



EUROPÄISCHE KOMMISSION
GENERALDIREKTION JUSTIZ, FREIHEIT UND SICHERHEIT

VERGLEICHENDE STUDIE
ÜBER
VERSCHIEDENE ANSÄTZE ZUR BEWÄLTIGUNG NEUER
HERAUSFORDERUNGEN FÜR DEN SCHUTZ DER PRIVATSPHÄRE,
INSBESONDERE AUFGRUND TECHNOLOGISCHER ENTWICKLUNGEN

Vertragsnummer.: JLS/2008/C4/011 – 30-CE-0219363/00-28

SCHLUSSBERICHT

Eingereicht von:



LRDP KANTOR Ltd (Leader)

In Zusammenarbeit mit



Centre for Public Reform

Januar 2010

INHALT

	<u>Abs.:</u>	<u>Seite:</u>
– Forschungsteam		2
– Glossar & Internetverweise		3
I. Einführung	1 – 5	10
II. Übersicht über die Herausforderungen	6 – 14	13
III. Die Schwierigkeiten im Umgang mit den Herausforderungen	15 – 18	17
IV. Grundvoraussetzungen	19 – 25	21
V. Ergebnisse, Schlussfolgerungen & Empfehlungen	26 – 149	25
1. GRUNDANSATZ	26 – 29	25
2. GELTUNGSBEREICH DER EU-DATENSCHUTZREGELUNGEN	30 – 35	26
3. ANZUWENDENDEN RECHT	36 – 44	29
4. HARMONISIERUNG DES MATERIELLEN RECHTS	45 – 98	33
A. (NICHT-)HARMONISIERUNG INNERHALB VON EU/EWR	47 – 79	34
B. DIE NICHT-EU/EWR-LÄNDER	80 – 89	45
C. WIE EINE UMFASSENDE HARMONISIERUNG ERREICHT WERDEN KANN	90 – 98	48
5. ZUSAMMENARBEIT MIT NICHT-EU/EWR-LÄNDERN (EINSCHLIESSLICH BESCHEINIGUNGEN EINES “ANGEMESSENEN” DATENSCHUTZNIVEAUS)	99 – 103	51
6. ÜBERWACHUNG UND DURCHSETZUNG	104 – 108	53
7. RECHTE UND RECHTSBEHELFE FÜR EINZELPERSONEN	109 – 113	55
8. ZUSÄTZLICHE UND ALTERNATIVE MASSNAHMEN	114 – 151	56
– Anhangliste		70

EUROPÄISCHE KOMMISSION – GD JLS
**VERSCHIEDENE ANSÄTZE ZUR BEWÄLTIGUNG NEUER HERAUSFORDERUNGEN FÜR DEN
SCHUTZ DER PRIVATSPHÄRE, INSBESONDERE AUFGRUND TECHNOLOGISCHER
ENTWICKLUNGEN**
Schlussbericht

FORSCHUNGSTEAM:

	<u>Titel/Position:</u>	<u>Institution(en):</u>	<u>Nationalität:</u>
<u>Leitende Sachverständige:</u>			
Douwe Korff	Professor of International Law	London Metropolitan University, London, UK	NL
Ian Brown	Senior Research fellow	Oxford Internet Institute, University of Oxford, UK	UK
<u>Spezielle Sachverständige:</u>			
Peter Blume	Professor of Legal Informatics	Faculty of Law, University of Copenhagen, Copenhagen, Denmark	DK
Graham Greenleaf	Professor of Law	University of New South Wales, Sydney, Australia	AUS
Chris Hoofnagle	Senior Fellow	Berkeley Center for Law and Technology, University of California, Berkeley, CA, USA	USA
Lilian Mitrou	Assistant Professor	Department of Information and Communication Systems Engineering, University of the Aegean, Mytilene, Greece	GR
Filip Pospíšil, Helena Svatošová, Marek Tichý	Researchers	NGO <i>Iuridicum Remedium</i> , Prague, Czech Republic	CZ
<u>Berater/-innen:</u>			
Ross Anderson	Professor of Security Engineering	University of Cambridge, UK	UK
Caspar Bowden	Chief Privacy Adviser , Microsoft EME&A	Microsoft Corporation	UK
Katrin Nyman-Metcalf	Professor of International & Comparative Law	Tallinn Law School, Tallinn University of Technology, Tallinn, Estonia	EST
Paul Whitehouse	Former Chief Constable (Head of Police Force)	Sussex Police (retired) now Chairman of the Gangmasters Licensing Authority	UK

GLOSSAR & INTERNETVERWEISE:

- AEUV : Der Vertrag über die Arbeitsweise der Europäischen Union, neuer Name des Vertrages zur Gründung der Europäischen Gemeinschaft. Der AEUV wurde durch den *Vertrag von Lissabon** ergänzt, aber nicht ersetzt.
- AG 29 : Die “Artikel 29 Datenschutzgruppe” (oder Arbeitsgruppe/Working Group/*Groupe de Travail*) wurde mit der *EG** Basisdatenschutzrichtlinie (Richtlinie 95/46/EG) eingesetzt und veröffentlicht wichtige Stellungnahmen und Orientierungshilfen hinsichtlich der Anwendung und Auslegung dieser Richtlinie und der anderen Datenschutzrichtlinien. Siehe:
http://ec.europa.eu/justice_home/fsj/privacy/workinggroup/index_de.htm
- APEC : Asiatisch-pazifisches Wirtschaftsforum (Asia-Pacific Economic Cooperation), siehe: <http://www.apec.org/>
- APPA : Asia Pacific Privacy Agencies (Asiatisch-pazifische Datenschutzbehörden), siehe: <http://www.privacy.gov.au/aboutus/international/appa>
- ASEAN : Verband Südostasiatischer Nationen (Association of Southeast Asian Nations), siehe: <http://www.aseansec.org/>
- BBB : Better Business Bureau OnLine Privacy Seal, ein US-amerikanisches Datenschutz-Gütesiegel, siehe: <http://www.bbbonline.org/privacy/>
- BCRs : Binding Corporate Rules (Verbindliche unternehmensinterne Vorschriften), Selbstregulierungsregeln, die Datenschutzkonformität in (multinationalen) Unternehmen gewährleisten sollen, gefördert durch die AG 29*, siehe die AG-29-Dokumente WP153, 154 und 155, einsehbar auf:
http://ec.europa.eu/justice_home/fsj/privacy/workinggroup/wpdocs/2008_de.htm
- CCTV : Videoüberwachung (Closed-Circuit Television)
- Charta der Grundrechte der Europäischen Union: 2000 in Nizza proklamiert; wurde mit dem *Vertrag von Lissabon** ein verbindlicher Rechtsakt. Im Gegensatz zur Europäischen Menschenrechtskonvention (*EMRK**) beinhaltet die Charta eine spezifische Bestimmung zur Gewährleistung des Datenschutzes, Artikel 8. Siehe:
http://www.europarl.europa.eu/charter/default_de.htm
- Cloud computing: Computing, bei dem die Daten des Nutzers sowie die von ihm verwendeten Anwendungen nicht mehr auf dem Personal Computer (PC) des Nutzers installiert sind, sondern auf Servern angeboten werden und ihm/ihr mithilfe von Browsern über das Internet zur Verfügung gestellt werden.

EUROPÄISCHE KOMMISSION – GD JLS
**VERSCHIEDENE ANSÄTZE ZUR BEWÄLTIGUNG NEUER HERAUSFORDERUNGEN FÜR DEN
SCHUTZ DER PRIVATSPHÄRE, INSBESONDERE AUFGRUND TECHNOLOGISCHER
ENTWICKLUNGEN**
Schlussbericht

Dataveillance	:	Die Überwachung von Einzelpersonen über die “Datenspuren”, die sie in der elektronischen/Informations-Gesellschaft, z. B. im Internet oder durch Zahlungen mit Kredit- oder Debitkarten hinterlassen
DNS	:	(auch DNA), Desoxyribonukleinsäure, eine Nukleinsäure, beinhaltet den genetischen Code. Sie wird immer häufiger in der Forensik und in anderen Bereichen zur Identifizierung eingesetzt, ebenso wie in der medizinischen Behandlung
DPA	:	Datenschutzbehörde (Data Protection Authority) (auch bezeichnet als [Abteilung des] Beauftragten für Datenschutz oder den Schutz der Privatsphäre, etc.)
Dritte Säule	:	Der Teil der <i>EU*</i> , der früher die polizeiliche und justizielle Zusammenarbeit in Strafsachen umfasste. Es gab des Weiteren eine erste Säule, die die <i>EG*</i> umfasste, und eine zweite Säule, die die gemeinsame Außen- und Sicherheitspolitik der EU umfasste. Die Säulen wurden durch den <i>Vertrag von Lissabon*</i> aufgelöst.
EDSB	:	Der Europäische Datenschutzbeauftragte, verantwortlich für die Datenschutzkonformität innerhalb der EU-Institutionen und Berater hinsichtlich der Datenschutzgesetze und -politik; siehe: http://www.edps.europa.eu/EDPSWEB/
EG	:	Europäische Gemeinschaft, der ursprüngliche Teil der heutigen <i>EU*</i> , machte bis zum <i>Vertrag von Lissabon*</i> (der diese auflöste) die „erste Säule“ der EU aus
EGMR	:	Der Europäische Gerichtshof für Menschenrechte, zuständig für die Achtung der Europäischen Menschenrechtskonvention (<i>EMRK*</i>), siehe: http://www.echr.coe.int/echr/Homepage_En
EMRK	:	Die Europäische Menschenrechtskonvention, das wichtigste europäische Instrument für Menschenrechte. Für die Durchsetzung ist der Europäische Gerichtshof für Menschenrechte (<i>EGMR*</i>) zuständig (siehe den dortigen Link)
EPA	:	Elektronische Patientenakte
ER	:	Europarat, die älteste und umfassendste europäische Organisation. Der ER schuf sowohl die Europäische Menschenrechtskonvention (<i>EMRK*</i>) als auch das <i>Übereinkommen Nr. 108*</i> (unter vielen anderen Verträgen).
(ER) CJ-PD	:	Projektgruppe Datenschutz (des Europarats); arbeitet unter dem Europäischen Ausschuss für rechtliche Zusammenarbeit (CDCJ) des <i>ER*</i> , siehe:

EUROPÄISCHE KOMMISSION – GD JLS
**VERSCHIEDENE ANSÄTZE ZUR BEWÄLTIGUNG NEUER HERAUSFORDERUNGEN FÜR DEN
SCHUTZ DER PRIVATSPHÄRE, INSBESONDERE AUFGRUND TECHNOLOGISCHER
ENTWICKLUNGEN**

Schlussbericht

http://www.coe.int/T/E/Legal_Affairs/Legal_co-operation/Steering_Committees/cdcj/

- Erste Säule : Ein anderer Name für die Europäische Gemeinschaft (EG*), den ursprünglichen Teil der heutigen EU*. Es gab des Weiteren eine zweite Säule, die die gemeinsame Außen- und Sicherheitspolitik der EU umfasste, und eine *dritte Säule**, die die polizeiliche und justizielle Zusammenarbeit in Strafsachen umfasste. Die Säulen wurden durch den *Vertrag von Lissabon** aufgelöst.
- ER-Übereinkommen Nr. 108: Übereinkommen zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten, Council of Europe Treaty Series (CETS) Nr. 181 vom 28. Januar 1981 (in Kraft getreten am 1. Oktober 1985), der erste internationale Datenschutzvertrag. Ein Zusatzprotokoll zum Übereinkommen (CETS Nr. 108 von 2001, in Kraft seit 2004) legt zusätzliche Anforderungen in Bezug auf Aufsichtsbehörden (DPAs*) und grenzüberschreitende Datenflüsse fest.
- EU : Europäische Union, siehe: <http://europa.eu/>
- EuGH : Der Europäische Gerichtshof, vollständiger Name: der Gerichtshof der Europäischen Union (EU*), siehe: http://curia.europa.eu/jcms/jcms/Jo2_6999/
- EuroPriSe : Das Europäische Datenschutzgütesiegel, geschaffen mit Unterstützung der EU-Kommission, siehe: <https://www.european-privacy-seal.eu/>
- EWK : Europäischer Wirtschaftsraum, eine Gruppe von Ländern, die mit der EU* in Verbindung stehen, aber keine Mitgliedstaaten sind. Seit dem Beitritt Österreichs, Finnlands und Schwedens gibt es nur drei EWK-Staaten: Island, Liechtenstein und Norwegen. EWK-Staaten müssen den gemeinschaftlichen Besitzstand, einschließlich der EG Datenschutzrichtlinien, auf die gleiche Weise wie die EU-Mitgliedstaaten umsetzen. Daher die Verweise auf "EU/EWK-Länder" im Text
- FRA : Agentur der Europäischen Union für Grundrechte (Fundamental Rights Agency), siehe: http://fra.europa.eu/fraWebsite/home/home_en.htm
- IP-Adresse : Ein auf dem „Internetprotokoll“ basierender Zahlencode, der für die Kommunikation zwischen mit dem Internet verbundenen Geräten verwendet wird. Die IP-Adresse identifiziert das Gerät (üblicherweise ein Personal Computer oder PC), das für die Kommunikation verwendet wird.
- MMS : Multimedia Messaging Service, wird verwendet, um multimediale Inhalte via Kurznachrichten („SMS“) zu übertragen, üblicherweise über ein Mobiltelefon (siehe auch SMS*)

EUROPÄISCHE KOMMISSION – GD JLS
**VERSCHIEDENE ANSÄTZE ZUR BEWÄLTIGUNG NEUER HERAUSFORDERUNGEN FÜR DEN
SCHUTZ DER PRIVATSPHÄRE, INSBESONDERE AUFGRUND TECHNOLOGISCHER
ENTWICKLUNGEN**

Schlussbericht

- NGO : Eine Nichtstaatliche Organisation (Non-Governmental Organisation) (im Gegensatz zu staatlichen oder zwischenstaatlichen Organisationen [Inter-Governmental Organisation, IGO])
- OECD : Die Organisation für wirtschaftliche Zusammenarbeit und Entwicklung (Organisation for Economic Cooperation and Development), siehe: <http://www.oecd.org/>
- P3P : Platform for Privacy Preferences, eine Technologie zur Verbesserung des Datenschutzes (*PET**), die versucht, den Nutzern zu ermöglichen, über die Datenschutzpraktiken von Internetseiten Bescheid zu wissen und die von ihnen gewünschten Einstellungen zu treffen, siehe: <http://www.w3.org/P3P/>
- PBD : Eingebauter Datenschutz (Privacy By Design). Ein Konzept im Computerbereich, das bei der Planung ansetzt und ursprünglich von Ontarios Beauftragtem für den Schutz der Privatsphäre entwickelt wurde, jedoch (z.B.) auch vom Datenschutzbeauftragten des Vereinigten Königreichs unterstützt wird. Es fördert die Erstellung und Anwendung datenschutzfreundlicher Systeme, siehe: <http://www.privacybydesign.ca/> und: http://www.ico.gov.uk/about_us/news_and_views/current_topics/privacy_by_design.aspx
- PETs : Technologien zur Verbesserung des Datenschutzes (Privacy Enhancing Technologies)
- PIA : Datenschutz-Folgenabschätzung (Privacy Impact Assessment), eine Abschätzung von Produkten, Diensten, Programmen oder Systemen, die vor deren Umsetzung durchgeführt wird, um deren Datenschutzfreundlichkeit sicherzustellen; in einigen gerichtlichen Zuständigkeiten obligatorisch.
- PNR : Die sogenannten Fluggastdatensätze (Passenger Name Records); eine Liste mit Informationen über Passagiere auf internationalen Flügen, deren obligatorische Sammlung und Weitergabe heftige Kontroversen im Bereich des Datenschutzes auslöste. Siehe Stellungnahme 2/2004 der Artikel 29 Datenschutzgruppe (AG29*) vom 29. Januar 2004 (WP87), einsehbar auf: http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2004/wp87_en.pdf (Vgl. Auch die diesbezüglichen Ansichten und Entscheidungen des ER und der Kommission, unter: http://ec.europa.eu/justice_home/fsj/privacy/thridcountries/index_en.htm)
- Prümer Vertrag : Ein internationales Abkommen zur polizeilichen Zusammenarbeit, das ursprünglich von Belgien, Deutschland, Spanien, Frankreich, Luxemburg, den Niederlanden und Österreich am 27. Mai 2005 unterzeichnet wurde und seit Inkrafttreten des Vertrags von Lissabon* einen Teil des allgemeinen Rechtsrahmens der Europäischen Union darstellt und in allen Mitgliedsstaaten umgesetzt wird. Siehe:

EUROPÄISCHE KOMMISSION – GD JLS
**VERSCHIEDENE ANSÄTZE ZUR BEWÄLTIGUNG NEUER HERAUSFORDERUNGEN FÜR DEN
SCHUTZ DER PRIVATSPHÄRE, INSBESONDERE AUFGRUND TECHNOLOGISCHER
ENTWICKLUNGEN**

Schlussbericht

<http://europa.eu/rapid/pressReleasesAction.do?reference=IP/07/803>

- Qui tam*: Eine Abkürzung des Lateinischen “*qui tam pro Domino rege quam pro sic ipso in hac parte sequitur*” mit der Bedeutung “wer sowohl für den König als auch für sich selbst in dieser Angelegenheit klagt.” In Bezug auf eine spezielle Bestimmung des US Federal Civil False Claims Act verwendet, die es Privatbürgern erlaubt, im Namen der US-Regierung gegen staatlich beauftragte Unternehmen und andere, die öffentliche Mittel erhalten oder nutzen, wegen Betrugs Anklage zu erheben. Im Erfolgsfall erhält der besagte Bürger einen Anteil des wiedererlangten Geldes.
- RFID : Radio Frequency Identification, winzige Transponder, die an Kleidung, Reisepässen, etc. angebracht werden können. Siehe die Empfehlung C (2900) 3200 (final) der EU-Kommission vom 12.5.2009 über *the implementation of privacy and data protection principles in applications supported by radio-frequency identification*. Einsehbar auf:
http://ec.europa.eu/information_society/policy/rfid/documents/recommendation_nonrfid2009.pdf
- Safe Harbor : sicherer Hafen; eine Vereinbarung zwischen der EU und den USA; US-amerikanische Unternehmen können erklären, dass sie die europäischen Datenschutzgrundsätze erfüllen und werden dann von der US Federal Trade Commission (FTC) beaufsichtigt, siehe:
http://ec.europa.eu/justice_home/fsj/privacy/thridcountries/adequacy-faq1_de.htm
- SMS : (Short Messaging Service); auch bekannt als Kurznachrichten, werden üblicherweise via Mobiltelefon versendet (siehe auch *MMS**)
- SNS : soziale Online-Netze (Social Networking Site), z. B. FaceBook.
- Solange*: Als “*Solange-Problem*” wird das Problem bezeichnet, welches auftritt, wenn nationale (Verfassungs-) Gerichte sich weigern, den Vorrang des EU-Rechts anzuerkennen, falls sie der Ansicht sind, dass dieses die grundlegenden Menschenrechtsanforderungen der relevanten nationalen Verfassung nicht erfüllt. Das Problem ist zwar hauptsächlich in Deutschland aufgetreten, besteht aber auch in anderen Ländern mit starkem verfassungsrechtlichem Schutz der Menschenrechte, wie etwa Italien.
- SWIFT : Die Society for Worldwide Interbank Financial Telecommunication, eine Interbanken-Organisation, die internationale Banküberweisungen vereinfacht und Gegenstand einer erheblichen Kontroverse im Bereich des Datenschutzes war. Siehe Stellungnahme 10/2006 der Artikel 29 Datenschutzgruppe (AG29*) vom 22.November 2006 (WP128), einsehbar auf:
http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2006/wp128_en.pdf

EUROPÄISCHE KOMMISSION – GD JLS
**VERSCHIEDENE ANSÄTZE ZUR BEWÄLTIGUNG NEUER HERAUSFORDERUNGEN FÜR DEN
SCHUTZ DER PRIVATSPHÄRE, INSBESONDERE AUFGRUND TECHNOLOGISCHER
ENTWICKLUNGEN**

Schlussbericht

TRUST-e	:	Ein US-amerikanisches Datenschutz-Gütesiegel, siehe: http://www.truste.com/
TrustGuard	:	Ein US-amerikanisches Datenschutz-Gütesiegel mit dem Ziel, gleichzeitig Datenschutz und Informationssicherheit für Kunden sowie Identitätsschutz für Unternehmen sicherzustellen, siehe: http://www.trust-guard.com/
ULD	:	Das Unabhängige Landeszentrum für Datenschutz des deutschen Bundeslandes Schleswig-Holstein, das auch das europäische Datenschutzgütesiegel-System (<i>EuroPriSe</i> *) verwaltet
Vertrag von Lissabon	:	am 13. Dezember 2007 in Lissabon unterzeichnet, AB 2007/C 306/01. Der Vertrag von Lissabon ergänzt (aber ersetzt nicht) den Vertrag über die Europäische Union (EUV) und den Vertrag zur Gründung der Europäischen Gemeinschaft (EGV, umbenannt in Vertrag über die Arbeitsweise der Europäischen Union oder AEUV*). Der Vertrag von Lissabon straffte die Entscheidungsprozesse innerhalb der EU und löste die drei „Säulen“ der EU auf (siehe Erste Säule* und Dritte Säule*)
VRM	:	Vendor Relationship Management, ein kundenorientiertes (und datenschutzfreundliches) Datenverwaltungssystem (im Gegensatz zu unternehmensorientierten, für gewöhnlich weniger datenschutzfreundlichen Customer-Relationship-Management-Systemen.
WTO	:	Die Welthandelsorganisation (World Trade Organisation), siehe: http://www.wto.org/

Für die Definitionen der Kernkonzepte in der Datenschutzrichtlinie siehe Artikel 2 der Richtlinie. Dazu gehören:

- “personenbezogene Daten “ (Artikel 2(a))
- “Verarbeitung [personenbezogener Daten]” (Artikel 2(b))
- “Datei mit personenbezogenen Daten”/”Datei” (Artikel 2(c))
- “für die Verarbeitung Verantwortlicher” (Artikel 2(d))
- “Auftragsverarbeiter” (Artikel 2(e))
- “Dritter” (Artikel 2(f))
- “Empfänger” (Artikel 2(g))
- “Einwilligung der betroffenen Person” (Artikel 2(h))

EUROPÄISCHE KOMMISSION – GD JLS
**VERSCHIEDENE ANSÄTZE ZUR BEWÄLTIGUNG NEUER HERAUSFORDERUNGEN FÜR DEN
SCHUTZ DER PRIVATSPHÄRE, INSBESONDERE AUFGRUND TECHNOLOGISCHER
ENTWICKLUNGEN**
Schlussbericht

Der Bericht verweist auch auf verschiedene EU-Projekte und -programme. Für weitere Informationen dazu siehe die folgenden Internetseiten:

EuroPriSe : <https://www.european-privacy-seal.eu/>

PRIME : <https://www.prime-project.eu/>

PRISE : <http://www.prise.oeaw.ac.at/>

Für die verschiedenen Webanwendungen, auf die im Text verwiesen wird, siehe die entsprechenden Internetseiten:

Amazon : <http://www.amazon.com/> und nationale Seiten, etwa:
<http://www.amazon.de/>

Boing Boing : <http://boingboing.net/>

Facebook : <http://www.facebook.com/>

Flickr : <http://www.flickr.com/>

Google : <http://www.google.com/> und nationale Seiten, etwa:
<http://www.google.co.uk/>

MySpace : <http://www.myspace.com/>

YouTube : <http://www.youtube.com/>

- o – O – o -

I. Einführung

1. Dies ist der Schlussbericht einer Studie, die von der Generaldirektion Justiz, Freiheit und Sicherheit der Europäischen Kommission in Auftrag gegeben und zwischen Oktober 2008 und August 2009 unter der Leitung ihrer Datenschutzgruppe durchgeführt wurde. Er folgt auf einen im Dezember 2008 eingereichten Anfangsbericht, einen im März 2009 eingereichten Zwischenbericht (auf der Grundlage der Anmerkungen der Kommission überarbeitet) und einen im August 2009 eingereichten Entwurf für den Schlussbericht. Dieser wurde unter Berücksichtigung der Abschlussbemerkungen der Kommission erstellt.
2. Die Studie wurde von Prof. Douwe Korff von der London Metropolitan University und Dr. Ian Brown vom Oxford Internet Institute der Oxford University durchgeführt, und zwar mit Unterstützung der folgenden Sachverständigen innerhalb und außerhalb Europas: Prof. Peter Blume (Dänemark), Prof. Graham Greenleaf (Australien), Prof. Chris Hoofnagle (USA), Prof. Lilian Mitrou (Griechenland), Filip Pospíšil, Helena Svatošová, Marek Tichy (Tschechische Republik); und mit Beratung von: Prof. Ross Anderson (UK), Caspar Bowden (UK/Frankreich), Paul Whitehouse (UK), and Prof. Katrin Nyman-Metcalf (Estland). (Details siehe Seite 2, oben)
3. Das Ziel der Studie war es, festzustellen, welche Herausforderungen an den Schutz personenbezogener Daten sich aus aktuellen gesellschaftlichen und technischen Phänomenen, wie etwa jenen in der folgenden Liste, ergeben:
 - ✓ *Internet;*
 - ✓ *Globalisierung;*
 - ✓ *die fortschreitende Verbreitung personenbezogener Daten und ihrer Erhebung;*
 - ✓ *die immer höhere Leistung und Speicherkapazität von Computern und anderen Geräten zur Datenverarbeitung;*
 - ✓ *spezielle neue Technologien wie RFID, Biometrie, Gesichtserkennung (und andere Erkennungsverfahren);*
 - ✓ *die zunehmende Überwachung (und „Dataveillance“);*
 - ✓ *die immer weiter verbreitete Verwendung personenbezogener Daten zu Zwecken, für welche diese ursprünglich nicht erhoben wurden, insbesondere in Bezug auf die nationale Sicherheit und den Kampf gegen das organisierte Verbrechen und Terrorismus -*und einen Bericht zu erstellen, der eine vergleichende Analyse der Reaktionen der verschiedenen regulierenden und nicht regulierenden Systeme (innerhalb und außerhalb der EU) auf diese Herausforderungen enthält und der prüft, ob der Rechtsrahmen der Datenschutzrichtlinie der EG (Richtlinie 95/46/EC) noch hinlänglichen Schutz bietet oder ob angesichts der besten Lösungsansätze, die ermittelt wurden, Änderungen erwogen werden sollten. Dies ist der genannte Bericht.
4. Das Team hat, wie von der Kommission gefordert, alle wichtigen Aspekte bei der Umsetzung der Richtlinie in den Rechtssystemen einiger ausgewählter EU-Mitgliedsländer genau analysiert (sowohl bezüglich materiellrechtlicher Bestimmungen als auch formeller Verfahren und Aufsicht) und sich auch der Frage nach

EUROPÄISCHE KOMMISSION – GD JLS
**VERSCHIEDENE ANSÄTZE ZUR BEWÄLTIGUNG NEUER HERAUSFORDERUNGEN FÜR DEN
SCHUTZ DER PRIVATSPHÄRE, INSBESONDERE AUFGRUND TECHNOLOGISCHER
ENTWICKLUNGEN**

Schlussbericht

Überschneidungen gerichtlicher Zuständigkeiten (Rechtskonflikten) innerhalb der EU gewidmet. Außerdem haben wir das diesbezügliche regulierende System in den Vereinigten Staaten von Amerika, sowohl auf föderaler als auch auf einzelstaatlicher Ebene, in zwei repräsentativen Bundesstaaten; in zwei weiteren OECD-Mitgliedsländern außerhalb der EU und in zwei Nicht-OECD-Mitgliedsländern außerhalb des Europäischen Wirtschaftsraums untersucht. Die Studie hat damit mehr als ein Dutzend völlig verschiedene Rechtssysteme behandelt.

Daraus ergibt sich eine Reihe von Country Reports (Länderberichten), die zusammen mit diesem Schlussbericht eingereicht werden und die folgenden Länder und gerichtlichen Zuständigkeiten umfassen:

**BEHANDELTE LÄNDER UND GERICHTLICHE
ZUSTÄNDIGKEITEN:**

A. Europäische Länder:

- Tschechische Republik
- Dänemark
- Frankreich
- Deutschland
- Griechenland
- Vereinigtes Königreich

**B. Länder und gerichtliche Zuständigkeiten
außerhalb Europas:**

- USA:
 - Föderale Ebene
 - Kalifornien
 - New Jersey
- Australien
- Hong Kong
- Indien
- Japan

5. Der vorliegende Schlussbericht wurde, gemäß dem Vertrag und den Wünschen der Kommission, kurz gehalten und auf die Hauptthemen der Studie beschränkt. Weitere Informationen und Analysen stehen in separaten Berichten und Unterlagen, die zusammen mit diesem Schlussbericht eingereicht wurden, zur Verfügung (siehe Anhangliste am Ende dieses Berichts). Diese wurden zwar größtenteils bereits mit dem Zwischenbericht eingereicht, jedoch auf der Grundlage der Anmerkungen der Kommission erweitert. Insbesondere:
- **Abschnitt II** dieses Schlussberichts gibt einen Überblick über die Herausforderungen, welche sich unserer Analyse zufolge aus den zuvor unter Absatz 3 erwähnten Phänomenen ergeben.

EUROPÄISCHE KOMMISSION – GD JLS
**VERSCHIEDENE ANSÄTZE ZUR BEWÄLTIGUNG NEUER HERAUSFORDERUNGEN FÜR DEN
SCHUTZ DER PRIVATSPHÄRE, INSBESONDERE AUFGRUND TECHNOLOGISCHER
ENTWICKLUNGEN**

Schlussbericht

Für weitere Details siehe: Working Paper No. 1: The challenges to European data protection laws and principles - An overview of the global social and technical developments and of the challenges they pose to data protection.

- **Abschnitt III** enthält unsere Gesamtzusammenfassung und -beurteilung der aktuellen EU-Datenschutzregelung und der Schwierigkeiten, welche sich aus dieser bei der Bewältigung der zuvor erwähnten Herausforderungen ergeben. Dabei wird auch auf ähnliche (oder gegensätzliche) Probleme in den Ländern und gerichtlichen Zuständigkeiten außerhalb der EU verwiesen, wie unter Abschnitt V weiter ausgeführt wird (für Verweise siehe den Überblick zu diesem Abschnitt weiter unten).
- **Abschnitt IV** geht kurz auf bestimmte weiter gefasste aber wesentliche Fragen ein, welche in jeder Überarbeitung der Datenschutzregelung der EU zu berücksichtigen sind.

Für weitere Details siehe: Working Paper No. 1 (bereits erwähnt); Douwe Korff, *Paper No. 4: The Legal Framework*, in: Ian Brown & Douwe Korff, Privacy & Law Enforcement, study for the UK Information Commissioner, 2004, (in dem mit diesem Bericht eingereichten Material enthalten); und die Country Reports (insbesondere der Country Report über Deutschland).

- **Abschnitt V** enthält unsere genaueren Schlussfolgerungen und Empfehlungen. Diese basieren auf der in Abschnitt III dargelegten Gesamtbeurteilung und berücksichtigen die in Abschnitt IV vorgestellten Grundvoraussetzungen. Dieser Abschnitt soll, anhand der großen Menge an in der Studie gewonnenen vergleichenden Informationen, die geeignetsten und effektivsten Reaktionen auf die verschiedenen Herausforderungen aufzeigen, einschließlich der besten rechtlichen Ansätze, der besten Vorgehensweisen und anderer, innovativer Lösungen für die Herausforderungen (insbesondere auch Lösungen, die in Europa noch nicht vollständig erprobt sind) mit Vorschlägen, wie diese zur Bewahrung und Stärkung der EU-Datenschutzregelung angewandt werden könnten.

Für weitere Details (insbesondere auch zu den zugrundeliegenden Analysen) siehe: Working Paper No. 2: Data protection laws in the EU - The difficulties in meeting the challenges posed by global social and technical developments, und die Country Reports.

- Abschließend enthält dieser Bericht noch ein **Glossar** für Fachbegriffe (oben, S. 3), ein **Vergleichsdiagramm** (im Anhang) und eine **Zusammenfassung**. Die Zusammenfassung wird, zur einfachen Weitergabe, als separates Schriftstück eingereicht.

