

**Innenausschuss**  
**Wortprotokoll**  
83. Sitzung

**Öffentliche Anhörung**

am Montag, 22. Oktober 2012, von 11.00 Uhr bis 13.00 Uhr  
Paul-Löbe-Haus, Raum E 200  
Konrad-Adenauer-Str.1, 10557 Berlin

Vorsitz: Wolfgang Bosbach, MdB  
Gerold Reichenbach, MdB

Öffentliche Anhörung von Sachverständigen  
zur

„Datenschutzgrundverordnung“

- a) *Vorschlag für eine Verordnung des Europäischen Parlaments und des Rates zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr (Datenschutz-Grundverordnung)*  
KOM(2012)11 endg.  
**Ratsdok.-Nr. 5853/12**
- b) Mitteilung der Kommission an das Europäische Parlament, den Rat, den Europäischen Wirtschafts- und Sozialausschuss und den Ausschuss der Regionen  
*Der Schutz der Privatsphäre in einer vernetzten Welt*  
*Ein europäischer Datenschutzrahmen für das 21. Jahrhundert*  
KOM(2012)9 endg.  
**Ratsdok.-Nr. 5852/12**
- c) Antrag der Abgeordneten Dr. Konstantin von Notz, Volker Beck (Köln), Kai Gehring, weiterer Abgeordneter und der Fraktion BÜNDNIS 90/DIE GRÜNEN  
*EU-Datenschutzreform unterstützen*  
**BT-Drucksache 17/9166**

	<u>Seite</u>
<b>I. Anwesenheitsliste</b>	4
<ul style="list-style-type: none"> <li>• Mitglieder des Deutschen Bundestages</li> <li>• Bundesregierung, Bundesrat, Fraktionen</li> </ul>	
<b>II. Sachverständigenliste</b>	6
<b>III. Sprechregister der Sachverständigen und Abgeordneten</b>	7
<b>IV. Protokollierung der Anhörung</b> Bandabschrift	8
<b>V. Anlage A:</b>	
Schriftliche Stellungnahmen der Sachverständigen – Ausschussdrucksachen-Nr.: 17(4)584A ff.	
<ul style="list-style-type: none"> <li>• <b>Professor Dr. Dres. h. c. Spiros Simitis</b> 44 Goethe-Universität, Frankfurt am Main – 17(4)584A</li> <li>• <b>Professor Dr. Ralf B. Abel</b> 47 Rechtsanwalt, PRA Legal, Hamburg 17(4)584B</li> <li>• <b>Dr. Imke Sommer</b> 52 Landesbeauftragte für Datenschutz und Informationsfreiheit der Freien Hansestadt Bremen, Bremerhaven – 17(4)584C</li> <li>• <b>Professor Niko Härting</b> 62 Rechtsanwalt, Berlin – 17(4)584D</li> <li>• <b>Professor Dr. Gerrit Hornung</b> 64 Universität Passau – 17(4)584E</li> <li>• <b>Karsten Neumann</b> 74 Landesbeauftragter für Datenschutz und Informationsfreiheit Mecklenburg-Vorpommern a. D. – 17(4)584G</li> <li>• <b>Dr. Ulrich Wuermeling</b> 80 Rechtsanwalt, Latham &amp; Watkins LLP, Frankfurt am Main 17(4)584F</li> </ul>	
<b>Anlage B:</b>	
Weitere Stellungnahmen:	
<ul style="list-style-type: none"> <li>• Bundesbeauftragter für den Datenschutz und die Informationsfreiheit, Peter Schaar, Berlin/Bonn – 17(4)469 83</li> <li>• Gesellschaft für Datenschutz und Datensicherheit, Bonn – 17(4)518 86</li> </ul>	

• Bundesvereinigung der Deutschen Arbeitgeberverbände (BDA), Berlin – 17(4)541	94
• BfDI - Konferenz der Datenschutzbeauftragten des Bundes und der Länder, Bonn – 17(4)546	100
• Bundesrechtsanwaltskammer, Berlin – 17(4)556	127
• Gesamtverband der Deutschen Versicherungswirtschaft e.V. (GDV), Berlin – 17(4)565	130
• Deutscher Notarverein, Berlin – 17(4)568	143
• Bundessteuerberaterkammer, Berlin – 17(4)577	146
• Zentralverband der deutschen Werbewirtschaft (ZAW), Berlin – 17(4)587	153
• Handelsverband Deutschland (HDE) Deutschland, Berlin – 17(4)588	163
• Bundesverband der Deutschen Industrie e.V. (BDI), Berlin – 17(4)590	172
• Deutsche Kreditwirtschaft, Berlin – 17(4)593	179

## **I. Anwesenheitsliste Mitglieder des Deutschen Bundestages**

**Bundesregierung**

**Bundesrat**

**Fraktionen und Gruppen**

**II. Liste der Sachverständigen für die öffentliche Anhörung am  
22. Oktober 2012**

- |    |  |  |
|----|--|--|
| 1. | Professor Dr. Ralf B. Abel               | Rechtsanwalt,<br>PRA Legal, Hamburg  |
| 2. | Professor Niko Härting                   | Rechtsanwalt, Berlin   |
| 3. | Professor Dr. Gerrit Hornung             | Universität Passau   |
| 4. | Karsten Neumann                          | Landesbeauftragter für Datenschutz<br>und Informationsfreiheit<br>Mecklenburg-Vorpommern a.D.  |
| 5. | Professor Dr. Dres. h. c. Spiros Simitis | Goethe-Universität, Frankfurt am<br>Main   |
| 6. | Dr. Imke Sommer                          | Landesbeauftragte für Datenschutz<br>und Informationsfreiheit der Freien<br>Hansestadt Bremen, |
| 7. | Dr. Ulrich Wuermeling                    | Rechtsanwalt,<br>Latham & Watkins LLP, Frankfurt<br>am Main                                    |

### **III. Sprechregister der Sachverständigen, Abgeordneten und Bundesregierung**

<b><u>Sprechregister der Sachverständigen</u></b>	<b>Seite</b>
<b>Professor Dr. Ralf B. Abel</b>	7, 27
<b>Professor Niko Härting</b>	9, 32, 36
<b>Professor Dr. Gerrit Hornung</b>	12, 41
<b>Karsten Neumann</b>	15, 38
<b>Professor Dr. Dres. h. c. Spiros Simitis</b>	17, 30, 35, 40
<b>Dr. Imke Sommer</b>	19, 31
<b>Dr. Ulrich Wuermeling</b>	21, 26, 33, 35

