellt die Neuerung in Art. 75 Abs. 2 der Regulation dar, wonach die von einer Datenbearbeitung betroffenen Personen sowohl am Ort der Datenbearbeitung als auch am Wohnort ihre Rechte geltend machen kann.

- Auch die Organisation der Datenschutzbehörden wird, soll es nach dem Entwurf der Regulation gehen, eine erhebliche Änderung erfahren: Das neue «data protection board» wird die Art.-29-Arbeitsgruppe ablösen und künftig für die einheitliche Umsetzung der Regulation zuständig sein (Art. 66 Ziff. 1). Die Mitgliedstaaten haben, um den Austausch innerhalb der EU möglichst einfach zu gestalten,

### Kurz & bündig

Die Kommission hat Anfangs 2012 Entwürfe für eine «Regulation» und eine «Directive» zur Vereinheitlichung des Datenschutzrechts vorgelegt. Mit dem darin enthaltenen «right to be forgotten» und dem Strafenkatalog würde ein bedeutender Schritt in Richtung Harmonisierung des Datenschutzrechts getan und einer lange anstehenden Forderung nachgekommen. Es ist zu hoffen, dass der Gedanke der Entwürfe in der definitiven Fassung immer noch zu erkennen sein wird.

eine Datenschutz-Behörde als direkten Kontakt zum «data protection board» zu benennen.

■ Als wohl weitestreichende Neuerung betreffend Datenschutz im Polizei- und Justizbereich dürfte der geplante erweiterte Anwendungsbereich der Richtlinie zu erwähnen sein: Neu sollen die darin enthaltenen Grundsätze auch für innerstaatliche Bearbeitungen gelten. Angesichts der heftigen Diskussionen, welche dieser Vorschlag bei den Ausarbeitungen des Rahmenbeschlusses<sup>14</sup> in den Jahren 2005 bis 2007 ausgelöst hatte, stellt dies eine bemerkenswerte Erweiterung dar. Allerdings muss sich erst zeigen, ob die Anwendung der Richt-

linie auch auf innerstaatliche Datenbearbeitungen nicht erneut an der zweifelsohne noch immer vorhandenen Skepsis der Mitgliedstaaten scheitern wird.

■ Erwähnt werden soll an dieser Stelle schliesslich auch die erfreuliche Entwicklung dahingehend, dass die speziellen Bedürfnisse von Kindern besser berücksichtigt werden. So weist Erwägung 29 der Regulation explizit darauf hin, dass Kinder besonderen Schutz bedürfen, da sie sich der Konsequenzen einer Bekanntgabe ihrer Daten unter Umständen nicht bewusst sind. Art. 17 der Regulation hält im Zusammenhang mit dem «right to be forgotten» denn auch fest, dass insbesondere Daten, wel-

che im Kindesalter durch die betroffene Person veröffentlicht wurden, korrekt und umfassend gelöscht werden müssen. Dieser Passus dürfte vor allem für Facebook-Profile etc. relevant werden.

Der inoffizielle Entwurf für die «Directive» folgte diesem Grundgedanken und hielt in Art. 12 Ziff. 2 fest, dass die Information eines Staates über Datenbearbeitungen auch für Kinder verständlich erfolgen muss. Die nun veröffentlichte Version spricht nur noch davon, dass die Information in «an intelligible form, using clear and plain language» zu erfolgen habe. Hingegen hat der Passus, wonach Aktivitäten speziell zur Information von Kindern ebenfalls zum Aufgabenbereich der Datenschutzbehörden gehören, den Sprung vom inoffiziellen in den offiziellen Entwurf geschafft (Art. 52 Ziff. 2 der «Directive»).

### Folgen für die Schweiz?

Beide Entwürfe werden in ihrer definitiven Fassung eine Weiterentwicklung des Schengen-Besitzstandes darstellen und sind daher von der Schweiz umzusetzen. Dabei dürften insbesondere die Strafenkataloge und das «right to be forgotten» in ihrer Umsetzung Auswirkungen auf die schweizerische Datenschutz(rechts)landschaft haben. Konkrete Aussagen sind aufgrund des Entwurfsstadiums der Bestimmungen noch nicht möglich.

Die Neuorganisation des «data protection board» birgt für die unmittelbare Tätigkeit der Datenschutzbeauftragten wohl keine Implikationen. Durch die Schaffung einer einzigen Ansprechstelle pro Mitgliedstaat ändert sich aber mittelbar die Struktur der Organisation der europäischen «Datenschutz-Szene». Föderalistisch aufgebauten Staaten