- o – O – o -

II. Übersicht über die Herausforderungen¹

6. In groben Zügen gibt es bei den in dieser Studie behandelten Entwicklungen zwei (ineinander verwobene) Stränge. Der erste Strang besteht aus den Herausforderungen, welche durch die technischen Entwicklungen entstehen; der zweite aus den Herausforderungen, welche sich aus sozialen und politischen Veränderungen und Entscheidungen ergeben. Sie sind insofern ineinander verwoben, als viele neue Technologien selbst sowohl die effektive Anwendung des Datenschutzes erschweren (obwohl einige auch dabei helfen können), als auch neue, intrusivere Strategien fördern, oder dazu verwendet werden, diese auszuweiten.
7. Seit die Europäische Kommission 1990 erstmals die Datenschutzrichtlinie vorschlug, haben wir dramatische Veränderungen im Bereich der Technologie erlebt. Das Internet trifft man nun nicht mehr nur in Universitätslabors an, sondern mittlerweile in 56% der europäischen Haushalte und in 95% der Firmen in OECD-Staaten. Die Rechenleistung von Computern gehorcht noch immer dem Mooreschen Gesetz, das besagt, dass sich die Transistorendichte alle 18-24 Monate verdoppelt – sie hat also einen ungefähr tausendmal so hohen Wert erreicht wie noch vor 20 Jahren. Die Speicherkapazität von Computern und die Kommunikationsbandbreite steigen sogar noch stärker – sie verdoppeln sich alle 12 Monate und wachsen dadurch alle zehn Jahre auf ein Tausendfaches. Dieses exponentielle Wachstum hat die Möglichkeiten für Organisationen, personenbezogene Daten zu erheben, zu speichern und zu verarbeiten, enorm erweitert. Unser heutiges Umfeld ist bestimmt von Sensoren wie Überwachungskameras und Mobiltelefonen, biometrischen und elektronischen Identifikatoren, die dazu verwendet werden, Daten mit Einzelpersonen in Verbindung zu bringen. In der digitalen Welt hinterlässt fast jede Kommunikation und jeder Zugriff auf eine Internetseite einen detaillierten Fußabdruck. Durch das Internet und mobile Information Appliances (Smartphones, PDAs etc.) können große Mengen personenbezogener Daten leicht von einer gerichtlichen Zuständigkeit in eine andere bewegt werden. Mittels Data Mining wird versucht, Muster in großen Sammlungen von personenbezogenen Daten zu finden um einerseits Personen „von Interesse“ zu finden und andererseits zu versuchen, deren Interessen und Vorlieben vorherzusagen. Rund um diese Technologien sind neue multinationale Unternehmen entstanden, die weltweit Kunden haben. Kleinere Unternehmen lagern die Verarbeitung der Daten von Angestellten und Kunden an Unternehmen in Entwicklungsländern aus.
8. In immer größerem Ausmaß werden von den Regierungen Informationen über ihre Staatsbürger analysiert und ausgetauscht. Dies geschieht als Reaktion auf die Angst vor Terroranschlägen. Einzelpersonen verwenden soziale Online-Netze zum Austausch von Informationen über sich selbst und ihre Familie, Freunde und Kollegen. Die Omnipräsenz personenbezogener Daten und deren Erhebung bedeutet, dass sich die Standardsituation verändert. Die „Standardsituation“ ändert sich dahingehend, dass

¹ Für sämtliche Details und Verweise siehe Working Paper No. 1: The challenges to European data protection laws and principles - An overview of the global social and technical developments and of the challenges they pose to data protection. Dieser Abschnitt ist im Wesentlichen nur eine kurze Zusammenfassung der dort im Detail besprochenen Sachverhalte.

EUROPÄISCHE KOMMISSION – GD JLS
**VERSCHIEDENE ANSÄTZE ZUR BEWÄLTIGUNG NEUER HERAUSFORDERUNGEN FÜR DEN
SCHUTZ DER PRIVATSPHÄRE, INSBESONDERE AUFGRUND TECHNOLOGISCHER
ENTWICKLUNGEN**

Schlussbericht

staatliche und private Stellen nicht mehr entscheiden müssen, Daten zu erheben, sondern dass sie sich bemühen müssen, keine (immer sensibleren) Daten zu erheben.²

9. Diese technische Entwicklung mündet in den heute wesentlichen sozialen und politischen Tendenzen. Wir machen uns alle Sorgen wegen des Terrorismus, Kinderpornographie und schwerer international organisierter Kriminalität. Der Staat macht sich außerdem Sorgen wegen explodierender Budgets für das Gesundheitswesen, für Bildung und Sozialfürsorge. Die Regierungen wollen „gutes“ Verhalten fördern und von „schlechtem“ Verhalten abhalten (in einem viel weiteren Sinne als „nicht-kriminell“ vs. „kriminell“). In manchen Staaten – in der EU vor allem im Vereinigten Königreich – glauben die Behörden, dass sie, je mehr Informationen ihre Beamten bekommen und austauschen können, umso besser soziale Probleme wie Teenagerschwangerschaften, Fettleibigkeit oder „Extremismus“, der zu Terrorismus führen kann, in den Griff bekommen können. E-Government Systeme beinhalten typischerweise große Mengen an sensiblen personenbezogenen Daten über eine ganze Bevölkerung, die zwischen den verschiedenen Ministerien mittels von der Gesetzgebung vorgesehenen „Gateways“ ausgetauscht werden können. „Back Office“ Systeme konzentrieren sich auf eine effektivere Datenverarbeitung und das Ermöglichen von neuen Services (darunter auch die Aufdeckung und Prävention von Betrug in den Bereichen Unterstützungszahlungen und Steuererklärung) außerhalb des Blickfeldes der Bürger. „Portale“ ermöglichen es den Bürgern, online mit der Regierung zu interagieren und Informationen, z. B. zu Steuerklärungen, bereitzustellen oder Unterstützungen zu beantragen ohne dass dem Bürger oder der Regierung Kosten durch persönliche Unterhaltungen, Telefongespräche oder die manuelle Bearbeitung von Formularen entstehen. Elektronische Patientenakten (EPAs), digitalisierte Krankengeschichten, werden unter anderem in Frankreich, den USA, Kanada, Deutschland und dem Vereinigten Königreich national spezifiziert. Der Großteil dieser Projekte konzentriert sich auf Interoperabilitätsstandards, die es den verschiedenen Anbietern von Leistungen der Gesundheitsfürsorge (staatlichen und privaten) ermöglichen, medizinische Informationen auszutauschen, wenn Patienten an unterschiedlichen Orten behandelt werden. Da die Kosten dafür sinken ist es wahrscheinlich, dass die Genomsequenzierung bei Patienten zur Routine werden wird. Das Älterwerden der Baby Boomer Generation in Nordamerika und Europa wird einen starken Kostendruck dahingehend auslösen, dass ältere Patienten mit chronischen Krankheiten ambulant behandelt werden. Aus diesem Grund werden voraussichtlich auch mehr und detailliertere Informationen zu physiologischen Indikatoren und mehr Daten zum allgemeinen Lebensstil von älteren und weniger gesunden Menschen automatisch gesammelt werden. Die Strafverfolgungsbehörden und Geheimdienste bemühen sich darum, Zugang zu der großen Menge an personenbezogenen Daten zu bekommen, die durch Datensysteme, die für völlig andere Zwecke geschaffen wurden, verfügbar wurden. Diese Tendenz hat sich seit 2001 unter der Rubrik „nationale Sicherheit“ und zu Zwecken der Terrorismusbekämpfung verstärkt. Dies betrifft auch die Überwachung von finanziellen Transaktionen zur Reduzierung der Geldwäsche. Viele Regierungen haben veranlasst, dass Internetdienstanbieter ihre Netzwerke ahör-

² Wir verwenden „Standardeinstellungen“ hier zur Beschreibung einer sozio-organisatorischen Haltung, nicht für eine technische Voreinstellung. Das Thema der Standardeinstellungen für Anwendungen (einschließl. Webanwendungen) wird weiter unten in Abschnitt V, Unterabschnitt V.8 behandelt. Siehe auch Abschnitt V, Unterabschnitt V.2 (ii), Abs. 35.

EUROPÄISCHE KOMMISSION – GD JLS
**VERSCHIEDENE ANSÄTZE ZUR BEWÄLTIGUNG NEUER HERAUSFORDERUNGEN FÜR DEN
SCHUTZ DER PRIVATSPHÄRE, INSBESONDERE AUFGRUND TECHNOLOGISCHER
ENTWICKLUNGEN**

Schlussbericht

kompatibel machen müssen und Daten über die Kommunikation ihrer Kunden speichern, sodass Beamten später darauf zugreifen können. Der Datenschutz wird in Zusammenhang mit derartigen staatlichen Bestimmungen als ein Hindernis angesehen.

10. Im Zuge dessen, dass Einzelhändler sich im Internet etabliert haben und neue E-Businesses wie beispielweise Amazon beachtliche Anteile am globalen Markt gewonnen haben, nutzten diese Unternehmen aus, dass ihre Server über die Möglichkeit verfügen, detaillierte Transaktionsakten über die Aktivitäten ihrer Kunden/-innen zu erstellen. E-Commerce Geschäfte können nicht nur das Kaufverhalten ihrer Kunden/-innen sehen, sondern auch jedes Produkt, das ein/e Kunde/in ansieht und wie lange sie es ansehen, bevor sie sich entscheiden, es zu erwerben oder nicht. Anbieter für Online-Marketing Lösungen (advertising networks) können das Surfverhalten von Einzelpersonen über tausende von Internetseiten verfolgen. Dienstleistungsanbieter wie z. B. Suchmaschinen können alle Daten speichern, die sie von einem Nutzer bekommen, so z. B. Suchbegriffe. Die Artikel 29 Datenschutzgruppe übte Druck aus, sodass Unternehmen wie Google die gesammelten Daten nicht für unbegrenzte Zeit speichern. Allerdings sind viele Internet-Geschäftsmodelle von Werbeeinahmen abhängig, und so wird weiterhin Druck bestehen, Werbung unter Verwendung von Daten über die Interessen der Nutzer/-innen effektiver auf diese abzustimmen. Für die gewöhnlichen Nutzer/-innen gestaltet es sich schwierig, wenn nicht überhaupt unmöglich, dieser Art von Überwachung zu entgehen.
11. “Web 2.0” Technologien ermöglichen es den Nutzern/-innen, Texte, Audio- und Videodateien in Blogs, auf Foto- und Videoseiten wie Flickr und YouTube und den heute omnipräsenten sozialen Netzwerken wie MySpace und Facebook auszutauschen. In Verbindung mit Foto- und Videokameras, über die fast jedes Mobiltelefon verfügt, können Einzelpersonen Informationen über sich selbst und die Menschen ihres Umfeldes in bislang ungekanntem Ausmaß veröffentlichen. Soziale Netzwerke haben heute hunderte Millionen Mitglieder auf der ganzen Welt und bekannte Blogs wie z. B. BoingBoing können in puncto Leserschaft mit nationalen Zeitungen konkurrieren.
12. Zusätzlich tendieren sowohl die Technologien als auch die Politik der Regierungen dazu, die Datenerhebung und -verbreitung zu globalisieren und die Datenspeicherung zu zerstreuen. Gewöhnliche Bürger und auch Straftäter und Terroristen reisen und handeln in vielen Staaten. Die neuen Reisepass-Standards der Internationalen Zivilluftfahrts-Organisation besagen, dass Fingerabdrücke und Gesichtsbilder auf den Chips der neuen elektronischen Reisepässe gespeichert sein müssen. Die EU verlangt nun, dass die Reisepässe der Schengen-Staaten diese Daten beinhalten müssen, zum Teil als Reaktion auf die Drohung der USA, sonst den europäischen Staaten den „Visa Waiver Status“ (und somit die Visumfreiheit) abzuerkennen. Bei umfangreichen Testläufen wurden signifikante Schwierigkeiten beim Erfassen und Überprüfen von Fingerabdrücken und Iriscans festgestellt, vor allem bei Menschen mit Behinderung. Personenbezogene Daten kommen sehr viel weiter herum, über das Internet, durch soziale Online-Netze und Onlineshops – aber auch im Zusammenhang mit internationaler Zusammenarbeit zwischen staatlichen Behörden, wo darauf abgezielt wird, mutmaßliche Fußball-Hooligans, illegale Migranten/-innen oder von Menschenhandel betroffene Migranten/-innen, Umstürzler/-innen, Terroristen/-innen und Pädophile zu identifizieren. Bekommt man eines der eben erwähnten Labels, sei es von irgendeiner Behörde oder auch nur auf einer sozialen Internetseite in irgendeinem Staat, kann ein solches Stigma schnell alles

EUROPÄISCHE KOMMISSION – GD JLS
**VERSCHIEDENE ANSÄTZE ZUR BEWÄLTIGUNG NEUER HERAUSFORDERUNGEN FÜR DEN
SCHUTZ DER PRIVATSPHÄRE, INSBESONDERE AUFGRUND TECHNOLOGISCHER
ENTWICKLUNGEN**

Schlussbericht

beherrschend werden, ohne dass man die Gelegenheit hat, diejenigen Personen, die ursprünglich dafür verantwortlich waren, zur Rechenschaft zu ziehen (oder auch nur ausfindig zu machen). Der Europäische Gerichtshof für Menschenrechte stellte kürzlich fest, dass der pauschale Charakter der britischen DNS-Datenbank gegen das in der Europäischen Menschenrechtskonvention verankerte Recht auf Privatsphäre verstößt – dennoch tauschen die Strafverfolgungsbehörden unter dem „Verfügbarkeitsgrundsatz“ (Haager Programm) und dem Vertrag von Prüm in immer größerem Maß derartige Daten aus – laut dem Europäischen Datenschutzbeauftragten ohne „völlig zufriedenstellenden“ Datenschutz.

13. Abschließend sollten auch noch die Grenzen der Technologien berücksichtigt werden. Die zum Einsatz kommenden Technologien haben oftmals inhärente, schwerwiegende Einschränkungen. Die Gesichtserkennung und Ganganalyse sind von der Perfektion weit entfernt. Biometrische Daten sind nicht so eindeutig, wie oft angenommen wird. Die Erstellung von Profilen krankt an inhärenten Einschränkungen. Das US-amerikanische National Research Council (Nationaler Forschungsrat) veröffentlichte kürzlich einen Bericht über Technologien zur Terrorismusbekämpfung und schloss: *„es gibt keinen Konsens darüber, weder in der hierfür zuständigen Wissenschaftsgemeinde noch im Komitee, ob in Anbetracht des derzeitigen Standes der Wissenschaft eine der Technologien zur Verhaltensüberwachung oder zur physiologischen Überwachung überhaupt zum Einsatz im Kontext der Terrorismusbekämpfung bereit ist.“* (Übersetzung: V.G./S.H.) Dies ist ein fundamentales Problem, das darauf beruht, dass die Suche nach potentiellen Terroristen/-innen eine extrem hohe Anzahl an falsch positiven Ergebnissen produziert und dass es für Terroristen/-innen sehr einfach ist, ihr Verhalten so anzupassen, dass ihre Absichten verschleiert werden. Es bestehen auch Bedenken, dass das Data Mining zu automatisierter Diskriminierung führen könnte und Personen ungerecht behandelt werden aufgrund von Vermutungen über ihr Verhalten, die auf früheren Daten über ihre Transaktionen beruhen.
14. In jeder Auseinandersetzung mit den Auswirkungen neuer technologischer Entwicklungen müssen diese Einschränkungen ernsthaft berücksichtigt werden. Setzt man zu großes Vertrauen in Technologien, so wundervoll diese auch scheinen mögen, so führt dies aller Voraussicht nach zu schwerwiegenden Ungerechtigkeiten und schlechter Governance. Effektiver Datenschutz sorgt nicht nur für Privatsphäre im engeren Sinn, sondern auch für Schutz gegen solche Tendenzen und Folgen.

- o – O – o -

III. Die Schwierigkeiten im Umgang mit den Herausforderungen: Zusammenfassung & Übersicht³

15. Die wesentlichen Grundsätze, Bestimmungen und Kriterien des Datenschutzes, die in Europa vom ER und der EU entwickelt wurden und auch weltweit auf breiter Basis, vor allem von der OECD, als solche unterstützt wurden, haben sich bewährt, auch wenn sie vielleicht in mancher Hinsicht verstärkt werden müssen. Ein Beleg dafür, dass sie auf breite Zustimmung stoßen, ist die Tatsache, dass sie immer häufiger als Grundlage für die Gesetzgebung in vielen Teilen der Welt dienen, unter anderem in Asien und Afrika.⁴

Weniger Einfluss hatten sie auf die Datenschutzgesetze in den USA: Einige Datenschutzgesetze der USA enthalten einige der wesentlichen Datenschutzgrundsätze, aber der Anwendungsbereich dieser Gesetze ist sehr beschränkt und viele Bereiche der Datenerhebung unterliegen anderen Bestimmungen, z. B. den Bestimmungen gegen unfaire oder irreführende Geschäftspraktiken.⁵ Das hat jedoch höchstens zur Betonung der insgesamten Schwäche des US-amerikanischen Modells (soweit man hier von einem einzigen Modell sprechen kann) beigetragen. Die wesentlichen europäischen Grundsätze sollten daher nochmals bestätigt und verstärkt werden. Außerdem sollten die Bemühungen, dass sie weltweit übernommen werden, fortgesetzt werden.

Dies wird in Abschnitt V, Unterabschnitt V.1 weiter ausgeführt (mit Verweis insbesondere auf das Working Paper No. 2).

³ Die in diesem Abschnitt besprochenen Aspekte werden unten unter Abschnitt V weiter ausgeführt. Für sämtliche Details (besonders auch der zugrundeliegenden Analysen) und Verweise siehe Working Paper No. 2: Data protection laws in the EU - The difficulties in meeting the challenges posed by global social and technical developments, das zusammen mit diesem Bericht eingereicht wird. Anmerkung: Es handelt sich dabei um eine neue, erweiterte Version desselben Working Papers, das mit dem Zwischenbericht eingereicht wurde.

⁴ Das ER Übereinkommen zum Datenschutz (CETS Nr. 108) und die EG Richtlinie (Richtlinie 95/46/EG) sind zweifelsohne die wichtigste Inspiration für alle europäischen Datenschutzgesetze und auch für die Gesetze in Staaten, die die Mitgliedschaft bei der EU anstreben und in anderen Staaten wie Russland. Betreffend die asiatisch-pazifische Region siehe die vergleichende Übersicht von Graham Greenleaf, Twenty-one years of Asia-Pacific data protection, Privacy Laws & Business International, Issue 101, Oktober 2009 und dabei besonders sein Kommentar, dass „Den größten Einfluss auf die Datenschutzgrundsätze [in der asiatisch-pazifischen Region] üben die OECD-Leitsätze und die EU-Richtlinie aus; das APEC Privacy Framework hatte dagegen bisher noch keinen direkten Einfluss. Im Gegenteil scheint der Einfluss der EU Richtlinie im Laufe der Zeit sogar zu wachsen.“ (Übersetzung: V.G./S.H.) (Conclusions, p. 11). Besonders die Rechtsvorschriften in der Sonderverwaltungsregion Macau werden nach dem Vorbild der Richtlinie (via die portugiesische Gesetzgebung) gestaltet; der chinesische Gesetzesentwurf von 2006-7 war ebenfalls stark von der EU beeinflusst, ebenso wie die südkoreanische Gesetzgebung. Mäßige Fortschritte werden auch bei der Einführung von Datenschutz in Afrika gemacht, hauptsächlich mit der Hilfe von CNIL, der französischen Datenschutzbehörde. Aufgrund dieser Hilfe sind die entstehenden Gesetze auf diesem Kontinent ebenfalls eindeutig von europäischen Instrumenten beeinflusst. Für Belege, dass der neue südafrikanische Gesetzesentwurf so gestaltet wurde, dass er mit der Richtlinie konform ist siehe den Artikel von Iain Currie in Privacy Laws & Business International, Issue 101, Oktober 2009. Erwähnt werden sollte auch die vor kurzem begonnene Arbeit der Internationalen Konferenz der Beauftragten für den Datenschutz und den Schutz der Privatsphäre, die mit der „Barcelona-Initiative“ weltweite Standards etablieren will, die auf den europäischen beruhen, und die Reaktion eines breiten Zusammenschlusses von zivilgesellschaftlichen Organisationen, die sich durch ihre „Erklärung von Madrid“ vom 3. November 2009 mit dieser Initiative auseinandersetzen.

⁵ Siehe *Country Report on the USA*, Abschnitte 2 und 4.

EUROPÄISCHE KOMMISSION – GD JLS
**VERSCHIEDENE ANSÄTZE ZUR BEWÄLTIGUNG NEUER HERAUSFORDERUNGEN FÜR DEN
SCHUTZ DER PRIVATSPHÄRE, INSBESONDERE AUFGRUND TECHNOLOGISCHER
ENTWICKLUNGEN**

Schlussbericht

16. Trotzdem ist ihre spezifische Anwendung und Durchsetzung viel weniger erfolgreich und die neuen technologischen Entwicklungen – intrusiveres Ubiquitous Computing und omnipräsentes und intrusiveres Erheben und Verwenden personenbezogener Daten; „die Erstellung von Profilen“; die omnipräsente Internationalisierung dieser Art von Verarbeitung; nutzergenerierte Web-Inhalte; etc. – drohen die Anwendung der Grundsätze sogar noch weiter zu erschweren, sogar auf dem Papier (obwohl einige der Technologien auch bei ihrer Anwendung helfen können).
17. Die folgenden Gebiete sind jene, aus denen hauptsächlich Herausforderungen für die Datenschutzgesetze der EU entstehen; alle werden in Abschnitt V (wie angegeben) weiter ausgeführt:
- ✓ Einige Aspekte unterliegen der Richtlinie nicht und müssen nicht in einzelstaatliches Recht umgesetzt werden; diese Ausnahmen werden insbesondere im neuen „Web 2.0-Umfeld“ problematischer werden.

Dies wird in Abschnitt V, Unterabschnitt V.2 weiter ausgeführt (mit Verweis insbesondere auf Working Paper No. 2).

- ✓ Es bestehen immer noch größere Rechtskonflikte, sogar innerhalb von EU/EWR, aber besonders in Bezug auf für die Verarbeitung Verantwortliche in Nicht-EU/EWR-Ländern; und diese Konflikte werden stark zunehmen.

Dies wird in Abschnitt V, Unterabschnitt V.3 weiter ausgeführt, wieder mit Verweis insbesondere auf Working Paper No. 2.

- ✓ Es bestehen immer noch große Unterschiede in der Anwendung und Auslegung sogar der grundlegenden Datenschutzkonzepte und -vorschriften, sogar innerhalb von EU/EWR, und noch größere Unterschiede zwischen EU/EWR und anderen Ländern; in einer allgemein internationalisierten Welt der Datenverarbeitung werden diese Unterschiede zunehmend zum Problem werden.

Diese Unterschiede resultieren zum Teil aus der unzulänglichen oder mangelhaften Umsetzung der Richtlinie durch die Mitgliedstaaten, und zum Teil aus den Unterschieden in der Auslegung und Anwendung der Richtlinie. Die Mechanismen für eine volle, harmonisiertere Umsetzung der Richtlinie wurden nicht voll ausgeschöpft. Im Speziellen, aus unserer Sicht:

- hat die Europäische Kommission nicht energisch genug Durchsetzungsmaßnahmen gegen die Mitgliedstaaten, die die Richtlinie nicht ordnungsgemäß umgesetzt haben, ergriffen und
- Die Mechanismen in der Richtlinie, die auf eine umfassendere Harmonisierung abzielen, wurden nicht ausreichend genutzt. Zum Teil sind auch die auf eine umfassendere Harmonisierung abzielenden Verfahren selbst mangelhaft und müssen überarbeitet werden.

EUROPÄISCHE KOMMISSION – GD JLS
**VERSCHIEDENE ANSÄTZE ZUR BEWÄLTIGUNG NEUER HERAUSFORDERUNGEN FÜR DEN
SCHUTZ DER PRIVATSPHÄRE, INSBESONDERE AUFGRUND TECHNOLOGISCHER
ENTWICKLUNGEN**

Schlussbericht

Dies wird in Abschnitt V, Unterabschnitt V.4 weiter ausgeführt, mit Verweis sowohl auf das Working Paper No. 2 als auch auf eine andere Studie der Kommission zur Artikel 29 Datenschutzgruppe.

- ✓ Die Europäische Kommission hat das Verfahren zur Bescheinigung eines „angemessenen Datenschutzniveaus“ nur in einer begrenzten Anzahl von Ländern angewendet. Global hatte dieses Verfahren daher geringere Auswirkungen als erhofft; und infolgedessen wurde die Entwicklung von starken Datenschutzgesetzen in Nicht-EU/EWR-Ländern weniger stark gefördert, als dies der Fall hätte sein können.

Dies wird in Abschnitt V, Unterabschnitt V.5 weiter ausgeführt.

- ✓ Sogar innerhalb von EU/EWR sind die Durchsetzungsmaßnahmen der nationalen Datenschutzbehörden häufig nicht stark oder umfassend. Mit einigen namhaften Ausnahmen (besonders Neuseeland und teilweise, im Privatsektor, Südkorea) ist die Durchsetzung in den meisten außereuropäischen Staaten, einschließlich der USA, sogar noch schwächer. Die Durchsetzung wird aber im neuen, globalen technischen Umfeld sowohl wichtiger als auch schwieriger werden (allerdings kann auch hier die Technologie in manchen Fällen hilfreich sein).

Dies wird in Abschnitt V, Unterabschnitt V.6 weiter ausgeführt mit Verweis, was die Verfahren der DPAs in EU/EWR betrifft, auf eine von der Agentur der EU für Grundrechte in Auftrag gegebene Studie und, was die Durchsetzung außerhalb von EU/EWR betrifft, mit Verweis auf die Country Reports über Nicht-EU/EWR-Länder.

- ✓ Die Geltendmachung der Rechte betroffener Personen, entweder individuell oder mit der Hilfe von NGOs, gestaltet sich in und außerhalb von Europa oft schwierig und wird durch verschiedene Aspekte behindert. Allerdings ist der Datenschutz in einigen außereuropäischen Ländern, besonders in den USA, zwar allgemein schwächer, dafür werden dort aber einige spezielle Mittel angeboten, die als Beispiel für die Stärkung der Macht von Einzelpersonen über ihre Daten in EU/EWR herangezogen werden könnten.

Dies wird in Abschnitt V, Unterabschnitt V.7 weiter ausgeführt.

- ✓ Zusätzliche und alternative Mittel zur Verbesserung des Datenschutzes, darunter technische Mittel wie Verschlüsselung, Anonymisierung, Identitätsmanagement-Tools und andere (angebliche) Technologien zur Verbesserung des Datenschutzes (PETs), sind immer noch eher unausgereift, oft schwach in ihrer Anwendung und Wirkung und werden zu oft so angewendet, dass sie ineffektiv sind. Manche sind kaum mehr als ein Feigenblatt. Andere (z. B. die Anonymisierung) werden angesichts des technologischen Fortschritts zunehmend nutzlos. Auch bekämpfen sie die Probleme oft nicht im richtigen Moment, nämlich besonders in der Planungsphase, oder sie sind nicht benutzerfreundlich. Im neuen technischen Umfeld wird diesen Mitteln erneut – und kritischere – Aufmerksamkeit geschenkt werden müssen. Manche technisch vergleichsweise einfachen Lösungen, z. B. dass Standardeinstellungen verschiedener Anwendungen ein hohes Datenschutzniveau aufweisen müssen, oder die Vergabe von Datenschutz-Gütesiegeln, können zur Sicherstellung eines angemessenen Schutzes beitragen.

EUROPÄISCHE KOMMISSION – GD JLS
**VERSCHIEDENE ANSÄTZE ZUR BEWÄLTIGUNG NEUER HERAUSFORDERUNGEN FÜR DEN
SCHUTZ DER PRIVATSPHÄRE, INSBESONDERE AUFGRUND TECHNOLOGISCHER
ENTWICKLUNGEN**

Schlussbericht

Dies wird in Abschnitt V, Unterabschnitt V.8 weiter ausgeführt.

18. Jede seriöse Überarbeitung der europäischen Datenschutzregelung muss sich mit sämtlichen oben erwähnten Problemen auseinandersetzen – die ausnahmslos durch die sozialen und technischen Veränderungen, die auf uns zukommen (oder schon stattgefunden haben) massiv verschärft werden. Die Herausforderungen wachsen. Es handelt sich jedoch hauptsächlich um Herausforderungen in Bezug auf Aspekte der Anwendung, Auslegung und Effektivität der Durchsetzung/Geltendmachung von Rechten: Die wesentlichen Datenschutzgrundsätze werden nicht in Frage gestellt, sondern müssen vielmehr nochmals bestärkt und in größerem Umfang praktisch angewendet werden.

- o – O – o -

IV. Grundvoraussetzungen

19. Manche Fragen sind so grundlegend, dass sie in jeder Überarbeitung der Datenschutzregelung der EU zu berücksichtigen sind. Sie können nicht außer Acht gelassen werden (oder als „zu legalistisch“ abgetan werden), ohne damit die zentralen Werte in den europäischen Verfassungen zu gefährden. Aus diesem Grund sind sie hier kurz beschrieben und bilden die Grundlage für all unsere genaueren Schlussfolgerungen und Empfehlungen.

Soziopolitische Voraussetzungen:

20. Die neuen Entwicklungen in der Informations- und Kommunikationstechnik sind zwar von großem Nutzen, bergen jedoch auch neue Gefahren für Einzelpersonen und ihre Beziehung zu mächtigen (öffentlichen und privaten) Behörden. Darunter fallen nicht nur neue Gefahren für die Privatsphäre im herkömmlichen Sinn (Freiheit von Eingriffen und Überwachung), sondern auch neue Gefahren für die persönliche Autonomie und persönliche Freiheit, einschließlich politischer Freiheit, und sogar für die gesamte Gesellschaft.
21. Für die Privatsphäre im herkömmlichen Sinn reicht es wohl, das berühmte *Volkszählungsurteil* des Deutschen Bundesverfassungsgerichts aus dem Jahr 1983 zu zitieren:⁶

Mit dem Recht auf informationelle Selbstbestimmung wären eine Gesellschaftsordnung und eine diese ermöglichende Rechtsordnung nicht vereinbar, in der Bürger nicht mehr wissen können, wer was wann und bei welcher Gelegenheit über sie weiß. Wer unsicher ist, ob abweichende Verhaltensweisen jederzeit notiert und als Information dauerhaft gespeichert, verwendet oder weitergegeben werden, wird versuchen, nicht durch solche Verhaltensweisen aufzufallen. Wer damit rechnet, daß etwa die Teilnahme an einer Versammlung oder einer Bürgerinitiative behördlich registriert wird und daß ihm dadurch Risiken entstehen können, wird möglicherweise auf eine Ausübung seiner entsprechenden Grundrechte (Art. 8, 9 GG) verzichten. Dies würde nicht nur die individuellen Entfaltungschancen des Einzelnen beeinträchtigen, sondern auch das Gemeinwohl, weil Selbstbestimmung eine elementare Funktionsbedingung eines auf Handlungsfähigkeit und Mitwirkungsfähigkeit seiner Bürger begründeten freiheitlichen demokratischen Gemeinwesens ist.

Die Gesellschaft, die durch die in Working Paper No. 1 angeführten sozialen und technologischen Entwicklungen fast unbedacht zu entstehen droht, ist nicht mehr das in diesem Zitat vorgesehene „freiheitliche demokratische Gemeinwesen“.

22. Doch die neuen Technologien bergen noch weitere, neuere Gefahren: Immer häufigere und zunehmend automatische Analysen einer immer größeren Zahl an immer noch leichter zugänglichen Daten drohen, die Menschen zu bloßen Objekten zu machen, die

⁶ *Volkszählungsurteil*, BVerfGE Bd. 65, S. 1 ff.

EUROPÄISCHE KOMMISSION – GD JLS
**VERSCHIEDENE ANSÄTZE ZUR BEWÄLTIGUNG NEUER HERAUSFORDERUNGEN FÜR DEN
SCHUTZ DER PRIVATSPHÄRE, INSBESONDERE AUFGRUND TECHNOLOGISCHER
ENTWICKLUNGEN**

Schlussbericht

auf der Grundlage von computergenerierten „Profilen“, Wahrscheinlichkeiten und Vorhersagen behandelt (und sogar diskriminiert) werden und die dabei nur geringe oder keine Möglichkeiten haben, sich gegen die zugrundeliegenden Algorithmen zur Wehr zu setzen. Sollte der starke Datenschutz nicht aufrecht erhalten werden, so werden Entscheidungen „von großer Tragweite“ (wie etwa die Entscheidung, eine Person nicht anzustellen oder sie erst gar nicht zu einem Vorstellungsgespräch einzuladen; sie an der Staatsgrenze aufzuhalten und ihr vielleicht die Einreise zu verweigern; sie intrusiver Überwachung zu unterziehen und vielleicht zu verhaften, etc.) zunehmend getroffen „weil das so im Computer steht“, ohne dass selbst die Beamten/-innen oder Angestellten, die die Entscheidung umsetzen, den Grund vollständig erklären können. Die neuen Technologien tendieren naturgemäß dazu, die Machtverhältnisse von der Einzelperson in Richtung derer, die über die Daten der Einzelperson verfügen, zu verschieben. Damit bekommen die Begriffe „Datensubjekt“ und „Datenkontrolleur/-in“ eine tiefere, düsterere Bedeutung. Zum Teil kann dem zwar manchmal mithilfe einiger Technologien entgegengewirkt werden, diese sind jedoch weitaus schwächer und *naturgemäß* weniger effektiv als oft behauptet oder geglaubt wird. Wenn wir die neuen Technologien nicht unter Kontrolle bringen, dann wird ihre uneingeschränkte Nutzung unsere demokratische Gesellschaft selbst unterminieren. Und das Instrument, mit dem wir sie unter Kontrolle bringen können, heißt Datenschutz.