#### **Sprechregister der Abgeordneten**

<b>Vors. Wolfgang Bosbach</b>	7, 9, 12, 14, 14, 17, 19, 21, 24, 29, 33
<b>Stephan Mayer (Altötting)</b>	24
<b>Dr. Konstantin von Notz</b>	29, 40
<b>Gerold Reichenbach</b>	29, 35, 37, 42
<b>Gisela Piltz</b>	34
<b>Jan Korte</b>	37

#### IV. Protokollierung der Anhörung

Vors. **Wolfgang Bosbach**: Meine sehr verehrten Damen und Herren, liebe Kolleginnen und Kollegen, meine Damen und Herren Sachverständigen, herzlich Willkommen zur Sachverständigenanhörung. Ich danke Ihnen, dass Sie unserer Einladung gefolgt sind, den Innenausschuss und den Deutschen Bundestag bei den anstehenden Beratungen mit Ihrer Kompetenz und Ihrer Erfahrung zu unterstützen. Die Bundesregierung wird im Laufe des Vormittags, gegen 12.00 Uhr, noch in Person von *PSt Dr. Ole Schröder* zu uns stoßen. Sie waren so freundlich und haben uns bereits eine schriftliche Stellungnahme zu den Vorlagen übersandt. Für die eingegangenen Stellungnahmen bedanke ich mich recht herzlich. Das, was Sie sagen, auch die Antworten auf die Fragen und die vorab übersandten Stellungnahmen werden Gegenstand einer Gesamtdrucksache sein. Von der heutigen Veranstaltung wird ein Wortprotokoll gefertigt. Dieses Protokoll wird Ihnen zur Korrektur übersandt. Die Sitzung wird im Parlamentsfernsehen des Deutschen Bundestages übertragen. Wenn Sie sich noch ein bisschen schick machen wollen, besteht jetzt noch dazu die Gelegenheit.

Einleitend möchte ich jedem Sachverständigen die Gelegenheit geben, in einer Erklärung von längstens 5 Minuten zu diesem Anhörungsthema Stellung zu nehmen. Ich verspreche Ihnen – Sie können gar nicht alles, was Ihnen im Kopf herumschwirrt, in 5 Minuten unterbringen –, dass Sie die Zeit und Gelegenheit haben werden, in der nachfolgenden Debatte alles noch zu sagen, was Sie in 5 Minuten nicht unterbringen konnten. Wir müssen hier auch an die kleineren Fraktionen denken, die noch ausreichend Zeit und Gelegenheit bei der nachfolgenden Fragerunde bekommen sollten. Wenn Sie damit einverstanden sind, darf ich als ersten Sachverständigen Herrn Prof. Dr. Ralf Abel aus Hamburg aufrufen.

SV **Professor Dr. Ralf Abel** (Rechtsanwalt, PRA Legal, Hamburg): Vielen Dank, Herr Vorsitzender. Meine Damen und Herren, worüber wir heute zu sprechen haben, ist das „Öl der Wissensgesellschaft“ – so ist es einmal ausgedrückt worden. Es ist ein Gegenstand, der sehr tief in das berufliche und geschäftliche Leben sowie in das alltägliche Leben aller Menschen eingreift. Es geht – nicht mehr und nicht weniger – um eine Regulierung der Kommunikation. Wenn darüber steht: „Datenschutz“ – dann ist das ein Begriff, von dem man glaubt, er sei vielleicht nur auf einen bestimmten Bereich der Rechtsetzung beschränkt, aber in Wirklichkeit ist es die Regulierung der Kommunikation. Aus diesem Grund halte ich es für außerordentlich wichtig, sehr, sehr sorgfältig darüber nachzudenken, was die Kommission vorgelegt hat. Und ich möchte mich heute – in Anlehnung an Ihre Einleitung – in meinem Statement insbesondere auf die verfassungsrechtlichen Gesichtspunkte beschränken. Dort gibt es ganz erhebliche Konstruktionsfehler, die auch verfassungsrechtlich mehr als bedenklich sind, grenzwertig, wenn nicht sogar



schon über die Grenze hinausgehen. Zunächst der erste Punkt: Die uferlose Anwendung des Schutzgegenstandes: Schutzgegenstand sind nicht Daten, Schutzgegenstand ist vielmehr das Persönlichkeitsrecht. Das Persönlichkeitsrecht lässt sich nicht ohne Weiteres definitorisch fassen. Wir haben bereits im Bundesdatenschutzgesetz versucht, die Begriffe „Daten“ bzw. „personenbezogene Daten“ zu beschreiben. Der Gegenstand, der aber im Verordnungsentwurf genannt wird, geht weit darüber hinaus, ist so uferlos weit, dass er eigentlich alle und jede Daten umfasst. D. h., es wird in weitgehende Freiheitsrechte eingegriffen und es ist nicht klar, wo eigentlich die Abgrenzung, z. B. zur Pressefreiheit, liegen soll, denn auch dort hat man ja einen ähnlichen Schutzgegenstand, nämlich das Persönlichkeitsrecht und die freie Meinungsbildung, die Wissensbildung, die Nutzung von Wissen, also das, was wir eben auch hier mit dieser Regelung limitieren, einschränken wollen. Der zweite Punkt ist eine fehlende Differenzierung des Schutzgegenstandes. Es fehlt die Differenzierung nach dem Schutzbedarf. Hier wird recht pauschal in Grundrechte eingegriffen. Es sind die Grundrechte der Informationsfreiheit (Art. 5 GG), aber auch die Grundrechte aus Art. 12, Art. 14 und Art. 2 Abs. 1 GG, die Nutzung von Wissen – auch das eine Frage der Selbstentfaltung –, geschützt durch Art. 2 Abs. 1 GG. Ganz undifferenziert wird ein Regime vorgeschlagen, das einheitlich die unterschiedlichsten Grundrechtseingriffe regeln soll. Darin liegt ein Verstoß gegen die Verhältnismäßigkeit, wenn nicht nach Schutzbedarf differenziert wird, sondern ganz pauschal ein bürokratisches Regime errichtet wird. Nächster Punkt: Zu Grunde wird ein Prinzip gelegt, das zwar im deutschen Bundesdatenschutzgesetz zu finden ist, das aber inzwischen sehr in Frage gestellt wird in der Diskussion der letzten ein, zwei Jahre, nämlich das so genannte Verbotssprinzip. Ein Prinzip, das eigentlich sonst im Waffenrecht, im Atomrecht, beim Kriegswaffenkontrollgesetz und Ähnlichem gilt, nämlich, dass zunächst einmal jede Form von Datenverarbeitung, also von Wissens- und Informationsverarbeitung, verboten ist. Es sei denn, man findet eine gesetzliche Grundlage oder eine andere Rechtsgrundlage. Das kann man im öffentlichen Bereich machen und das ist dort auch richtig. Dort folgt es den gängigen öffentlich-rechtlichen Prinzipien, die für Behörden gelten. Im Bereich der Privatwirtschaft kann dies so nicht gelten, sondern das Verbotssprinzip steht einer Flexibilisierung der Rechtsgrundlage entgegen und führt zu Ergebnissen, die praktisch – ich befasse mich schon seit vielen Jahren auch in der Praxis mit den dann auftretenden Fragen – nicht mehr zu klären sind. Das beste Beispiel ist die Cloud. Man braucht gedankliche Klimmzüge, um das Arbeiten in einer Cloud – so wie es heute immer üblicher wird – überhaupt noch rechtlich fassen zu können. Das könnte man unter dem heutigen deutschen Rechtsregime eigentlich nicht mehr machen. Dieses Problem würde allerdings durch die jetzige Konstruktion der Grundverordnung zementiert. Schließlich habe ich als vierten und vorletzten, verfassungsrechtlich bedenklichen Punkt das Bedenken, dass in Verbindung mit dem Verbotssprinzip die

