Bayerisches Staatsministerium
des Innern

Rede des Bayerischen Staatsministers des Innern,
Joachim Herrmann,

anlässlich einer
Datenschutzveranstaltung
am 30. November 2012 in München (Hanns-Seidel-Stiftung)

Thema: „Erwartungen an die Reform des Europäischen Datenschutzrechts- Ein Meinungsaustausch zwischen Politik, Wissenschaft und Datenschutz-Praxis“

Es gilt das gesprochene Wort!

12.12.2012 16:55

Anrede!

Einleitende Worte, Anlass

Ein Jahr nach dem Bekanntwerden der **Vorschläge** der **EU-Kommission** für eine **Gesamtreform** des **Europäischen Datenschutzrechts** ist es Zeit für eine erste **Zwischenbilanz**. Deshalb **freue ich mich**, dass Sie unserer Einladung nach München so zahlreich gefolgt sind und sich an diesem **Meinungsaustausch** von Politik, Wissenschaft und Datenschutz-Praxis **beteiligen**.

Unser erklärtes **Ziel** ist es, die **Debatte** in den europäischen Gremien weiterhin sorgfältig, problembewusst und **konstruktiv** zu **begleiten**.

Grundhaltung der Bayerischen Staatsregierung

Meine Damen und Herren, die **Bayerische Staatsregierung** hat schon frühzeitig deutlich gemacht, **wie wichtig** ihr eine erfolgreiche **Modernisierung** des **Datenschutzrechts** in **Europa ist**. Ich betone das bewusst gleich zu Beginn der Veran-

staltung; denn leider werden allzu oft Kritik und Verbesserungswünsche zu Vorschlägen der EU-Kommission vorschnell in das **Schema „Bayern gegen Brüssel“** eingeordnet.

Deshalb will ich nochmals klarstellen: Es geht uns **keinesfalls** um ein **Verhindern**, sondern eindeutig um ein **Verbessern** des **Reformvorhabens**. Gemeinsam mit Ihnen, meine Damen und Herren, mit Ihren Ideen und Anliegen wollen wir dazu beitragen, das **Datenschutzrecht** in Europa **optimal fortzuentwickeln**.

vier Eckpunkte

Ich will in die heutige Debatte **vier Eckpunkte** einbringen, die mir besonders **wichtig erscheinen**.

erster Eckpunkt: Prioritätensetzung, kein Paketansatz

Der **erste Eckpunkt** hat mit klarer **Prioritätensetzung** und **politischem Realismus** zu tun.
Datenverarbeitung ist heute **allgegenwärtig** – im beruflichen wie im privaten Leben. Das bringt natürlich auch **viele**

zusätzliche **Gefahren** mit sich. Wir haben inzwischen eine veränderte Bedrohungslage.

Die unablässigen **Datenspuren** von **Smartphones** und anderen IT-Verfahren wecken die **Neugierde** von **Vertriebsmanagern**. Sie wollen mehr über das Verhalten ihrer Kunden erfahren. Davon geht ein **weit größeres Risiko für** die **Privatsphäre** aus als von allen Datenbeständen der Sicherheitsbehörden in Europa.

Oberste **Priorität** haben für mich deshalb klare, zukunftstaugliche **Datenschutzstandards in der Wirtschaft**. Ganz unabhängig von allen politischen und fachlichen Vorbehalten gegen den Vorschlag für eine Richtlinie zum Datenschutz bei Polizei und Justiz halte ich es daher für **dringend geboten**, den so genannten **Paketansatz** zu **überdenken**.

Eine **Gesamtreform** des Europäischen Datenschutzrechts mit Regelungen für die Wirtschaft, für die Behörden der **27 Mitgliedstaaten** und für die Datenverarbeitung bei Polizei und Justiz **führt** zwangsläufig **zu Verzögerungen**. Sie gehen letztlich zu Lasten der vordringlichen Herausforderungen im privaten Datenschutzrecht.

Ich halte diese **Paketlösung** im Übrigen nicht nur für rechtspolitisch verfehlt. Ich halte sie **auch** für **wirtschaftspolitisch inkonsequent**. Gerade **wenn wir** die **strukturschwächeren Volkswirtschaften** in Europa **stärken wollen**, indem wir etwa den Betrieben in Griechenland, Portugal oder Spanien neue Geschäftsmodelle und Kundenkreise eröffnen, **brauchen wir** dazu die Wachstumspotentiale der **Online-Wirtschaft**.