Verweis: Für weitere Details siehe Working Paper No. 1 (zusammengefasst unter I, oben und Abschnitt V, Unterabschnitt V.8, unten.).

Europäische verfassungsrechtliche Voraussetzungen:

23. Der Datenschutz wird zunehmend in der Rechtsprechung des Europäischen Gerichtshofs für Menschenrechte, unter Artikel 8 der Europäischen Menschenrechtskonvention, und in der EU-Gesetzgebung (in letzterem Fall vor allem durch die „allgemeinen Rechtsgrundsätze des Gemeinschaftsrechts“, die Charta der Grundrechte der Europäischen Union und die Rechtsprechung des Gerichtshofs der Europäischen Union) anerkannt. Deshalb haben die wesentlichen Datenschutzgrundsätze und -bestimmungen nun effektiv Verfassungsrang. Dies sollte bei jeder Änderung der EG-Datenschutzrichtlinie(n) volle Berücksichtigung finden. Sollte eine abgeänderte Richtlinie diese grundlegenden Anforderungen nicht erfüllen, so würde dies zu rechtlichen Problemen und negativen Entscheidungen in Luxemburg und (was ihre Umsetzung in den und durch die Mitgliedsstaaten betrifft) in Straßburg führen. Bei jeder Änderung der Basisrichtlinie sollte es ein Hauptziel sein, derartige Verstöße nicht nur zu vermeiden, sondern sogar ganz sicherzustellen, dass jede neue EU-Datenschutzregelung – über die immer noch drei „Säulen“ der EU hinweg – die grundlegenden europäischen Anforderungen im Bereich der Menschenrechte vollständig erfüllt.

Verweis: Für weitere Details siehe Douwe Korff, *Paper No. 4: The Legal Framework*, in: Ian Brown & Douwe Korff, Privacy & Law Enforcement, study for the UK Information Commissioner, 2004 (in dem mit diesem Bericht eingereichten Material enthalten).

24. Der Datenschutz ist in den Verfassungen mehrerer EU-Mitgliedsstaaten, etwa Dänemark, Deutschland und Griechenland, fest verankert. Sollte eine EU-Datenschutzregelung es in irgendeiner Weise verabsäumen, die verfassungsrechtlichen

EUROPÄISCHE KOMMISSION – GD JLS
**VERSCHIEDENE ANSÄTZE ZUR BEWÄLTIGUNG NEUER HERAUSFORDERUNGEN FÜR DEN
SCHUTZ DER PRIVATSPHÄRE, INSBESONDERE AUFGRUND TECHNOLOGISCHER
ENTWICKLUNGEN**

Schlussbericht

Anforderungen dieser Mitgliedsstaaten zu erfüllen, so verursacht dies wohl erhebliche Spannungen zwischen der einzelstaatlichen und der EG/EU-Gesetzgebung. Ein gutes Beispiel hierfür stellt der *Solange*-Beschluss des deutschen Bundesverfassungsgerichts dar, welcher kürzlich in Bezug auf den Vertrag von Lissabon bekräftigt wurde. Die unten angeführten Zitate sollen diese Spannungen veranschaulichen:

Zitate:

EuGH-Urteil Stauder:

(Rechtssache 29/69, *Erich Stauder gegen Stadt Ulm*, [1969], *Sammlung der Rechtsprechung* S. 419, Abs. 3-4)

Die einheitliche Geltung des Gemeinschaftsrechts würde beeinträchtigt, wenn bei der Entscheidung über die Gültigkeit von Handlungen der Gemeinschaftsorgane Normen oder Grundsätze des nationalen Rechts herangezogen würden. Die Gültigkeit solcher Handlungen kann nur nach dem Gemeinschaftsrecht beurteilt werden, denn dem vom Vertrag geschaffenen, somit aus einer autonomen Rechtsquelle fließenden Recht können wegen seiner Eigenständigkeit keine wie immer gearteten innerstaatlichen Rechtsvorschriften vorgehen, wenn ihm nicht sein Charakter als Gemeinschaftsrecht aberkannt und wenn nicht die Rechtsgrundlage der Gemeinschaft selbst in Frage gestellt werden soll. **Daher kann es die Gültigkeit einer Gemeinschaftshandlung oder deren Geltung in einem Mitgliedstaat nicht berühren, wenn geltend gemacht wird, die Grundrechte in der ihnen von der Verfassung dieses Staates gegebenen Gestalt oder die Strukturprinzipien der nationalen Verfassung seien verletzt.**

Fortsetzung umseitig

Vgl. im Gegensatz dazu:

Entscheidung des deutschen Bundesverfassungsgerichts über die Verfassungsmäßigkeit des Vertrages von Lissabon:

(Entscheidung des deutschen Bundesverfassungsgerichts [BVerGE], 2BvE 2/08, 30. Juni 2009, Abs. 240)

Wenn Rechtsschutz auf Unionsebene nicht zu erlangen ist, prüft das Bundesverfassungsgericht, ob Rechtsakte der europäischen Organe und Einrichtungen sich unter Wahrung des gemeinschafts- und unionsrechtlichen Subsidiaritätsprinzips [...] in den Grenzen der ihnen im Wege der begrenzten Einzelermächtigung eingeräumten Hoheitsrechte halten ...

Ein wichtiges Urteil in Rumänien, das während der Vorbereitungsphase dieses Berichtes veröffentlicht wurde, zeigt, dass sich die oben genannten Spannungen nicht auf die „alten“ Mitgliedsstaaten beschränken. Am 8. Oktober 2009 erklärte das Rumänische Verfassungsgericht ein Gesetz, welches die Mobilfunkbetreiber und Internetdienstanbieter zur 6-monatigen Speicherung von Kommunikationsdaten verpflichtet hätte, für verfassungswidrig.⁷ Das Gesetz sollte zur Umsetzung der EG-

⁷

Siehe: http://sofiaecho.com/2009/10/09/797385_romanian-constitutional-court-data-retention-law-

EUROPÄISCHE KOMMISSION – GD JLS
**VERSCHIEDENE ANSÄTZE ZUR BEWÄLTIGUNG NEUER HERAUSFORDERUNGEN FÜR DEN
SCHUTZ DER PRIVATSPHÄRE, INSBESONDERE AUFGRUND TECHNOLOGISCHER
ENTWICKLUNGEN**

Schlussbericht

Richtlinie über die Vorratsspeicherung von Daten (Richtlinie 2006/24/EC) dienen und das Urteil deutet darauf hin, dass die Erfordernisse der Richtlinie selbst ebenfalls die verfassungsrechtlichen Anforderungen des Landes verletzen.

An dem zuvor Genannten lässt sich erkennen, dass das Thema Datenschutz innerhalb der EU sehr leicht die *Solange*-Probleme wieder aufflammen lassen kann. Deshalb ist es von äußerster Wichtigkeit, dass eine abgeänderte EU-Datenschutzregelung (besonders dann, wenn sie für alle derzeit von den drei „Säulen“ abgedeckten Bereiche gelten soll) die Anforderungen der EMRK und der Verfassungen der Mitgliedsstaaten erfüllt (insbesondere aber nicht ausschließlich die diesbezüglichen Anforderungen der deutschen Verfassung, welche vom dortigen Bundesverfassungsgericht erarbeitet wurden).

Verweise: Für weitere Details siehe insbesondere den *Country Report on Germany*, und die vergleichende Analyse in Working Paper No. 2. Siehe außerdem Abs. 43, unten.

25. Auch in manchen der behandelten Nicht-EWR-Ländern kann die Verankerung des Datenschutzes in der Verfassung von Bedeutung sein. Dies trifft vor allem auf Japan und Hongkong zu. Jedoch wurde der Datenschutz in diesen Ländern noch nicht vollständig im Rahmen eines allgemeineren verfassungsmäßigen Schutzes der Privatsphäre entwickelt. In Australien ist der Datenschutz kaum oder gar nicht in der Verfassung verankert. In anderen Ländern in Asien und im pazifischen Raum ist die Lage ähnlich verschieden. Es gibt daher in ganz Asien und im pazifischen Raum, zumindest derzeit, kein harmonisierendes Element, das mit den europäischen Menschenrechtsstandards vergleichbar wäre. In den USA beschränkt sich der verfassungsrechtliche Schutz auf föderaler Ebene weitgehend auf Einschränkungen des Zugangs zu personenbezogenen Daten und deren Nutzung für die Regierung (selbst dies gilt hauptsächlich nur für US-Staatsbürger/-innen), wobei dieser häufig unter Berufung auf den 1. Zusatzartikel aufgehoben wurde (für aktuellere Entwicklungen siehe Abs. 34, unten). Manche Bundesstaaten haben zwar den verfassungsrechtlichen Schutz auf einzelstaatlicher Ebene ausgeweitet, liegen jedoch in dieser Hinsicht immer noch weit hinter europäischen Ländern wie etwa Deutschland.

Verweise: Für weitere Details siehe die *Country Reports* über die oben genannten Nicht-EU-Länder.

V. Schlussfolgerungen & Empfehlungen

1. GRUNDANSATZ [weitere Ausführung der vorigen Abschnitte]

26. Jede Überarbeitung der Datenschutzregelung der EU sollte zunächst ausdrücklich anerkennen, dass die Anforderungen der EMRK und der Charta der Grundrechte der Europäischen Union sowie der Verfassungen der Mitgliedsstaaten zu erfüllen sind.⁸ Die Erfüllung der diesbezüglichen soziopolitischen und verfassungsrechtlichen Voraussetzungen (in allen früher von den drei „Säulen“ abgedeckten Bereichen) wird in dem neuen globalen soziopolitischen und technischen Umfeld von noch entscheidenderer Bedeutung sein.
27. Datenschutzgesetze in der EU (in allen früher von den drei „Säulen“ abgedeckten Bereichen) können und sollten weiterhin auf den wesentlichen Datenschutzgrundsätzen und -kriterien der Richtlinie 95/46/EC beruhen. Die Anwendung dieser breiten Standards muss zwar näher erläutert werden (wie unten, insbesondere unter Unterabschnitt V.4, näher ausgeführt wird), doch die Standards selbst bedürfen zur Bewältigung der neuen Herausforderungen keiner größeren Änderung. Ganz im Gegenteil widerspiegeln sie europäische und nationale Verfassungs-/Menschenrechtsstandards der eben erwähnten Art, welche stark bekräftigt werden müssen.
28. Bei jeder Überarbeitung, die auf die Bewältigung der neuen Herausforderungen ausgerichtet ist, muss das Hauptaugenmerk auf den folgenden (zusammenhängenden) Aspekten liegen, die in den angegebenen Unterabschnitten behandelt werden:
- der problematische Ausschluss gewisser Angelegenheiten aus dem Geltungsbereich der Richtlinie (V.2);
 - die schwierige Frage des „anzuwendenden Rechts“ (V.3);
 - die Notwendigkeit weitaus stärkerer Harmonisierung (auf einem hohen Niveau) in EU/EWR, und zwar mit verschiedenen Mitteln, u.a. strengeren Durchsetzungsmaßnahmen seitens der Kommission (V.4);
 - die Notwendigkeit vermehrter Zusammenarbeit mit Nicht-EU-Ländern und stärkerer Anerkennung von „angemessenen“ Bemühungen außerhalb der EU. (V.5);
 - die Notwendigkeit, die genauere Einhaltung und stärkere Durchsetzung des geltenden Rechts auf innerstaatlicher Ebene durch die DPAs sicherzustellen (V.6);
 - die Notwendigkeit, die Rechte und Rechtsbehelfe für Einzelpersonen (die möglicherweise mit oder durch relevante NGOs tätig werden) zu stärken (V.7); und
 - die Notwendigkeit, zusätzliche und alternative Maßnahmen weiterzuentwickeln (unter Berücksichtigung der inhärenten Grenzen und praktischen Beschränkungen solcher Maßnahmen) (V.8).

⁸ Mit Inkrafttreten des Vertrages von Lissabon am 1. Dezember 2009 wurde die Charta rechtsverbindlich. Artikel 8 anerkennt das eigenständige Recht auf den Schutz personenbezogener Daten und Artikel 16 des Vertrages über die Arbeitsweise der Europäischen Union sieht die Einrichtung eines homogenen Rechtsrahmens durch die Union und ihre Mitgliedsstaaten vor, der dieses Grundrecht bei jeder Tätigkeit der Union umsetzt. Außerdem wurden durch den Vertrag die früheren drei „Säulen“ abgeschafft.

29. Besonders der zweite und der dritte Aspekt hängen eng zusammen, da die entscheidende Frage im Bereich des „anzuwendenden Rechts“ (d.h. sicherzustellen, dass jeder in EU/EWR ablaufende Vorgang nur einem, leicht zu erkennenden, einzelstaatlichen Recht unterliegt und niemals keinem) nur durch weitaus stärkere Harmonisierung bei der Anwendung der Richtlinie gelöst werden kann. Außerdem sind strenge Datenschutzregelungen im Allgemeinen natürlich ohne Zweck, wenn diese entweder wichtige Bereiche nicht umfassen oder nicht richtig oder vollständig eingehalten und durchgesetzt werden.

Unsere diesbezüglichen Schlussfolgerungen und Empfehlungen sind unten angeführt.

2. GELTUNGSBEREICH DER EU-DATENSCHUTZREGELUNGEN

(i) Die ehemalige erste und dritte Säule betreffende Angelegenheiten:

30. **Ergebnis/Schlussfolgerung:** Die Tätigkeiten in den Bereichen, welche vor Inkrafttreten des Vertrages von Lissabon als erste und dritte „Säule“ der EU⁹ bezeichnet wurden, sind immer enger verknüpft und werden zunehmend untrennbar (vgl. z.B. die SWIFT- und PNR-Kontroversen). In dieser Hinsicht ist die Abschaffung der verschiedenen Säulen zu begrüßen. Außerdem ist der Grundsatz der ehemaligen dritten Säule der „dauerhaften Eigentümerschaft“ von Daten undurchführbar, da er die Möglichkeit voraussetzt, dass ein Herkunftsland wirklich die Kontrolle über Daten, die an Behörden in einem anderen Land weitergegeben werden, behalten kann. Er ist zudem unvereinbar mit der ebenfalls gestellten Anforderung der „Verfügbarkeit“ (im Prümmer Vertrag verankert), die den Datenschutzgrundsätzen völlig widerspricht.
31. Wir glauben, dass der Preis für erhöhte Polizei- und Sicherheitszusammenarbeit ein garantierter Datenschutz, sowohl in den Mitgliedsstaaten als auch in allen in diesem Bereich tätigen EU-Institutionen, sein muss und zwar auf dem höchsten von irgendeiner Verfassung der Mitgliedsstaaten und den europäischen Menschenrechtsvorschriften erforderten Niveau. Die Kooperation innerhalb der EU bei Angelegenheiten, die die ehemalige dritte Säule betreffen, ist ernsthaft gefährdet, wenn der Datenschutz (wie in der früheren ersten Säule) nicht zumindest auf diesem Niveau gewährleistet wird. Die Harmonisierung des Datenschutzes in polizeilichen Angelegenheiten sollte auf der Empfehlung des Europarats R(87)15 beruhen, auf die sich die Instrumente der EU (und des ER) im Bereich der Polizeizusammenarbeit, wie etwa der Schengen- und der Europol-Vertrag, regelmäßig berufen (jedoch ohne sie in ihrer gesamten Tragweite zu übernehmen oder in der Praxis ihre Grundsätze zu befolgen).

Anmerkung: Manche mögen vielleicht der Meinung sein, dass, abseits der Frage nach der richtigen Umsetzung von EU-Recht in einzelstaatlichem Recht, der Grad des nationalen Datenschutzes keine Angelegenheit der EG- oder EU-Rechtsvorschriften darstellt. Diese Meinung konnte jedoch, wie unter Unterabschnitt V.3 und V.4 erklärt wird, schon in der ehemaligen ersten Säule, wegen des starken Zusammenspiels zwischen Harmonisierung und der Frage nach dem „anzuwendenden Recht“, nicht aufrechterhalten werden. Würde man die Richtlinie auf die frühere dritte Säule

⁹

Siehe vorhergehende Fußnote.

EUROPÄISCHE KOMMISSION – GD JLS
**VERSCHIEDENE ANSÄTZE ZUR BEWÄLTIGUNG NEUER HERAUSFORDERUNGEN FÜR DEN
SCHUTZ DER PRIVATSPHÄRE, INSBESONDERE AUFGRUND TECHNOLOGISCHER
ENTWICKLUNGEN**

Schlussbericht

ausweiten oder Regelungen, welche jenen zum Thema „anzuwendendes Recht“ in der Richtlinie ähneln, auf diesen Bereich anwenden, so würde der Grad des Schutzes von polizeilichen Daten in allen EU-/EWR-Ländern zu einem dringenden Anliegen für Länder mit starkem diesbezüglichen Verfassungsschutz. Diese könnten es, in einem derart sensiblen Kontext, nicht akzeptieren, dass ausländische Gesetze, die nicht den eigenen verfassungsrechtlichen Anforderungen entsprechen, auf die eigenen Bürger/-innen angewandt werden: siehe Absatz 24, oben. Eigentlich ruft sogar schon der Verfügbarkeitsgrundsatz dieselben Bedenken hervor, auch wenn diese noch nicht an die Gerichte weitergeleitet wurden.

32. Das Obengenannte erfordert strenge gesetzliche Regelungen, welche die europäischen „Qualitätsanforderungen“ für „Rechtsvorschriften“ erfüllen, wie sie der Europäische Gerichtshof für Menschenrechte beschreibt: Einschränkungen der „Verfügbarkeit“ und der Vorratsspeicherung von Daten (einschließlich Kommunikations- und DNA-Daten); strenge Beschränkungen der Nutzung von „Profilen“; sowie starker Verfahrensschutz mit vollständigem Zugang zu den nationalen und europäischen Gerichten für Einzelpersonen, die von derartigen Maßnahmen betroffen sind, und die volle Zuständigkeit dieser Gerichte, alle Einzelheiten jedes Falls auf ihre Begründetheit hin zu überprüfen.

Verweis: Working Paper No. 2, Abschnitt 2, Unterabschnitt 2.1.

33. **Empfehlung:** Die wesentlichen in der Richtlinie verankerten Datenschutzgrundsätze, -regelungen und -kriterien müssen „nahtlos“ auf die Tätigkeiten in allen Bereichen, die früher zu den verschiedenen Säulen gehörten, angewandt werden. Dies bezieht sich auch auf die Anwendung der (beschränkten) Ausnahmen für Tätigkeiten innerhalb der früheren dritten Säule, welche unter Artikel 13 der Richtlinie aufgeführt sind. Für die Bewältigung der Herausforderungen bedarf es stärkerer Harmonisierung, oder zumindest Annäherung, der Datenschutzregelungen zu diesen Tätigkeiten in der EU, auf der Grundlage der Empfehlung des Europarats R (87) 15. Auch vollständiger Rechtsschutz in den nationalen Gerichten, und durch den EuGH, ist notwendig, wobei die betroffenen Personen die volle Klagebefugnis haben (und der Europäische Gerichtshof für Menschenrechte die letzte Instanz darstellt).

(ii) **Ausnahmen für rein persönliche Verarbeitung und das Recht auf freie Meinungsäußerung, insbesondere was soziale Online-Netze und das „Bloggen“ im „Web 2.0“ betrifft:**

34. **Ergebnis/Schlussfolgerung:** Nutzergenerierter Inhalt (UGC) wird in der neuen Online-Umgebung, insbesondere durch SNS, das „Bloggen“ und „Twittern“ sowie ähnliche Phänomene, massiv zunehmen: Eine Flut an derzeit noch nicht digitalisierten Informationen wartet nur darauf, das neue „Web 2.0“ zu überschwemmen. Dabei macht der UGC wohl den größten Anteil aus – oder zumindest einen Anteil, der jenem des von Institutionen generierten Inhalts gleichkommt. Die besonderen Ausnahmen in der Richtlinie in Bezug auf „rein persönliche Verarbeitung“ und „das Recht auf freie Meinungsäußerung“ werden auf dieses Phänomen sehr schwer anzuwenden sein. Bei beiden besteht die Gefahr, dass einerseits Tätigkeiten, welche direkte Auswirkungen auf den Datenschutz haben, von den gesetzlichen Regelungen ausgenommen werden, und dass andererseits „scharfe“ Regelungen, welche zur Regulierung (vermutlich) gut organisierter Institutionen geschaffen wurden, auf simple Tätigkeiten, die gewöhnliche

EUROPÄISCHE KOMMISSION – GD JLS
**VERSCHIEDENE ANSÄTZE ZUR BEWÄLTIGUNG NEUER HERAUSFORDERUNGEN FÜR DEN
SCHUTZ DER PRIVATSPHÄRE, INSBESONDERE AUFGRUND TECHNOLOGISCHER
ENTWICKLUNGEN**

Schlussbericht

Personen im Rahmen ihres Alltags erledigen, angewandt werden. Dies war einer der Kritikpunkte am Lindqvist-Urteil des EuGH, welches die volle Härte der Basisrichtlinie auf die kleine Internetseite einer schwedischen Pfarrgemeinde anwandte.

Wir sollten anmerken, dass in Nicht-EU/EWR-Ländern mit verfassungsrechtlichem Schutz konkurrierender Rechte wie Privatsphäre und freier Meinungsäußerung weitgehend dieselben Probleme bestehen: Die Frage, wie man solche Rechte in Einklang bringen soll, ist zwar unvermeidlich, muss aber in vielen Ländern erst noch richtig gestellt werden. In den USA war man früher der Meinung, dass der 1. Zusatzartikel zur Verfassung (der das Recht auf freie Meinungsäußerung schützt) für gewöhnlich stärker wiegt als das Recht auf Privatsphäre, und verschiedene „Torts“ (zivilrechtliche Delikte), wie etwa Verleumdung und die (unrechtmäßige) „öffentliche Bekanntgabe von privaten Informationen einer Person“ wurden unter dem 1. Zusatzartikel tatsächlich stark beschnitten. In jüngerer Vergangenheit haben jedoch datenschutzähnliche Gesetze wie etwa jene zu Kreditauskünften und Finanzdienstleistungen den Überprüfungen durch den 1. Zusatzartikel standgehalten: siehe Country Report über die USA, Abschnitte 1.5 und 1.6. Es ist zwar noch zu früh, um von einer Konvergenz der Ansätze der USA und der EU zu sprechen, diese Entwicklungen bedeuten aber durchaus, dass die Unterschiede abgenommen haben.

Verweise: Working Paper No. 1, Abschnitt über *Social networking and user-generated content* (pp. 11-12); Working Paper No. 2, Abschnitt 2, Unterabschnitt 2.2. Country Report on the USA, Abschnitte 1.5 und 1.6.

35. **Empfehlung:** Es sollte möglich sein, die Datenschutzvorschriften in schwächerer Form auf relativ triviale Tätigkeiten im Internet anzuwenden. Besonders problematisch ist der Versuch, einzelne gewöhnliche Internetnutzer/-innen der vollen Härte der Regelungen, welche für die „für die Verarbeitung Verantwortlichen“ gelten, zu unterwerfen. Wir glauben, dass sich dieses Problem am besten durch die Regulierung der Dienste, die gewöhnliche Nutzer/-innen in Anspruch nehmen, lösen lässt: die sozialen Online-Netze; die Seiten, die „Blogs“ anbieten; etc. Derartige Anbieter sollten insbesondere Standardeinstellungen für ihre Internetseiten sowie datenschutzfreundliche Dienste und Werkzeuge anbieten müssen. Gewöhnliche Nutzer/-innen, die solche Seiten verwenden, ohne die Standardeinstellungen zu verändern, sollten die angemessene Erwartung haben können, dass sie keine Datenschutzvorschriften verletzen. Falls durch die Standardeinstellungen der Schutz der Privatsphäre und der personenbezogenen Daten nicht gewährleistet ist, dann sollte dafür die Internetseite, die die Einstellungen gewählt hat, die Hauptverantwortung tragen. Dies würde die Möglichkeit offenhalten, Regelungen für torts [zivilrechtliche Delikte oder fautes] zu verabschieden (oder, falls diese bereits existieren, beizubehalten), die es erlauben, Einzelpersonen aufgrund von unrechtmäßiger oder ungerechtfertigter öffentlicher Bekanntgabe privater Informationen oder „Eingriffen“ über das Internet oder über andere allgegenwärtige Kommunikationssysteme wie SMS oder MMS zur Verantwortung zu ziehen. Diese Regelungen funktionieren in den USA recht gut (unter Berücksichtigung der oben erwähnten Probleme in Bezug auf den 1. Zusatzartikel) und wurden vor Kurzem in Neuseeland durch die dortige Rechtsprechung geschaffen. Sie werden von Rechtsreformkommissionen in Australien und Hongkong empfohlen. Solche Regelungen könnten durch die Möglichkeit gestärkt werden, einstweilige gerichtliche Verfügungen, oder Anordnungen der DPAs zu erwirken, welche die Entfernung von UGC fordern, der in den Augen der betroffenen Person oder der DPA gesetzeswidrig ist.

EUROPÄISCHE KOMMISSION – GD JLS
**VERSCHIEDENE ANSÄTZE ZUR BEWÄLTIGUNG NEUER HERAUSFORDERUNGEN FÜR DEN
SCHUTZ DER PRIVATSPHÄRE, INSBESONDERE AUFGRUND TECHNOLOGISCHER
ENTWICKLUNGEN**

Schlussbericht

Dies könnte wiederum von dem/der Poster/-in mit der Begründung, dass keine Gesetzeswidrigkeit vorliegt, angefochten werden. Wir glauben, dass in vielen EU-Mitgliedsstaaten derartige Lösungen bereits möglich sind (teils auf der Grundlage des Zivilrechts, teils – insbesondere was die Standardeinstellungen der SNS betrifft – auf der Grundlage des Datenschutzgesetzes).

Verweise: Country Reports über Australien und Hongkong, Abschnitt 1.7 in beiden Fällen, und über die USA, Abschnitte 1.5 und 1.6.

3. ANZUWENDENDENES RECHT

36. **Ergebnis/Schlussfolgerung:** Alle Arten der Datenverarbeitung, einschließlich der Verarbeitung personenbezogener Daten, werden zunehmend internationalisiert. Das ist bei Tätigkeiten im Internet naturgemäß der Fall und wird sich in einer Ära des „Cloud Computing“ noch verstärken. Auch die an der Verarbeitung beteiligten Akteure sind immer unterschiedlicher, immer häufiger auf verschiedene Länder aufgeteilt und haben zudem oft schwer zu unterscheidende Aufgaben und Verantwortlichkeiten. Dies wird wegen der Mehrdeutigkeit und verschiedenen Umsetzung der Regelungen zum „anzuwendenden Recht“ in der Richtlinie, auch in EU/EWR, zunehmend zu Rechtskonflikten führen.
37. Insbesondere müssen, der Basisrichtlinie zufolge, die Mitgliedsstaaten ihre nationalen Datenschutzgesetze in EU/EWR auf Verarbeitungen anwenden, die *„im Rahmen der Tätigkeiten einer Niederlassung ausgeführt werden, die der für die Verarbeitung Verantwortliche im Hoheitsgebiet dieses Mitgliedstaats besitzt.“* Wenn jedoch *„der Verantwortliche eine Niederlassung im Hoheitsgebiet mehrerer Mitgliedstaaten besitzt, ergreift er die notwendigen Maßnahmen, damit jede dieser Niederlassungen die im jeweils anzuwendenden einzelstaatlichen Recht festgelegten Verpflichtungen einhält“*. (Artikel 4(1)(a) der Basisrichtlinie) Dies bedeutet, dass die Frage, welches Recht auf eine bestimmte Verarbeitung anzuwenden ist, zuallererst davon abhängt, (i) wer der für die Verarbeitung Verantwortliche ist (Dies ist häufig nicht einfach festzustellen und wird in dem neuen globalen technischen Umfeld, das in Working Paper No. 1 beschrieben wird, noch schwieriger werden.); (ii) wo der für die Verarbeitung Verantwortliche seine „Niederlassung“ besitzt (und die Frage nach der „Niederlassung“ ist im Gemeinschaftsrecht generell alles andere als einfach zu beantworten); (iii) in welchem „Rahmen“, die Verarbeitung erfolgt; und (iv) welche „Niederlassung“ des für die Verarbeitung Verantwortlichen betroffen ist (was sich häufig nur schwer genau feststellen lässt) – und all das berücksichtigt noch nicht einmal den zweiten Halbsatz über für die Verarbeitung Verantwortliche mit einer *„Niederlassung im Hoheitsgebiet mehrerer Mitgliedstaaten“*. Die Regelungen unter Artikel 4(1)(a) sind ganz einfach vollkommen verworren und im neuen globalen technischen Umfeld unmöglich anzuwenden. Es überrascht also nicht, dass die Regelungen in den Mitgliedsstaaten unterschiedlich umgesetzt werden, was zu Rechtskonflikten führt (welche in der Praxis nur deshalb nicht allzu gravierend sind, weil die am Papier konkurrierenden und widersprüchlichen Gesetze in der Praxis oft nicht durchgesetzt werden).

Verweis: D Korff, EG Studie zur Durchführung der Datenschutzrichtlinie 95/46/EC, 2002, Abschnitt 4, „applicable law“, die (auf der Grundlage einer detaillierteren Analyse im Bericht zu dieser Studie) zu dem folgenden Schluss kommt:

EUROPÄISCHE KOMMISSION – GD JLS
**VERSCHIEDENE ANSÄTZE ZUR BEWÄLTIGUNG NEUER HERAUSFORDERUNGEN FÜR DEN
SCHUTZ DER PRIVATSPHÄRE, INSBESONDERE AUFGRUND TECHNOLOGISCHER
ENTWICKLUNGEN**

Schlussbericht

Es bestehen ernste Probleme bei der Umsetzung der ersten Hauptregelung der Richtlinie: „Jeder Mitgliedstaat wendet die Vorschriften, die er zur Umsetzung dieser Richtlinie erläßt, auf alle Verarbeitungen personenbezogener Daten an, die im Rahmen der Tätigkeiten einer Niederlassung ausgeführt werden, die der für die Verarbeitung Verantwortliche im Hoheitsgebiet dieses Mitgliedstaats besitzt.“ Diese Regelung wird nicht vollständig oder richtig – und insbesondere nicht konsequent in allen Mitgliedsstaaten umgesetzt, wodurch sich genau jene Rechtskonflikte ergeben, die Artikel 4 der Richtlinie zu vermeiden versucht. Dies ergibt sich zum Teil aus der unzulänglichen Umsetzung von Artikel 4 der Richtlinie, aber zum Teil auch aus der übermäßigen Komplexität der Regelung selbst. (Übersetzung V.G./S.H.)

38. Es bedarf auch noch weiterer Untersuchungen zu der Anwendung dieser Regelungen auf öffentliche und, insbesondere, halböffentliche Behörden, welche in den Mitgliedsstaaten zunehmend an der Verarbeitung personenbezogener Daten, etwa in so sensiblen Bereichen wie Gesundheit und Strafgerichtsbarkeit, beteiligt sind.
39. Die Regelungen der Richtlinie im Bereich des anzuwendenden Rechts sind auch wirklich unmöglich auf Nicht-EU-/EWR-Unternehmen und -Organisationen anzuwenden, welche in Europa tätig sind – insbesondere wenn diese im Internet tätig sind (was bei fast allen der Fall ist und mit Sicherheit bei allen der Fall sein wird). Dem Anschein nach verpflichten die Regelungen all diese Unternehmen und Organisationen, alle Datenschutzgesetze aller 27 Mitgliedsstaaten gleichzeitig einzuhalten. Dies ist unmöglich, angesichts der immer noch erheblichen Unterschiede zwischen den Gesetzen und der Schwierigkeit, all ihre Anforderungen an Unternehmen und Organisationen mit einer Niederlassung außerhalb der EU/des EWR im Bereich der Verarbeitung im Internet überhaupt zu kennen.
40. Auch die Regelungen zum „anzuwendenden Recht“ in Bezug auf Nicht-EU/EWR-Länder mit „angemessenem“ Datenschutz sind unklar.¹⁰ Insbesondere legt die Richtlinie nicht fest, ob diese, für die Zwecke des „anzuwendenden Rechts“, wie EU/EWR-Länder oder wie Nicht-EU/EWR-Länder zu behandeln sind.
41. In den untersuchten Ländern außerhalb der EU (alle „unangemessen“ nach den Maßstäben der EU) wird die Frage des „anzuwendenden Rechts“ als ein Teil der Frage des extraterritorialen Geltungsbereichs der nationalen Datenschutzgesetze gesehen. Diese Frage bleibt in manchen gerichtlichen Zuständigkeiten offen. In der australischen Gesetzgebung ist sie jedoch der Inhalt einer speziellen Bestimmung, wobei der Geltungsbereich dieser Bestimmung auch wieder Auslegungssache ist.

Verweis: Country Report on Australia, Abschnitt 2.5

42. All diese Probleme sind gravierend und behindern international tätige Unternehmen und Organisationen, indem sie ihnen die Einhaltung der Datenschutzregelungen und -grundsätze erschweren. In dem neuen, im Allgemeinen internationalisierten, sozio-technischen Umfeld, und insbesondere (aber nicht ausschließlich) in Zusammenhang mit dem Internet, werden diese Probleme erheblich verstärkt.

