15. Oktober 2012

Vorschläge der Europäischen Kommission zum EU-Datenschutz

I. Allgemein

- Die EU-Kommission hat am 25. Januar 2012 Vorschläge für eine Neuregelung des Datenschutzes auf EU-Ebene vorgelegt. Es handelt sich um Vorschläge für eine Richtlinie, die sich auf den Datenschutz im Bereich der Strafverfolgung bezieht sowie für eine sogenannte Datenschutz-Grundverordnung, die die Wirtschaft und die öffentliche Verwaltung (außer Strafverfolgung) betrifft.

- Deutschland begrüßt uneingeschränkt das Ziel der Kommission, das europäische Datenschutzrecht zu reformieren. Wir brauchen dringend eine Reform des Datenschutzes im Bereich der Wirtschaft und die Reform muss eine Europäische sein. Das Datenschutzrecht muss zudem den Erfordernissen des Internetzeitalters angepasst werden. Ob hierfür die vorgeschlagenen Instrumente ausreichen, wird derzeit in Brüssel im Rat, im Europäischen Parlament intensiv diskutiert.

- Insbesondere die Datenschutz-Grundverordnung ist von hohem öffentlichen Interesse. Der Bundestags-Innenausschuss hat für den 22. Oktober 2012 eine öffentliche Sachverständigenanhörung beschlossen. Der Bundesrat hat - flankiert von einer detaillierten Stellungnahme - Subsidiaritätsrüge erhoben. Der Bundesminister des Innern hat zu einer Internationalen Konferenz eingeladen, die am 17. und 18. Oktober 2012 in Berlin stattfindet. Sie widmet sich Grundsatzfragen des Datenschutzes, die im Zuge der Brüsseler Beratungen von den Mitgliedstaaten gestellt worden sind.

- Im Rat der Europäischen Union wurden bislang 33 von 91 Artikeln der Datenschutz-Grundverordnung erörtert. Im Mittelpunkt der bisherigen Erörterungen standen u.a. Fragen der Umsetzbarkeit bzw. Internettauglichkeit der Regelungen sowie der Angemessenheit in Bezug auf die jeweiligen Risiken der Datenverarbeitung. Der Vorschlag der Datenschutz-Grundverordnung enthält im Grundsatz eine sogenannte Einheitslösung („One-Size-fits-All-Modell"), d.h. jede Datenverarbeitung wird regulatorisch zunächst als „gleich gefährlich" eingestuft. Dies hat zur Folge, dass Schutzmechanismen wie die Einwilligung, Informations- und Nachweispflichten eine unendliche Vielzahl von höchst unterschiedlichen Fällen passen müssen. Durch das Internet und zunehmende Verbreitung von elektronischen Geräten im Alltag (z.B. Auto, elektronisches Notizbuch, Stromzähler etc.) droht für zahlreiche Fallgruppen die Gefahr einer Überdimensionierung. Für andere Fall-

gruppen droht die Gefahr, dass die Schutzmechanismen zu allgemein ausgestaltet sind und größeren Risiken nicht angemessen begegnet werden kann (z.B. „Freizeichnung" von Facebook durch nur eine Einwilligung).

- Die Bundesregierung hält es ebenso wie andere Mitgliedstaaten für erforderlich, dass das Datenschutzrecht auf europäischer Ebene unter bestimmten Aspekten grundsätzlich erörtert wird. Hierzu gehört die Unterscheidung zwischen dem Datenschutz im Verhältnis des Bürgers zum Staat und im Bereich der Wirtschaft. Im Verhältnis Staat-Bürger gibt es zahlreiche bereichsspezifische Bestimmungen in Deutschland, die ein sehr hohes Niveau an Datenschutz sicherstellen. Die Spielräume, die der deutsche Gesetzgeber hier – auch mit Blick auf die Rechtsprechung des Bundesverfassungsgerichts – bisher nutzen konnte, gilt es zu bewahren. Im Bereich der Wirtschaft verlangen die Mechanismen des europäischen Binnenmarktes demgegenüber eine möglichst abschließende Europäische Regelung des Datenschutzrechts.