## Fussnoten

- 1 JOHANN WOLFGANG VON GOETHE, Faust, der Tragödie erster Teil, Stuttgart 1986 (Reclams Universal-Bibliothek Nr. 1), Vers 701.
- 2 Konsolidierte Fassung des Vertrags über die Europäische Union, ABI. C 83/2010, 13ff. (im Folgenden: EUV); konsolidierte Fassung des Vertrags über die Arbeitsweise der Europäischen Union, ABI. C 83/2010, 47 ff. (im Folgenden: VAEU).
- 3 Siehe dazu DIRECTORATE-GENERAL FOR INTERNAL POLICIES, POLICY DEPARTMENT «CITIZEN'S RIGHTS AND CONSTITUTIONAL AFFAIRS», Justice, Freedom and Security, Towards a new EU legal framework for data protection and privacy, Recommendation 1, abrufbar unter <<http://www.ceps.be/ceps/download/6351>> (zuletzt besucht am 26.3.2012).
- 4 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, ABI. L 282/1995, 31 ff.
- 5 Rahmenbeschluss 2008/977/JI des Rates vom 27. November 2008 über den Schutz personenbezogener Daten, die im Rahmen der polizeilichen und justiziellen Zusammenarbeit in Strafsachen verarbeitet werden, ABI. L 350/2008, 60 ff.
- 6 Einsehbar unter <[http://ec.europa.eu/justice/newsroom/data-protection/opinion/090709\\_en.htm](http://ec.europa.eu/justice/newsroom/data-protection/opinion/090709_en.htm)> bzw. <[http://ec.europa.eu/justice/newsroom/data-protection/opinion/101104\\_en.htm](http://ec.europa.eu/justice/newsroom/data-protection/opinion/101104_en.htm)> (zuletzt besucht am 26.3.2012).
- 7 Abrufbar unter <[http://ec.europa.eu/justice/data-protection/document/review2012/com\\_2012\\_11\\_en.pdf](http://ec.europa.eu/justice/data-protection/document/review2012/com_2012_11_en.pdf)> (zuletzt besucht am 26.3.2012).
- 8 Abrufbar unter <[http://ec.europa.eu/justice/data-protection/document/review2012/com\\_2012\\_10\\_en.pdf](http://ec.europa.eu/justice/data-protection/document/review2012/com_2012_10_en.pdf)> (zuletzt besucht am 26.3.2012).
- 9 Siehe <<http://www.statewatch.org/news/2011/dec/ep-dp-leas-draft-directive.pdf>>; <<http://statewatch.org/news/2011/dec/eu-com-draft-dp-reg-inter-service-consultation.pdf>> (zuletzt besucht am 26.3.2012).
- 10 Übereinkommen vom 28. Januar 1981 zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten, abrufbar unter <<http://conventions.coe.int/treaty/ger/treaties/html/108.htm>> (zuletzt besucht am 26.3.2012).
- 11 Regulation – Explanatory Memorandum, 3.1, 6. Inwieweit eine Harmonisierung aufgrund der weiten Formulierungen und der doch teilweise sehr an eine Rahmengesetzgebung erinnernden Struktur der Regulation möglich ist, wird sich zeigen.
- 12 Directive – Explanatory Memorandum, 3.2, 6.
- 13 Siehe <[http://ec.europa.eu/bepa/european-group-ethics/docs/activities/peter\\_hustinx\\_presentation\\_\(2\)\\_15th\\_rt\\_2011.pdf](http://ec.europa.eu/bepa/european-group-ethics/docs/activities/peter_hustinx_presentation_(2)_15th_rt_2011.pdf)> (zuletzt besucht am 26.3.2012), 19.
- 14 Siehe dazu ausführlich SANDRA STÄMPFLI, Das Schengener Informationssystem und das Recht der Informationellen Selbstbestimmung, Diss. Bern 2009, 138.

dürfte diese Forderung Kopfzerbrechen bereiten – die einzelnen Datenschutzbeauftragten der Länder oder Kantone drohen mit dieser Regelung an Einfluss zu verlieren, wenn die Vertretung des jeweiligen Staates in Datenschutzfragen nur noch durch eine Behörde – und nicht, wie bis anhin im Falle der Schweiz – durch zwei Vertreter(innen), erfolgen darf.

Welche weiteren Einflüsse die neuen Regelungen haben werden, lässt sich aufgrund deren aktuell lediglich provisorischen Charakters noch nicht seriös eruieren.

### **Beurteilung**

Die Geschichte der EU hat gezeigt, dass Entwürfe für Richtlinien, Rahmenbeschlüsse und selbst bloss «Communications» meist mehr versprechen, als sie schlussendlich halten können. Der Aufbruch zu neuen Ufern wird oftmals zur Reise in altbekannten Gewässern, da die Einwände der Mitgliedstaaten die vorgeschlagenen Lösungen regelmässig erheblich «beschneiden». Kompromisse müssen gefunden, ursprünglich strikte Regelungen verwässert werden, um nicht das Scheitern eines ganzen Gesetzgebungsprojekts zu riskieren. Insofern ist fraglich, wie viel der derzeit vorliegenden Entwürfe am Ende des Verfahrens noch Bestand haben wird.

Allerdings erfinden die beiden Vorschläge das Rad auch nicht gänzlich neu – die Kommission hält an den Grundsätzen fest, die bereits bekannt und verankert sind. Dies könnte für eine eher zurückhaltende Überarbeitung der Entwürfe sprechen.

Es ist zu hoffen, dass sowohl der Strafenkatalog wie auch das «right to be forgotten» die Überarbeitung ohne grosse Verwässerung überstehen werden, kommt doch die

Kommission mit der Schaffung dieser Bestimmungen einer schon lange anstehenden Pendezenach.

Wie das «right to be forgotten» schliesslich umgesetzt und inwieweit eine gemeinsame Rechtsprechung bezüglich des Strafenkatalogs (der primär von nationalen Gerichten angewandt werden muss) erreicht werden kann, ist zum jetzigen Zeitpunkt noch unklar. Es bleibt zu hoffen, dass die Harmonisierungsbestrebungen in diesen Bereichen weiterverfolgt werden.

Inwieweit die besagte Harmonisierung jedoch von Erfolg gekrönt sein wird, ist doch eher fraglich; beide Entwürfe lassen den Mitgliedstaaten noch immer sehr viel Interpretationsspielraum bei der Umsetzung der Bestimmungen.

Die weitere Entwicklung der «Regulation» und der «Directive» werden auch von Schweizer, insbesondere von kantonaler Seite weiterhin beobachtet werden müssen, nicht zuletzt, um den Anschluss an das «data protection board» nicht zu verpassen. Es bleibt also auch im Jahr 2012 spannend ... ■

## Meine Bestellung

- 1 Jahresabonnement digma (4 Hefte des laufenden Jahrgangs)  
à **CHF 158.00** bzw. bei Zustellung ins Ausland **EUR 131.00** (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 