Verweis: Working Paper No. 2, Abschnitt 3.

¹⁰ Die Frage nach der Bescheinigung eines „angemessenen“ Datenschutzniveaus an sich wird unter Unterabschnitt V-8, unten, behandelt.

EUROPÄISCHE KOMMISSION – GD JLS
**VERSCHIEDENE ANSÄTZE ZUR BEWÄLTIGUNG NEUER HERAUSFORDERUNGEN FÜR DEN
SCHUTZ DER PRIVATSPHÄRE, INSBESONDERE AUFGRUND TECHNOLOGISCHER
ENTWICKLUNGEN**

Schlussbericht

43. Ein weiteres Kernproblem stellt, angesichts der nationalen verfassungsrechtlichen Anforderungen einiger Mitgliedsstaaten (wie unter Absatz 24, oben, beschrieben), der Zusammenhang zwischen den Regelungen zum „anzuwendenden Recht“ und der Harmonisierung dar. Nach den Regelungen zum „anzuwendenden Recht“ werden die Verarbeitung in einem Mitgliedsstaat und die Verarbeitung in Bezug auf die Personen in diesem Mitgliedsstaat mit Sicherheit manchmal – bzw. im neuen sozio-technischen globalen Umfeld häufig – dem Datenschutzgesetz eines anderen Mitgliedsstaates unterliegen. Sollte jedoch das anzuwendende „ausländische“ Gesetz die verfassungsrechtlichen Anforderungen des Staates, in dem sich die Personen befinden, nicht erfüllen, so würde dies weitere *Solange*-Probleme nach sich ziehen: Aller Wahrscheinlichkeit nach würde das Verfassungsgericht des betroffenen Staates die Anwendung des ausländischen Gesetzes verweigern, soweit dieses die Anforderungen des Staates nicht erfüllt, selbst wenn dies tatsächlich bedeutet, dass die Anwendung der europäischen Regelungen zum „anzuwendenden Recht“ verweigert wird. In einer so sensiblen verfassungsrechtlichen Angelegenheit wie der Verarbeitung von personenbezogenen Daten können, mit anderen Worten, Regelungen zum „anzuwendenden Recht“, die die Gesetze eines Staates umgehen, dessen Bürger/-innen von der Verarbeitung betroffen sind, nur akzeptiert werden, wenn sie mit Regelungen gekoppelt werden, welche sicherstellen, dass alle nationalen Regelungen in allen Mitgliedsstaaten die einzelstaatlichen verfassungsrechtlichen Höchstanforderungen jedes Mitgliedsstaates erfüllen.
44. **Empfehlung:** Bessere, klarere und eindeutige Regelungen zum anzuwendenden Recht sind dringend erforderlich. Wir würden vorläufig Regelungen der folgenden Art vorschlagen:
- In EU/EWR, sollten die Regelungen unserer Ansicht nach einfach, wie ursprünglich geplant, auf dem „Herkunftsland“-Grundsatz beruhen. Dies löst vielleicht nicht alle Probleme: Uns ist bewusst, dass Angelegenheiten wie etwa die „Niederlassung“ auch im weiteren europäischen Rahmen schwierig sind. Es würde jedoch zumindest die Probleme verringern und sie in verschiedenen Zusammenhängen des Gemeinschaftsrechts aufeinander abstimmen. Eine unabdingbare Grundvoraussetzung dafür ist jedoch, wie bereits in Absatz 42, oben, erklärt, die stärkere Harmonisierung, oder zumindest ein hoher Grad an Annäherung, der Gesetze der Mitgliedsstaaten. Diese Harmonisierung fehlt derzeit immer noch in vielen entscheidenden Bereichen: siehe Unterabschnitt V4, unten, A. Die grundlegenden Werkzeuge, um stärkere Harmonisierung zu erreichen (oder zumindest zu fördern) sind zwar vorhanden (insbesondere in Form der Artikel 29 Datenschutzgruppe), sie werden jedoch derzeit nicht effektiv genutzt und müssen gestärkt werden (siehe Unterabschnitt V4, unten, B).
- Nicht-EU/EWR-Unternehmen etc. mit einer Vertretung (d.h. mit einer „Niederlassung“) in EU/EWR sollten die Möglichkeit haben, nur das Gesetz des EU-/EWR-Landes, in dem sie ihre Hauptniederlassung (ihre europäische Zentrale) besitzen, zu erfüllen und sollten ansonsten wie EU-/EWR-Unternehmen behandelt werden (unter der Voraussetzung, dass sie auch die EU-/EWR-Regelungen zu Datentransfers an Drittstaaten ohne angemessenen Schutz erfüllen und damit personenbezogene Daten, die sie an ihre [weltweite] Zentrale im Drittstaat versenden, gemäß dem EU-/EWR-Datenschutzgesetz behandeln.).

EUROPÄISCHE KOMMISSION – GD JLS
**VERSCHIEDENE ANSÄTZE ZUR BEWÄLTIGUNG NEUER HERAUSFORDERUNGEN FÜR DEN
SCHUTZ DER PRIVATSPHÄRE, INSBESONDERE AUFGRUND TECHNOLOGISCHER
ENTWICKLUNGEN**

Schlussbericht

Anmerkung: Dies entspricht dem allgemeinen Gemeinschaftsrecht, laut dem Nicht-EU-Unternehmen mit einer Niederlassung in der EU wie EU-Unternehmen behandelt werden.

–Die Regelungen zum „anzuwendenden Recht“ in Bezug auf Nicht-EU/EWR-Unternehmen etc. ohne eine Vertretung in EU/EWR, die jedoch „Mittel“ in EU/EWR verwenden (für gewöhnlich Nicht-EU/EWR-Unternehmen, die EU/EWR-Bürgern/-innen und -Unternehmen Produkte oder Dienste über das Internet anbieten, ohne eine Niederlassung in EU/EWR zu besitzen) sollten vereinfacht werden, damit auch sie sich an das Gesetz in nur einem relevanten EU-/EWR-Land halten können. Man könnte auch in Erwägung ziehen, diese Rechtswahl innerhalb der verbindlichen unternehmensinternen Vorschriften (BCRs) zu ermöglichen. Die Angemessenheit der Rechtswahl wäre eine der zu prüfenden Angelegenheiten bei der Bewertung der Angemessenheit und Eignung der BCRs.

–Siehe erste Anmerkung, unten. Nicht-EU/EWR-Unternehmen etc., die in ihrem Land einem „angemessenen“ Gesetz unterliegen (wie dies die Kommission beschlossen hat) sollten gleich wie EU-/EWR-Unternehmen behandelt werden; d.h. sie sollten nur die eigenen („angemessenen“) Gesetze erfüllen müssen – unter der Voraussetzung, dass die betroffenen Staaten auch die in EU/EWR getroffenen Maßnahmen zur Sicherstellung der andauernden harmonisierten/angenäherten Anwendung des Gesetzes erfüllen (was wiederum unter Unterabschnitt V.4, unten, genauer ausgeführt wird).

Anmerkungen:

–Der letztere Vorschlag erfordert möglicherweise die Gewährung eines Mitspracherechts an die betroffenen Nicht-EU/EWR-Länder, z.B., in Form von Voll- oder Teilmemberschaft oder Beobachterstatus bei der AG 29, und regelmäßige Prüfungen der andauernden „Angemessenheit“.

– Auch die Möglichkeit, dass sich Nicht-EU/EWR-Länder dem ER-Übereinkommen Nr. 108 und seinem Fakultativprotokoll anschließen, muss berücksichtigt werden. Dies wäre besonders interessant, wenn ein Ergebnis veröffentlicht werden könnte, laut dem der Schutz in Staaten, die sich dem Übereinkommen und Protokoll anschließen, *ipso facto* für „angemessen“ erachtet wird. Diesbezüglich sind jedoch noch einige Probleme zu lösen.

–Im letzten vorläufigen Vorschlag wird auch davon ausgegangen, dass die „angemessenen“ Gesetze extraterritorial für die relevanten Nicht-EU/EWR-Unternehmen gelten, insbesondere was ihre Tätigkeit in EU/EWR betrifft. Das muss nicht unbedingt der Fall sein, wenn das Beispiel von Australien (extraterritoriale Wirkung auf die Daten über australische Bürger/-innen beschränkt) häufig vorkommt. Das Beispiel von Japan hingegen (extraterritoriale Wirkung gilt für jedes Unternehmen mit einer Vertretung in Japan) erfüllt dieses Kriterium. Natürlich dient dies nur zur Betonung der komplexen Schwierigkeiten in diesem Bereich. Dies ist mit Sicherheit ein Problem, das die Kommission (und die AG 29) bei zukünftigen Überlegungen zu den Gesetzen in Nicht-EU/EWR-Ländern berücksichtigen müssen.

Verweise:

Wir sind uns der Komplexität dieser Probleme durchaus bewusst und das Obengenannte stellt nur Vorschläge zur Diskussion dar. Wir halten dies jedoch für eines der wichtigsten Probleme: Die derzeitigen Regelungen zum „anzuwendenden Recht“ sind unmöglich komplett zu verstehen oder einzuhalten. In einem zunehmend globalisierten Umfeld mit „Cloud Computing“ sind diesbezüglich Klärung und Vereinfachung dringend notwendig.

4. HARMONISIERUNG DES MATERIELLEN RECHTS

45. In diesem Unterabschnitt werden unter A (Abs. 47 – 78) zuerst kurz unsere Ergebnisse und Schlussfolgerungen zu einigen wesentlichen Punkten, in denen es sogar in EU/EWR noch an Harmonisierung fehlt, dargelegt. Dann wird unter B (Abs. 79 – 88) kurz erläutert, dass sich diese Punkte in Nicht-EU/EWR-Ländern nicht viel klarer gestalten. Erst dann werden wir unter C (Abs. 89 – 96) unsere Empfehlungen abgeben, wie eine solche Harmonisierung in all diesen Belangen (und anderen) erreicht werden könnte. Es sollte betont werden, dass das Ziel dieser kurzen Zusammenfassungen nicht Vollständigkeit ist, sondern es soll gezeigt werden, dass es immer noch große Unterschiede sowohl innerhalb von EU/EWR als auch zwischen EU/EWR-Ländern und anderen Ländern gibt, mit denen man sich beschäftigen muss, wenn der Datenschutz im neuen globalen technischen Umfeld ausreichend gewährleistet werden soll.

Anmerkung: Dieser Unterabschnitt muss notgedrungen kurz sein und kann daher der Komplexität dieser Fragen nicht gerecht werden. Daher wird auf die ausführlichere Besprechung in Abschnitt 4 des Working paper No. 2 verwiesen. Für noch weitere Details siehe die Vergleichende Zusammenfassung der nationalen Gesetze, die 2002 von Douwe Korff für die Kommission geschrieben und von dieser 2003 veröffentlicht wurde.¹¹ Siehe auch das diesem Bericht beigelegte Comparative Chart.

46. Bevor wir auf die spezifischen Fragen eingehen, sollte angemerkt werden, dass man argumentieren könnte, dass bis zu einem gewissen Grad direkte Regelungen in Bezug auf das „anzuwendende Recht“ das Problem der vielen großen Unterschiede auch lösen könnten: Dies würde es den Ländern erlauben, bis zu einem gewissen Grad ihren eigenen Weg zu gehen. Dies würde jedoch, wie in Abschnitt IV unter Abs. 24 und oben unter Abs. 43 angemerkt, zumindest in EU/EWR schnell zu Konflikten zwischen nationalem Verfassungsrecht und EU-Recht führen und es würden überdies dadurch die *Solange*-Probleme wieder auftreten. Stark abweichende Nicht-EU-Gesetze könnten auch als nicht „angemessen“ angesehen werden und mithin von der EU oder von den Mitgliedsstaaten nicht akzeptiert werden. Daher glauben wir, dass es einer „Angleichung“ der nationalen Rechtsvorschriften bedarf und zwar auf einem Niveau, das mindestens die Anforderungen der strengsten Verfassungen (u. a., aber nicht nur

¹¹ Douwe Korff, Studie zur Durchführung der Datenschutzrichtlinie 95/46/EC – Vergleichende Zusammenfassung der nationalen Gesetze, 2003, einsehbar auf http://ec.europa.eu/justice_home/fsj/privacy/studies/index_de.htm (nur auf Englisch). Diese Studie von 2003 ist teilweise inzwischen überholt. Wo dies relevant war, haben wir sie im Working Paper No. 2 unter Einbeziehung der Informationen der Experten der aktuellen Studie aktualisiert. In besagtem Working Paper behandeln wir auch ein spezielles Problem, das für viele Aspekte des Datenschutzes relevant ist und von zentraler Bedeutung für das neue Umfeld ist, aber hier nicht weiter ausgeführt wird: die Erstellung von Profilen.

EUROPÄISCHE KOMMISSION – GD JLS
**VERSCHIEDENE ANSÄTZE ZUR BEWÄLTIGUNG NEUER HERAUSFORDERUNGEN FÜR DEN
SCHUTZ DER PRIVATSPHÄRE, INSBESONDERE AUFGRUND TECHNOLOGISCHER
ENTWICKLUNGEN**

Schlussbericht

Deutschland) und der EMRK klar erfüllt. Wir sind überzeugt, dass, sollte dies versäumt werden, es zu großen Problemen in Bezug auf nationale und europäische Menschenrechtsvorschriften und in Bezug auf die Gültigkeit und den Vorrang des EG/EU-Rechts kommen wird. Die Harmonisierung wenigstens innerhalb von EU/EWR ist eine wesentliche Voraussetzung für die Bewältigung der neuen Herausforderungen. Unsere Schlussfolgerungen hinsichtlich unangemessener Harmonisierung sind daher ernstzunehmend: Dies ist eine der größten Herausforderungen, die in jeder Überarbeitung der Datenschutzregelung der EU/ des EWR behandelt werden sollte.

A. (NICHT-)HARMONISIERUNG INNERHALB VON EU/EWR

(i) Kernkonzepte und Definitionen (Artikel 2 der Richtlinie)

47. **Ergebnis/Schlussfolgerungen:** Die Definitionen vieler Kernkonzepte in der Richtlinie lassen noch viele wesentliche Fragen offen.¹² So gibt es z. B. bei den Konzepten „personenbezogene Daten“ und „betroffene Person“ Unklarheiten hinsichtlich Anonymisierung und Pseudonymisierung, Re-Identifizierbarkeit, Daten über „Dinge“ in Zusammenhang mit Personen (etwa IP-Adressen und Verkehrs- und Standortdaten) und hinsichtlich der „Erstellung von Profilen“. Die nationalen Rechtsvorschriften und Gepflogenheiten geben immer noch sehr unterschiedliche Antworten auf diese Fragen. Obwohl die AG 29 in ihrer *Stellungnahme zum Begriff „personenbezogene Daten“*¹³ bezüglich dieser Probleme einige nützliche Orientierungshilfen gegeben hat, fürchten wir dennoch, dass diese Fragen sowohl auf EU- als auch auf nationaler Ebene unangemessen behandelt werden und dabei die ernstesten Probleme mit der Re-Identifizierung, die schon seit einigen Jahren bekannt sind (zumindest den Computerexperten) nicht berücksichtigt werden.¹⁴ Die ernsthaften Probleme, die davon herrühren, dass es fast unmöglich ist, personenbezogene Daten im neuen sozio-technischen globalen Umfeld völlig zu anonymisieren, stellen einige der wesentlichsten Herausforderungen an den Datenschutz dar und sollten einen zentralen Platz in jeder Debatte über eine Überarbeitung der europäischen Datenschutzregelung einnehmen.
48. In der Basisrichtlinie sind zusätzlich in mancher Hinsicht selbst die Definitionen von „für die Verarbeitung Verantwortlicher“ und „Auftragsverarbeiter“ (und somit auch von „Dritter“ und „Empfänger“) verwirrend und in der Praxis ist es – besonders in komplexen internationalen Organisationen, wie beispielweise multinationalen Unternehmen oder Unternehmensgruppen – oft schwierig festzustellen, wer ein für die Verarbeitung Verantwortlicher ist und wer ein Auftragsverarbeiter (oder ein Empfänger der ein Dritter oder kein Dritter ist). Außerdem divergieren hier auch die

¹² Abgesehen von den im Text erwähnten Konzepten sollte angemerkt werden, dass ebenfalls unklar ist, welche Arten von „unstrukturierten“ manuellen Akten in das Konzept der „Dateien mit personenbezogenen Daten“ fallen, und welche nicht. Allerdings ist dies, außer in sehr speziellen Fällen, im digitalen Zeitalter weniger wichtig. Die Frage, was eine (gültige) Einwilligung ausmacht wird weiter unten in Abschnitt iii erörtert.

¹³ *Stellungnahme 4/2007 zum Begriff „personenbezogene Daten“*, 20. Juni 2007 (WP136), wird ausführlicher im *Working Paper No. 2*, Abschnitt 4.1 behandelt.

¹⁴ Siehe besonders den (für Nicht-Computerexperten) bahnbrechenden Text von Paul Ohm, *Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization*, Colorado Law, Legal Studies Research Paper Series, Working Paper Number 09-12, 13. August 2009, in Internet einsehbar auf: <http://ssrn.com/abstract=1450006>. Auf diesem Text basierende Kommentare wurden an das *Working Paper No. 2* angefügt.

EUROPÄISCHE KOMMISSION – GD JLS
**VERSCHIEDENE ANSÄTZE ZUR BEWÄLTIGUNG NEUER HERAUSFORDERUNGEN FÜR DEN
SCHUTZ DER PRIVATSPHÄRE, INSBESONDERE AUFGRUND TECHNOLOGISCHER
ENTWICKLUNGEN**

Schlussbericht

Rechtsvorschriften in den Mitgliedstaaten. Auch dieses Problem wird im neuen, komplexen, global-technischen Umfeld viel wichtiger werden; es hat bedeutende Auswirkungen besonders in Hinblick auf das „anzuwendende Recht“ – und dennoch gibt es auf diesem Gebiet viel weniger klare Orientierungshilfen und es herrscht weiterhin Verwirrung.¹⁵

Verweis: Working Paper No. 2, Abschnitt 4.1.

(ii) Die Datenschutzgrundsätze (Artikel 6 der Richtlinie)

49. **Ergebnis/Schlussfolgerungen:** Die Datenschutzgrundsätze sind in den Rechtsvorschriften aller Mitgliedstaaten festgehalten, und zwar bis auf wenige Ausnahmen unter Verwendung von identischen oder sehr ähnlichen Begriffen wie in der Richtlinie. Allerdings werden in manchen Rechtsvorschriften etwas uneinheitliche Begriffe verwendet; in den Rechtsvorschriften eines Staates werden die Datenschutzkriterien (siehe weiter unten, unter iii) mitten in den Grundsätzen erörtert; in anderen werden noch weitere Grundsätze hinzugefügt. Darüber hinaus ergänzen manche Länder die Grundsätze durch Erklärungen oder Anmerkungen, wodurch sie manchmal gestärkt, manchmal aber auch geschwächt werden.
50. Der Grundsatz der Zweckangabe und -bindung wird in den Rechtsvorschriften der meisten Mitgliedstaaten unter Verwendung von identischen oder sehr ähnlichen Begriffen wie in der Richtlinie festgelegt. Allerdings, und trotz der ähnlichen Formulierungen, lässt gerade die Vagheit der Richtlinie Raum für unterschiedliche Anwendung. Demnach überprüfen die verschiedenen Mitgliedstaaten hier Unterschiedliches, angefangen bei den „angemessenen Erwartungen“ einer betroffenen Person, bis zur „Fairness“, oder sie führen verschiedene „Abwägungen“ durch. In manchen Ländern werden recht großzügige Ausnahmen von diesem Grundsatz gemacht, besonders was für die Verarbeitung Verantwortliche im öffentlichen Sektor betrifft. In anderen werden die Zweckbestimmungen manchmal in allzu groben Zügen definiert, wodurch der Grundsatz selbst untergraben wird. So spricht die britische Gesetzgebung allgemein von „polizeilichen Zwecken“ (und erlaubt damit, dass Daten, die für einen polizeilichen Zweck erhoben wurden, für jeden solchen Zweck verwendet werden können), wo die deutsche Gesetzgebung streng zwischen der „Abwehr dringender Gefahr“, „allgemeiner und besonderer Vorbeugung“ und „Untersuchung und Verfolgung von [mutmaßlichen] Straftaten“ unterscheidet.¹⁶ Noch deutlicher verstößt das britische Datenschutzgesetz (Data Protection Act) gegen die Richtlinie, wenn es „medizinische Forschung“ zur Liste der medizinischen Zwecke, die unter Artikel 8(3) der Richtlinie aufgeführt werden, hinzufügt. Denn dadurch wird die Zweckbindung in dieser Hinsicht umgangen (entgegen den klaren Orientierungshilfen der AG 29 in diesem Punkt).¹⁷

¹⁵ Dass es in bestimmten komplexen Fällen schwierig ist, zu ermitteln, wer ein für die Verarbeitung Verantwortlicher ist und wer ein Auftragsverarbeiter, wurde kürzlich auf der Konferenz der Datenschutzbehörden im Jänner 2009 in Barcelona festgestellt. Dort wurde vorgeschlagen, dass akzeptiert werden könnte, dass die jeweiligen Rollen und Verantwortungsbereiche gemischt sind bzw. geteilt werden. Allerdings wurden hier die Auswirkungen eines solchen Ansatzes auf die Frage des „anzuwendenden Rechts“ nicht berücksichtigt.

¹⁶ Siehe Douwe Korff, The feasibility of a seamless system of data protection rules for the European Union, Studie für die Europäische Kommission (1996 – 97, veröffentlicht 1999).

¹⁷ Siehe das „Arbeitspapier Verarbeitung von Patientendaten in elektronischen Patientenakten (EPA)“ der AG 29, WP131 vom 15. Februar 2007. Anmerkung: Die Auswirkungen von unzureichend definierten Zwecken

51. Die Vorschriften für die sekundäre Verarbeitung von nicht-sensiblen personenbezogenen Daten zu Forschungszwecken ohne die Einwilligung der betroffenen Person sind auch sonst sehr unterschiedlich. Einige Mitgliedstaaten bieten überhaupt keine Garantien (und verstoßen so deutlich gegen die Richtlinie); andere sehen minimale (d. h. unzureichende) Garantien vor (z. B. dass Daten nicht für Entscheidungen über betroffene Personen, oder nur zum Zweck der jeweiligen Forschung verwendet werden dürfen); und wieder andere sehen relativ abstrakte „Abwägungsvorgänge“ vor oder halten nur fest, dass die Forschung auf einem „angemessenen Forschungsplan“ basieren muss. Andererseits legt die Gesetzgebung in manchen Ländern detaillierte Bestimmungen fest, die die Daten und die Verarbeitung beschränken und vorschreiben, dass Forschungen von einer akademischen „Ethikkommission“ bewilligt werden müssen, oder die verlangen, dass die Forscher bei der Datenschutzbehörde eine Sondergenehmigung beantragen, die verschiedene Bedingungen vorschreiben muss (diese zusätzlichen Bedingungen stehen manchmal auch bereits im Gesetz selbst).

Verweis: Working Paper No. 2, Abschnitt 4.2.

(iii) Die Datenschutzkriterien (Artikel 7 der Richtlinie)

*Verarbeitung auf der Basis einer gesetzlichen Genehmigung*¹⁸

52. **Ergebnis/Schlussfolgerungen:** In vielen nationalen Rechtsvorschriften werden die Kriterien bezüglich der rechtlichen Verpflichtungen, Aufgaben und Befugnisse unter Verwendung von identischen oder sehr ähnlichen Begriffen wie in der Richtlinie wiederholt. Es müssen zwei allgemeine, grundsätzliche Punkte vorgebracht werden. Erstens beziehen sich diese Kriterien meist auf die Verarbeitung auf der Basis einer Art von gesetzlicher Genehmigung:¹⁹ In Bezug auf die EMRK beziehen sie sich auf die Verarbeitung personenbezogener Daten (die, im Sinne der Konvention, *ipso facto* eine „Einmischung“ in das Privatleben bedeutet) die vom „Gesetz“ vorgesehen ist. Zweitens beinhalten die Kriterien den anderen Schlüsselbegriff, der in Artikel 8 EMRK verwendet wird, und zwar „notwendig“. Dies bedeutet, dass die Rechtsvorschriften, auf denen die Verarbeitung basiert, den Anforderungen von „Gesetz“ und „Notwendigkeit“ (einschließlich Spezifität (specificity) und Verhältnismäßigkeit (proportionality)) gerecht werden müssen, die der Europäische Gerichtshof für Menschenrechte in seiner Rechtsprechung ausführlich dargelegt hat.²⁰ In den vergangenen Jahren entschied der

in rechtlichen Bestimmungen, und von dem Streben nach „Einwilligung“ für die Verarbeitung von ungenügend definierten Zwecken werden unter iv erörtert. Die weit reichenden Konsequenzen der Notwendigkeit, die Zwecke eng zu definieren, betonen selbst die Wichtigkeit von weiteren Orientierungshilfen und weiterer Harmonisierung in dieser Hinsicht.

¹⁸ Diese hier verwendete Formulierung bezieht sich auf die zwei Kriterien in den Abs. (c) und (e) des Artikels 7 der Richtlinie, d. h.: „die Verarbeitung [die] für die Erfüllung einer rechtlichen Verpflichtung erforderlich [ist], der der für die Verarbeitung Verantwortliche unterliegt“ und „die Verarbeitung [die] erforderlich [ist] für die Wahrnehmung einer Aufgabe, die im öffentlichen Interesse liegt oder in Ausübung öffentlicher Gewalt erfolgt und dem für die Verarbeitung Verantwortlichen oder dem Dritten, dem die Daten übermittelt werden, übertragen wurde“. Wir sollten besonders anmerken, dass sich die „rechtlichen Verpflichtungen“, auf die in Artikel 7(c) Bezug genommen wird, nicht aus einem Vertrag oder einer vorvertraglichen Situation ergeben, denn diese werden in Artikel 7(b) behandelt; und dass die „Aufgaben“ und „Gewalt“, auf die in Artikel 7(e) Bezug genommen wird, gesetzlich gewährte Aufgaben und Befugnisse sind.

¹⁹ Siehe vorhergehende Fußnote.

²⁰ Für weitere Details siehe Douwe Korff, *Paper No. 4: The Legal Framework*, in: Ian Brown & Douwe

EUROPÄISCHE KOMMISSION – GD JLS
**VERSCHIEDENE ANSÄTZE ZUR BEWÄLTIGUNG NEUER HERAUSFORDERUNGEN FÜR DEN
SCHUTZ DER PRIVATSPHÄRE, INSBESONDERE AUFGRUND TECHNOLOGISCHER
ENTWICKLUNGEN**

Schlussbericht

Europäische Gerichtshof für Menschenrechte wiederholt, dass nationale Rechtsvorschriften zur Verarbeitung personenbezogener Daten diese Qualitätsanforderungen nicht erfüllen. Durch diese Fälle wurden auch Zweifel daran geweckt, ob der Zweck (oder die Zwecke), für welche personenbezogene Daten verarbeitet wurden, präzise genug definiert worden war(en).²¹

53. Es ist klar, dass in einigen Mitgliedstaaten die Bestimmungen, auf die sich die Erlaubnis zur Verarbeitung (und zum Austausch und „Data Mining“) von personenbezogenen Daten stützen, vor allem im öffentlichen und halböffentlichen Sektor, diesen Standards nicht entsprechen. Dies wird einerseits rein innerstaatliche Probleme verursachen, andererseits (und dies ist relevanter für diese Studie) aber auch Probleme in Bezug auf andere Staaten und die EG/EU, wenn solche mangelhaften Rechtsvorschriften aufgrund der Bestimmungen zum „anzuwendenden Recht“ auch außerhalb einzelner Staaten angewendet werden. Dies wird sicherlich viel häufiger vorkommen, denn im neuen internationalisierten Umfeld wird die Datenverarbeitung vermehrt Rechtsvorschriften von Staaten unterliegen, in denen die betroffene Person nicht ihren Wohnsitz hat (bzw. von Staaten, wo die Person sich zum Zeitpunkt der Datenerhebung gerade aufhält).

Verweis: Working Paper No. 2, Abschnitt 4.3 (unter dieser Überschrift).

Verarbeitung auf der Basis einer Einwilligung

54. **Ergebnis/Schlussfolgerungen:** Im Hinblick auf die „informationelle Selbstbestimmung“ ist die Verarbeitung auf der Basis einer Einwilligung eindeutig von zentraler Bedeutung, aber mit dem Vorbehalt, dass (laut Artikel 7(a) der Richtlinie) eine derartige Einwilligung „ohne Zwang, für den konkreten Fall und in Kenntnis der Sachlage“ erfolgen muss. Aber obwohl dieser Aspekt so zentral ist, wird er nicht von allen Mitgliedstaaten einheitlich gehandhabt. So wird in manchen Rechtsvorschriften

Korff, Privacy & Law Enforcement, Studie für den Datenschutzbeauftragten, 2004, von der britischen ICO-Internetseite:

http://www.ico.gov.uk/upload/documents/library/corporate/research_and_reports/legal_framework.pdf. Für eine Übersicht über die Anforderungen der EMRK bezüglich „Gesetz“ („law“), „legitimate Interessen“ (Zweck) („legitimate aim“ (purpose)), „Notwendigkeit“ („necessity“), usw., siehe S. 9 – 15. Der Text fasst detailliert folgende Rechtssachen des EGMR zusammen: Amann gegen die Schweiz (Urteil vom 16. Februar 2000) und Rotaru gegen Rumänien (Urteil vom 4. Mai 2000). Weniger detailliert werden folgende, weiter zurückliegende, Rechtssachen behandelt: Leander gegen Sweden (26. März 1987), Gaskin gegen das Vereinigte Königreich (Urteil vom 7. Juli 1989), Peck gegen das Vereinigte Königreich (28. Januar 2003), und weitere (S. 16 – 33); sowie folgende Rechtssachen des EuGH: Österreichischer Rundfunk gegen Österreich (verbundene Rechtssachen C-465/00 (Rechnungshof gegen ÖRF et al.), C-138/01 und C-139/01 (Christa Neukomm und Lauermann gegen ÖRF)) (Verweise auf Vorabentscheidungen des Österreichischen Verfassungsgerichtshofs und des Obersten Gerichtshofs), Schlussantrag des Generalanwalts Tizzano vom 14. November 2002; Urteil vom 20. Mai 2003) und Lindqvist gegen Sweden (Rechtssache C-101/01 Bodil Lindqvist gegen Åklagarkammaren i Jönköping) (Verweis auf eine Vorabentscheidung des Göta Hovrätt), Schlussantrag des Generalanwalts Tizzano vom 19. September 2002; Urteil vom 6. November 2003) (S. 33 – 44). Für eine kürzere Übersicht siehe Douwe Korff, The need to apply UK data protection law in accordance with European law, Data Protection Law & Practice, Mai 2008. Auf einige neuere Rechtssachen des EGMR wird in der nächsten Fußnote verwiesen. Sie bestätigen die Vorgehensweise des Gerichtshofs in Straßburg in den oben erwähnten Rechtssachen und bestärken die Rechtsprechung sogar noch. Ein weiteres einflussreiches Urteil, das nach der ICO-Studie 2004 gefällt wurde, ist I. gegen Finnland (Urteil vom 17. Juli 2008): Diese Rechtssache hat große Auswirkungen für die Verarbeitung von Gesundheitsdaten in elektronischen Patientenakten in Europa.

²¹ Siehe z. B. Copland gegen das Vereinigte Königreich, EGMR-Urteil vom 3. April 2007; S. & Marper gegen das Vereinigte Königreich, EGMR GC Urteil vom 4. Dezember 2008 (beide bestätigen die ältere Rechtsprechung).

EUROPÄISCHE KOMMISSION – GD JLS
**VERSCHIEDENE ANSÄTZE ZUR BEWÄLTIGUNG NEUER HERAUSFORDERUNGEN FÜR DEN
SCHUTZ DER PRIVATSPHÄRE, INSBESONDERE AUFGRUND TECHNOLOGISCHER
ENTWICKLUNGEN**

Schlussbericht

die Notwendigkeit, dass jede Einwilligung *offensichtlich* ohne Zwang, für den konkreten Fall und in Kenntnis der Sachlage etc. erfolgt, durch das Hinzufügen der Formulierung „ohne jeden Zweifel gegeben“ in der Definition von Einwilligung betont (Portugal, Spanien, Schweden); in den luxemburgischen Rechtsvorschriften sind sogar sowohl die Formulierung „ohne jeden Zweifel gegeben“ als auch der Terminus „ausdrücklich“ in der Definition inkludiert. Die italienischen und deutschen Rechtsvorschriften verlangen, dass die Einwilligung (grundsätzlich) schriftlich erfolgen muss (sehen aber auch vor, dass die Einwilligung im Internet per „Mausklick“ gegeben werden kann). Im Gegensatz dazu weisen die von der britischen Datenschutzbehörde herausgegebenen Orientierungshilfen zu den Rechtsvorschriften darauf hin, dass die Einwilligung zur Verarbeitung von nicht-sensiblen Daten oft implizit sein kann.