Plädoyer für Stufenplan

Diese **Chancen** eines **digitalen Binnenmarkts** hängen aber nicht von einheitlichen Datenschutzstandards bei Polizei und Justiz, sondern vom raschen Gelingen

einer Reform des nicht-öffentlichen Datenschutzrechts ab. An die Stelle **politisch unrealistischer Pakete** sollte daher ein klarer **Stufenplan** für ein kohärentes Europäisches Datenschutzrecht treten. **In** diesen **Stufenplan müssen auch** – mit klaren zeitlichen Vorgaben – **bisher ausgesparte Bereiche einbezogen** werden.

Ich nenne hier nur die **Regelungen** über elektronische **Kommunikationsdienste** oder die **Datenverarbeitung** der **EU-Organe und EU–Agenturen**. Auf diese Weise können wir systematische Brüche beheben.

Ein **gemeinsames Europäisches Datenschutzrecht** für die nationalen Polizeibehörden und die Strafgerichtsbarkeit hat in einem solchen Stufenkonzept **keine erhöhte Priorität**.

zweiter Eckpunkt: Verhältnis EU-Recht/ nationales Recht

Der **zweite Eckpunkt** betrifft den **ungelösten Konflikt** beim Datenschutz im **öffentlichen Bereich**; und zwar zwischen dem vorrangig anzuwendenden **Unionsrecht** und dem **Datenschutzrecht der Mitgliedstaaten**.

Ganz unabhängig von Fragen der Subsidiarität und der Rechtsetzungskompetenzen **geht es auch hierbei** letztlich **um** sachgerechte, politisch kluge **Abschichtungen zwischen** sehr unterschiedlichen **Problemkomplexen**.

Die **Handlungserfordernisse** im **privaten Datenschutzrecht** sind klar und **unstreitig**. Nicht nur in Deutschland gibt es jedoch vielfach den **Wunsch**, dass bewährte **nationale Regelungen** über die Datenverarbeitung **bei öffentlichen Stellen fortbestehen**. Hier geht es etwa um den **Datenschutz in Schulen,** in den Gesundheits- und Sozialbehörden oder in **Gerichtsverfahren**. Es geht aber auch um die gerade im skandinavischen Raum

verfassungsrechtlich gewährleisteten **Rechte** wie z.B. den Anspruch **auf freien Informationszugang**.

keine Absenkung des Schutzniveaus

Bis jetzt ist nicht erkennbar, wie der Verordnungs-Vorschlag der Kommission für all diese unterschiedlichen Regelungsaufgaben im öffentlichen Datenschutz angemessene **Lösungen möglich macht**. **Eindeutig** ist aber: Wir **wollen keine Absenkungen** des **Schutzniveaus** bei staatlicher Datenverarbeitung **zulassen**!

Anforderungen des Volkszählungsurteils

Daher muss sich auch die **Datenschutz-Grundverordnung** beim Datenschutz zwischen Bürger und Staat **an den Anforderungen messen lassen**, die seit dem Volkszählungsurteil die nationale **Datenschutzgesetzgebung bestimmen**.

Diese Anforderungen kann die Verordnung in ihren derzeit 91 Artikeln offenkundig nicht erfüllen. Dort gibt es zwar Generalklauseln. Es **fehlt** aber an klaren und präzisen **Regelungen über Umfang** und

Zwecksetzung der **staatlichen Datenverarbeitung**.

Hier ist im Übrigen schon zweifelhaft, ob die **Schnittstellen** der **Datenschutz-Grundverordnung** für die nationale Gesetzgebung solche **Regelungen** überhaupt **erlauben würden**. Ich nenne hier nur verfassungsrechtlich gebotene Anforderungen an die **Videoüberwachung öffentlicher Räume**.

Damit stellt sich die Frage: Wäre **Weniger möglicherweise Mehr**? Wäre **weniger Verbindlichkeit** – etwa der Erlass einer Richtlinie an Stelle einer Verordnung – ein **Gewinn** an **Rechtssicherheit** und **Rechtsklarheit für** den **Datenschutz** im Verhältnis Bürger – Staat?

Alternativen

Zunächst **bleibt abzuwarten**, **ob** der klare **Weg** einer umfassenden **Ausklammerung** der Datenverarbeitung öffentlicher Stellen **im „Trialog“** zwischen Rat, Parlament und Kommission **vermittelbar ist**. Falls nein,

verbleibt letztlich als Alternative ein **Regelungsmodell** des deutschen Datenschutzrechts.

Das **Bundesdatenschutzgesetz** hat für das Verhältnis zu den Landesdatenschutzgesetzen eine **eigene Subsidiaritätsregelung entwickelt: Sobald** und soweit ein **Land** den **Datenschutz** gleichwertig **durch Landesgesetz geregelt hat**, **wird** das **Bundesrecht unanwendbar**.