eingräumten Kompetenzen der Aufsichtsbehörden zu einer modernen Form der Zensur führen könnten. Ich weiß, das ist ein sehr hartes Wort, ich bin mir dessen sehr wohl bewusst. Maßstab für Eingriffe kann und muss nach wie vor die Freiheit der Rede, die Freiheit der Wissensgenerierung, die Freiheit der Wissensnutzung sein. Und wenn man diese Freiheiten – es sind uralte demokratische Freiheiten, um die es geht – einschränken will, dann ist sicherlich am wenigsten eine Behörde dazu geeignet, wie es etwa in Art. 34 der Grundverordnung vorgeschlagen wird. In Fällen, in denen diese Behörde es – in völliger Unabhängigkeit – für richtig hält, auch Verbote aussprechen zu können, unter Umständen so lange, bis man sich europaweit darauf geeinigt hat, ob man ein bestimmtes Vorgehen für rechtmäßig halten kann oder nicht. Es ist eigentlich nichts anderes als das, was wir in anderen Bereichen als Zensur bezeichnet haben. Natürlich kommt der Einwand: Wo kämen wir denn hin, wenn wir auf das Verbotsprinzip und auf alle diese Eingriffe verzichten würden? Da kann ich nur sagen: Da kämen wir dorthin, wo wir heute mit völliger Selbstverständlichkeit im Presserecht stehen. Dort herrscht erst einmal der Grundsatz der Freiheit, der freien Rede, des freien Schreibens, und nur in besonderen Fällen, wo auch ein Schutzbedarf besteht, wird eingegriffen. Das macht der Entwurf in dieser Hinsicht gerade nicht, sondern das Gegenteil. Fünfter und letzter Punkt: „Delegated Acts“, d. h. die Möglichkeit, außerhalb demokratischer Legitimation einen Nebengesetzgeber oder einen Übergesetzgeber in Form der Kommission zu installieren. Man wird zwar sagen: Die „Delegated Acts“ – wir würden im Deutschen Verordnungsermächtigung sagen – würden sich nur auf Formales beziehen. Aber man darf nicht vergessen, dass man über diese Regulierungen, etwa im Bereich der Festlegung, welche Maßstäbe denn für die gewünschte Selbstregulierung gelten sollen – über diese scheinbar technische Maßstabsetzung – ,auch inhaltliche Normen setzt und man in der Lage ist, die bestehenden Normen z. B. auch schärfer, enger oder anders auszulegen, als es sich der Gesetzgeber gedacht hat. Dafür gibt es bereits im heutigen deutschen Recht Beispiele. Wir haben hier einen letztlich materiellen Nebengesetzgeber, der in der Wirklichkeit nicht mehr parlamentarisch kontrolliert wird. Mit diesen fünf Punkten möchte ich meine Bedenken und meinen Blick auf den verfassungsrechtlichen Teil abschließen. Vielen Dank.

Vors. **Wolfgang Bosbach**: Wir danken Ihnen, Herr Professor Dr. Abel. Nächster Sachverständiger, ebenfalls Rechtsanwalt, aber hier in Berlin, ist Professor Härting.

SV **Professor Niko Härting** (Rechtsanwalt, Berlin): Danke schön, Herr Vorsitzender. Meine Damen und Herren, Datenschutz ist ein Bürgerrechtsthema. In Deutschland ist das Datenschutzrecht durch das Volkszählungsurteil geprägt. Das Volkszählungsurteil, das 1983 dem Staat verfassungsrechtliche Grenzen bei der Sammlung von Informationen der Bürger setzte. Das Volkszählungsurteil ist