55. In Deutschland muss ein Antrag auf Einwilligung zur Verarbeitung der Daten zu einem anderen Zweck als dem primären speziell mit einem Formular etc. gestellt werden – aber in diesem Land (und auch in anderen) mangelt es an Klarheit darüber, ob die Einwilligung zu einer solchen sekundären Verarbeitung, die für den primären Zweck einer Vereinbarung nicht notwendig ist, zur Bedingung für das Treffen der primären Vereinbarung gemacht werden darf: Nach den bisherigen britischen Rechtsvorschriften war dies rechtmäßig, außer es lag eine Art von Missbrauch vor, die irische Datenschutzbehörde ist hier aber strenger.
56. Auch all diese Unterschiede werden im neuen, allgemein-internationalisierten Umfeld, einschließlich des Internets, immer problematischer werden. Die „Einwilligung“, die in einem Land rechtmäßig erfolgt – nach dem „anzuwendenden Recht“ zum Zeitpunkt der Datenerhebung – und nach diesem Recht gültig ist, kann als unzureichend oder ungültig eingestuft werden, wenn sie für weitere Verarbeitung in einem anderen Land (sogar in einem anderen Mitgliedstaat von EU/EWR) herangezogen wird, z. B. weil (nach Ansicht dieses zweiten Landes) die ursprüngliche Einwilligung unzureichend spezifisch war oder nach Meinung des zweiten Landes die betroffene Person dazu genötigt wurde etc.
57. Bei alledem wurden allgemeinere, grundlegende Fragen noch nicht einmal berücksichtigt – jene nach der Gültigkeit von Einwilligungen, die auf der Basis von Kleingedrucktem in Datenschutzerklärungen im Internet, die von niemandem (außer Datenschutzaktivisten und Rechtsanwälten) gelesen werden, erfolgen. Der Hinweis möge genügen, dass erstens sich auch hier die Art der Mitgliedstaaten, mit solchen „Einwilligungen“ umzugehen, unterscheiden kann und es bis jetzt noch keine klaren Orientierungshilfen der AG 29 gibt; und dass zweitens dieser Aspekt häufig allgemeinere Rechtsfragen berührt, wie beispielsweise den Verbraucherschutz, die Undurchsetzbarkeit bestimmter Standard-Geschäftsbedingungen, unlauteren Wettbewerb etc.

Verweis: Working Paper No. 2, Abschnitt 4.3 (unter dieser Überschrift). Siehe ebenda für Verweise auf das Einholen von Einwilligungen von Minderjährigen und für Orientierungshilfen der AG 29 in den Bereichen grenzüberschreitender Datenfluss, Arbeit, Schulen und Gesundheitsfürsorge etc.

Verarbeitung auf der Basis des „Abwägungskriteriums“

EUROPÄISCHE KOMMISSION – GD JLS
**VERSCHIEDENE ANSÄTZE ZUR BEWÄLTIGUNG NEUER HERAUSFORDERUNGEN FÜR DEN
SCHUTZ DER PRIVATSPHÄRE, INSBESONDERE AUFGRUND TECHNOLOGISCHER
ENTWICKLUNGEN**

Schlussbericht

58. **Ergebnis/Schlussfolgerungen:** Das „Abwägungskriterium“ (Artikel 7(f) der Richtlinie) ist schon seinem Wesen nach das vageste und offenste der Kriterien und bedarf daher vielleicht am dringendsten einer Erklärung, wie es in spezifischen Zusammenhängen angewendet werden kann und soll. Dies wird in den Rechtsvorschriften verschiedener Länder (Belgien, Irland, Vereinigtes Königreich) erkannt. Dort wird die Erlassung von weiteren Bestimmungen zur Anwendung des „Abwägungskriteriums“ in spezifischen Zusammenhängen ins Auge gefasst. Allerdings wurden aber bemerkenswerterweise von keinem dieser Länder tatsächlich solche präzisere Bestimmungen erlassen.
59. Gesamt gesehen bestehen auch nennenswerte Unterschiede in den Vorgehensweisen der Mitgliedstaaten in Bezug auf dieses Kriterium. Im Vereinigten Königreich bleibt es größtenteils den für die Verarbeitung Verantwortlichen überlassen zu entscheiden, ob sie nicht-sensible Daten auf der Basis dieses Kriteriums verarbeiten dürfen. In Deutschland gilt eine „Abwägung“ in der allgemeinen Formulierungsweise der Richtlinie nur für den Privatsektor. Ähnliche, aber mit präzisieren Worten beschriebene Abwägungsvorgänge gelten für den öffentlichen Sektor, obschon diese genau genommen dem Anwenden einer Prüfung der „Notwendigkeit“ näher kommen. Andere Länder wenden im Allgemeinen genauer definierte Vorgänge an oder legen fest, dass für die Verarbeitung auf der Basis dieses Kriteriums strenge prozessuale Anforderungen erfüllt werden müssen. Demnach verschieben die griechischen Rechtsvorschriften das Gleichgewicht stark in Richtung der betroffenen Person, indem sie die Verarbeitung nur erlauben, wenn „die Verarbeitung *absolut* notwendig ist für die Zwecke eines berechtigten Interesses, das von einem für die Verarbeitung Verantwortlichen oder von einem Dritten oder von Dritten, an die die Daten weitergegeben wurden, verfolgt wird und unter der Bedingung, dass solch ein berechtigtes Interesse *offensichtlich* über den Rechten und Interessen der [betroffenen Person] steht und deren Grundfreiheiten nicht beeinträchtigt werden.“ (Übersetzung: V.G./S.H.)
60. In Italien ist der „Abwägungsvorgang“ nur in von der Datenschutzbehörde präzisierten Fällen anzuwenden. Nach den finnischen Rechtsvorschriften müssen die für die Verarbeitung Verantwortlichen eine Genehmigung der Behörde einholen, wenn sie diesen Vorgang anwenden möchten (es sind aber auch vier spezielle Bestimmungen in den Rechtsvorschriften enthalten, die die Verarbeitung unter bestimmten Umständen, wie zum Beispiel bei einer Kundenbeziehung, erlauben; es handelt sich dabei sozusagen um spezifische Beispiele für die Anwendung dieses Vorgangs).
61. Auch diese Unterschiede können im neuen, allgemein-internationalisierten Umfeld Probleme verursachen, wenn Daten auf der Basis dieses Kriteriums in einem Mitgliedstaat erhoben werden und dann an einen Staat übermittelt werden, wo das Kriterium strenger ausgelegt wird. Des Weiteren kann es zu Problemen kommen, wenn ein für die Verarbeitung Verantwortlicher in einem Land, das das Kriterium weniger streng anwendet, versucht, Daten über betroffene Personen direkt (z. B. über das Internet oder telefonisch) auf dieser Basis zu erheben, und zwar nach den Vorschriften des Landes des für die Verarbeitung Verantwortlichen (die gewöhnlich das „anzuwendende Recht“ darstellen würden), die betroffenen Personen sich aber tatsächlich in einem anderen Mitgliedstaat, der in dieser Hinsicht strengere Rechtsvorschriften hat, befinden.

Verweis: Working Paper No. 2 (erweiterte Version), Abschnitt 4.3 (unter dieser Überschrift).

(iv) Verarbeitung sensibler Daten

62. **Eine Vorbemerkung:** Die Verarbeitung sensibler Daten wird im neuen, technisch-globalen Umfeld viel weiter verbreitet werden und sogar noch schwieriger zu kontrollieren sein: Bilder und Videoclips, die auf soziale Online-Netze hochgeladen werden, Kommentare zu „Blogs“ und in „Twitters“ „enthüllen“ sämtlich sehr häufig sensible Informationen, etwa über ethnische Zugehörigkeit, sexuelle Orientierung und religiöse Überzeugungen (oder sogar Strafsachen). Und diese werden nur allzu leicht an viele Personen weitergegeben, auch über nationale Grenzen hinweg. Wie bereits angemerkt gestaltet sich selbst die Bestimmung des „anzuwendenden Rechts“ für diese Art von Verarbeitung schwierig. Rechtskonflikte sind daher auf diesem Gebiet besonders problembehaftet.
63. **Ergebnis/Schlussfolgerungen:** Einige Mitgliedstaaten weiten die speziellen Bedingungen (genau genommen Ausnahmen von einem grundsätzlichen Verbot der Verarbeitung derartiger Daten in der Richtlinie und in den Rechtsvorschriften der Mitgliedstaaten) auf bestimmte, nicht in der Liste der Richtlinie beinhaltet, Arten von Daten aus. Dies betrifft insbesondere Daten über Schulden, Finanzkraft und Unterstützungszahlungen (Sozialhilfe). Manche Staaten schließen auch Daten über strafrechtliche Verurteilungen etc. in die allgemeine Liste der sensiblen Daten mit ein – was bedeutet, dass derartige Daten auf der Basis derselben Ausnahmen (Spezialkriterien) verarbeitet werden dürfen, wie die anderen sensiblen Daten (und insbesondere ebenfalls auf der Basis einer Einwilligung, was in Artikel 8(5) der Richtlinie nicht erwähnt wird).
64. Abgesehen davon möge es genügen, die Bestimmungen über die Verarbeitung sensibler Daten in einigen besonderen Bereichen darzulegen:
- Arbeit: Obwohl die Rechtsvorschriften einiger Mitgliedstaaten allgemeine Bestimmungen zur Verarbeitung sensibler Daten beinhalten, damit diese den Anforderungen des Arbeitsrecht gerecht wird, halten diese Gesetze im Sinne der Richtlinie kaum spezifische Details in dieser Hinsicht bereit. In manchen ist von der geplanten Verabschiedung spezieller Vorschriften (oder eines speziellen Gesetzes) die Rede, aber die meisten haben dies noch nicht in die Tat umgesetzt. Insgesamt wird die Situation diesbezüglich noch sehr stark bestimmt von separaten – und sehr unterschiedlichen – Bestimmungen in anderen Gesetzen als den die Richtlinie umsetzenden Datenschutzgesetzen. Die Datenschutzgesetze, oder spezifischere Bestimmungen, die auf der Grundlage der Datenschutzgesetze erlassen wurden, halten dabei (bis jetzt) kaum Orientierungshilfen in dieser Hinsicht bereit.²²
65. Die AG 29 hat eine allgemeine Stellungnahme bezüglich der Verarbeitung personenbezogener Daten in Arbeitgeber/Arbeitnehmer-Beziehungen veröffentlicht; des Weiteren eine Empfehlung hinsichtlich Daten in Beurteilungen von Arbeitnehmern; und ein Arbeitsdokument zur Überwachung der elektronischen Kommunikation von Beschäftigten; relevant ist außerdem die Stellungnahme der AG zu Filterdiensten für

²² Dies wird auch von einer kürzlich veröffentlichten Studie, die von der Agentur der Europäischen Union für Grundrechte in Auftrag gegeben wurde, bestätigt: siehe die Zusammenfassung des endgültigen Entwurfs der Comparative Legal Study on assessment of data protection measures and relevant institutions, von der Agentur der Europäischen Union für Grundrechte (FRA) in Auftrag gegebener Bericht (2009), Abs. 8.

EUROPÄISCHE KOMMISSION – GD JLS
**VERSCHIEDENE ANSÄTZE ZUR BEWÄLTIGUNG NEUER HERAUSFORDERUNGEN FÜR DEN
SCHUTZ DER PRIVATSPHÄRE, INSBESONDERE AUFGRUND TECHNOLOGISCHER
ENTWICKLUNGEN**

Schlussbericht

elektronische Post.²³ Diese Dokumente haben jedoch bis jetzt noch zu keiner größeren Annäherung geführt (geschweige denn einer Harmonisierung).

66. Wesentliches öffentliches Interesse: Einige der Datenschutzgesetze der Mitgliedstaaten sehen den Erlass von Dekreten und anderen ergänzenden Vorschriften hinsichtlich der Verarbeitung personenbezogener Daten für wichtige öffentliche Interessen vor – aber nur in einigen wenigen Mitgliedstaaten (nämlich im Vereinigten Königreich und in Frankreich) wurde dies auch getan und bei diesen Vorschriften sind die Normen, zumindest im Vereinigten Königreich, etwas missverständlich.
67. In ähnlicher Weise sehen einige Rechtsvorschriften die Erteilung von spezifischen *ad hoc* Genehmigungen durch die nationale Datenschutzbehörde vor – aber unseres Wissens wurden der Kommission noch keine mitgeteilt (wie es laut Artikel 8(6) der Richtlinie geschehen müsste). Ein Mitgliedstaat (Belgien) sieht die Erteilung von Genehmigungen für Menschenrechtsorganisationen vor. Diese dürfen dann sensible Daten ohne Einwilligung verarbeiten (siehe Art. 6 § 2(k) des belgischen Datenschutzgesetzes), allerdings ist dies an sich schon kontrovers und könnte gegen die Europäische Menschenrechtskonvention verstoßen; nach unserem besten Wissen wurden jedoch noch keine derartige Genehmigungen beantragt, zumindest nicht von den größeren internationalen Menschenrechtsorganisationen.
68. In diesem Zusammenhang sollte jedoch erwähnt werden, dass einige der Datenschutzgesetze der Mitgliedstaaten recht häufig auf andere innerstaatliche Gesetze – oder Rechtsvorschriften – verweisen und viele davon die Verarbeitung sensibler Daten sehr wohl erlauben. Es ist strittig, ob diese anderen Gesetze die „geeigneten Garantien“ enthalten, die laut Artikel 8(4) der Richtlinie in dieser Hinsicht geboten werden sollten. Solche andere Gesetze oder Bestimmungen sollten der Kommission mitgeteilt werden, dies scheint aber in keinem größeren Ausmaß stattgefunden zu haben. Dieser Bereich bleibt daher eher obskur, aber es ist klar, dass in vielen Ländern in vielerlei Hinsicht schwerwiegende Zweifel daran gehegt werden müssen, ob diese Bestimmungen in dieser Hinsicht die Richtlinie erfüllen. Außerdem ist klar, dass dadurch, dass diese Aspekte durch so viele verschiedene Gesetze (die meist überhaupt nicht dafür entworfen wurden, den Datenschutz zu regeln) geregelt sind, weiterhin große Unterschiede zwischen den Mitgliedstaaten bestehen.
69. Dies wiederum hätte schwerwiegende Auswirkungen zur Folge, wenn man sich auf solche Rechtsvorschriften in einer Situation berufen würde, wo die relevanten nationalen Rechtsvorschriften das „anzuwendende Recht“ in einem grenzüberschreitenden Kontext sind. Bis vor kurzem war dieser Aspekt wohl nicht so dringlich, da viele Fragen von „wesentlichem öffentlichen Interesse“ ausschließlich innerhalb des einzelstaatlichen Rechtsrahmens erledigt wurden und sich nur auf die Bürger und Einwohner des jeweiligen Einzelstaates bezogen. Jedoch bedeutet die stetig wachsende Zusammenarbeit innerhalb der EU, auch in den Bereichen Gesundheit, Sozialhilfe, Migration etc., dass es vermehrt zu grenzüberschreitenden (auf europäischer

²³ Dies sind: Stellungnahme 8/2001 bezüglich der Verarbeitung personenbezogener Daten in Arbeitgeber/Arbeitnehmer-Beziehungen (WP48 vom 13. September 2001); Empfehlung 1/2001 hinsichtlich Daten in Beurteilungen von Arbeitnehmern (WP42 vom 22. März 2001); Arbeitsdokument zur Überwachung der elektronischen Kommunikation von Beschäftigten (WP55 vom 29. Mai 2002); und Stellungnahme 2/2006 der Artikel 29-Datenschutzgruppe zu Datenschutzfragen bei Filterdiensten für elektronische Post (WP118 vom 21. Februar 2006).

EUROPÄISCHE KOMMISSION – GD JLS
**VERSCHIEDENE ANSÄTZE ZUR BEWÄLTIGUNG NEUER HERAUSFORDERUNGEN FÜR DEN
SCHUTZ DER PRIVATSPHÄRE, INSBESONDERE AUFGRUND TECHNOLOGISCHER
ENTWICKLUNGEN**

Schlussbericht

Ebene) Vereinbarungen kommen wird, und auch zu den entsprechenden Datenflüssen, die unter das Datenschutzrecht fallen.

70. Orientierungshilfen, insbesondere bezüglich was in diesem Zusammenhang „geeignete Garantien“ wären, sind daher dringend notwendig um eine (zunehmende) Angleichung der Datenschutzgarantien in diesen Bereichen zu begünstigen.
71. Strafrechtliche Verurteilungen: Die Rechtsvorschriften der Mitgliedstaaten unterscheiden sich erheblich in ihrer Herangehensweise an die Verarbeitung von Daten über strafrechtliche Verurteilungen etc. Einige inkludieren derartige Daten in die allgemeinen Kategorie der „sensiblen Daten“ (was Konsequenzen haben kann, insbesondere was die Zulässigkeit dieser Art von Verarbeitung mit der Einwilligung der betroffenen Person angeht), während andere speziellere Vorschriften zu strafrechtlichen Verurteilungen auf Daten über andere Rechtsstreitigkeiten oder Daten über „ernste soziale Probleme“ und „reine Privatsachen“ ausweiten. In den Gesetzen werden auch recht unterschiedliche Standards auf die Verarbeitung derartiger Daten angewendet. In einigen wird jegliche Verarbeitung derartiger Daten erlaubt, sofern sie „genehmigt ist von irgendeiner oder durch irgendeine Gesetzesbestimmung“ oder sofern sie irgendeinen „vom Gesetz vorgesehen Zweck“ verfolgt; oder sie wird erlaubt auf der Basis von vagen und subjektiven „Abwägungsvorgängen“; andere dagegen schreiben strenge Prüfungen der „Notwendigkeit“ vor und/oder verlangen, dass die für die Verarbeitung Verantwortlichen (besonders im Privatsektor) spezielle Bewilligungen oder Genehmigungen einholen. Es bestehen also in dieser Hinsicht noch eindeutig erhebliche Unterschiede zwischen den Rechtsvorschriften der Mitgliedstaaten.
72. Nationale Identitätsnummer: Es gibt verschiedene grundsätzliche Herangehensweisen an die Verwendung von nationalen Identitätsnummern und ähnlichen allgemeinen Kennzahlen. Manche Mitgliedstaaten erlauben den umfassenden Austausch dieser Nummern zwischen den öffentlichen Verwaltungen, sofern ihnen dies die Arbeit erleichtert. Andere wählen eine restriktive Vorgehensweise, bei der die Verwendung derartiger Nummern präziser geregelt (werden soll). Einige Länder erlauben die Verwendung dieser Nummern im Privatsektor, wenn die betroffene Person ihre Einwilligung gibt; andere sind wiederum restriktiver und befürchten insbesondere, dass die Verwendung dieser Nummern allzu leicht zur Vernetzung von Datenbanken und zu unkontrollierter Datenweitergabe führen kann.²⁴

Verweis: Working Paper No. 2 (erweiterte Version), Abschnitt 4.4

(v) Die Vorschriften zu grenzüberschreitenden Datenflüssen

73. Ergebnis/Schlussfolgerungen: Die Richtlinie behandelt zwei Arten der grenzüberschreitenden Datenflüsse: Datenflüsse innerhalb von EU/EWR und Datentransfers an Nicht-EU/EWR-Länder (so genannte „Drittländer“). In letzterem Fall wird noch weiter unterschieden in Drittländer mit und ohne „angemessenen“

²⁴ Im Vereinigten Königreich gibt es (bis jetzt) keine offiziellen nationalen Identitätsnummern, diese würden aber geschaffen werden, wenn das National Identity Register (Nationale Identitätsdatenbank) in Zusammenhang mit der Schaffung der National Identity Cards (nationale Personalausweise) eingerichtet wird. Andere weit verbreitete Kennzahlen, wie die National Insurance Number (Nationale Versicherungsnummer), die National Health Service Number (Nummer des Nationalen Gesundheitsdienstes) und Führerscheindetails, werden aber mit wenigen Einschränkungen sowohl vom öffentlichen als auch vom privaten Sektor häufig genutzt.

EUROPÄISCHE KOMMISSION – GD JLS
**VERSCHIEDENE ANSÄTZE ZUR BEWÄLTIGUNG NEUER HERAUSFORDERUNGEN FÜR DEN
SCHUTZ DER PRIVATSPHÄRE, INSBESONDERE AUFGRUND TECHNOLOGISCHER
ENTWICKLUNGEN**

Schlussbericht

Datenschutz. Die wesentlichen Vorschriften sind (oder waren) einfach: Innerhalb von EU/EWR und innerhalb der ehemals ersten Säule sollte der Datenfluss uneingeschränkt vonstattengehen. Nun wurde diese Säule jedoch abgeschafft und die Sache ist folglich, wie unten angemerkt, nicht mehr einfach. Der Datenfluss in Drittländer mit angemessenem Schutzniveau darf ebenfalls frei erfolgen (wenn der Schutz in einigen Bereichen angemessen ist, in anderen aber nicht, dann unter der Voraussetzung, dass die Daten in den Bereich mit angemessenem Schutz fallen) (Artikel 25(1)). Hingegen dürfen Daten grundsätzlich nicht in Drittländer ohne angemessenen Schutz übermittelt werden (auch nicht in Länder, deren Schutz in einigen Bereichen angemessen ist, nicht aber in anderen, wenn die Daten in einen Bereich mit nicht-angemessenem Schutz fallen), es sei denn, eine spezielle Bedingung wird erfüllt (Artikel 26(1)).

74. Aber auch diese Vorschriften werden nicht einheitlich angewendet. Erstens sehen nur wenige Staaten den freien Datentransfer innerhalb von EU/EWR ausdrücklich vor; in den meisten Staaten wird dies impliziert (indem nur der Datentransfer an Drittländer ausdrücklich eingeschränkt wird), aber nicht ausdrücklich festgeschrieben. Von den wenigen Staaten, die diese Freiheit stipulieren, verdeutlicht überdies nur einer (Österreich), dass diese Freiheit nur für die Verarbeitung innerhalb des Geltungsbereichs der Richtlinie gilt. Dies ist selbstverständlich wesentlich, denn es gibt keine Garantie, dass die Verarbeitung außerhalb des Geltungsbereichs der Richtlinie – insbesondere in der ehemals dritten Säule – unter angemessenem Datenschutz durchgeführt wird (vgl. Artikel 3(2), erstes Aufzählungszeichen, der Richtlinie). Die unkritische Anwendung der „Zone des freien Datenverkehrs“-Regelung in Artikel 1(2) der Richtlinie, sodass der Datentransfer innerhalb der ehemals dritten Säule der EU ebenfalls uneingeschränkt erfolgen kann, ist daher äußerst problematisch und wird mit Sicherheit zu Verletzungen der Datenschutzstandards führen. Natürlich wurde mit dem Inkrafttreten des Vertrags von Lissabon die Drei-Säulen-Struktur der EU offiziell aufgelöst. Es ist jedoch von zentraler Bedeutung, in dieser neuen Situation sogar noch mehr als zuvor, dass ein vollständiger und angemessener Datenschutz in allen Bereichen, die ehemals von den drei Säulen abgedeckt wurden, gewährleistet wird (wie oben unter 5.02(i) erörtert wird) – nur dann kann eine Regelung auf der Grundlage von Artikel 1(2) geschaffen werden, die auf jeglichen Datentransfer innerhalb von EU/EWR, nicht nur beschränkt auf den Bereich des Gemeinschaftsrechts, anzuwenden ist. Wenn die Herausforderungen des neuen, globalen technischen Umfelds bewältigt werden sollen, dann sollte dies besser früher als später geschehen.
75. Was den Datentransfer an Länder mit „angemessenem“ Datenschutzniveau angeht betrifft der Hauptunterschied – der ein wichtiger ist – die Situation, wenn die Kommission noch keine formale Feststellung der „Angemessenheit“ abgegeben hat. In Österreich, Griechenland, Luxemburg, Portugal und Spanien machen die Rechtsvorschriften deutlich, dass in Ermangelung einer Feststellung der Kommission zur „Angemessenheit“ nur die nationalen Behörden entscheiden können, ob ein bestimmtes Drittland „angemessenen“ Schutz bietet. Anders ausgedrückt: Bis bzw. wenn keine derartige einzelstaatliche (oder europäische) Feststellung in Bezug auf ein bestimmtes „Drittland“ vorliegt, unterliegt der Transfer personenbezogener Daten an dieses Land dem grundsätzlichen Verbot. In einigen Ländern, darunter im Vereinigten Königreich, wird die Beurteilung, wenn eine „Feststellung“ der Kommission fehlt, den für die Verarbeitung Verantwortlichen überlassen. Dies spiegelt die allgemein entspannte Herangehensweise, die auf begrenzte Einmischung setzt, der dortigen

EUROPÄISCHE KOMMISSION – GD JLS
**VERSCHIEDENE ANSÄTZE ZUR BEWÄLTIGUNG NEUER HERAUSFORDERUNGEN FÜR DEN
SCHUTZ DER PRIVATSPHÄRE, INSBESONDERE AUFGRUND TECHNOLOGISCHER
ENTWICKLUNGEN**

Schlussbericht

Behörden wider.²⁵ Dies scheint nicht mit den Ansichten der AG 29 konform zu gehen. Die AG räumt ein, dass „[i]n der Richtlinie [...] nicht festgelegt [ist], ob eine Behörde mit der Beurteilung der Angemessenheit des Datenschutzes in Drittländern betraut werden sollte“, aber schließt daraus, dass es daher zumindest möglich ist, dass „die innerstaatlichen Vorschriften in Mitgliedstaaten vorsehen, dass diese Aufgabe nationalen Datenschutzbehörden zu übertragen ist, deren Genehmigung einzuholen ist, bevor personenbezogene Daten in ein Drittland übermittelt werden dürfen.“ Aus dem nächsten Absatz geht hervor, dass die AG dies als die einzigen zwei wirklichen Optionen anzusehen scheint:²⁶

Neben der Beurteilung der Angemessenheit durch nationale Behörden aufgrund von innerstaatlichen Vorschriften sind nach der Richtlinie europaweite Angemessenheitsentscheidungen der Kommission möglich. Diese Entscheidungen bieten zusätzliche Rechtssicherheit und gewährleisten die einheitliche Rechtsanwendung in der gesamten Gemeinschaft ...

76. Das Problem entsteht aus der Verbindung der grundsätzlichen „freier Transfer innerhalb von EU/EWR“-Regelung mit der lockeren Einstellung im Vereinigten Königreich (und in einigen anderen Ländern), denn dadurch können die strengen Regelungen in den Ländern der ersten Kategorie leicht umgangen werden: Die Datenschutzbehörden dieser Länder können (im Sinne der Richtlinie) den Transfer personenbezogener Daten an Mitgliedstaaten mit weniger strengen Vorschriften nicht stoppen, und von diesen anderen Mitgliedstaaten aus können die Daten dann in Drittländer übermittelt werden, für die formal ein „angemessener“ Datenschutz nicht festgestellt wurde, weder auf EU-Ebene, noch durch die Behörden des Ausgangslandes, auf der Basis, dass der für die Verarbeitung Verantwortliche befindet, dass der Schutz dennoch ausreichend gewährleistet ist. Wir können nicht beurteilen, wie intensiv diese Gesetzeslücke genutzt wird (grundsätzlich besteht der Eindruck, dass die gesetzlichen Vorschriften zum Datentransfer allgemein nicht sehr genau befolgt werden) – aber es handelt sich dennoch klar um eine Gesetzeslücke. Des Weiteren wird im neuen Umfeld, in dem Daten ständig und routinemäßig an andere Gerichtsbarkeiten transferiert werden, dieses Problem – die bewusste oder unbewusste Nutzung dieser Gesetzeslücke – sehr schnell wachsen.
77. Zuletzt gibt es auch Unterschiede in der Anwendung der speziellen Bedingungen, unter denen Daten in Drittländer ohne „angemessenen“ Datenschutz übermittelt werden dürfen. Es möge hier die bloße Anmerkung genügen, dass auch hier die Bedingungen nicht einheitlich angewendet werden: Einige Mitgliedstaaten fügen zusätzliche, strengere Prüfungsvorgänge oder Anforderungen hinzu, z. B. dass die Ausnahme bezüglich des Transfers zur Wahrung der lebenswichtigen Interessen der betroffenen Person nur dann angewendet werden darf, wenn die betroffene Person nicht in der Lage ist, ihre Einwilligung zum Transfer zu geben. Ein Mitgliedstaat weicht die Vorschriften in Bezug auf Datenübermittlung an Steuerbeamte in Drittländern ohne Schutz extrem stark auf, während einige andere die vorgeschriebene Ausnahme bezüglich der

²⁵ Siehe die Aussage des britischen Datenschutzbeauftragten auf S. 180 der Vergleichenden Zusammenfassung (Fußnote 11, oben).

²⁶ AG 29 Arbeitspapier über eine gemeinsame Auslegung des Artikels 26 Absatz 1 der Richtlinie 95/46/EG vom 24. Oktober 1995 (Fußnote 12, oben), S. 5.

EUROPÄISCHE KOMMISSION – GD JLS
**VERSCHIEDENE ANSÄTZE ZUR BEWÄLTIGUNG NEUER HERAUSFORDERUNGEN FÜR DEN
SCHUTZ DER PRIVATSPHÄRE, INSBESONDERE AUFGRUND TECHNOLOGISCHER
ENTWICKLUNGEN**

Schlussbericht

Übermittlung von Daten aus öffentlichen Registern nicht vorsehen. Hier hat die AG 29 ein Arbeitspapier veröffentlicht, besonders um auszudrücken:²⁷

[dass sie] besorgt [ist] über die unterschiedlichen Auslegungen des Artikels 26 Absatz 1, was eine einheitliche Anwendung in den verschiedenen Mitgliedstaaten erheblich erschwert.

Sie fügt hinzu:

Für die Gruppe ist das Papier ein wichtiger Bestandteil ihrer Strategie für die Datenübermittlung an Drittländer. Es sollte daher in Verbindung mit anderen Unterlagen gelesen werden, die die Gruppe zu diesem Thema bereits vorgelegt hat, insbesondere den Papieren über „verbindliche Unternehmensregelungen“, Standardvertragsklauseln und die Angemessenheit des Schutzniveaus in Drittländern, einschließlich des Systems des sicheren Hafens (Safe-Harbor-System).

78. Das Papier gibt Hinweise dazu, wie die verschiedenen speziellen Bedingungen für den Datentransfer an Drittländer ohne angemessenes Schutzniveau, wie sie in Artikel 26(1) der Richtlinie festgeschrieben sind, anzuwenden sind. Dies hat allerdings zu keinen nennenswerten Veränderungen in den Handhabungen der Mitgliedstaaten geführt. Insbesondere die oben erwähnten „strengen“ Länder sind immer noch der Meinung, auf dem Papier, dass Daten aus ihrer Gerichtsbarkeit nicht in Länder übermittelt werden sollten, denen sie (oder die Kommission) kein angemessenes Datenschutzniveau bescheinigt haben; und die „lockeren“ Länder sind immer noch der Ansicht, dass die Beurteilung den für die Verarbeitung Verantwortlichen überlassen werden kann. Tatsächlich stellen die „strengen“ Länder nach unserem besten Wissen nie Bescheinigungen über ein angemessenes Datenschutzniveau aus, wenn die Länder nicht schon zuvor von der Kommission als angemessen eingestuft wurden.
79. Insgesamt scheint also der Artikel 26 in vielen Mitgliedstaaten, ob auf dem Papier streng oder weniger streng, mehr verletzt als erfüllt zu werden. Eine einheitlichere Auslegung dieser wichtigen Bestimmung ist eindeutig dringend notwendig; und dies sollte mit einer einheitlichen Strategie zur Sicherstellung der tatsächlichen Erfüllung in allen Mitgliedstaaten kombiniert werden. Wie unter C weiter unten erörtert wird, sind wir der Ansicht, dass vor allem die AG 29 bei der Erreichung dieses Ziels helfen kann.

B. Die Nicht-EU/EWR-Länder

80. Auch wenn die Richtlinie und die OECD-Leitsätze die Rechtsvorschriften vieler Nicht-EU/EWR-Länder beeinflussten, so sind diese Rechtsvorschriften dennoch formal mit keinen der beiden verbunden. Es ist daher nicht weiter verwunderlich, dass in diesen Ländern die oben erörterten Aspekte auf noch unterschiedlichere Weise gehandhabt werden – und dass dort, wo Unklarheit herrscht, was oft vorkommt, noch weniger Orientierungshilfen vorhanden sind, um Abhilfe zu schaffen. Einige kurze vergleichende Zusammenfassungen mögen genügen, um dies zu veranschaulichen:
81. Definitionen: In den Nicht-EU/EWR-Ländern ist der Ansatz für die Definition von „personenbezogener Information“ (oder „personenbezogenen Daten“) im Grunde dem der EU sehr ähnlich, obwohl es einige Abweichungen im Wortlaut und in den Ansätzen

²⁷ *Idem*, Zusammenfassung, S. 2.