Damit sind – wie auch im Verwaltungsverfahrensrecht des Bundes – die **Grundkonflikte** zwischen den Gestaltungsspielräumen der Länder und dem Geltungsvorrang des Bundesrechts **gut gelöst**. Solch eine „eingebaute Subsidiaritätsklausel“ vermeidet– ganz im Sinne des Lissabon-Vertrages – einen **Bruch** mit gewachsenen **Rechts- und Organisationsstrukturen**. Sie würde damit auch die **Akzeptanz** eines einheitlichen **Europäischen Datenschutzrechts** deutlich **verbessern**.

Dritter Eckpunkt: Kohärenz, Europäischer Datenschutz-ausschuss

Der dritte Eckpunkt betrifft den so genannten **Kohärenzmechanismus** und die **Arbeitsweise** des Europäischen **Datenschutzausschusses**.

Natürlich will ich an dieser Stelle **keine Grundsatz-Debatte** eröffnen, die dem Erfolg des Reformvorhabens nicht dienlich sind. Dennoch **will** ich **ganz deutlich sagen:** Die **Verfahrensregelungen** zur **Abstimmung** der europäischen Datenschutzbehörden sind **sehr aufwändig**. Und sie sind nur deshalb nötig, weil Kommission und Europäischer Gerichtshof ein **verfassungsrechtlich nach wie vor umstrittenes Verständnis** hinsichtlich der **„völligen Unabhängigkeit“** der Datenschutzaufsichtsbehörden im nicht-öffentlichen Bereich durchgesetzt haben.

Mit einer Aufsichtsbehörde unter parlamentarisch **kontrollierter Regierungsverantwortung** wäre ein harmonisierter **Vollzug** europäischen Datenschutzrechts

qualitativ gleichwertig und dazu noch deutlich wirkungsvoller.

Gerade aber wenn die völlig **unabhängige Aufgabenwahrnehmung** auch beim **Datenschutz** in der **Wirtschaft** unter Hintanstellung aller Einwände das Ziel sein soll, dann müssen das **Kohärenzverfahren** und der Zusammenschluss zum **Europäischen Datenschutzausschuss Widerspruch** auslösen.

Denn hier beginnt ein Prozess, der diese **völlig unabhängige Aufgabenwahrnehmung** der nationalen Datenschutzbehörden **auszuhöhlen droht**. Die Einwirkungsmöglichkeiten stehen den Durchgriffsrechten klassischer Ministerialaufsicht kaum nach. Es **geht mir deshalb** vorrangig **um** eine **Begrenzung**.

Verfahrensrechtliche Absicherungen

Meine Damen und Herren, wenn wir **Kompetenzen** und datenschutzrechtliche Verantwortung **auf** die **europäische Ebene verlagern**, **brauchen wir** überdies

verfahrensrechtliche **Absicherungen**; Absicherungen, die der Kommissionsvorschlag **bislang** leider **nicht vorsieht**.

Er **überlässt es** vielmehr dem **Datenschutz-Ausschuss**, durch Leitlinien und Empfehlungen zahlreiche für den praktischen Vollzug wichtige Fragestellungen zu klären.

Das heißt, der **Datenschutzausschuss wird etwa Leitlinien** zum Adresshandel oder zum Verfahren der Auskunfteien **entwickeln**, die **an** die **Stelle gesetzlicher Regelungen** der Mitgliedstaaten treten.

Diese weitreichenden **Befugnisse dürfen** nach unserer Überzeugung **nicht in** einem wenig **transparenten, rein exekutiven Verfahren ausgeübt** werden. Ich halte es für **unerlässlich**, dass der **Datenschutzausschuss** – ähnlich wie im europäischen und nationalen Rechtsetzungsverfahren – zu einer **Anhörung** der beteiligten Kreise **verpflichtet wird**.

Zusätzliche Transparenz und Rückkoppelung mit den Organen der Gesetzgebung können wir außerdem **erreichen**, indem wir eine **besondere Datenschutz-Kommission einrichten**; eine Kommission, wie es sie bei uns in Bayern zur Unterstützung des Landesbeauftragten für den Datenschutz gibt.

Ein solches **Gremium würde dazu beitragen**, dass **Rat und Parlament** „auf Augenhöhe“ mit der Kommission **in** den **Vollzug** des europäischen Datenschutzrechts **eingebunden sind**. Nur so können wir sicherstellen, dass alle an der europäischen Rechtsetzung beteiligten Organe eigenständig beurteilen, ob bei bestimmten Entwicklungen in der Praxis Nachsteuerungsbedarf besteht.

vierter Eckpunkt: fehlende neue Impulse

Meine Damen und Herren, der **vierte** und letzte **Eckpunkt betrifft** ein erhebliches **Defizit** des Verordnungsvorschlags: das **Fehlen neuer Impulse**.