nach wie vor wichtig. Datenschutz ist aber auch unter den modernen Bedingungen der Informationsgesellschaft ein Bürgerrechtsthema, und da ist es nicht nur ein Bürgerrechtsthema im Verhältnis des Staates zum Bürger, da ist es auch ein Bürgerrechtsthema bei der Regulierung der Kommunikation unter den Bürgern, und da geht es nicht nur um den Schutz der Persönlichkeitsrechte der Bürger, da geht es auch um den Schutz gegen den allzu fürsorglichen Staat, wenn es um die Ausübung von Kommunikationsgrundrechten, von Grundrechten der wirtschaftlichen Betätigungsfreiheit, aber auch der Freiheit der Wissenschaft und Forschung bis hin zur Religionsfreiheit geht. Das ist unter den heutigen Bedingungen zu bedenken. Daten, auch personenbezogene Daten – es gibt kaum Daten unter den heutigen Bedingungen, bei denen sich nicht in irgendeiner Weise einen Personenbezug herstellen lässt – sind der Rohstoff der Kommunikation und auch der Rohstoff wirtschaftlicher Betätigung. Die sich dadurch stellende Notwendigkeit der Abwägung kommt in dem Entwurf in der jetzigen Fassung viel zu kurz. Herr Dr. Masing, Richter am Bundesverfassungsgericht, hat letzte Woche bei der vom BMI veranstalteten Datenschutzkonferenz darauf hingewiesen, dass Datenschutz unter den heutigen Bedingungen stets auch Kommunikationsregulierung bedeutet. Des Weiteren hat er darauf hingewiesen, dass die von der EU-Kommission vorgeschlagene Vollharmonisierung auch eine Vollzentralisierung bedeutet. D. h., wir haben bei dem Vorschlag, den wir aus Brüssel bekommen haben, das Zusammenspiel regulierter Kommunikation und einer zentralen Überwachung durch Behörden, die, – wenn das, was hier aus Brüssel vorgeschlagen worden ist, Wirklichkeit wird – jedenfalls nicht mehr, oder weitgehend nicht mehr, der Kontrolle durch das Bundesverfassungsgericht unterliegt oder – anders gesagt – gar keiner wirksamen verfassungsrechtlichen Kontrolle nach unseren Maßstäben, solange es keine Verfassungsbeschwerde auf europäischer Ebene gibt. Da heißt es: wachsam sein, was dort geschieht, und um die Kommunikationsgrundrechte und andere Grundrechte der Bürger in Deutschland und Europa besorgt sein. Das Datenschutzrecht ist ohne Zweifel dringend reformbedürftig. Da muss man sich ein bisschen zurück in die Zeit vor diesem Vorschlag versetzen. Da bestand unter allen Datenschutzexperten Einigkeit, dass das Datenschutzrecht, wie es jetzt ist, auf viele Fragen, die die Informationstechnik stellt, keine befriedigenden Antworten enthält oder – mit anderen Worten – das Datenschutzrecht, wie wir es jetzt haben, nicht internettauglich ist. Darüber waren sich eigentlich alle einig. Das Problem der Vorschläge aus Brüssel ist, dass hier nach dem Prinzip der vollständigen Selbstbeschränkung vorgegangen wird. Die Brüsseler Vorschläge erheben nicht einmal den Anspruch, Antworten auf die neuen Fragen, die wir in den letzten zehn Jahren zunehmend haben, was die Herausforderung des Internets angeht, zu finden. Sie beschränken sich darauf, die althergebrachten Grundsätze fortzuschreiben, sie hier und da um ein paar neue oder auch nur nach dem ersten Anschein neue Vorschläge zu ergänzen, wie das Recht auf Vergessen, aber im

Wesentlichen soll alles so bleiben, wie es ist. Das muss man kritisieren und dabei kann es nicht bleiben. Die wesentlichen Probleme, die wir in der Anwendung des geltenden Datenschutzrechts haben und auf die wir keine befriedigenden Antworten in dem Brüsseler Vorschlag haben, sind:

Erstens: Der unklare Anwendungsbereich. Wir streiten uns seit mittlerweile 15 Jahren darüber, was eigentlich im Internet unter personenbezogenen Daten zu verstehen ist. Etwa bei Cookies oder IP-Adressen gibt es bis heute unterschiedliche Auffassungen. Das ist grundlegend, denn damit steht und fällt die gesamte Anwendbarkeit des Datenschutzrechts auf Sachverhalte wie das Profiling, das Tracking im Netz. Hierauf gibt es in dem Vorschlag aus Brüssel keine Antworten. Zweitens: Wir haben Gegenläufigkeit von Äußerungs- und Datenschutzrecht. Jeder Student im unteren bis mittleren Semester lernt beim § 823 BGB, wenn wir von Persönlichkeitsverletzungen sprechen, dass dort die Verletzung die Rechtswidrigkeit nicht indiziert. Das ist genau das Umgekehrte des Verbotsprinzips, das wir im Datenschutzrecht haben. So bekommen wir, wenn wir, wie es zunehmend der Fall ist, Sachverhalte haben, wo Äußerungsrecht und Datenschutzrecht parallel laufen, – ich erinnere nur an den Fall „Spickmich.de“ des BGH – große Schwierigkeiten, hier aus dem Datenschutzrecht noch befriedigende Lösungen abzuleiten. Wir haben es schon in der Stellungnahme des DAV zum Datenschutz, die wir ein Jahr vor der Vorlage der Brüsseler Vorschläge gemacht haben, z. B. wie folgt formuliert: Das Verbotsprinzip gehört bei Daten, die ein selbstverständlicher Bestandteil der alltäglichen Kommunikation sind, abgeschafft. Wo es um alltägliche Kommunikation geht, bin ich der festen Überzeugung, dass es nicht zukunftsweisend ist, dort noch mit dem Verbotsprinzip zu arbeiten. Damit stellt sich die Herausforderung, Bereiche, für die das Verbotsprinzip nicht mehr angemessen erscheint, von anderen Bereichen – Stichwort Gesundheitsdaten – abzugrenzen. Aber hier bedarf es innovativer Vorschläge, die in dem Brüsseler Vorschlag fehlen. Der Brüsseler Vorschlag enthält keinerlei Regelung zum Profiling. Das, worüber wir alle doch diskutieren, wenn es um Google und Konsorten geht, dazu haben wir keine Regelungsvorschläge. Das ist überraschend und unbefriedigend. Um mich kurz zu fassen: Wir haben in dem Brüsseler Vorschlag völlig unzureichende Transparenzregelungen, d. h. Informationspflichten der Anbieter sind nur mit sehr allgemeinen Begriffen geregelt. Da heißt es beispielsweise zu den Informationspflichten: Zu informieren sei über Informationen, die unter Berücksichtigung der besonderen Umstände, unter denen die personenbezogenen Daten erhoben werden, notwendig sind, um gegenüber der betroffenen Person eine Verarbeitung nach Treu und Glauben zu gewährleisten. Als praktizierender Jurist – versuchen Sie da einmal auf einer solchen Grundlage Datenschutzbestimmungen zu formulieren. Da ist der Streit mit Aufsichtsbehörden usw. von vorneherein vorgezeichnet. Danke schön!