EUROPÄISCHE KOMMISSION – GD JLS
**VERSCHIEDENE ANSÄTZE ZUR BEWÄLTIGUNG NEUER HERAUSFORDERUNGEN FÜR DEN
SCHUTZ DER PRIVATSPHÄRE, INSBESONDERE AUFGRUND TECHNOLOGISCHER
ENTWICKLUNGEN**

Schlussbericht

für die dazugehörenden Definitionen gibt. Da es an richterlicher Auslegung fehlt, ist es schwierig zu beurteilen, ob diese signifikante Unterschiede signalisieren; dies scheint allerdings nicht der Fall zu sein, außer eventuell in Hong Kong, wo das Appellationsgericht den Begriff „personenbezogene Daten“ auslegte und entschied, dass es sich nicht um „personenbezogene Daten“ handelt, wenn die Informationen ohne die Absicht, die Einzelperson zu identifizieren, erhoben wurden. Manche Gesetze beziehen sich nur auf systematisch organisierte Datenerfassung. Die indischen Rechtsvorschriften verwenden den Begriff „personenbezogene Daten/Informationen“ überhaupt nicht.

82. Die Rechtsvorschriften in Nicht-EU/EWR-Ländern verwenden nicht konsequent die Ausdrücke „für die Verarbeitung Verantwortlicher“ und „Auftragsverarbeiter“. Einige verwenden den Begriff „Verarbeitung“ und „Datennutzer“ (Hong Kong) während andere den Begriff „Verarbeitung“ zwar verwenden, ihn aber nicht definieren (Japan).

Verweise: Hong Kong report, 2.2; Japan report, 2.2; India report, 3.2.

83. Datenschutzgrundsätze: Die Rechtschriften in den meisten der Nicht-EU/EWR-Länder, die in diese Studie mit eingeschlossen sind, zeigen hier noch unterschiedlichere Herangehensweisen, da sie nicht versuchen, sich nach einer anderen Vorlage außer den OECD-Leitsätzen zu richten. Trotzdem versuchen Australien, Hong Kong und Japan, den Grundsatz der Zweckmäßigkeit umzusetzen (obwohl Australien und Japan recht großzügige Ausnahmen für die sekundäre Verarbeitung erlauben). Indien hat bis jetzt noch keine allgemeinen Datenschutzgesetze, aber die indischen Rechtsvorschriften zu Kreditauskünften wenden das Konzept der Zweckmäßigkeit sehr streng an (ebenso die entsprechenden australischen Rechtsvorschriften, die Hongkonger hingegen weniger).

Verweise: Australia report, 2.2; Hong Kong report, 2.2; Japan report, 2.2; India report, 3.2.

84. Datenschutzkriterien: In den in dieser Studie inkludierten Gerichtsbarkeiten in Asien und im pazifischen Raum befindet sich das Konzept der ‚rechtmäßigen Verarbeitung‘ nicht ausdrücklich im Zentrum der Datenschutzgesetzgebung und es befindet sich wohl auch implizit nicht dort. In diesen Gerichtsbarkeiten gibt es die Annahme nicht, dass die Verarbeitung berechtigt sein muss, und ansonsten unrechtmäßig ist. Stattdessen wird davon ausgegangen, dass die Verarbeitung (auch wenn dieser Terminus unter Umständen nicht verwendet wird) rechtmäßig ist, solange sie keinen der Datenschutzgrundsätze (Erhebung, Verwendung, Weitergabe, Sicherheit etc.) verletzt. Im Wesentlichen wird dies selten zu Unterschieden in der Praxis führen, aber es stellt einen deutlich anderen Ansatz und eine deutlich andere Einstellung dar. Direkte Vergleiche zwischen diesen Rechtsvorschriften und den Rechtsvorschriften der EU, die Thema des restlichen Abschnitts sind, sind daher schwierig.

85. In diesen gerichtlichen Zuständigkeiten ist es folglich erforderlich, in einem bestimmten Kontext eigens zu überprüfen, ob es einer Einwilligung oder einer Art von Benachrichtigung bedarf, damit personenbezogene Daten erhoben werden dürfen und dies in keinem Verstoß resultiert; und wenn eine Einwilligung, eine gesetzliche Genehmigung oder eine ‚Abwägung‘ des öffentlichen Interesses bedeutet, dass eine sekundäre Verwendung oder Weitergabe keinen Verstoß gegen den Verwendungs- oder Weitergabegrundsatz darstellen. Anders gesagt ist die Frage, die gestellt werden muss, gewöhnlich, ob ein einzelner Fall der Erhebung, Verwendung oder Weitergabe „rechtmäßig“ ist; und es geht weniger um die allgemeinere Frage, ob es sich um eine

EUROPÄISCHE KOMMISSION – GD JLS
**VERSCHIEDENE ANSÄTZE ZUR BEWÄLTIGUNG NEUER HERAUSFORDERUNGEN FÜR DEN
SCHUTZ DER PRIVATSPHÄRE, INSBESONDERE AUFGRUND TECHNOLOGISCHER
ENTWICKLUNGEN**

Schlussbericht

„zulässige Verarbeitung“ ist im Sinne eines bestimmten „Kriteriums“ handelt. Beides führt jedoch oft zur selben Antwort.

86. Die USA erkennen grundsätzlich keinen Verhältnismäßigkeitsgrundsatz bei der Datenerhebung an. Durch den sektoralen Ansatz der USA werden zudem verschiedene Situationen der Opt-In Einwilligung, des Opt-Out und No-Opt geschaffen. Eine Opt-In Einwilligung kann in manchen Bereichen notwendig sein, und in anderen, wo die fraglichen Daten ebenso sensibel sind, wieder nicht. Siehe den USA report, Abschnitt 7.6. Der Ansatz der USA konzentriert sich mehr auf den Formalismus, den angegebenen Grad der Einwilligung zu erreichen, und prüft nicht sehr gründlich, wie gut die Einzelpersonen über die Auswirkungen ihrer Einwilligung informiert sind. Zudem setzen viele Unternehmen den Kauf eines ihrer Produkte oder einer ihrer Dienstleistungen mit der Einwilligung zu sekundärer Verwendung gleich; dies wird auch in einer Reihe von Gesetzen widerspiegelt, die Konsumenten/-innen mit einer „bestehenden Geschäftsbeziehung“ mit einem Unternehmen von bestimmten Einwilligungsanforderungen ausnehmen.

Verweis: USA report, Abschnitte 4.3 und 7.6.

87. Verarbeitung sensibler Daten: Der US-amerikanische Rechtsrahmen schafft keinen allgemeinen Schutz von Daten basierend auf ihrer Sensibilität allein. Die Hintergrundüberprüfung von Bewerbern/-innen vor Beschäftigungsbeginn unterliegt jedoch einer erheblichen Regulierung (sie wird wie die Kreditauskünfte gehandhabt) basierend auf Datenschutzgrundsätzen. Andererseits unterliegen Personaldaten und andere am Arbeitsplatz erhobene Daten keinem sektoralen Datenschutzgesetzes. In den USA werden Festnahmen und strafrechtliche Verurteilungen wie öffentliche Aufzeichnungen behandelt; allgemein können diese Informationen für so gut wie jeden Zweck verwendet werden.

Verweis: USA report, Abschnitte 5.1, 5.5 und 5.7

88. Grenzüberschreitende Datenflüsse: In Nicht-EU/EWR-Ländern variieren die Einschränkungen für den grenzüberschreitenden Datenfluss stark. In den in dieser Studie untersuchten Ländern Asiens und des pazifischen Raums gestaltet sich die Situation folgendermaßen (wir lassen hier die Schwierigkeiten beiseite, die durch die Position der Vertreter/Treuhänder entstehen und durch Fragen der [begrenzten] extraterritorialen Auswirkungen der relevanten Gesetze):

- (a) Australien hat eine Beschränkung des Datenexports in seinem Datenschutzgesetz betreffend Organisationen des Privatsektors (NPP 9), die in Kraft ist und lose auf den Artikeln 25 und 26 der Richtlinie basiert, aber schwächer ist; sie war nie Gegenstand einer eingereichten Beschwerde, geschweige denn einer gerichtlichen Entscheidung;
- (b) In der Verordnung (s. 33) der Sonderverwaltungsregion Hong Kong gibt es eine Beschränkung des Datenexports, die aber nie in Kraft gesetzt wurde; wäre sie in Kraft, wäre sie mindestens so stark wie die Bestimmungen der Richtlinie;
- (c) In Indien gibt es keine Beschränkungen des Datenexports;
- (d) Japan kennt keine Beschränkung des Datenexports, die über die üblichen „Zweckmäßigekeitsanforderungen“ bezüglich Verwendung und Weitergabe hinaus geht, und auch diese sind leicht zu umgehen.

EUROPÄISCHE KOMMISSION – GD JLS
**VERSCHIEDENE ANSÄTZE ZUR BEWÄLTIGUNG NEUER HERAUSFORDERUNGEN FÜR DEN
SCHUTZ DER PRIVATSPHÄRE, INSBESONDERE AUFGRUND TECHNOLOGISCHER
ENTWICKLUNGEN**

Schlussbericht

89. Von den anderen Ländern Asiens und des pazifischen Raums verfügen nur die Sonderverwaltungsregion Macau (ein starkes Gesetz basierend auf der Richtlinie), Südkorea (basierend auf Einwilligung) und Taiwan (ein schwaches und ungenutztes Gesetz) über Beschränkungen des Datenexports. Neuseeland ist gerade dabei, ein minimalistisches Gesetz zu erlassen.

Verweise: Australia report, 6; Hong Kong report, 6; India report, 7; Japan report, 5.

**C. WIE EINE UMFASSENDE HARMONISIERUNG ERREICHT
WERDEN KANN**

90. **Empfehlung:** Wie weiter oben bereits angemerkt ist das Erreichen einer viel umfassenderen Harmonisierung der Datenschutzbestimmungen innerhalb der EU eine Grundvoraussetzung für eine wirkungsvolle Datenschutzregelung in EU/EWR, die die Herausforderungen des neuen, globalen technischen Umfelds bewältigen kann. Ein Weg, dies zu erreichen, wäre es, die Basisrichtlinie (und damit wahrscheinlich auch die Tochterrichtlinien) durch eine (unmittelbar geltende) Verordnung zu ersetzen (was ursprünglich beim Verfassen der Richtlinie in Betracht gezogen worden war), oder durch eine viel enger gefasste, völlig neue Richtlinie. Dies würde jedoch sowohl Fragen hinsichtlich der Subsidiarität und Gesetzgebungsbefugnisse aufwerfen als auch weniger flexible Vorschriften zur Folge haben. Wir haben uns daher auf die Alternative konzentriert: die Suche nach Wegen, die zu einer umfassenderen Harmonisierung innerhalb des Rahmens der Basisrichtlinie, so wie sie besteht, führen. Es gibt verschiedene Wege dies zu erreichen, nicht alle sind miteinander unvereinbar:
91. Erstens sind wir bezüglich der EU/EWR-Mitgliedstaaten der Ansicht, dass die Kommission viel härter gegen Mitgliedstaaten, die die Bestimmungen der Richtlinie offensichtlich nicht ausreichend erfüllen (am Papier oder in der Praxis), vorgehen könnte. Des Weiteren sollte die Kommission ihre Durchsetzungsbefugnisse einsetzen, um eine umfassendere Harmonisierung zu erreichen (in der Weise wie unter Abs. 94, unten, vorgeschlagen wird).
92. Allerdings sind wir der Meinung, dass die zentralste Rolle in dieser Hinsicht der AG 29 zukommen könnte: Obschon ihre Stellungnahmen etc. nicht bindend sind, verfügt sie über das Fachwissen und die direkte Verbindung zu den einzelstaatlichen Gepflogenheiten, um in der Lage zu sein, harmonisierte Auslegungen und Anwendungsarten der Bestimmungen der Richtlinie zu formulieren. Ein Kritikpunkt an der AG 29 allerdings ist, dass sie bisweilen gemeinsam, auf EU-Ebene, Ansichten und Auslegungen, und Vorschläge für die Anwendung der Richtlinien vorbringt, die ihre Mitglieder innerstaatlich nicht umsetzen können (oder wollen). Mitunter stehen die innerstaatlichen Gesetzestexte im Weg; oder die DPAs haben ganz einfach nicht die gesetzliche Befugnis, Auslegungen oder Lösungen, auf die man sich auf europäischer Ebene geeinigt hat, auch innerstaatlich durchzusetzen.
93. Nach unserem Dafürhalten gibt es in dieser Hinsicht einen ausgedehnten Spielraum für eine Stärkung der Datenschutzregelung der EU. Die AG 29 veröffentlicht bereits jetzt viele wichtige Ansichten, Arbeitsdokumente und Stellungnahmen über die Auslegung und Anwendung der Richtlinie. Abgesehen vom oben erwähnten Kritikpunkt, dass diese nicht immer innerstaatlich umgesetzt werden, werden diese Ansichten in Europa und

EUROPÄISCHE KOMMISSION – GD JLS
**VERSCHIEDENE ANSÄTZE ZUR BEWÄLTIGUNG NEUER HERAUSFORDERUNGEN FÜR DEN
SCHUTZ DER PRIVATSPHÄRE, INSBESONDERE AUFGRUND TECHNOLOGISCHER
ENTWICKLUNGEN**

Schlussbericht

außerhalb hoch geachtet, und zwar als maßgebliche Darlegungen der richtigen Auslegung und Anwendung der EU- (und weltweiten) Standards. Die zentrale Frage ist, wie gewährleistet werden kann, dass diese Ansichten und Stellungnahmen eine tatsächliche Auswirkung auf nationaler Ebene haben – ohne dass der AG 29 Befugnisse zugesprochen werden, die richtigerweise bei der Kommission und den Gerichtshöfen bleiben sollten.

94. Wir schlagen vor, dass die AG 29 ersucht wird, in Absprache mit der Kommission (die in jedem Fall als ihr Sekretariat fungiert) mehr und tiefer schürfende Untersuchungen der einzelstaatlichen Rechtsvorschriften und Gepflogenheiten durchzuführen, in der Absicht, „optimale Verfahren“ und Auslegungsvorschläge zu formulieren (was sie im Grunde bereits tut), aber mit der zusätzlichen Anforderung, dass die Mitgliedstaaten berichten müssen, inwieweit sie diesen Vorschlägen nachkommen (oder inwieweit sie ihrer Meinung nach diesen Vorschlägen nicht nachkommen müssen sollten). Es obläge dann der Kommission, wenn nötig, herauszufinden, ob die Orientierungshilfen der AG 29 diejenigen sind, denen die Mitgliedstaaten in ihren Rechtsvorschriften folgen sollen. Dabei sollten Durchsetzungsmaßnahmen als ein übliches Mittel angesehen werden, dies zu kontrollieren (vgl. unsere Empfehlung zu stärkeren Durchsetzungsmaßnahmen in Abs. 91, oben). Die Grundidee ist, dass die AG 29 Hinweise zur richtigen Auslegung und innerstaatlichen Anwendung der Richtlinien gibt (was sie bereits macht); und dass die Kommission, sofern sie auch der Meinung ist, dass die vorgeschlagenen Auslegungen und Anwendungen die richtigen sind, diese aber von einigen Mitgliedstaaten nicht befolgt werden, Durchsetzungsmaßnahmen gegen diese Staaten ergreift. Die fraglichen Staaten könnten dann einlenken – wodurch es zu einer Harmonisierung käme. Oder sie könnten die von der Kommission bestätigte Auslegung der AG 29 beim EuGH anfechten – in diesem Fall käme es dann zu einer endgültigen, maßgeblichen Entscheidung, welche ebenfalls eine umfassendere Harmonisierung unterstützen würde.
95. Wir glauben, dass dafür keine Änderung der Richtlinie erforderlich ist. Es würde aber dennoch eine wesentliche Veränderung signalisiert im Ansatz der Kommission zur Sicherstellung, dass die Richtlinien einheitlicher umgesetzt und angewendet werden, wobei Stellungnahmen der AG 29 tatsächlich, in geeigneten Fällen, von der Kommission durchgesetzt würden (natürlich unter der Aufsicht des EuGH).
96. Als einen sehr bescheidenen Schritt in diese Richtung, der ein solches Handeln der AG 29 und der Kommission ermöglichen soll, empfehlen wir, dass zumindest die Ansichten der AG 29 und das Ausmaß und die Art, wie diese in den einzelstaatlichen Rechtsvorschriften und Gepflogenheiten widerspiegelt werden, in einer besser strukturierten und umfassenderen Form zugänglich gemacht werden, und dass die Aufmerksamkeit der relevanten Verwaltungs- und Justizbehörden auf einzelstaatlicher und EU-Ebene darauf gelenkt wird.

Verweis: Eine diesbezügliche Empfehlung wurde bereits in den Empfehlungen einer anderen diesjährigen Studie der EU-Kommission abgegeben, die eine Evaluation of the contribution of Working Party 29 to the work of the Commission in the field of Data Protection (Evaluation des Beitrags der Arbeitsgruppe 29 zur Arbeit der Kommission auf dem Gebiet des Datenschutzes) durchführte: siehe Empfehlung 7 dieser Studie, die wie folgt lautet:

EUROPÄISCHE KOMMISSION – GD JLS
**VERSCHIEDENE ANSÄTZE ZUR BEWÄLTIGUNG NEUER HERAUSFORDERUNGEN FÜR DEN
SCHUTZ DER PRIVATSPHÄRE, INSBESONDERE AUFGRUND TECHNOLOGISCHER
ENTWICKLUNGEN**

Schlussbericht

Wir empfehlen, dass die AG 29 die Möglichkeit der Schaffung einer Datenbank oder einer ähnlichen Online-Quelle prüft, in der die relevanten Abschnitte aller Stellungnahmen und Arbeitsdokumente der AG 29 auf strukturierte Weise gespeichert sind, sodass Kommentare zu einem umfassenderen Thema (etwa zum Konzept der personenbezogenen Daten oder zum anzuwendenden Recht) in jedem davon leicht gefunden und zueinander in Beziehung gesetzt werden können; und dass die Mitglieder der AG 29 ersucht werden, ähnliche Details aus ihren jeweiligen einzelstaatlichen Rechtsvorschriften und Gepflogenheiten zur selben Quelle beizusteuern. Wir glauben, dass dadurch ein sehr bedeutender Beitrag sowohl zum „europäischen Mehrwert“, der bereits allgemein von der AG 29 erbracht wird, als auch zur Harmonisierung der (Anwendung der) einzelstaatlichen Rechtsvorschriften und Gepflogenheiten geschaffen werden würde.

Wir sind der Ansicht, dass diese Quelle zu allen drei im jüngsten Arbeitsprogramm der AG 29 unter der Überschrift „Effizientere Arbeitsweise der Artikel 29 - Datenschutzgruppe“ erwähnten Unterthemen beitragen würde: Sie würde zur Entwicklung von Leitsätzen bzw. Standards beitragen, die Effizienz der AG 29 in Bezug auf nationale Verfahrensweisen steigern, und bei der Durchsetzung helfen. Sie würde der AG 29 des Weiteren zweifelsohne in ihren beratenden Aufgaben für die Kommission behilflich sein.

Anmerkung: Die Anfänge einer solchen Quelle wurden schon in Zusammenhang mit einem EG „e TEN“-Programm geschaffen, bei der Schaffung eines Europäischen Datenschutzgütesiegels, „EuroPriSe“, das soeben endete. Für die an diesem Projekt mitarbeitenden Experten wurde ein Kriterienkatalog auf der Grundlage der Datenschutzrichtlinien erstellt und ein Kommentar entworfen, der genau die eben erwähnten Orientierungshilfen enthält, mit Verweisen auf die Dokumente der AG 29 und nationale Verfahrensweisen. Der Kommentar wurde von der Kommission und den am Projekt beteiligten DPAs sehr gelobt und ist bei Unternehmen sehr gefragt.²⁸
(Übersetzung: V.G./S.H.)

97. Grundsätzlich können das ER Übereinkommen Nr. 108 (mit seinem Fakultativprotokoll) und der dazugehörige Beratende Ausschuss und die Projektgruppe Datenschutz (CJ-PD) auch eine nützliche Rolle spielen, besonders in Bezug auf die Nicht-EU/EWR- und Nicht-ER-Staaten. Der Beratende Ausschuss und die CJ-PD veröffentlichen sicherlich wichtige Leitlinien zur Anwendung der wesentlichen Datenschutzgrundsätze (die das Übereinkommen und die EU-Richtlinie teilen) in bestimmten Bereichen, wie etwa Polizeiarbeit, Austausch von justiziellen Informationen in Strafsachen etc.²⁹ Allerdings hat dies zu keiner umfassenderen Harmonisierung zwischen den Staaten geführt, die an diesem Übereinkommen teilnehmen, geführt als zwischen den EU/EWR-Mitgliedstaaten, im Gegenteil: Die Harmonisierung, wie

²⁸ Der Kriterienkatalog und der Kommentar des EuroPriSe wurden vom Teamleader des aktuellen Projektes erstellt, der auch bei jenem Projekt ein leitender Rechtsberater war, zusammen mit Rechtsanwälten der Datenschutzbehörde Schleswig-Holsteins, und mit weiterem Input der Madrider und der französischen Datenschutzbehörden. Der Kommission wurden diese Dokumente vorgelegt (NB der Kommentar wird aus kommerziellen Gründen nicht veröffentlicht). [originale Fußnote im AG 29 Evaluationsbericht]. Diese Empfehlung wurde auf Wunsch der Kommission ergänzt durch eine weitere Anmerkung des Teamleaders jener Evaluation (der auch der Teamleader der vorliegenden Studie ist). Diese Anmerkung wurde dem AG 29 Evaluationsbericht als Attachment 2 beigefügt.

²⁹ Diese Behörden haben sich auch mit einigen Bereichen befasst, mit denen sich ebenfalls (und im Allgemeinen auf ähnliche Weise) EU/EWR befasst haben, wie beispielweise Videoüberwachung und Verträge zu grenzüberschreitender Datenübermittlung. Siehe: http://www.coe.int/t/e/legal_affairs/legal_co-operation/data_protection/documents/reports_and_studies_of_data_protection_committees/2Committee%20Studies%20and%20reports.asp#TopOfPage.

EUROPÄISCHE KOMMISSION – GD JLS
**VERSCHIEDENE ANSÄTZE ZUR BEWÄLTIGUNG NEUER HERAUSFORDERUNGEN FÜR DEN
SCHUTZ DER PRIVATSPHÄRE, INSBESONDERE AUFGRUND TECHNOLOGISCHER
ENTWICKLUNGEN**

Schlussbericht

mangelhaft sich auch sein mag, ist zwischen den EU/EWR-Mitgliedstaaten doch besser als die Harmonisierung zwischen den Staaten des ER Übereinkommens.

98. Letztlich möchten wir anmerken, dass es außerhalb von EU/EWR/ER keine Institution gibt, bei der Aussicht darauf bestünde, dass sie viel zur Harmonisierung beitragen könnte. Das APEC Privacy Framework hatte keine Auswirkungen in dieser Hinsicht. Die Abkommen der ASEAN in Bezug auf die Harmonisierung der Rechtsvorschriften zum elektronischen Geschäftsverkehr könnten bis 2015 harmonisierende Auswirkungen in den Mitgliedsländern haben, aber das bleibt abzuwarten. Die Tagung der Asia Pacific Privacy Agencies (APPA) entbehrt einer institutionellen Grundlage wie sie die AG 29 hat, und sie hat auch keine Erfolge oder Ambitionen in Bezug auf Harmonisierung vorzuweisen. Dadurch wird die Arbeit der AG 29 weltweit sogar noch wichtiger.

**5. ZUSAMMENARBEIT MIT NICHT-EU/EWR-LÄNDERN
(EINSCHLIESSLICH BESCHEINIGUNGEN EINES “ANGEMESSENEN”
DATENSCHUTZNIVEAUS)**

99. **Ergebnis/Schlussfolgerungen:** Im Kontext des neuen, sozio-technischen Umfelds, und v. a. auch der Globalisierung, ist es aus europäischer Perspektive von entscheidender Bedeutung, andere (nicht-europäische) Staaten anzuregen, Gesetze zum Datenschutz bzw. zum Schutz der Privatsphäre zu erlassen, die aus dieser Perspektive „angemessen“ sind. Die Basisrichtlinie sieht natürlich spezielle Verfahren genau zu diesem Zweck vor und „belohnt“ Staaten, die „angemessene“ Gesetze erlassen, nach einer Prüfung durch die Kommission (die auch die Ansichten der AG 29 miteinbezieht). Allerdings wurde dieses Verfahren bis jetzt nur in einem halben Dutzend Fällen angewendet, darunter drei britische Territorien in Europa (und der eher spezielle Fall des „sicheren Hafens“ („Safe Harbor“) der USA und der noch umstrittenere US-amerikanische Fall der PNR-Daten).³⁰ Die Kommission hat in den 15 Jahren seit Inkrafttreten der Richtlinie bisher noch keine einzige Entscheidung über die Angemessenheit der rechtlichen Regelungen von Gerichtsbarkeiten in Asien oder im pazifischen Raum getroffen.
100. Obwohl wir anerkennen, dass ein „angemessenes“ Datenschutzniveau formal nur nach einem strengen Verfahren bescheinigt werden kann, könnte hinsichtlich der Staaten, die wirklich ein angemessenes Schutzniveau bieten, die begrenzte Nutzung dieses Verfahrens das falsche Signal für andere, besonders nicht-europäische Staaten, ausgesendet haben. Insbesondere in den Ländern Asiens und des pazifischen Raums war ursprünglich das Vorhaben, dass die Rechtsvorschriften eines Landes die europäischen Angemessenheitsstandards erfüllen, sehr wichtig, da man der Ansicht war, dass dies positive Auswirkungen auf den Handel haben würde. Dies kann anhand der folgenden (rein hypothetischen) Beispiele veranschaulicht werden:

³⁰ Die Länder, die momentan von der Bescheinigung eines „angemessenen“ Datenschutzniveaus profitieren sind die Schweiz, Kanada, Argentinien, Jersey, Guernsey und die Isle of Man. Der Datenschutz einiger Länder (darunter Ungarn) wurde in der Vergangenheit als „angemessen“ beurteilt, aber da diese mittlerweile der EU beigetreten sind, gilt dieses Verfahren für sie nicht mehr: Sie müssen die Richtlinien nun voll einhalten und umsetzen. Obwohl es keine formale Feststellung bezüglich Australien gab, gab die AG 29 eine grundsätzliche negative Stellungnahme ab (Stellungnahme 3/2001 vom 26. Januar 2001, WP40). Allerdings wurde angedeutet, dass einige der Kritikpunkte der AG 29 missverständlich waren, einige davon wurden nun von der Gesetzgebung behandelt, wie das Gutachten für die Kommission von Bygrave und Greenleaf 2005 über die Angemessenheit des Schutzniveaus in Australien ausführt. Das bedeutet nicht, dass die Schlussfolgerungen in WP40 falsch waren, sondern nur, dass die Situation komplexer ist als dort dargestellt.

EUROPÄISCHE KOMMISSION – GD JLS
**VERSCHIEDENE ANSÄTZE ZUR BEWÄLTIGUNG NEUER HERAUSFORDERUNGEN FÜR DEN
SCHUTZ DER PRIVATSPHÄRE, INSBESONDERE AUFGRUND TECHNOLOGISCHER
ENTWICKLUNGEN**

Schlussbericht

- (i) eine Feststellung, dass Südkoreas Datenschutzregelung betreffend den Privatsektor angemessen ist, während es die japanische mangels Durchsetzung nicht ist;
- (ii) eine Feststellung, dass innerhalb Chinas die Regelung in Macau angemessen ist, die von Hong Kong dagegen nicht, weil Unzulänglichkeiten in der Durchsetzung bestehen und aufgrund dessen, dass die Beschränkungen des Datenexports nicht in Kraft sind;
- (iii) als Alternative dazu eine Feststellung, dass die Rechtsvorschriften Hong Kongs angemessen sind, die taiwanesischen jedoch nicht;
- (iv) eine Feststellung, dass die Rechtsvorschriften Neuseelands angemessen sind, die australischen aber nicht.

Innerhalb jedes dieser Gerichtsbarkeiten-Paare dürfte eine derartige Feststellung bedeutenden Druck dahingehend ausüben, dass die Datenschutzgesetze, die „unangemessen“ sind, verstärkt werden (einhergehend mit vorhersehbarem Unmut über die EU), und zwar aufgrund der wahrgenommenen Position im Vergleich zum anderen, „ebenbürtigen“, Staat. Alle Staaten Asiens und des pazifischen Raums würden sich außerdem wahrscheinlich fragen: „Wollen wir, dass unsere Rechtsvorschriften als „unangemessen“ eingestuft werden?“

101. Allerdings hat dieses Argument stetig an Kraft verloren und ist hohl geworden. Die Länder Asiens und des pazifischen Raums gehen 2009 wahrscheinlich weniger davon aus, dass dies eine ernste Frage ist, als sie es 1999 getan hätten. Dem Safe-Harbor-System der USA ein angemessenes Datenschutzniveau zu bescheinigen war aus dieser Perspektive der Glaubwürdigkeit der europäischen Position auch nicht förderlich, vor allem, wenn man dies dem gegenüberstellt, dass einigen Gerichtsbarkeiten Asiens und des pazifischen Raums, die, wie jeder objektive Beobachter feststellen würde, eine größere Bedeutung hinsichtlich des Datenschutzes haben als der Safe Harbor, kein angemessenes Niveau bescheinigt wurde. Dennoch hat die Aussicht auf eine Bescheinigung eines angemessenen Datenschutzniveaus ihre Macht noch nicht völlig eingebüßt und wird vom neuseeländischen Beauftragten für den Schutz der Privatsphäre ausdrücklich als ein Grund angeführt, warum der aktuelle neuseeländische Gesetzesentwurf zur Stärkung der Datenexportbestimmungen Gesetzeskraft erlangen sollte.

Anmerkung: Dies ist eine andere Frage als die, ob die Standards der Richtlinie als ein gutes Modell für neue Datenschutzgesetze in Asien und im pazifischen Raum angesehen werden. Die Antwort auf diese Frage scheint immer noch „ja“ zu sein, und das jüngste in dieser Region erlassene Gesetz, das der Sonderverwaltungsregion Macau, lehnt sich eng an die Richtlinie an (via die portugiesische Gesetzgebung). Ebenso ist der chinesische Gesetzesvorschlag von 2006-7 stark von der EU beeinflusst.

102. Wir erkennen an, dass es eine Reihe anderer Faktoren gibt, die berücksichtigt werden müssen und die diese recht direkte Schlussfolgerung relativieren und die einfachen Beispiel aus Abs. 100 verkomplizieren: (i) die Kommission wartet für gewöhnlich darauf, bis ein Land einen Antrag auf Beurteilung der Angemessenheit stellt (obwohl sie nicht darauf warten müsste können wir verstehen, dass es politisch schwierig sein kann, ein Verfahren ohne einen derartigen Antrag einzuleiten); (ii) das Feststellen der „Angemessenheit“ – und noch mehr das mögliche Feststellen einer „Unangemessenheit“ – haben potentielle politische Auswirkungen, die über den Bereich

EUROPÄISCHE KOMMISSION – GD JLS
**VERSCHIEDENE ANSÄTZE ZUR BEWÄLTIGUNG NEUER HERAUSFORDERUNGEN FÜR DEN
SCHUTZ DER PRIVATSPHÄRE, INSBESONDERE AUFGRUND TECHNOLOGISCHER
ENTWICKLUNGEN**

Schlussbericht

des Datenschutzes hinausgehen und die ebenfalls berücksichtigt werden müssen; und (iii) die Kommission hat außer der öffentlichen Bescheinigung von Angemessenheit andere Methoden zur Verfügung, mit denen sie höhere Datenschutzstandards in Nicht-EU/EWR-Ländern fördern kann.

103. **Empfehlung:** Hier können wir nur festhalten, dass das „Angemessenheits“-Verfahren (bis jetzt?) nicht die Auswirkungen hat, die es haben könnte. Unserer Meinung nach sollte das Verfahren, und die Zeit, die seine Anwendung dauert, überprüft werden. Vielleicht wären einstweilige Entscheidungen eine Antwort. In jedem Fall sollten die anderen, weniger formellen Maßnahmen, wie technische Unterstützung, enge Zusammenarbeit (einschließlich der „Partnerschaft“ von EU- und Nicht-EU-DPAs) und andere Verfahren, fortgeführt und gefördert werden. In der Zwischenzeit ist es auf politischer Ebene wichtig, die Tendenz umzukehren, dass Artikel 25 der Richtlinie seinen potentiellen internationalen Einfluss verliert.

6. ÜBERWACHUNG UND DURCHSETZUNG: Die Rolle der Datenschutzbehörden (DPAs) und Gerichte:

104. **Ergebnis/Schlussfolgerungen:** Die DPAs verfügen über umfassendes Verständnis und Wissen und bieten nützliche Orientierungshilfen zu den Rechtsvorschriften – aber in Bezug auf die Durchsetzung sind sie nicht effektiv: Die „Kontrolle“ der Einhaltung des Datenschutzes durch die DPAs ist im Allgemeinen schwach und ineffektiv. Wir möchten hier die Schlussfolgerungen eines wichtigen Berichts für die Agentur der EU für Grundrechte zitieren, der parallel zu diesem Bericht verfasst wurde:

Dieser vergleichende Bericht zeigt die wesentlichen Mängel des aktuellen Systems zum Schutz der personenbezogenen Daten in den 27 EU-Mitgliedstaaten auf. Unzulänglichkeiten sind feststellbar im Mangel an Unabhängigkeit, an ausreichenden Ressourcen und an angemessenen Befugnissen mancher Datenschutzbehörden. Die Einhaltung der Datenschutzgesetze in der Praxis einiger Mitgliedstaaten lässt ebenso Bedenken aufkommen. Gesetzesreformen sind auch vonnöten im Bereich Sanktionen und Entschädigungsleistungen, um ein höheres Maß an Durchsetzung der relevanten Rechtsvorschriften und an Schutz der Opfer von Verstößen im Bereich personenbezogene Daten zu erreichen.