Der **Verordnungs-Vorschlag** wird zwar groß als Datenschutz-Konzept für das 21. Jahrhundert angekündigt. Weite Teile **beruhen** aber auf Modellen der geltenden **Datenschutz-Richtlinie aus dem Jahr 1995.** Vermeintliche Innovationen wie

- das **Recht auf Datenübertragbarkeit**,
- das **„Recht, Vergessen zu werden“**
  oder
- **Regelungen zur Profilbildung**

sind kaum mehr als **schon jetzt geltende Schutzrechte**, die nur etwas konkretisiert werden.

Alle **Grundprinzipien gehen** noch **von** klassischen **Verarbeitungsprozessen aus**, die eine klar nachvollziehbare Verantwortungskette schaffen. Schon die **heute üblichen Verarbeitungsprozesse** im Internet z.B. im Rahmen Sozialer Netzwerke, **lösen** diese **Verantwortungsstrukturen** aber mehr oder weniger **auf**.

Die moderne Datenverarbeitung ist allgegenwärtig. Der Datenverkehr explodiert förmlich. Deshalb wird es **für den Einzelnen immer schwieriger**, sein **Recht auf informationelle Selbstbestimmung wahrzunehmen**.

Meine Damen und Herren, denken Sie nur daran, **wie oft Sie** schon über Ihr **Smartphone** oder einen Internetdienst mit wenigen Klicks

- **Einwilligungen** abgegeben,
- Zweckänderungen erlaubt oder
- **Datenübermittlungen** über **sich und andere ausgelöst** haben.

Schutzmechanismen wie Transparenz und Information **laufen** vor dem Hintergrund immer komplexerer technologischer Verfahren **vielfach ins Leere**.

„Datenschutz durch Technik“

Wir **brauchen deshalb zusätzliche Instrumente**. Nur so können wir die informationelle Selbstbestimmung auch unter den

Bedingungen der digitalen Gesellschaft optimal schützen.

Ein guter, aber noch auszubauender Ansatz ist dabei vor allem das **Prinzip „Datenschutz durch Technik“**. Es greift Ansätze im nationalen Recht und auch eine Initiative des Bundesrats zum Datenschutz in Sozialen Netzwerken auf.

Dabei wird bislang **ausschließlich** der **Datenverarbeiter selbst in die Pflicht genommen**. Das Prinzip gilt damit für Kauf- oder Investitionsentscheidungen bei IT-Verfahren sowie für Unternehmen mit eigenen IT-Entwicklungen.

Allerdings stoßen wir dort an **Grenzen**, wo die **Bestimmung** des für die Datenverarbeitung **Verantwortlichen Schwierigkeiten bereitet**; oder wo der Verantwortliche z.B. als Endverbraucher nicht sachkundig genug ist, um über technische Optionen zu entscheiden.

Zusätzliche Verantwortungsebene

Insoweit würde ich mir eine **zusätzliche Verantwortungsebene** wünschen, die schon die **Hersteller und Anbieter** von Datenverarbeitungsverfahren **einbindet**. Dabei sollte keine Sonderform einer „Produkthaftung“ entstehen, die Innovationsbereitschaft bremst. **Sinnvoll wäre es** vielmehr, die **Einbindung** mit Anreizen wie **Gütesiegeln** oder ähnlichem **zu flankieren**.

„digitale Verkehrssicherungspflicht“

Wenn wir das **Prinzip** „Datenschutz durch Technik“ konsequent **umsetzen**, verbessern wir im Übrigen nicht nur den Schutz der informationellen Selbstbestimmung. Wir **erreichen gleichzeitig** auch eine gewisse **„digitale Verkehrssicherungspflicht“**.

Untersuchungen bestätigen immer wieder: **Nach dem Stand der Technik geschützte IT-Systeme** sind Schadprogrammen **weniger ausgesetzt** als nicht gepflegte Systeme. Sie tragen dazu bei, die **Risiken krimineller Übergriffe im Internet** für den

Einzelnen wie für die gesamte Gemeinschaft der Nutzer **zu begrenzen**.

Ausblick, Wünsche, Schlussworte

Meine Damen und Herren, **mit** meinen **vier Eckpunkten** habe ich nur einige **„Großbaustellen“** bei der Reform des Europäischen Datenschutzrechts **angesprochen**.

Die **hochkarätigen Referenten**, die wir gemeinsam mit der Hanns-Seidel-Stiftung für diese Veranstaltung **gewinnen konnten**, werden auf die Brüsseler Vorschläge **noch vertieft eingehen**.

Ich **wünsche Ihnen** und uns allen jetzt noch **interessante und gewinnbringende Stunden**, die wichtige Impulse für die weitere Debatte geben.