Vors. **Wolfgang Bosbach**: Wir danken Ihnen, Herr Professor Härting. Es ist ein klassischer Fall objektiver Unmöglichkeit, in 5 Minuten alles unterzubringen, was Sie wissen. Wenn nachher die Fragerunde kommt, machen Sie es einfach wie die Politiker: Beantworten Sie einfach nicht erst die Frage, sondern sagen Sie erst einmal, was Ihnen wichtig ist. Das habe ich gehört. Das soll es schon einmal gegeben haben. Die weiteste Anreise offensichtlich, Herr Professor Dr. Hornung, Sie haben jetzt das Wort.

SV **Professor Dr. Gerrit Hornung** (Universität Passau): Vielen Dank Herr Bosbach, vielen Dank auch für die Einladung. Es ist praktisch Common Sense und wurde bereits gesagt, dass die Reformbedürftigkeit des europäischen Datenschutzrechts mit Händen zu greifen ist. Man muss sich klar machen, dass die Richtlinie von 1995 ist, die ersten Entwürfe von 1991. Das ist eine Zeit, in der es kein World Wide Web gab – das muss man sich klar machen. Deswegen gebührt der Kommission – aus meiner Sicht – Lob dafür, dass sie diese Herkules-Aufgabe angegangen ist. Ich würde auch sagen, dass man die Kommission darin unterstützen sollte. Es gibt vieles in dem Entwurf, was man besser machen kann, und ich werde gleich noch einige Aspekte ansprechen, die man aus meiner Sicht auch substantiell besser machen könnte. Aber ich denke, wir sollten die Gelegenheit nicht vorbeistreichen lassen, mit Hilfe dieses Entwurfs etwas Besseres zu machen. Ich habe einige Punkte, die ich substantiell anders machen würde. Bevor ich aber dazu komme, habe ich einen Punkt, den ich so lassen würde, wie er ist: Das ist das Verbotsprinzip. Ich bin an diesem Punkt absolut anderer Auffassung als meine beiden Vorredner und würde das gerne kurz ausführen. Die Kritik am Verbotsprinzip – von den beiden Kollegen, zusammen mit dem Kollegen Schneider aus München wiederholt vorgetragen – geht aus meiner Sicht von einer unvollständigen Prämisse aus und zieht aus dieser unvollständigen Prämisse die falschen Schlussfolgerungen. Die unvollständige Prämisse liegt darin, dass die private Wirtschaft, die Daten verarbeitet, Grundrechtsträger ist, deswegen anders als der Staat behandelt werden muss und mehr Datenverarbeitungsbefugnis als der Staat haben muss. Diese Prämisse ist richtig, sie ist aber insofern unvollständig als sie suggeriert, dass das nicht der Fall sei. Wenn man sich das geltende Datenschutzrecht anschaut, dann ist aber genau das der Fall. Die private Wirtschaft verfügt über vielfältige generalklauselartige Ermächtigungsgrundlagen für die Datenverarbeitung, so dass im Ergebnis die meisten Verarbeitungen in der privaten Wirtschaft zulässig sind. Man kann da an einigen Punkten nachjustieren und das „Spickmich.de“-Beispiel ist tatsächlich ein Beispiel, wo ich Ihnen, Herr Härting, Recht geben würde: Da müssen wir nachjustieren. Aber im Grundsatz würde ich sagen, dass man an diesem Prinzip festhalten sollte. Diese Zulässigkeit für die Wirtschaft erfolgt auf der Basis von Abwägungen. Jetzt kann man diese Abwägungen, wie es vorgeschlagen wird, auf die Frage des Anwendungsbereichs des Datenschutzrechts verlagern. Das kann

man machen. Was aus meiner Sicht nicht möglich ist, ist, diese Abwägung grundsätzlich anders durchzuführen. Wir können also entweder das Datenschutzrecht erst gar nicht anwenden, oder wir kommen dahin, dass es Anwendung findet, die Datenverarbeitung aber im Ergebnis zulässig ist. Aus meiner Sicht handelt es sich im Wesentlichen um eine regelungstechnische Frage. Dann habe ich vier Punkte von vielen Punkten, die ich gerne kurz anreißen möchte, weil sie aus meiner Sicht der Überarbeitung bedürfen. Erstens: Eine erforderliche Überarbeitung wäre aus meiner Sicht die Präzisierung hinsichtlich des mitgliedstaatlichen Spielraums. Die Mitgliedstaaten dürfen Rechtsgrundlagen für die Wahrnehmung einer Aufgabe regeln. Aus meiner Sicht ist nicht klar, was mit dieser Aufgabe gemeint ist. Um ein konkretes, gerade in Deutschland kontrovers diskutiertes Beispiel zu nehmen: Der private Zugang zu Melderegisterdaten. Das ist eine der umstrittenen Fragen dieses Jahres gewesen. Bedeutet der Vorschlag jetzt, die verbleibende Kompetenz der Mitgliedstaaten – sprich Deutschland – ist, nur noch die Aufgabe: „Wir führen ein Melderegister“ zu regeln und alles Weitere soll aus der Grundverordnung folgen? Das wäre aus meiner Sicht mit deutschen rechtstaatlichen und anderen verfassungsrechtlichen Grundsätzen nicht zu vereinbaren. Oder bedeutet es wie bisher, dass der deutsche Gesetzgeber dafür verantwortlich ist, welche Daten wie lange im Register gespeichert sind, welche Zugriffsformen dort ermöglicht sind und unter welchen Voraussetzungen das erfolgt? Sind all die Fragen, über die Sie alle in diesem Jahr gestritten haben, weiterhin Ihnen überlassen oder soll das abschließend in Brüssel geregelt sein? Das ist aus meiner Sicht nicht klar, man kann darüber streiten und ich denke, dass es präzisiert werden muss. Zweitens: Die Kommission springt zu kurz bei den neuen Betroffenenrechten, insbesondere bleibt sie dort stark hinter der Begrifflichkeit zurück. Dieses ominöse Recht auf „Vergessen werden“: Ich schreibe das inzwischen bei Vorträgen in dreifachen Anführungszeichen, weil es aus meiner Sicht weder ein „Recht“ ist, noch ein Recht „auf“ etwas und schon gar nicht ein Recht auf „Vergessen werden“. Jedenfalls nicht so, wie es im Moment dort geregelt ist. Das Grundproblem ist, dass der Presse- und Meinungsfreiheitsbereich – man kann darüber streiten, ob zu Recht oder zu Unrecht – den Mitgliedstaaten überlassen bleibt. Und das ist meiner Meinung nach der grundlegende Webfehler: Man kann kein unionsweites Recht auf „Vergessen werden“ haben und dann mitgliedstaatliche Rechte auf Meinungsfreiheit, Presserecht usw. – wenn man es etwas überspitzt ausdrücken will, mitgliedstaatliche Rechte auf „Erinnern“ – die einem Recht auf „Vergessen werden“ gerade entgegen laufen. Drittens: Der technische Datenschutz. Das ist ein Punkt, bei dem der Vorschlag viel zu kurz springt. Es gibt keine verbindlichen Vorgaben für den technischen Datenschutz. Es gibt keine verbindlichen Vorgaben für Audits und Gütesiegel. Die Frage des Datenschutzauditgesetzes soll der Kommission überlassen bleiben, etwas, über das Sie alle hier im Bundestag gestritten haben. Der Entwurf ist aus meiner Sicht viel zu technikfern. Und es ist