Zusammenfassung des endgültigen Entwurfs der Comparative Legal Study on assessment of data protection measures and relevant institutions (Vergleichenden Studie über die Bewertung der Datenschutzmaßnahmen und relevante Institutionen), Abs. 8. Der Bericht wurde von der Agentur der Europäischen Union für Grundrechte (FRA) 2009 in Auftrag gegeben.
(Übersetzung: V.G./S.H.)

In diesen allgemeinen Aspekten nehmen wir Bezug (und verweisen) auf die FRA-Studie und möchten nur anmerken, dass die schwache Durchsetzung in vielen Ländern bereits in einer viel früheren Studie³¹ festgestellt wurde und dass sich diese Situation seither nicht sehr verbessert zu haben scheint.

105. Hier möchten wir uns auf einige spezifischere Überlegungen beschränken. Erstens sind wir der Ansicht, dass die DPAs oft erst zu spät zu Rate gezogen werden: Sie werden um

³¹ Douwe Korff, EG Studie über Case-law on compliance, 1998.

EUROPÄISCHE KOMMISSION – GD JLS
**VERSCHIEDENE ANSÄTZE ZUR BEWÄLTIGUNG NEUER HERAUSFORDERUNGEN FÜR DEN
SCHUTZ DER PRIVATSPHÄRE, INSBESONDERE AUFGRUND TECHNOLOGISCHER
ENTWICKLUNGEN**

Schlussbericht

ihre Meinung zu Systemen gefragt, die größtenteils schon „in Stein gemeißelt“ sind, vor allem im öffentlichen Sektor. Dies kann sogar bei sogenannten „Vorabkontrollen“ der Fall sein, wenn diese erst durchgeführt werden, wenn das System schon endgültig geplant wurde (mit erheblichen Kostenauswirkungen). Ein zweites Problem besteht darin, dass eine Reihe von Datenschutzbehörden noch über zu wenig technische Kernkompetenz verfügen: Es gibt immer noch zu viele Rechtsanwälte und nicht genug System- und Computerexperten in den Behörden.

106. Es besteht weiterhin eine grundlegendere Frage über die – aus unserer Sicht bis zu einem gewissen Grad unvereinbaren – Funktionen der DPAs. Sie haben Beratungsfunktion und sollen Orientierung geben. Sie legen auch das Gesetz aus – und sind manchmal sogar Quasi-Gesetzgeber. Sie sollen die Rechte der betroffenen Personen vertreten. Und sie sollen das Gesetz vollziehen. Unserer Meinung nach wird damit zu viel von einer einzelnen Behörde verlangt. Eine Gefahr besteht darin, dass sie als Aufsicht führende Behörden „Gefangene“ derjenigen werden, über die sie Aufsicht führen, insbesondere Industrie und staatliche Behörden. Dieses Phänomen beschränkt sich keineswegs nur auf die Datenschutzbehörden: Es wurde bei vielen modernen Aufsichtsbehörden beobachtet. Aber es dient ebenfalls dazu, die Spannungen zwischen den verschiedenen Funktionen dieser Behörden aufzuzeigen.
107. Wir sind der Anschauung, dass dieses Problem – diese Spannungen – in jeglicher Überarbeitung der Richtlinie weiter erörtert werden sollte. Möglicherweise sollte darüber nachgedacht werden, die „weichen“ beratenden und Aufsichtsfunktionen der Behörden von der „harten“ Rolle des Gesetzesvollzugs zu trennen. Letzteres könnte grundsätzlich den Gerichten überlassen werden (die auch in Fällen von Einzelpersonen handeln könnten: siehe Abschnitt V.7, unten) und (bei ernsteren oder allgemeineren Verstößen) den für die Strafverfolgung zuständigen Behörden. Die DPAs, die Experten in diesen Angelegenheiten sind, könnten natürlich immer noch als Berater bei Gericht hinzugezogen werden; sie könnten sogar das Recht erhalten, ihre Stellungnahmen *ex officio* abzugeben und sie könnten das Recht bekommen, *ex officio* vor Gericht zu erscheinen, sooft es um eine Rechtssache geht, in der Fragen des Datenschutzes auftauchen. In jedem Fall sollten in dem Ausmaß, indem Fragen des Datenschutzes in die Hände der Gerichte (oder der speziellen Tribunale wie in Großbritannien) gegeben werden, die betroffenen Personen und die für die Verarbeitung Verantwortlichen im selben Maße Zugang haben.
108. **Empfehlungen:** Wir empfehlen, dass „Vorabkontrollen“ bei jedem die Gesamtbevölkerung betreffenden System in einem Mitgliedstaat durchgeführt werden, insbesondere im öffentlichen Sektor – aber (i) bevor diese in Stein gemeißelt sind (d. h., damit sollte in der frühen Planungsphase begonnen werden) und (ii) von besser (technisch) qualifizierten Mitarbeitern. Es ist beachtenswert, dass die australische Regierung vor kurzem vorgeschlagen hat, dass der dortige Beauftragte für den Schutz der Privatsphäre die Befugnis erhalten soll, von den staatlichen Behörden die Ausarbeitung einer Datenschutz-Folgeabschätzung (Privacy Impact Assessment) (Australia report, 8.2) zu verlangen. Im Privatsektor könnten diese Rolle Datenschutzkontrollen oder (wirkliche und effektive) Datenschutzgütesiegel übernehmen – stark gefördert dadurch, dass die Vorschriften für die öffentliche Auftragsvergabe datenschutzkonformen Produkten und Dienstleistungen einen Wettbewerbsvorteil einräumen (wie dies in Schleswig-Holstein in Deutschland bereits der Fall ist). Wir werden auf letzteren Vorschlag in Unterabschnitt V.8 über *Zusätzliche*

und alternative Maßnahmen noch zurückkommen. Ganz allgemein sind wir der Ansicht (ohne hier vorschnell urteilen zu wollen), dass darüber nachgedacht werden könnte, die bisher bei den DPAs liegende Zuständigkeit für die Durchsetzung der Vorschriften, weitgehend den Gerichten und für die Strafverfolgung zuständigen Behörden zu übertragen.

7. RECHTE UND RECHTSBEHELFE FÜR EINZELPERSONEN

109. **Ergebnis/Schlussfolgerung:** Eine der wichtigsten Anforderungen an eine neue Datenschutzregelung in EU/EWR (und darüber hinaus) ist die Stärkung von Einzelpersonen, insbesondere durch die Beseitigung von Hindernissen bei Rechtsstreitigkeiten wie etwa Kostenregelungen in manchen Ländern (vor allem England), welche Klagen für Einzelpersonen effektiv unmöglich machen.³²
110. **Empfehlungen:** Einzelpersonen sollte es ermöglicht werden, effektiven Schadenersatz sowie einstweilige und dauerhafte gerichtliche Verfügungen zu erwirken, und zwar in raschen, einfachen und kostengünstigen Verfahren vor kompetenten, unabhängigen und unparteiischen Gerichten. Während, nach dem Subsidiaritätsprinzip, die Details solcher Rechtsbehelfe den Mitgliedsstaaten überlassen werden sollten, sollte das grundsätzliche Recht auf derartige Rechtsbehelfe genauer verdeutlicht werden, als es derzeit der Fall ist. Insbesondere die Grundanforderungen, die zu erfüllen sind, um die Effektivität des unter Artikel 22 erwähnten „Rechtsbehelfs“ wirklich zu gewährleisten, sollten in der AG 29 diskutiert werden. Die AG 29 sollte zudem diesbezügliche Orientierungshilfen veröffentlichen, während die Kommission, in Übereinstimmung mit unseren Empfehlungen unter Unterabschnitt V.4.C (insbesondere Abs. 94), nicht zögern sollte, bei Nichterfüllung dieser Anforderungen Durchsetzungsmaßnahmen zu ergreifen.
111. Wir sind der Ansicht, dass es auch stärker in Erwägung gezogen werden sollte, Einzelpersonen in dieser Hinsicht unter die Arme zu greifen, indem es Nichtregierungs-/zivilgesellschaftlichen Organisationen ermöglicht wird, derartige Verfahren zu unterstützen oder sich an diesen formell zu beteiligen, oder im Namen von Gruppen von betroffenen Personen zu handeln, ohne wiederum das Risiko exorbitant teurer Urteile einzugehen (wenn zur Vermeidung lästiger Rechtsstreitigkeiten nötig, nach Prüfungen oder Erlaubnis vonseiten des Gerichts). Vollwertige „Sammelklagen“, wie sie in den USA möglich sind, sind in europäischen Rechtssystemen zwar kaum vorgesehen, manchmal sind jedoch recht ähnliche Vorgehensweisen verfügbar und wir sind der Ansicht, dass diese für Einzelpersonen potentiell von größerem Nutzen sind als die schwache Unterstützung, die betroffene Personen vonseiten der DPAs erhalten. Eine separate Studie zu den Verfahren und Rechtsbehelfen, die Einzelpersonen und NGOs zur Verfügung gestellt werden könnten und sollten, wäre im Rahmen jeder Überarbeitung der Richtlinie nützlich. Solch eine Studie könnte auch ungewöhnlichere, aber möglicherweise nützliche, Regelungen prüfen, wie etwa das in den USA

³² Zu diesem Problem siehe die Consultation Response der Foundation for Information Policy Research (FIPR) zum Civil Litigation Costs Review, welches im Juli 2009 von Lord Jackson durchgeführt wurde und Folgendes angab: „Soweit wir dies in Erfahrung bringen konnten, hat es den Anschein, dass England für uns Bürger wohl der schlechteste Ort zur Durchsetzung unserer digitalen Rechte ist.“ (Übersetzung V.G/S.H.) Das Dokument spricht sich, zumindest in Menschenrechtsfällen (was Datenschutzfragen einschließen würde), für weniger beschwerliche Regelungen für Einzelkläger/-innen (oder diese unterstützende NGOs) aus, wie es sie in anderen Ländern wie etwa Deutschland gibt. Das Dokument ist verfügbar unter: <http://www.fipr.org/090730jackson.pdf>.

EUROPÄISCHE KOMMISSION – GD JLS
**VERSCHIEDENE ANSÄTZE ZUR BEWÄLTIGUNG NEUER HERAUSFORDERUNGEN FÜR DEN
SCHUTZ DER PRIVATSPHÄRE, INSBESONDERE AUFGRUND TECHNOLOGISCHER
ENTWICKLUNGEN**

Schlussbericht

verfügbare „Qui Tam“-Verfahren (näher beschrieben im Country Report zu diesem Land). Natürlich sollte solch eine Studie anerkennen, dass primär die Mitgliedsstaaten entscheiden, wie Richtlinien umgesetzt werden sollen. Es ist jedoch vielleicht hilfreich, genauer über die Vorteile und Nachteile und die Effektivität oder Ineffektivität verschiedener solcher Verfahren Bescheid zu wissen.

112. Auch die Festlegung einer standardisierten, pauschalierten Schadenersatzleistung für die Verletzung der Rechte einer Person sollte in Betracht gezogen werden. Diese Schadenersatzleistung muss höher sein als die Kosten für die Nichteinhaltung.
113. Außerdem sind kostenfreie und einfache Systeme für den Schutz der Rechte von betroffenen Personen in speziellen Kontexten, wie etwa Direktmarketing, effektiv und erfreuen sich großer Beliebtheit. In den meisten EU/EWR-Staaten sowie in Neuseeland, Südkorea, Australien und Indien gibt es Präferenzdienste für Post, Fax und Telefon. Die USA bieten eine Website zum kostenlosen Abruf von Verbraucherberichten an, welche sehr beliebt ist. In der „Nicht anrufen“-Liste des Systems finden sich nun, für den Bereich des Telemarketings, 160 Millionen Telefonnummern. Derartige Systeme erfreuen sich auf der ganzen Welt großer Beliebtheit, da sie gut beworben werden, leicht zu benutzen sind und effektive Abhilfe gegen den Erhalt unerwünschter Briefe, Faxe, Anrufe oder SMS zu Werbezwecken bieten (auch wenn die Daten der betroffenen Personen notwendigerweise auf den relevanten Unterdrückungslisten gespeichert werden müssen und die Systeme die Personen damit nicht davor schützen, „eingetragen“ zu werden.)

8. ZUSÄTZLICHE UND ALTERNATIVE MASSNAHMEN

114. In diesem letzten Abschnitt möchten wir einige Maßnahmen kritisch beleuchten, welche, wie manche glauben, eine Alternative zu den vorhandenen Mitteln zur Gewährleistung der Einhaltung der Datenschutzgesetze und –grundsätze darstellen oder diese ergänzen können. Manche dieser Maßnahmen sind schon seit einem Jahrzehnt oder einem noch längeren Zeitraum durchaus bekannt und manche werden von der Richtlinie selbst gefördert. Es hat jedoch den Anschein, dass bis jetzt keine ausreichenden Anreize für deren Anwendung durch die für die Verarbeitung Verantwortlichen geschaffen wurden – trotz der Forderung der Richtlinie nach „geeigneten technischen und organisatorischen Maßnahmen [...], die für den Schutz [...] personenbezogener Daten erforderlich sind“ (Artikel 17(1)). Außerdem erzielen sie oft auch nicht den gewünschten Erfolg. Wir werden der Reihe nach sowohl den potentiellen Nutzen als auch die Grenzen – und die häufig trügerischen, oder gebrochenen, Versprechungen – der folgenden Maßnahmen behandeln:

- ✓ **Technologien zur Verbesserung des Datenschutzes (PETs)**, einschließlich der Verschlüsselung (als ein Mittel zur Sicherstellung, dass zumindest die Datensicherheitsanforderungen eingehalten werden) und des damit verbundenen Problems der Benachrichtigung über Sicherheitsverletzungen; der Ent-Identifizierung; sowie anderer, wie etwa P3P, und Systeme für den Zugriff der betroffenen Personen.

EUROPÄISCHE KOMMISSION – GD JLS
**VERSCHIEDENE ANSÄTZE ZUR BEWÄLTIGUNG NEUER HERAUSFORDERUNGEN FÜR DEN
SCHUTZ DER PRIVATSPHÄRE, INSBESONDERE AUFGRUND TECHNOLOGISCHER
ENTWICKLUNGEN**

Schlussbericht

- ✓ **Datenschutzfreundliches Identitätsmanagement**, einschließlich der (heute weitgehend veralteten) zentralisierten Systeme, der aktuelleren „nutzerorientierten“ Systeme, der „Vendor Relationship Management“-Systeme und der Verwendung von Identitätskarten zu verschiedenen Zwecken.
- ✓ **Eingebauter Datenschutz**, einschließlich der Durchführung von Datenschutz-Folgenabschätzungen;
- ✓ **Datenschutzkontrollen der Nutzer/-innen und Standardeinstellungen**;
- ✓ **Sektorielle Selbst- und Ko-Regulierung**; und
- ✓ **Datenschutz-Gütesiegel**.

(i) Technologien zur Verbesserung des Datenschutzes (PETs):

Verschlüsselung

115. Eine junge technologische Entwicklung, welche dabei helfen kann, zumindest manche Datenschutzerfordernungen zu erfüllen, ist die Verfügbarkeit von Verschlüsselung, und von damit verbundenen Informationssicherheits-Mechanismen. Im Jahr 1990 wurde die Verschlüsselung außerhalb von Regierungen und der Finanzdienstleistungsindustrie kaum zum Schutz von Daten verwendet. Heute ist sie in jeden Webbrowser integriert, um die sichere Übermittlung von Zahlungskarteninformationen im elektronischen Geschäftsverkehr zu ermöglichen; und die meisten E-Mail-Programme erlauben die Verschlüsselung der Nachrichten vor der Übermittlung. Dennoch werden durch Malware und aufgrund des unzureichenden Schutzes auf den Servern immer noch Zahlungskarteninformationen von den eigenen Computern der Nutzer/-innen gestohlen. Die E-Mail-Verschlüsselung wird von Einzelpersonen und von den meisten Unternehmen nur sehr selten verwendet, was zum Teil auf das „Henne und Ei“-Problem zurückzuführen ist, dass die Verschlüsselung nur dann funktioniert, wenn sie sowohl vom Sender als auch vom Empfänger der Nachricht unterstützt wird.
116. Die gängigen Betriebssysteme wie Microsoft Windows, Linux und Apples MacOS erlauben die Verschlüsselung der gespeicherten Daten, was das Risiko verringert, dass Diebe auf die Daten auf gestohlenen Computern und Wechseldatenträgern wie CDs und USB-Sticks zugreifen können. Dies ist besonders wichtig bei mobilen Geräten und Laptops, die leicht verloren gehen oder gestohlen werden und auf deren Daten ansonsten einfach zugegriffen werden könnte. Für „Cloud“-Internetdienste (wie Google Docs) wäre es möglich, Daten nur verschlüsselt zu speichern und sogar zu verarbeiten und damit sicherzustellen, dass der Zugriff den Eigentümern der Daten vorbehalten bleibt. Es bedarf jedoch noch weiterer Forschung zur „sicheren Datenverarbeitung durch Dritte“ und zu anderen Methoden für die Verbesserung des Schutzes von in Cloud-Diensten gespeicherten Daten.
117. Natürlich muss die Verschlüsselung aktiviert und richtig konfiguriert sein, um die Daten vor unerlaubtem Zugriff sowie unerlaubter Veränderung zu schützen. Einige der schwerwiegendsten Verletzungen des Schutzes personenbezogener Daten der letzten Jahre waren auf fehlende oder falsch konfigurierte Datensicherheitsmaßnahmen zurückzuführen. Dies war etwa der Fall, als die Regierung des Vereinigten Königreichs

EUROPÄISCHE KOMMISSION – GD JLS
**VERSCHIEDENE ANSÄTZE ZUR BEWÄLTIGUNG NEUER HERAUSFORDERUNGEN FÜR DEN
SCHUTZ DER PRIVATSPHÄRE, INSBESONDERE AUFGRUND TECHNOLOGISCHER
ENTWICKLUNGEN**

Schlussbericht

im Jahr 2007 die Aufzeichnungen zum Kindergeld von 25 Millionen Personen verlor und als in den Jahren 2003 und 2006 die finanziellen Daten von mehreren Millionen Kunden/-innen der TJX Companies kompromittiert wurden. Diese Verletzungen demonstrierten auch die schwachen organisatorischen Praktiken beim allgemeinen Systementwurf und -management.

118. Die Verschlüsselung schützt auch nicht davor, dass die verschlüsselten Daten von privaten oder öffentlichen Organisationen zum Zwecke der Werbung oder der Erstellung von „Profilen“ verwendet werden, oder dass sie von „Insidern“ mit Zugriffsberechtigung für die unverschlüsselten Informationen missbraucht werden. Der Datenschutzbeauftragte des Vereinigten Königreichs belegte, dass es einen erheblichen kriminellen Markt für personenbezogene Daten gibt, die durch die Korruption oder Täuschung von Personal gestohlen werden, das am Arbeitsplatz über legitimen Zugriff auf große Datenbanken verfügt. Die Verschlüsselung ist bei Weitem kein Allheilmittel im Bereich des Datenschutzes.

Ein damit verbundenes, spezielles Problem: die Benachrichtigung über Sicherheitsverletzungen

119. Wir sind der Ansicht, dass die Benachrichtigung über Sicherheitsverletzungen weniger eine Frage der Rechtsbehelfe ist, sondern eher eine Ergänzung des Sicherheitsgrundsatzes, da sie die Pflichten der für die Verarbeitung Verantwortlichen im Falle einer Sicherheitsverletzung erweitert, indem sie diese dazu verpflichtet, unter gewissen Umständen die DPAs und die betroffenen Personen zu benachrichtigen.. Ein Verstoß gegen die Anforderungen der Benachrichtigung über Sicherheitsverletzungen sollte wie ein Verstoß gegen den Datenschutzgrundsatz betrachtet werden, mit allen sich daraus ergebenden Folgen. Das heißt, dass sie nicht als Rechtsbehelf gesehen werden sollte, wie dies manchmal vorgeschlagen wird. Eine effektive Benachrichtigung über Sicherheitsverletzungen würde jedoch dazu beitragen, die Effektivität der vorhandenen Rechtsbehelfe zu erhöhen.

Ent- und Re-Identifizierung

120. Prinzipiell möchte man meinen, dass die Ent-Identifizierung oder Anonymisierung personenbezogener Daten durch die für die Verarbeitung Zuständigen das Risiko des Missbrauchs verringern kann. In der Praxis traf dies jedoch, selbst im „alten“ Umfeld, nur im Rahmen eines fortlaufenden Schutzes zu, welcher dem Schwierigkeitsgrad der Re-Identifizierung der betroffenen Personen angemessen war. Darin beinhaltet waren strenge Zugriffsbeschränkungen für die vollständigen Datenbestände, Kontrollen von Abfragen, die einzelne Datensätze kollektiv re-identifizieren können sowie die Anerkennung, dass organisatorische Mängel, Sicherheitslücken und politische Kursänderungen allesamt die Umkehrung der Mechanismen zur Ent-Identifizierung zur Folge haben könnten. Selbst heutzutage ist die Ent-Identifizierung schwer zu erreichen.
121. Im neuen sozio-technischen globalen Umfeld, welches Working paper No. 1 beschreibt, ist die Identifizierung von betroffenen Personen, durch die verbreitete Verfügbarkeit von Datenbeständen zur Bevölkerung wie etwa Wählerverzeichnissen, Kreditauskünften und sozialen Netzwerken, häufig bzw. für gewöhnlich ein Leichtes, selbst nach der Entfernung offensichtlicher personenbezogener Daten wie Namen, Geburtsdaten oder Postleitzahlen. Die Fortschritte in der Informatik zeigen, dass wir

EUROPÄISCHE KOMMISSION – GD JLS
**VERSCHIEDENE ANSÄTZE ZUR BEWÄLTIGUNG NEUER HERAUSFORDERUNGEN FÜR DEN
SCHUTZ DER PRIVATSPHÄRE, INSBESONDERE AUFGRUND TECHNOLOGISCHER
ENTWICKLUNGEN**

Schlussbericht

den Punkt bereits weit überschritten haben, an dem „anonymisierte“ Datenbestände wie etwa Aufzeichnungen über Suchanfragen, Filmbewertungen oder in Anspruch genommene medizinische Behandlungen ohne potentielle Datenschutzverletzungen der breiten Masse zugänglich gemacht werden konnten. Paul Ohm drückt es folgendermaßen aus: „Die Anonymisierung ist ein gebrochenes Versprechen und kann in dem neuen Umfeld die Privatsphäre nicht schützen.“³³ (Übersetzung V.G/S.H.) Wie bereits unter Abschnitt IV.A (Abs. 47) erwähnt, sind wir der Ansicht, dass die ernststen Probleme, die sich aus der beinahe unmöglichen vollständigen Anonymisierung personenbezogener Daten im neuen sozio-technischen globalen Umfeld ergeben, einige der größten Herausforderungen an den Datenschutz stellen und dass diese bei jeder Diskussion über eine Überarbeitung der Datenschutzregelung zentrale Themen darstellen sollten. Bis dahin sollte der Grundansatz darin bestehen, die Erhebung und sogar die anfängliche Speicherung personenbezogener Daten auf das absolute Minimum zu reduzieren. (Vgl. den deutschen – aber auch europäischen – Grundsatz der „Datenminimierung“ und den australischen „Grundsatz der Anonymität“ (anonymity principle)): Sobald Daten einmal erhoben und gespeichert wurden, ist es fast unmöglich, sie zu beseitigen oder (um Ohms Äußerung aufzugreifen) wirklich, dauerhaft zu anonymisieren.

Andere PETs (P3P, Online-Zugriff der betroffenen Personen, Sonstige)

122. Abseits der sicheren Datenspeicherung und -übermittlung wurden auch Technologien zur Verbesserung des Datenschutzes (PETs) entwickelt, welche die bessere technologische Durchsetzung des Datenschutzgesetzes ermöglichen. Diese können sowohl die Transparenz der Verarbeitung erhöhen als auch die für bestimmte Funktionen nötigen personenbezogenen Daten verringern oder beseitigen – wodurch sie das Risiko des Diebstahls durch Insider in Organisationen und der Wiederverwendung der Daten für unerwartete Zwecke reduzieren. Sie haben jedoch alle ihre Grenzen. Im Folgenden möchten wir einige dieser Technologien behandeln:

P3P:

123. Die wesentlichen PETs können die Informationen über die Verarbeitung, welche von den Zuständigen durchgeführt wird, automatisch weitergeben, und zwar mit Software, die den betroffenen Personen dabei hilft, diese Informationen leichter zu verstehen als durch das Lesen komplizierter legalistischer Datenschutzerklärung. Eines dieser Systeme, welches in den späten 1990ern entwickelt wurde, war das Platform for Privacy Preferences Project (P3P). Die Artikel 29 Datenschutzgruppe hat angemerkt, dass auf einer durchsetzbaren Rechtsgrundlage Folgendes der Fall ist: „P3P kann dazu beitragen, Datenschutzhinweise zu normen. Dies bietet zwar an sich noch keinen Schutz der Privatsphäre, könnte aber, einmal eingeführt, die Transparenz stark fördern und Maßnahmen zu einem besseren Schutz der Privatsphäre unterstützen.“³⁴ P3P wurde jedoch von Aktionsgruppen als ein „kompliziertes und verwirrendes Protokoll, das den Schutz der Privatsphäre für Internetnutzer/-innen erschwert“³⁵ (Übersetzung V.G/S.H.) kritisiert. Sein Wert bleibt damit zweifelhaft.

³³ Paul Ohm, Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization (Fußnote 14, oben).

³⁴ WP 37, angenommen am 21. November 2000

³⁵ Electronic Privacy Information Center and Junkbusters (2000), Pretty Poor Privacy: An Assessment of P3P and Internet Privacy. Available at <http://epic.org/reports/pretypoorprivacy.html>.

Online-Zugriff der betroffenen Personen:

124. Das in der Richtlinie erwähnte Auskunftsrecht muss von den betroffenen Personen für gewöhnlich anhand eines teuren und zeitaufwändigen Briefwechsels mit den für die Verarbeitung Zuständigen wahrgenommen werden. Werkzeuge für den Online-Zugriff der betroffenen Personen können es ausreichend authentifizierten Personen erlauben, all die Daten zur eigenen Person einzusehen, über die die für die Verarbeitung Zuständigen verfügen. Aus nachvollziehbaren Sicherheitsgründen speichern Organisationen jedoch häufig einige personenbezogene Daten offline. Äußerst besorgniserregend ist auch die Tatsache, dass Einzelpersonen dazu gezwungen (oder einfach überredet) werden können, Zugriff auf die Daten Dritter, wie etwa Arbeitgeber oder Eltern, zu gewähren. Ohne Garantien gegen derartigen Missbrauch stellt der Online-Zugriff der betroffenen Personen eher eine Gefahr als eine Hilfe dar.

Sonstige:

125. Technisch höherentwickelte PETs bieten unerwartete Fähigkeiten, wie etwa anonyme Kommunikation über das öffentliche Internet; elektronisches Geld, das sich der Anonymität des Geldes in der physischen Welt annähert; und anonyme Referenzen, die belegen, dass eine Person über eine Zugriffsberechtigung für bestimmte Ressourcen verfügt, ohne ihre Identität preiszugeben. In einer Mitteilung (COM/2007/0228) aus dem Jahr 2007 fordert die EU-Kommission die Industrie, die Aufsichtsbehörden und die staatlichen Behörden dazu auf, die Konsumenten besser aufzuklären und häufiger PETs einzusetzen, denn dadurch *„verspricht sich die Kommission sowohl einen besseren Schutz der Privatsphäre als auch eine einfachere Einhaltung der Datenschutzbestimmungen [...] [und] eine sinnvolle Ergänzung zum geltenden Rechtsrahmen und seinen Durchführungsvorschriften.“* Es stellt jedoch immer noch eine Herausforderung dar, diese Technologien in nutzbarer Form in Programmen für den Massenmarkt einzusetzen.

(ii) Datenschutzfreundliches Identitätsmanagement

126. Das Identitätsmanagement ist ein florierender technologischer Bereich, der darauf abzielt, die Internetnutzer/-innen bei der Handhabung ihrer Beziehungen zu Dienst Anbietern zu unterstützen, insbesondere durch den Nachweis, dass eine Person das Zugriffsrecht für bestimmte Ressourcen (wie etwa für ein Kundenkonto) hat. Diese Technologien haben einen entscheidenden Einfluss auf den Datenschutz und können so gestaltet werden, dass sie die Verfolgung und zentralisierte Überwachung aller Online- und Offline-Tätigkeiten einer Person erleichtern. Sie können, alternativ dazu, auch die personenbezogenen Daten, die an Zweit- und Drittparteien preisgegeben werden, stark minimieren und es so den Einzelpersonen erlauben, im Internet denselben Grad an Privatsphäre zu genießen wie in der Offline-Welt.
127. Eine Vielzahl an Lösungen wurde bereits vorgeschlagen. Bei den anfänglichen zentralisierten Systemen (wie Microsofts Passport) bestanden bedeutende potentielle Datenschutzprobleme wie etwa ein Sammelpunkt für die Überwachung der Nutzer/-innen und ein persistenter Identifikator, welcher zur Verbindung der Nutzerinformationen über verschiedene Dienstanbieter hinweg verwendet werden konnte. Passport wurde teilweise aufgrund der Datenschutzbedenken für Kunden/-innen eingestellt. Die jüngeren „Einmalanmeldungs-“ oder „föderativen“ Systeme zum

EUROPÄISCHE KOMMISSION – GD JLS
**VERSCHIEDENE ANSÄTZE ZUR BEWÄLTIGUNG NEUER HERAUSFORDERUNGEN FÜR DEN
SCHUTZ DER PRIVATSPHÄRE, INSBESONDERE AUFGRUND TECHNOLOGISCHER
ENTWICKLUNGEN**

Schlussbericht

Identitätsmanagement wie etwa Open ID leiden auch noch an manchen dieser Probleme, werden jedoch von Unternehmen wie Yahoo! und Google weitgehend unterstützt.

128. Besseren Schutz der Privatsphäre bieten „nutzerorientierte“ Systeme zum Identitätsmanagement wie etwa Microsofts CardSpace, IBMs Idemix und die Projekt-Prototypen des 6. Europäischen Rahmenforschungsprogramms Datenschutz- und Identitätsmanagement für Europa (PRIME). Diese Systeme erlauben den Nutzern/-innen die Kontrolle ihrer eigenen identifizierenden Informationen und minimieren die von den Dienst Anbietern benötigten personenbezogenen Daten. Sie verhindern, dass mehrere Organisationen die Informationen über bestimmte Einzelpersonen in Verbindung bringen und erlauben es den Nutzern/-innen, anonyme „Referenzen“ anzugeben, die verschiedene Merkmale beweisen (wie etwa die Berechtigung, ein Fahrzeug zu lenken oder altersabhängige Produkte zu kaufen) ohne dabei irgendwelche identifizierenden Informationen preiszugeben. CardSpace ist nun zwar in den neuen Versionen von Microsofts Betriebssystem und Webbrowser integriert, wird aber bis jetzt von den Dienst Anbietern nur in Maßen unterstützt. Somit werden diese Technologien derzeit sehr selten genutzt. Wir sind der Ansicht, dass ihre zukünftige Akzeptanz vielleicht von erheblicher Koordinierung, Standardisierung und möglicherweise der Auftragsvergabe vonseiten der Regierung abhängt, um die nötigen Anreize für Konsumenten/-innen, Unternehmen und Systementwickler/-innen zu schaffen.
129. Vendor Relationship Management (VRM) ist ein verwandtes Konzept, das Einzelpersonen bei der Handhabung ihrer Beziehungen zu und ihres Datenaustausches mit Unternehmen unterstützt und nicht den umgekehrten Weg geht, wie das bei Customer-Relationship Management-Systemen der Fall ist. VRM-Systeme, welche es den Nutzern/-innen erlauben, die Daten auf ihren eigenen Computern zu sichern, schützen die Privatsphäre besser als jene, die die Daten auf zentralen Servern speichern. Diese Systeme befinden sich jedoch noch in einer frühen Entwicklungsphase.
130. Viele Länder mit nationalen Identitätssystemen ergänzen die Karten zur Unterstützung der Online-Interaktionen von Nutzern/-innen mit der Regierung und manchmal dem Privatsektor um Funktionen zum Identitätsmanagement. Die einfachsten Systeme erlauben es den Nutzern/-innen, den Besitz einer Karte und der dazu gehörenden nationalen Identitätsnummer physisch und aus der Ferne zu „beweisen“, mit all den Datenschutzauswirkungen, die sich aus der Verwendung eines langfristigen allgemeinen Identifikators ergeben. Manche Karten weisen Datenschutzmerkmale auf, wie zum Beispiel eine Zugriffskontrolle (nur Autorisierte dürfen die Karteninformationen verwenden), die Verwendung domänenspezifischer Identifikatoren (die es verhindern, dass personenbezogene Aufzeichnungen zufällig über verschiedene Regierungsabteilungen hinweg verbunden werden) und die selektive Weitergabe von Informationen, welche an die bestimmte Anwendung angepasst ist. Österreich und Deutschland haben derartige Datenschutzmaßnahmen in ihre nationalen Karten am stärksten integriert. Doch auch diese weisen noch inhärente Schwächen auf. Es sollte vielleicht hinzugefügt werden, dass die nationalen Systeme, ohne Standardisierung auf europäischer Ebene, wahrscheinlich keine Auswirkungen auf den Weltmarkt haben werden.