II. Im Einzelnen

- Eine stärkere Harmonisierung würde nicht nur im europäischen Rahmen zu mehr Klarheit und Wettbewerbsgleichheit führen. Sie ist auch Voraussetzung für eine bessere Durchsetzung europäischer Datenschutzstandards gegenüber Anbietern aus Drittstaaten. Für globale Unternehmen wie Facebook und Google ist der europäische Markt mit einer halben Milliarde Teilnehmern einer der attraktivsten der Welt. Die Europäer können verlangen, dass weltweit agierende Unternehmen ihre Dienste an diesen Markt anpassen.

- Der Verordnungsvorschlag der Kommission muss sich daran messen lassen, ob und inwieweit er offene Fragen im Zusammenhang mit dem Internet beantwortet und dabei dessen Innovationspotential wahrt. Das neue Datenschutzrecht muss Grenzen setzen, ohne Chancen des vernetzten Miteinanders im Informationszeitalter zu verspielen. Es muss so technikneutral und entwicklungsoffen sein, dass es die nächsten 20 Jahre trägt.

Der Vorschlag der Kommission ist nach Systematik und Regelungstechnik konservativ und lehnt sich an dem geltenden Datenschutzrecht an. Anwendungsfragen, wie z.B. beim Cloud Computing oder die datenschutzrechtliche Zulässigkeit des „Like-it"-Button, würden sich bei der neuen Verordnung in gleicher Weise stellen. Mit Ausnahme weniger Regelungen lässt sich nicht erkennen, dass gerade große Unternehmen klareren Regeln unterworfen wären. Das „Recht auf Vergessenwerden" (Art. 17 Abs. 2) wird zudem auch unter grundsätzlichen und praktischen Gesichtspunkten sehr kontrovers diskutiert.

- Bei Regelungen, die auf spezifische Dienste ausgerichtet sind wie z.B. das auf soziale Netzwerke bezogene „Recht auf Datenübertragbarkeit" (Art. 18), ist offen, wie sich diese auf andere Dienste oder Datenverarbeitungen außerhalb des Internets übertragen lassen. Kann etwa ein Kunde beim Wechsel seiner Versicherung „seine" bei der alten Versicherung gespeicherten Daten in Form einer Kopie mitnehmen? Hieran schließen sich bedeutsame Fragen der technischen Infrastruktur an, die zusätzlich zu klären sind, da Datenformate flächendeckend vereinheitlicht werden müssten.

- Bei der Anwendung des Datenschutzrechts und der Datenschutzkontrolle auf Privatpersonen stellen sich wichtige Fragen im Zusammenhang mit anderen Grundrechten wie der Meinungsfreiheit und der Informationsfreiheit. Der Verordnungsvorschlag erfasst die Verarbeitung personenbezogener Daten durch Jedermann, soweit die Daten einer unbestimmten Vielzahl von Personen zugänglich sind. z.B. auf eigenen Webseiten, in Blogs und sozialen Netzwerken. Privatpersonen treffen dann die gleichen Pflichten der Verordnung wie Unternehmen. Dazu gehört z.B. die Erstellung eines Datenschutzkonzepts. Dies gilt auch, wenn sie zwar zu ausschließlich privaten oder familiären Zwecken handeln, zugleich aber eine Gewinnerzielungsabsicht haben (z.B. bei Ebay). Mitgliedstaaten wie z.B. Schweden schlagen daher vor, alltägliche, d.h. im allgemeinen nicht als riskant bewertete *Datenverarbeitung durch „Privatpersonen wie Du und ich"* vom Anwendungsbereich des EU-Datenschutzrechts stärker auszunehmen.