doch sehr auffällig, dass Grundbegriffe des technischen Datenschutzes wie Anonymisierung oder Pseudonymisierung in dem Entwurf noch nicht vorkommen. Das ist aus meiner Sicht eine Form von Technikferne, die die entscheidenden technischen Fragen komplett der Kommission überlassen soll, und insoweit dringend korrekturbedürftig. Das bringt mich zu meinem letzten Punkt. Viertens, mein Hauptkritikpunkt, der inzwischen von vielen anderen geteilt wird: die Rolle der Kommission. Herr Dr. Abel hat dazu schon etwas gesagt und ich würde das noch etwas schärfer machen. Die Rolle der Kommission ist zweifach stark. Zum einen hinsichtlich der tertiären Rechtsetzung, zum anderen hinsichtlich dieses ominösen Konsistenzmechanismus, der aus meiner Sicht in der jetzigen Form ein bürokratisches Problem darstellt. Bei der tertiären Rechtsetzung ist es so, dass es geradezu auffällt, wenn man einen Artikel findet, an dem nicht als letzter Absatz steht, dass die Kommission das Nähere regelt. Das ist nicht nur in der Menge, sondern auch in dem Detaillierungsgrad, der der Kommission überlassen bleibt, aus meiner Sicht nicht mit dem AEUV zu vereinbaren. Das ist ein primärrechtliches Problem, denn primärrechtlich dürfen solche tertiären Rechtsakte nicht nur wesentliche Vorschriften einer Richtlinie oder einer Verordnung regeln, und das ist aus meiner Sicht hier nicht gewahrt. Das beste Beispiel ist der Arbeitnehmerdatenschutz. Da gibt es nämlich eine Vorschrift, die überlässt diesen den Mitgliedstaaten zur weiteren Regelung, und dann gibt es trotzdem am Ende einen Absatz, wonach die Kommission das Nähere regeln soll. Für mich ist überhaupt nicht klar, nach welchen Maßstäben die Kommission in diesem Bereich tätig sein und wie das Verhältnis zu den Mitgliedstaaten sein soll. Im Kohärenzmechanismus sehe ich schließlich einen starken Widerspruch – das ist mein letzter Punkt – zur Stellung der nationalen Aufsichtsbehörden. Man muss sich klar machen, dass die Kommission die Mitgliedstaaten dazu zwingt, vollständig unabhängige Aufsichtsbehörden vorzusehen. Im Rahmen des Kohärenzmechanismus soll dann aber die Kommission in Einzelfällen eine Letztentscheidungsbefugnis haben, die nun weder in ihrer Zusammensetzung noch in ihrer Organisation, noch ihrer Arbeitsweise irgendetwas mit einer vollständig unabhängigen Datenschutzaufsichtsbehörde gemein hat. Das scheint mir doch ein grundsätzlicher organisationeller Webfehler des Reformentwurfs zu sein. Ich würde sagen, dass in beiden Punkten hinsichtlich der Kommission einiges verändert werden müsste.

Vors. **Wolfgang Bosbach:** Wir danken Ihnen, Herr Dr. Hornung. Jetzt begrüßen wir für den Bundesminister des Innern den PSt Dr. Ole Schröder. Nun kommen wir zum nächsten Sachverständigen. Herr Neumann, Sie sind der ehemalige Landesbeauftragte für Datenschutz und Informationsfreiheit des Landes Mecklenburg-Vorpommern. Herzlich Willkommen, Sie haben das Wort.