(iii) Datenschutz-Folgenabschätzungen und eingebauter Datenschutz

131. Sowohl die Technologien zur Verbesserung des Datenschutzes als auch das datenschutzfreundliche Identitätsmanagement haben erhebliches Potential für den Schutz der Privatsphäre von Einzelpersonen. Am allerwichtigsten ist es jedoch, die politischen Entscheidungsträger und Wirtschaftsführer davon zu überzeugen, den Auswirkungen neuer Informationssysteme auf den Datenschutz angemessene Beachtung zu schenken, bevor diese in Auftrag gegeben werden. Die Anzahl der erhobenen und verarbeiteten personenbezogenen Daten kann von Details entscheidend beeinflusst werden, welche beschlossen wurden lange bevor die Systemarchitekten/-innen und Programmierer/-innen die Arbeit an neuen Datenbankanwendungen aufnehmen. Es ist weitaus einfacher, datenschutzfreundliche Systeme zu erstellen, wenn Datenschutzangelegenheiten, mit dem Hauptaugenmerk auf der Datenminimierung und Sicherheit, in einer frühen Planungsphase berücksichtigt werden. Gravierende Datenschutzverletzungen können sich aus Systemen ergeben, die sensible personenbezogene Daten über mehrere Millionen oder mehrere zehn Millionen Personen beinhalten, hunderttausenden Mitarbeitern/-innen den Zugriff gewähren und eine lange Speicherfrist vorsehen. Dies lässt sich bei zahlreichen E-Government-Anwendungen beobachten und ist im Nachhinein äußerst schwer zu beheben.
132. Zwei bestimmte Versuche zur Förderung der frühen Einplanung des Datenschutzes durch Organisationen sollten erwähnt werden. Datenschutz-Folgenabschätzungen (PIAs) sind nun in vielen gerichtlichen Zuständigkeiten einschließlich der USA obligatorisch und verpflichten staatliche Behörden zur Abschätzung der Datenschutzrisiken neuer Strategien, bevor Systeme in Auftrag gegeben werden. Wie bereits erwähnt, plant auch die australische Regierung den dortigen Beauftragten für den Schutz der Privatsphäre dazu zu ermächtigen, von staatlichen Behörden PIAs zu verlangen. Der Datenschutzbeauftragte des Vereinigten Königreichs regt die Regierung und Unternehmen zur Durchführung von Abschätzungen an, um Datenschutzbedenken schon am Beginn von Projekten anzugehen. Dabei soll das Hauptaugenmerk auf einem systematischen Vorgehen liegen, bei welchem die Risiken gehandhabt und die Ansichten aller von den neuen Systemen Betroffenen mit einbezogen werden. Der eingebaute Datenschutz ist ein Ansatz, der ursprünglich von Ontarios Beauftragtem für den Schutz der Privatsphäre entwickelt wurde und der die Erstellung und den Betrieb von Systemen unterstützt, welche die Erhebung, Sicherung, Verarbeitung und Vorratsspeicherung personenbezogener Daten minimieren. Dies umfasst sowohl Unternehmenspolitik und -praktiken als auch die Details der verwendeten Technologien. Bei diesem Ansatz werden Datenschutz-Folgeabschätzungen während des gesamten Lebenszyklus eines Systems eingesetzt, von der anfänglichen Planung zum Betrieb, den Erweiterungen bis schließlich zur Stilllegung. Für die Effektivität der Methodik bedarf es der Unterstützung durch die oberen Führungskräfte, welche sicherstellen, dass die Datenschutzerfordernungen in die Geschäftsszenarien (Business Cases) für neue Systeme integriert und während des gesamten Lebenszyklus eingehalten werden.

(iv) Datenschutzkontrollen der Nutzer/-innen und Standardeinstellungen

133. Viele Internetseiten bieten den Nutzern/-innen detaillierte Informationen, und Kontrolloptionen, zu der Menge der erhobenen personenbezogenen Daten und der Art ihrer Verarbeitung. Das P3P-Protokoll wurde entworfen, um die Datenschutzpraktiken von Internetseiten detailliert an den Webbrowser zu übermitteln, doch Kontroversen in

EUROPÄISCHE KOMMISSION – GD JLS
**VERSCHIEDENE ANSÄTZE ZUR BEWÄLTIGUNG NEUER HERAUSFORDERUNGEN FÜR DEN
SCHUTZ DER PRIVATSPHÄRE, INSBESONDERE AUFGRUND TECHNOLOGISCHER
ENTWICKLUNGEN**

Schlussbericht

Bezug auf die Grundeinstellungen sowie andere Definitionsprobleme gehörten zu den Gründen für die nicht weitverbreitete Nutzung dieser Funktionen. Browser sind für gewöhnlich mit einer „Cookie Cutter“-Funktion für die Handhabung der mit den Internetseiten ausgetauschten Informationen ausgestattet, wobei manche Internetseiten den Zugriff bei vollständigem Blocken aller Cookies beschränken. Die Endnutzer/-innen verwenden die Funktionen zum Umgang mit Cookies nur in Grenzen und daher haben die (häufig großzügigen) Standardeinstellungen in Browsern erhebliche Auswirkungen auf das allgemeine Datenschutzniveau.

134. Die meisten Anbieter für Online-Marketing-Lösungen folgen den vom Internet Advertising Bureau erstellten Verhaltensregeln für „behavioural targeting“ von Werbung, welche festlegen, dass Nutzer/-innen sich gegen die Anzeige von Werbungen, die auf ihrem früheren Surfverhalten basieren, entscheiden können sollten. Google erlaubt es den Nutzern/-innen, ihr durch das Surfen im AdSense-Netzwerk erstelltes Interessensprofil zu aktualisieren. Soziale Online-Netze wie Facebook bieten detaillierte Optionen an, um den Zugriff auf einzelne Profile und freigegebene Inhalte zu beschränken, wobei in der Forschung herausgefunden wurde, dass diese Kontrollen oft schwer zu verwenden und nicht gut sichtbar sind. Die Starteinstellungen werden von den Nutzern/-innen selten geändert und haben deshalb starke Auswirkungen, weshalb die Artikel 29 Datenschutzgruppe in einer kurz zurückliegenden Stellungnahme (5/2009) vorschlägt, dass diese standardmäßig die Privatsphäre schützen sollten.
135. Im Allgemeinen ist die „Ermächtigung der Nutzer/-innen“ zwar seit den Anfängen des World Wide Web ein zentrales Thema in den Bemühungen zur Verbesserung des Online-Datenschutzes, für ungeschulte Nutzer/-innen sind diese Werkzeuge jedoch zu kompliziert. In der aktuellen Forschung im Bereich der Verhaltensökonomik wurde auch herausgefunden, dass wenige Menschen die Zeit oder die Lust für die Durchführung häufiger, detaillierter Risikoanalysen der abstrakten potentiellen Bedrohungen durch zukünftige Datenschutzverletzungen haben, wodurch die Effektivität dieser isolierten Lösungen beschränkt wird.

(iii) Sektorielle Selbst- oder Ko-Regulierung

137. Die Richtlinie fördert, unter Artikel 27, bereits die Verwendung von sektoriellen Verhaltensregeln, sowohl auf nationaler als auch auf europäischer Ebene. Die AG 29 hat ausführliche, nützliche Orientierungshilfen angeboten, und zwar zu den von derartigen Verhaltenskodizes zu beinhaltenden Angelegenheiten sowie zum „zusätzlichen Nutzen“, den diese Kodizes mit sich bringen sollten.³⁶ Der genaue Status von Kodizes, bei welchen man sich davon „überzeugt“ hat, dass sie den relevanten einzelstaatlichen Vorschriften entsprechen, ist nicht ganz geklärt: Die Richtlinie fordert nicht, dass deren Prüfung auf eine formelle „Anerkennung“ solcher Kodizes hinausläuft oder dass diese

³⁶ Siehe insbesondere das Arbeitsdokument WP29 Beurteilung der Selbstkontrolle der Wirtschaft: wann ist sie ein sinnvoller Beitrag zum Niveau des Datenschutzes in einem Drittland? (WP07 vom 14. Januar 1998). Dieses Dokument behandelt zwar die Frage, wann man den von Kodizes gebotenen Schutz für die Datenübertragung an Drittstaaten ohne angemessene Datenschutzgesetze als „angemessen“ bezeichnen kann, die Kriterien für derartige Kodizes sind jedoch genauso relevant für die Bewertung von Kodizes in den Mitgliedsstaaten sowie EU-weite Kodizes. Eine ausführliche Beleuchtung von Verhaltenskodizes findet sich in: Douwe Korff, Data Protection Law In Practice In The EU, FEDMA/DMA, Brüssel/New York, 2005, S. 159 – 166; Der Text oben bezieht sich auf dieses Kapitel des Buches.

EUROPÄISCHE KOMMISSION – GD JLS
**VERSCHIEDENE ANSÄTZE ZUR BEWÄLTIGUNG NEUER HERAUSFORDERUNGEN FÜR DEN
SCHUTZ DER PRIVATSPHÄRE, INSBESONDERE AUFGRUND TECHNOLOGISCHER
ENTWICKLUNGEN**

Schlussbericht

irgendeine Art von formellem Status im Rechtssystem des Mitgliedsstaates erhalten. Die diesbezüglichen nationalen Praktiken unterscheiden sich. Deshalb ist in den Niederlanden die „Anerkennung“ eines Kodex durch die Datenschutzbehörde für die Gerichte nicht bindend, während in Irland eine stärkere formelle Integration der Kodizes in die gesetzlichen Regelungen möglich ist und diese rechtsverbindlich werden können. Doch unabhängig von seinem genauen Status wird ein Kodex, dessen Übereinstimmung mit den Gesetzen bestätigt wurde, eine bedeutende, zumindest quasi-legislative Funktion einnehmen. In diesem Sinne bestätigt die ausdrückliche Erwähnung solcher Kodizes in der Richtlinie einen allgemeineren Trend zur zunehmenden Vermischung gesetzlicher und sogenannter selbst-regulierender, jedoch effektiv quasi-legislativer, Bestimmungen³⁷. In dieser Hinsicht gehen somit Verhaltenskodizes nahtlos in formellere Systeme ergänzender Bestimmungen, wie etwa die von der französischen Datenschutzbehörde erlassenen „vereinfachten Bestimmungen“, über. Im öffentlichen Sektor stehen tendenziell eher die ergänzenden Regelungen im Vordergrund, im Privatsektor eher die Verhaltenskodizes (wobei im Vereinigten Königreich – umstrittenerweise – unverbindliche Verhaltenskodizes und „Protokolle“ auch im öffentlichen Sektor, und in Verbindung mit dem Datenaustausch zwischen öffentlichen bzw. zwischen öffentlichen und privaten Behörden, weitverbreitet sind). In jedem Fall sind die Regelungen häufig das Ergebnis enger Zusammenarbeit zwischen den Aufsicht führenden Behörden (Ministerien, Datenschutzbehörden, etc.) und den betroffenen Sektoren, wobei für gewöhnlich (aber leider nicht immer) auch Vertretungen anderer Interessensgruppen (eigentlich häufig die wichtigsten Interessensgruppen), wie Konsumenten/-innen, Patienten/-innen, etc., einen Beitrag leisten.

138. Der Ansatz der AG 29 in Bezug auf Kodizes wurde auf die aktuellsten Systeme ähnlicher Maßnahmen auf Unternehmensebene, die „verbindlichen unternehmensinternen Vorschriften“ (BCRs) übertragen.³⁸
139. Dies ist nicht der richtige Rahmen, um zu analysieren, ob derartige selbst- (oder quasi-selbst-) regulatorischen Maßnahmen, Verhaltenskodizes oder BCRs im Allgemeinen nützlich sind oder nicht. Es reicht wohl, zu bemerken, dass diese Vorgehensweise auf europäischer Ebene nur begrenzt angenommen wurde, wobei der European Code of Practice for the Use of Personal Data in Direct Marketing der FEDMA das größte positive Beispiel darstellt (obwohl selbst hier, nach jahrelangen Diskussionen, die zusätzlichen Regelungen zur Werbung für Minderjährige noch nicht verabschiedet oder unterschrieben wurden). Tatsächlich wurden die Langsamkeit und die akribische Detailgenauigkeit der AG 29 und der Kommission von der Industrie kritisiert und als der Hauptgrund für die geringe Zahl an vorgelegten Kodex-Entwürfen zur Genehmigung genannt. Verbindliche unternehmensinterne Vorschriften wurden von den nationalen DPAs vor allem in Bezug auf die Personaldaten multinationaler Unternehmen zur Genehmigung vorgelegt. Diese haben bisher anderen Betroffenen, wie etwa Kunden/-innen, kaum Schutz gewährt.

³⁷ Siehe den (vom Teamleader der vorliegenden Studie entworfenen) Abschnitt über „*Regulatory Trends and New Media*“ in der Studie der Kommission: The Future of Media and Advertising (Zukunft von Medien und Werbung) (die für gewöhnlich als Admedia-Studie bezeichnet wird), DG XIII/E, November 1995, Abschnitt D.1.

³⁸ Siehe das Arbeitsdokument der AG 29: Übermittlung personenbezogener Daten in Drittländer: Anwendung von Artikel 26 Absatz 2 der EU-Datenschutzrichtlinie auf verbindliche unternehmensinterne Vorschriften für den internationalen Datentransfer (WP77 vom 3. Juni 2003).

EUROPÄISCHE KOMMISSION – GD JLS
**VERSCHIEDENE ANSÄTZE ZUR BEWÄLTIGUNG NEUER HERAUSFORDERUNGEN FÜR DEN
SCHUTZ DER PRIVATSPHÄRE, INSBESONDERE AUFGRUND TECHNOLOGISCHER
ENTWICKLUNGEN**

Schlussbericht

140. Außerhalb von EU/EWR waren Kodizes in Australien und Hongkong von sehr beschränkter Bedeutung. In Japan hingegen spielten und spielen einige sektorielle „Leitlinien“ (z.B. METI-Leitlinien) eine entscheidende Rolle. Diese werden jedoch innerhalb des Sektors nur begrenzt entwickelt und eher vom Ministerium verhängt.
141. Wir sind der Ansicht, dass, auf der einen Seite, sektorielle oder unternehmensinterne Regelungen gefördert werden sollten: Sie helfen deutlich zu machen, wie die oft vagen und komplexen Regelungen in den Richtlinien auf konkrete Situationen angewandt werden sollten. Auf der anderen Seite sollten sie nicht verwendet werden, um es den für die Verarbeitung Verantwortlichen oder Gruppen von für die Verarbeitung Verantwortlichen zu ermöglichen, die Grundanforderungen der Richtlinien effektiv zu umgehen, indem sie die Regelungen in den europäischen Instrumenten „kreativ“ auslegen oder dehnen. Wir sind der Ansicht, dass aus diesem Grund der Entwurf solcher Regelungen erhebliche Anstrengungen und Beratungen – und damit Zeit – benötigen wird. Bei jeder Überarbeitung der Basisrichtlinie wäre jedoch die Frage diskussionswürdig, wie dieser Vorgang effizienter, und insbesondere weniger aufwändig für die AG 29, gestalten werden kann. Vielleicht kann das bei dem, im nächsten Unterabschnitt behandelten, europäischen Datenschutz-Gütesiegel verwendete System weiterhelfen: Bei diesem System werden die vorbereitenden Arbeiten von anerkannten unabhängigen Experten/-innen durchgeführt (die von den betroffenen Privatparteien, im Fall von Kodizes also von der Industrie, bezahlt werden). Deren Arbeit wird genau geprüft und (falls dies positiv ausfällt) von einer amtlichen Stelle, unter Einbeziehung nationaler Datenschutzbehörden, genehmigt. Wie im nächsten Unterabschnitt erwähnt wird, wäre es wohl eine Überlegung wert, eine spezielle Abteilung der Datenschutzbehörden in EU/EWR für den Umgang mit derartigen Angelegenheiten einzurichten, die quasi-kommerziell (oder zumindest vollständig eigenfinanziert) betrieben wird. Sollte die in diesem Unterabschnitt vorgebrachte Idee für lohnenswert erachtet werden, so könnte sie auch in Bezug auf den Entwurf von Verhaltenskodizes und BCRs nützlich sein.

(iv) Datenschutz-Gütesiegel

142. Datenschutz-Gütesiegel haben einen schlechten Ruf: siehe die scharfe, aber gerechtfertigte Kritik an Trust Guard, TRUST-e, BBB, etc. im Country Report über die USA (das Land, aus dem die meisten weltweiten Siegel stammen).³⁹ Wie dort beschrieben wird, liegt das Hauptproblem der freiwilligen Siegel in der Frage der Anreize.⁴⁰

Bei Datenschutz-Gütesiegel-Programmen gibt es ein erhebliches Problem im Bereich der Anreize: Für manche Unternehmen mit einer starken Nutzer-Basis gibt es wenige Anreize zur Zertifizierung ihrer Datenschutzpraktiken. So weisen, zum Beispiel, Google und MySpace keine TRUSTe-Datenschutz-Gütesiegel auf. Für kleinere Internetseiten am anderen Ende des Spektrums, die ihre Nutzer-Basis erweitern wollen, bestehen große Anreize zur Zertifizierung. TRUSTe und andere Datenschutz-Gütesiegel-Programme beziehen ihre Einnahmen aus der Vergabe von Siegeln und müssen daher ihr Ziel, verantwortungsvolle Praktiken sicherzustellen,

³⁹ Chris Hoofnagle, Country Report on the USA, S. 46 – 48, mit detaillierten Verweisen. Siehe Country Report on Japan für ähnliche Kritik am dortigen Datenschutz-Gütesiegel.

⁴⁰ *Idem*, S. 48.

EUROPÄISCHE KOMMISSION – GD JLS
**VERSCHIEDENE ANSÄTZE ZUR BEWÄLTIGUNG NEUER HERAUSFORDERUNGEN FÜR DEN
SCHUTZ DER PRIVATSPHÄRE, INSBESONDERE AUFGRUND TECHNOLOGISCHER
ENTWICKLUNGEN**

Schlussbericht

ausbalancieren und gleichzeitig der Verlockung zusätzlicher Einnahmen von Unternehmen mit schwachen Datenschutzpraktiken widerstehen.

143. Ein Versuch, diesem Problem einigermaßen Herr zu werden, wurde im Datenschutzgesetz des deutschen Bundeslandes Schleswig-Holstein unternommen. Das Gesetz gibt dort den öffentlichen Behörden des Landes die ausdrückliche Anweisung, bei der Vergabe von Aufträgen jenen IT-Produkten und -Dienstleistungen den Vorzug zu geben, deren Übereinstimmung mit dem dortigen Datenschutzgesetz anhand eines von der Datenschutzbehörde Schleswig Holstein (ULD) vergebenen Datenschutz-Gütesiegels bestätigt wurde.⁴¹ Dies soll keine ungerechte Beschränkung des fairen Wettbewerbs darstellen, sondern heißt, ganz im Gegenteil, dass datenschutzkonforme Produkte und Dienstleistungen eine faire Chance erhalten, sich mit den weniger nutzerfreundlichen Konkurrenten messen zu können.
144. Das System in Schleswig-Holstein diene als Vorlage für das vor Kurzem geschaffene europäische Datenschutz-Gütesiegel *EuroPriSe*, das vom ULD in Zusammenarbeit mit anderen, besonders französischen und spanischen DPAs, verwaltet wird. EuroPriSe wurde auf der Grundlage eines von der EU-Kommission im Rahmen ihres damaligen „e-TEN“-Programms finanzierten Pilotprojektes gegründet. Das Projekt erhielt die höchste verfügbare Note von den Evaluatoren der EU, die es im Kriterium „Unterstützung der EU-Politik im Bereich des Datenschutzes, der Befolgung und der Anwendung und direkte Relevanz für die EU-Politik im Bereich Vertrauen und Sicherheit“ (Übersetzung V.G./S.H.) mit „hoch“ beurteilten. Das EuroPriSe-Programm wurde auch von der (damaligen) Kommissarin Viviane Reding sehr begrüßt und vom europäischen Datenschutzbeauftragten Peter Hustinx stark unterstützt. Auch in einem Bericht zum Datenschutz im digitalen Zeitalter (*La vie privée à l'heure des mémoires numériques*), welcher im Juni dieses Jahres von der Commission des Lois des französischen Senats veröffentlicht wurde und in Frankreich als eine der wichtigsten gesetzlichen Initiativen im Bereich der Privatsphäre und des Datenschutzes seit der Umsetzung der EU-Datenschutzrichtlinie im Jahr 2004 gilt, wurde EuroPriSe gelobt. Zudem wurde festgestellt, dass diese Initiative Vorbildwirkung für nationale Programme hat und intensiviert werden sollte.
145. Wir schlagen vor, das EuroPriSe-Programm im Rahmen jeder Überarbeitung der Richtlinie näher zu diskutieren. Insbesondere sind wir der Ansicht, dass es äußerst nützlich wäre, in die Richtlinie eine Regelung zu integrieren, die jener in Schleswig-Holstein ähnelt und öffentlichen Behörden in den Mitgliedsstaaten sowie EU-Behörden die Anweisung gibt, nach Möglichkeit datenschutzkonformen Produkten und Dienstleistungen den Zuschlag zu erteilen. Falls dies nicht formell in der Richtlinie festgesetzt werden kann, so glauben wir, dass nichts gegen die Förderung solcher Vorschriften für die Auftragsvergabe auf anderem Wege spricht, z.B., indem die Kommission und die Mitgliedsstaaten diesen Ansatz unter politischen Gesichtspunkten verfolgen. Wir sind der Ansicht, dass derartige Vorschriften und Strategien für die Auftragsvergabe prinzipiell (jedoch unter Berücksichtigung der Anmerkung unten und des allgemeineren Vorbehalts unter Abs. 146) die bisher besten Anreize für starken, effektiven Datenschutz und ernsthafte Einhaltung der Datenschutzregelungen vonseiten

⁴¹ Siehe: <https://www.datenschutzzentrum.de/guetesiegel/index.htm>, oder für eine Zusammenfassung auf Englisch: https://www.datenschutzzentrum.de/faq/guetesiegel_engl.htm.

EUROPÄISCHE KOMMISSION – GD JLS
**VERSCHIEDENE ANSÄTZE ZUR BEWÄLTIGUNG NEUER HERAUSFORDERUNGEN FÜR DEN
SCHUTZ DER PRIVATSPHÄRE, INSBESONDERE AUFGRUND TECHNOLOGISCHER
ENTWICKLUNGEN**

Schlussbericht

kommerzieller Einrichtungen, die in Hinblick auf den Datenschutz sensible Produkte oder Dienstleistungen anbieten, bieten können.

Anmerkung: Jede derartige Maßnahme muss selbstverständlich sowohl das EU-Wettbewerbsrecht als auch das Gesetz zum freien Waren- und Dienstleistungsverkehr (und auch die Regelungen der WTO) berücksichtigen. Derartige Pläne müssen so gestaltet werden, dass sie das Risiko wettbewerbswidriger Wirkung oder ungerechter Beeinflussung des Handels zwischen Mitgliedsstaaten ausschließen. Die Regelung aus Schleswig-Holstein deutet jedoch darauf hin, dass dies möglich ist.

146. Ein weiterer Aspekt des (bereits erwähnten) EuroPriSe-Programms ist die Einrichtung einer Zertifikationsautorität für die Vergabe der Siegel und die Akkreditierung speziell geschulter und geprüfter unabhängiger Experten/-innen, die die primäre Evaluierung der Produkte durchführen. Die Autorität besteht im Wesentlichen aus den teilnehmenden DPAs und die Experten/-innen sind gründlich geschult und streng geprüft. Das System finanziert sich selbst, und zwar durch die Gebührenzahlungen der Unternehmen, die sich für das Siegel bewerben (und die ebenfalls, aber separat, die Experten/-innen auf der Grundlage individueller Abkommen bezahlen). Wie oben erwähnt ist in Schleswig-Holstein die DPA des Bundeslandes zu diesen Tätigkeiten formell berechtigt. Auf europäischer Ebene hat sich dies insofern als komplizierter erwiesen, als nicht alle nationalen DPAs aufgrund ihrer geltenden Gesetze formell am Programm beteiligt werden können. Bei der Überarbeitung der Richtlinie könnte es in Betracht gezogen werden, die Beteiligung an einem derartigen Programm als eine der Aufgaben von DPAs zu nennen. (Vgl. den aktuellen Artikel 28).
147. In der Tat wäre es vielleicht nützlich, die Einrichtung einer speziellen Behörde oder Abteilung der DPAs in EU/EWR zum Umgang mit derartigen Angelegenheiten in Erwägung zu ziehen, die in enger Verbindung zur AG 29 und der Kommission steht und die, ähnlich dem System der ULD, quasi-kommerziell (oder zumindest vollständig eigenfinanziert) betrieben wird. Wie bereits erwähnt, könnte solch einer Behörde oder Abteilung der Auftrag gegeben werden, sich nicht nur mit dem europäischen Datenschutz-Gütesiegel, sondern vielleicht auch mit der Vorbereitung der europäischen Verhaltenskodizes und mit den verbindlichen unternehmensinternen Vorschriften zu befassen, wobei in all diesen Fällen die anfängliche Arbeit unabhängigen (aber geprüften und richtig akkreditierten) Experten/-innen überlassen und die Schlussprüfung und Zertifizierung semi-kommerziell (selbst-finanziert) von der Behörde übernommen werden sollte.

Anmerkung: Die Frage nach dem Status einer derartigen Behörde und ihren formellen Beziehungen zu nationalen DPAs und den EU-Behörden ist kompliziert, wie schon im "e-TEN" EuroPriSe-Pilotprojekt bemerkt wurde. Die Gründung nationaler Zertifizierungs- und Akkreditierungsbehörden ist in Europa jedoch ein recht übliches Phänomen. Es gibt sogar eine aktuelle Verordnung, Verordnung (765/08) über die Vorschriften für die Akkreditierung und Marktüberwachung, die ab 1. Januar 2010 zum ersten Mal einen Rechtsrahmen für die Bereitstellung von Akkreditierungsleistungen in ganz Europa bieten wird, indem sie die Bestimmungen für die Durchführung der Akkreditierung festlegt, welche freiwillige Konformitätsbewertungen sowie gesetzlich vorgeschriebene Konformitätsbewertungen unterstützen. Eine Prüfung der grundlegenden Idee eines europäischen Systems zur Zertifizierung und Akkreditierung

EUROPÄISCHE KOMMISSION – GD JLS
**VERSCHIEDENE ANSÄTZE ZUR BEWÄLTIGUNG NEUER HERAUSFORDERUNGEN FÜR DEN
SCHUTZ DER PRIVATSPHÄRE, INSBESONDERE AUFGRUND TECHNOLOGISCHER
ENTWICKLUNGEN**

Schlussbericht

für das europäische Datenschutz-Gütesiegel könnte in diesem weiteren Kontext Inspiration finden.

148. All das Obengenannte muss jedoch mit großer Vorsicht angegangen werden. Alles hängt von der Strenge der Bedingungen für das Siegel und ihrer Durchsetzung ab. Das EuroPriSe-Programm ist in beiden Punkten erfolgreich, und zwar genau weil die angewandten Kriterien sehr streng sind und von Datenschutzbehörden aus Ländern mit starkem Datenschutz aufgestellt wurden und weil das Programm hauptsächlich von DPAs verwaltet wird, die nicht auf die Optimierung von Erträgen und das Erzielen von Gewinnen ausgerichtet sind (vielen DPAs ist es sogar gesetzlich untersagt, an auf Gewinn ausgerichteten Aktivitäten mitzuwirken). Programme ohne derartige Garantien können wahrscheinlich keine wirkliche Einhaltung der EU/EWR-Standards gewährleisten.
149. Natürlich sind das nur vorläufige Vorschläge. Wir sind jedoch der Ansicht, dass es in dem neuen sozio-technischen Umfeld wichtig sein wird, über neue Systeme zu verfügen, die effektiv und nicht übertrieben bürokratisch mit Maßnahmen umgehen können, die auf die Sicherstellung des angemessenen Datenschutzes in speziellen Sektoren, (multinationalen) Unternehmen oder Kontexten abzielen. Im Gegensatz zu den früheren, weitgehend diskreditierten Siegeln (etc.) sollten derartige Systeme (wie das EuroPriSe-System) jedoch eng mit den offiziellen Aufsichtsbehörden verbunden und nicht von kommerziellen Interessen getrieben werden.

(v) Schlussfolgerung

150. Wir befürchten, dass es keine „Patentlösung“ zur Sicherstellung des angemessenen Datenschutzes gibt. Das Gesetz ist naturgemäß oft schwer zu interpretieren und anzuwenden und entweder zu vage oder zu unflexibel. Die zusätzlichen und alternativen (nicht-rechtlichen oder quasi-rechtlichen) Maßnahmen leiden hingegen an ernsten, oft inhärenten, Schwächen. Bei manchen Maßnahmen und Technologien hat sich gezeigt, dass sie kaum mehr als Feigenblätter sind. Jede Überarbeitung muss auf realistischen und technisch korrekten Evaluierungen dieser Maßnahmen basieren. Das soll nicht heißen, dass sie sofort verworfen werden sollten. Sie müssen jedoch von technischen Experten/-innen und auch von Rechtsexperten/-innen genau geprüft werden: Wie es Ohms Artikel in Bezug auf einen (jedoch wesentlichen) Bereich, nämlich Ent- und Re-Identifizierung, verdeutlicht, haben die Gesetzgeber und politischen Entscheidungsträger auf der ganzen Welt die neuen Technologien und ihre Auswirkungen häufig nicht richtig verstanden.
151. Im Allgemeinen spielt, wie in den letzten Unterabschnitten erwähnt, die Frage der Anreize und der Ökonomik des Datenschutzes und der Datensicherheit eine zentrale Rolle. Wenn die rechtlichen Vorschriften den Schutz der Privatsphäre wirtschaftlich attraktiv machen (z.B., wie erwähnt, durch Anreize bei der Auftragsvergabe in Verbindung mit der Vergabe ernstzunehmender Datenschutz-Gütesiegel), oder Verstöße gegen Regelungen zu Datenschutz und Datensicherheit bestrafen (indem die Verantwortung für den Schutz jenen gegeben wird, die ihn am besten gewährleisten können, anstatt ihnen die Abwälzung der Kosten auf andere, wie etwa Kunden/-innen, zu erlauben), dann kann der Datenschutz eine Zukunft haben. Wir sind der Ansicht, dass dafür die richtige Kombination von Rechtsnormen und selbst- oder ko-regulierenden

EUROPÄISCHE KOMMISSION – GD JLS
**VERSCHIEDENE ANSÄTZE ZUR BEWÄLTIGUNG NEUER HERAUSFORDERUNGEN FÜR DEN
SCHUTZ DER PRIVATSPHÄRE, INSBESONDERE AUFGRUND TECHNOLOGISCHER
ENTWICKLUNGEN**

Schlussbericht

Regelungen und Mechanismen nötig ist. Wir hoffen, dass das Obengenannte dafür einen
Denkanstoß gibt.

- o – O – o -

Leitende Sachverständige:

Douwe Korff, Team Leader
Ian Brown, Co-Leader

Spezielle Sachverständige:

Peter Blume
Graham Greenleaf
Chris Hoofnagle
Lilian Mitrou
Filip Pospíšil
Helena Svatošová
Marek Tichy

Berater/-innen:

Ross Anderson
Caspar Bowden
Katrin Nyman-Metcalf
Paul Whitehouse

ATTACHMENTS:

- Working Paper No. 1 **The challenges to European data protection laws and principles**
(An overview of the global social and technical developments and of the challenges they pose to data protection)
- Working paper No. 2: **Data protection laws in the EU**
(A comparative-analytical overview of the difficulties the law has in meeting the challenges posed by the global social and technical developments)
- Country Reports: **European countries:**
 - Czech Republic
 - Denmark
 - France
 - Germany
 - Greece
 - United Kingdom

Non-European countries and jurisdictions:

 - USA:
 - ✓ Federal level
 - ✓ California
 - ✓ New Jersey
 - Australia
 - Hong Kong
 - India
 - Japan
- Comparative Chart of National Laws

- o – O – o -

NB: In addition to the above attachments, which are formally part of the study, the authors have also provided the Commission with several other reports, mentioned in the text or in footnotes, with most of which one or more members of the expert team were involved and on which they could therefore draw (unless the Commission already had those reports).