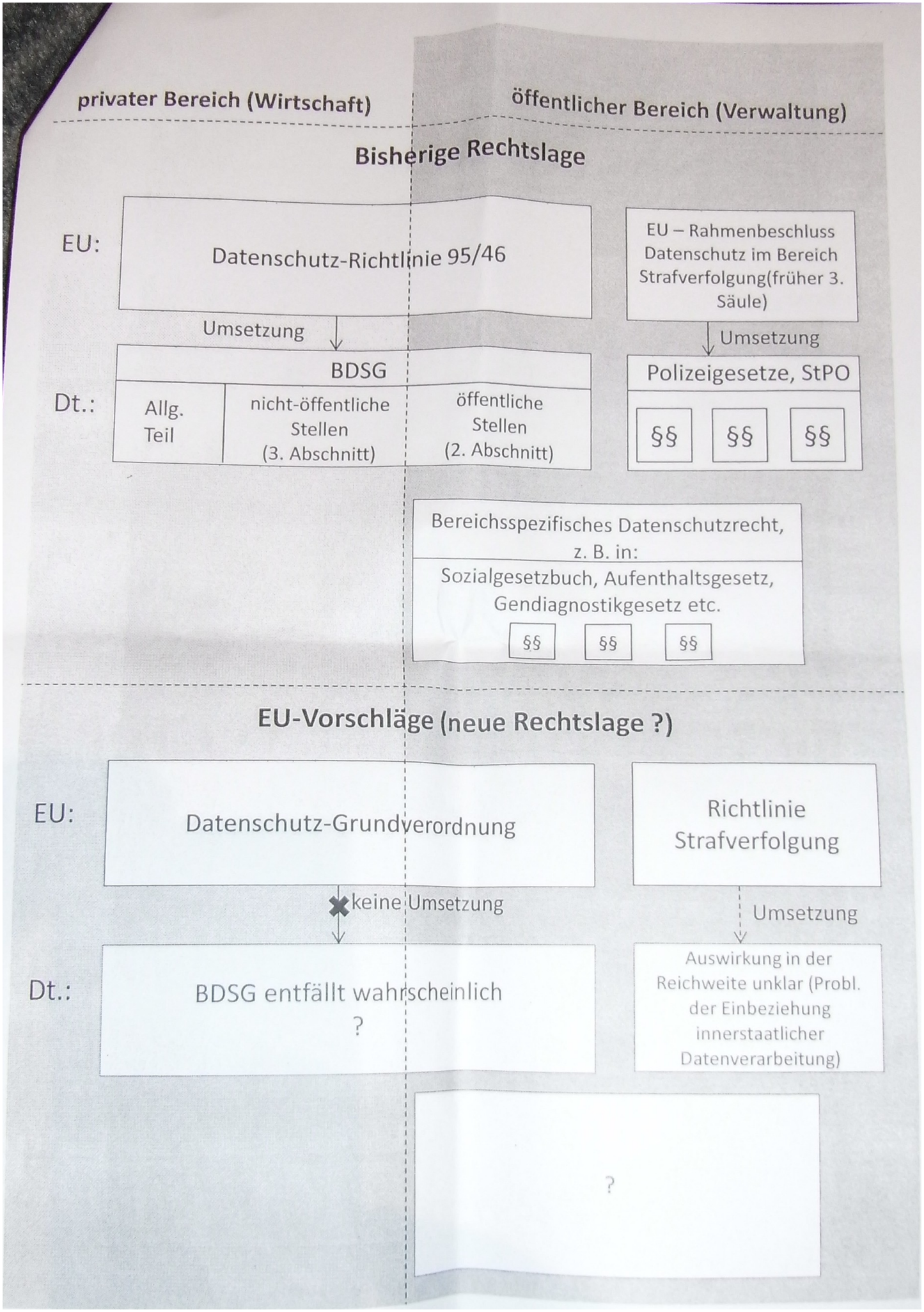
- Die Kommission erhofft sich durch den Verordnungsvorschlag eine Verringerung des Verwaltungsaufwandes. Das ist uneingeschränkt zu befürworten. Bürokratie, Verwaltungs- und Umsetzungsaufwand müssen sich in Grenzen halten. Die Mitgliedstaaten halten den bürokratischen Aufwand zahlreicher Vorschriften jedoch nicht für risikoadäquat (z.B. Informationspflichten in Art. 14, Strategien nach Art. 22). Eine systematische Umstellung auf ein an den Gefahren für das Persönlichkeitsrecht ausgerichtetes Risikomodell kann helfen, unnötigen Verwaltungsaufwand zu vermeiden. Die Reservierung eines Tisches im Restaurant macht es z.B. nicht notwendig, den Besteller über die Speicherdauer, seine Betroffenenrechte und die Kontaktdaten der Aufsichtsbehörde zu informieren, wie dies Artikel 14 des Verordnungsvorschlags derzeit vorsieht. Gerade Unternehmen, bei denen der Schwerpunkt nicht auf Datenverarbeitungen liegt, gilt es vor zusätzlichen Belastungen zu schützen.