SV **Karsten Neumann** (Landesbeauftragter für Datenschutz und Informationsfreiheit Mecklenburg-Vorpommern a. D.): Ich bedanke mich auch für die Einladung und versuche, in 5 Minuten das Wesentliche zusammenzufassen. In den bisherigen Stellungnahmen scheint „Webfehler“ das Wort des Tages zu sein. Ich würde an dieser Stelle auch auf einige hinweisen. Erstens: Wo sind die Vertreter der Kommission? Der Autor des Vorschlags ist nicht hier. Zweitens: Es ist eine europaweite Regelung. Es geht nicht nur um Deutschland. Sicherlich sind es unsere deutschen Interessen, die wir hier vertreten. Was wir aber im Auge behalten müssen, ist, dass alle elektronischen Kommunikationsvorgänge, die gerade im Raum stattfinden, all die Störgeräusche, personenbezogene Daten – im Übrigen in einer Alltagssituation – übermitteln; also ein Bereich, der nach Herrn Härting aus der Datenschutzverordnung herausgenommen werden soll. All diese Kommunikation findet mindestens europaweit, wenn nicht sogar international statt. Das ist eine große Herausforderung und ein Webfehler in unserer deutschen Diskussion, wenn wir das nicht im Auge behalten. Ich finde es sehr treffend formuliert, wie es Herr Hustinx, der Europäische Datenschutzbeauftragte, einmal zum Verordnungsvorschlag gesagt hat und zwar einen Tag nachdem er veröffentlicht wurde: Es mag ein kleiner Schritt für Deutschland sein, aber ein großer für Europa. Wer sich mit der Datenschutzpraxis in europäischen Ländern ein wenig beschäftigt hat oder beschäftigen musste, weiß, dass wir hier in Deutschland tatsächlich sehr weit vorne in der Auseinandersetzung mit dem Thema sind. Der Nachholbedarf in anderen europäischen Ländern, bis sie zu unserem Niveau kommen, ist enorm und insofern ist es völlig verständlich, dass die Europäische Kommission hier jetzt nicht noch einmal 100 Prozent darüber hinausgeht, was wir in Deutschland schon kaum umgesetzt haben. Das ist aus meiner Sicht eine Sache, die wir nicht aus den Augen lassen sollten. Es gibt eine große Übereinstimmung darin, dass das Datenschutzrecht, auch das deutsche Datenschutzrecht, modernisierungsfähig ist und modernisiert werden müsste. Bitte vergessen Sie nicht die Praxis in den Unternehmen, die noch lange nicht auf dem heutigen Stand der Gesetzgebung angekommen ist. Herr Dr. Abel hat das sehr schön verdeutlicht, wenn er sagt, dass diese Fragen erst seit wenigen Jahren in der Öffentlichkeit diskutiert werden, aber schon seit 1995 mit der Richtlinie und viel länger in Deutschland gesetzlicher Standard sind. Dann hat es nur eine Ursache, dass die Umsetzung des Datenschutzrechtes bis vor wenigen Jahren die Industrie und die Unternehmen nicht interessierte: Weil sie nicht verfolgt wurde, nicht kontrolliert wurde und nicht in der öffentlichen Debatte war, ist der einzige Grund, weshalb wir erst seit wenigen Jahren diese Diskussion so geführt haben. Herr Dr. Abel hat es auch deutlich gesagt: Es geht hier um das „Öl der Wissensgesellschaft“, um wirtschaftliche Interessen, um die Informationen, die Arbeitsplätze schaffen, die verwertet werden, die aber gleichzeitig in der Regel personenbezogene Daten von Bürgerinnen und Bürgern sind, die Grundrechte haben. Diese Abwägung zwischen dem Grundrecht und den Interessen der



einzelnen Grundrechtsträger ist die Aufgabe, die der Gesetzgeber leisten muss. Die Europäische Union hat hier, glaube ich, einen sehr ambitionierten Vorschlag gemacht. Im Kern beschränkt sie sich auf ca. 45 Paragraphen mit materiellrechtlichen Regelungen und versucht, das gesamte Thema zu umfassen. Das ist schon eine sportliche Aufgabe und aus meiner Sicht überraschend gut gelungen. Das Verbotssprinzip gerät hier wieder in die Diskussion. Die letzten Jahre haben gezeigt, dass an kaum einer Entscheidung des Bundesverfassungsgerichtes – ich kenne sie nicht alle – heute, nach über 20 Jahren, so deutlich wird, dass die Grundentscheidung goldrichtig war. Dieses Verbotssprinzip hat von Anfang an begriffen, dass die technische Entwicklung, die Entwicklung der Informations- und Kommunikationstechnik, in einem Maße voranschreitet und damit die Grundrechtsgefährdung in einem Maße zerfasert, dass man es nicht über Einzelregelungen fassen kann, sondern sich eigentlich nur mithilfe des Verbotssprinzips dieser Aufgabe stellen kann. Ich habe versucht, mich in meiner Stellungnahme auf wenige inhaltliche Punkte zu beschränken. Das eine ist die in der Debatte in Datenschutzkreisen heftig diskutierte vorgesehene Regelung zur Bestellungspflicht von betrieblichen Datenschutzbeauftragten. Hier ist die Kommission – das wissen wir alle – von dem ursprünglichen Vorschlag von 500 Mitarbeiterinnen und Mitarbeitern bereits auf 250 heruntergegangen. Man meint, das sei ein Kompromiss. Letztendlich ist es nur ein Kompromiss mit den Statistikern, weil nämlich nach der Statistik von Eurostat kleine und mittelständische Unternehmen bei 250 Mitarbeitern aufhören. Allerdings stellt sich die Frage: Ist die Nichtbestellungspflicht eines Datenschutzbeauftragten tatsächlich eine Entlastung für Unternehmen mit weniger als 250 Mitarbeitern? Die zweite Frage: Ist die Anzahl von Mitarbeitern überhaupt ein geeigneter Maßstab, um zu entscheiden, ob in diesem Unternehmen die Unterstützung der Umsetzung von Datenschutzrecht durch einen Datenschutzbeauftragten angemessen ist? Ja oder Nein? Aus meiner Sicht ganz klar Nein. Auch da ist die Datenschutzpraxis in Deutschland einer Meinung: Wir brauchen qualitative Kriterien und nicht zahlenmäßig die Anzahl der Mitarbeiter. Bei großen Unternehmen können wenige mehr Schaden anrichten als 1.500 Werftarbeiter, die zwar auch sehr viel mit Computern zu tun haben, aber wirklich wenig mit personenbezogenen Daten. Das ist der Punkt. Auch hierzu habe ich einen Vorschlag, wie dieses Kriterium inhaltlich definiert werden kann, unterbreitet. Ein Bereich, den die Datenschutzgrundverordnung zwar aufnimmt, ohne ihn aufzuführen, ist der Bereich des Arbeitnehmerdatenschutzes. Es macht auch aus der Sicht europaweit und international tätiger Konzerne überhaupt keinen Sinn, die Verarbeitung von Kundendaten einheitlich zu regeln, die von Mitarbeiterdaten aber nicht. Wenn dann ein Unternehmen weiterhin mit 27 nationalstaatlichen Arbeitnehmerdatenschutzbestimmungen zu tun hat, verpufft sozusagen der Effekt, den man durch eine einheitliche Regelung in dem anderen Bereich hätte. Hier also auch ein Vorschlag, wie im Rahmen einer Vollregelung durch die Kommission das

Thema Arbeitnehmerdatenschutz in dieser Verordnung aufgegriffen werden könnte. Letztendlich ein Vorschlag, wo die Kommission eines der deutschen Regelungsinstrumente übernommen hat, allerdings nicht vollständig, nämlich das so genannte Verfahrensverzeichnis, das sich auch in der Verordnung wiederfindet, allerdings nicht wie nach deutschem Recht, wo das Verfahrensverzeichnis für jedermann zugänglich ist, sondern ausschließlich als Informationsquelle für die Aufsichtsbehörden. Damit entfällt natürlich eine weitere Möglichkeit von externer Kontrolle – die wir gegenwärtig nach deutschem Datennutzerrecht haben und die auf europäischer Ebene angemessen wäre. Vielen Dank.