- Andererseits sollte erwogen werden, diejenigen stärker in die Pflicht zu nehmen, die elektronische Dienste oder Software anbieten, etwa durch datenschutzfreundliche Voreinstellungen. Es müssen wirksame Anreize für datensparsame Ge-

schäftsmodelle geschaffen werden. Deutschland hat hier eine bewährte Tradition, z.B. im Telemedienbereich nur pseudonyme Nutzungsprofile zuzulassen.

- Schließlich sieht die Kommission in dem Verordnungsvorschlag für sich selbst eine starke Rolle vor. Dies betrifft das Verhältnis zu den Mitgliedstaaten in besonderem Maße. Problematisch sind die zahlreichen Ermächtigungen an die Kommission zum Erlass von delegierten Rechtakten und Durchführungsbestimmungen. In 91 Artikeln finden sich insgesamt 45 Ermächtigungen, d.h. bei praktisch jeder zweiten Vorschrift. Dadurch erhält die Kommission die Möglichkeit zu datenschutzrechtlichen Detailregelungen, die in die unterschiedlichsten Rechtsgebiete hineinwirken können. Hier besteht die Möglichkeit, über Verfahren der regulierten Selbstregulierung zu detaillierten Bestimmungen zu gelangen und die Ermächtigungen der Kommission zu reduzieren. Hier gibt es anerkannte Vorbilder, etwa bei technischen Standardisierungen die DIN- und ISO-Normen, aber auch in anderen Rechtsbereichen wie dem Jugendmedienschutz. An europaweit einheitlichen Detailregelungen besteht zudem nicht überall der gleiche Bedarf. Was für den Bereich der Wirtschaft und des Binnenmarktes richtig ist, gilt nicht automatisch für den öffentlichen Bereich.

- Gerade im öffentlichen Bereich muss es grundsätzlich den Mitgliedstaaten und ihren Parlamenten überlassen bleiben, für ihre Behörden die notwendigen datenschutzrechtlichen Details selbst festzulegen. Fast alle modernen Fachgesetze enthalten Regelungen zum Schutz personenbezogener Daten, die Besonderheiten Rechnung tragen, z.B. im Sozialdatenschutz oder dem Gendiagnostikgesetz. Durch eine unmittelbar wirkende Verordnung würden diese bereichsspezifischen Regelungen überlagert und ein über Jahrzehnte entstandenes, austariertes System aufs Spiel gesetzt. Hierauf haben auch die Datenschutzbeauftragten von Bund und Ländern in ihren Stellungnahmen vom 22. März und 11. Juni 2012 deutlich hingewiesen. In verschiedenen Bereichen würde es zu einer Absenkung des Datenschutzniveaus kommen, wenn die vorgeschlagene Verordnung in Kraft träte. Dabei gebietet im öffentlichen Bereich weder der Binnenmarkt noch der freie Datenverkehr europäische Regelungen, die die nationalen Spielräume massiv und flächendeckend einschränken.


privater Bereich (Wirtschaft)
öffentlicher Bereich (Verwaltung)
Bisherige Rechtslage
EU:
Datenschutz-Richtlinie 95/46
EU – Rahmenbeschluss Datenschutz im Bereich Strafverfolgung(früher 3. Säule)
Umsetzung
Umsetzung
Dt.:
BDSG
Allg. Teil
nicht-öffentliche Stellen (3. Abschnitt)
öffentliche Stellen (2. Abschnitt)
Polizeigesetze, StPO
§§
§§
§§
Bereichsspezifisches Datenschutzrecht, z. B. in:
Sozialgesetzbuch, Aufenthaltsgesetz, Gendiagnostikgesetz etc.
§§
§§
§§
EU-Vorschläge (neue Rechtslage ?)
EU:
Datenschutz-Grundverordnung
Richtlinie Strafverfolgung
keine Umsetzung
Umsetzung
Dt.:
BDSG entfällt wahrscheinlich ?
Auswirkung in der Reichweite unklar (Probl. der Einbeziehung innerstaatlicher Datenverarbeitung)
?