Vors. **Wolfgang Bosbach**: Vielen Dank, Herr Neumann. Wir kommen auf den – je nach Betrachtungsweise – linken oder rechten Flügel. Sie sind nicht zum ersten Mal bei uns hier zu Gast und deswegen immer herzlich Willkommen, von der Goethe-Universität in Frankfurt am Main, Herr Prof. Dr. Simitis.

SV **Professor Dr. Dres. h. c. Spiros Simitis** (Goethe-Universität, Frankfurt am Main): Ich will mich eingangs auf fünf Punkte beschränken, von denen ich meine, dass sie für die gesamte Diskussion wichtig sind.

Mein erster Punkt: Datenschutz. Gleichviel, ob man seine Anfänge in den 70er Jahren, seine weitere Fortsetzung in den 80er Jahren oder seinen heutigen Zustand nimmt, der Datenschutz ist immer – und ich lege großen Wert darauf, das zu unterstreichen – eine Reaktion auf die Informations- und Kommunikationstechnologie. Wer deshalb über die Anforderungen des Datenschutzes spricht, sich mit ihnen auseinandersetzt oder sie ändern will, muss immer den Stand der Kommunikationstechnologie präsent haben und sich an diesem orientieren. Eine Alternative zu einer Revision der gegenwärtigen Regelung gibt es so gesehen nicht. Wir haben, wie sich am Internet zeigt, wieder einen Wendepunkt in der Technologie erreicht. Wir müssen darauf reagieren. Gleichviel freilich, welches Instrument man wählt und wie man im Einzelnen vorgeht, es ist fast schon zu spät.

Wer, wie wir es heute vorhaben, über die Verordnung diskutieren möchte, darf – das muss auch in Richtung Brüssel gesagt werden – nicht vergessen, dass sich beim Datenschutz, spätestens seit den 80er Jahren, ein grundlegender Wandel vollzogen hat. Reaktionen des Gesetzgebers haben sich mehr und mehr auf die bereichsspezifische Ebene verlagert. Dort kann man die Konflikte besser erkennen, dort lassen sich folglich auch effizientere Maßnahmen konzipieren. Eine „Grundregelung“, wie sie die Kommission anstrebt, lässt sich deshalb nicht richtig bewerten, ohne sie in die Gesamtheit der bereits bestehenden oder noch angestrebten Vorschriften einzufügen. Nur dann können sowohl ihre Tragweite als auch ihre Wirkung, ebenso wie die Gestaltung ihrer Vorschriften korrekt beurteilt werden. Ich erinnere Sie lediglich an das Beispiel der Telekommunikation, bei der die Kommission nicht gezögert hat, sich gezielt für besondere Vorschriften zu

entscheiden, und damit Funktion und Bedeutung bereichsspezifischer Regelungen unterstrichen hat. Ebenso klar ist aber auch, dass eine Diskussion, wie wir Sie heute hier führen, nur solange Sinn macht, wie die „Grundregelung“ nicht mit Kompetenzansprüchen unterlaufen werden darf. Eine Generaldirektion kann und darf also zwar grundsätzlich so reagieren, wie sie es möchte, muss sich aber dabei durchweg an der Grundordnung ausrichten.

Mein dritter Punkt – und da sind wir uns sicher alle einig –: Die Kommission hat das Recht, genau das Instrument zu wählen, das sie für angemessen ansieht. Der Übergang von der bislang maßgeblichen Richtlinie von 1995 zu einer Verordnung ist infolgedessen unstreitig zulässig. Zwei Bemerkungen drängen sich freilich auf: Die Mitgliedsländer – und das trifft Deutschland ganz besonders – haben, anders als früher, nicht mehr die Möglichkeit, die Verabschiedung abzuwarten und folglich erst in dem Augenblick, in dem die Verordnung in den nationalen Bereich umgesetzt werden soll, darüber nachzudenken, wie sich den Erwartungen des je spezifischen Mitgliedslandes am ehesten entsprechen ließe. Die Mitgliedsländer müssen vielmehr die Verordnung wörtlich übernehmen und sich uneingeschränkt an das halten, was sie vorschreibt. Deutschland ist daher genauso wie die anderen Mitgliedsländer mehr denn je verpflichtet, bereits zum jetzigen Zeitpunkt in die Diskussion einzusteigen, kritische Punkte vorzubringen sowie nötige Korrekturen anzustreben.

So sehr es zudem der Kommission freisteht, einer Verordnung den Vorzug zu geben, so deutlich geht damit die Pflicht einher, die mit ihr verbundenen Erwartungen klar und jederzeit nachvollziehbar zu formulieren. Nur wenn verständlich ist, was gefordert wird und wie im Einzelnen verfahren werden muss, kann die Verordnung ihrer Aufgabe genügen, verlässlich vorzugeben, wie sich der Umgang mit den Daten zu gestalten hat. Legt man jedoch diesen Maßstab an, fällt das Ergebnis fatal aus. An mindestens 40 Stellen wird nach einigen allgemeinen Sätzen alles Nähere nachträglichen Dekreten überlassen. Niemand, der hier sitzt, ist so gesehen in der Lage, die einschlägigen Vorschriften wirklich zu beurteilen, soweit sie mit dem Vorbehalt der Kommission verknüpft sind, sich zu einem späteren Zeitpunkt zum genauen Inhalt der jeweiligen Bestimmungen sowie in einem ganz anderen Regelungsinstrument zu äußern.

Mein vierter Punkt: Den Datenschutz als Reaktion auf die Informations- und Kommunikationstechnologie zu verstehen, bedeutet auch und vor allem, dass jede Datenschutzregelung notgedrungen vorläufig ist, weil sich die Technologie permanent ändert und der Gesetzgeber deshalb seiner Aufgabe nicht nachkommen kann, soweit er seine Vorgaben nicht als Annäherung versteht, die er ständig überprüfen muss, um die Notwendigkeit revidierter, der Technologie angepasster Anforderungen rechtzeitig auszumachen. Das Internet demonstriert die Aktualität genau dieser Aussage.

Aus eben diesem Grund möchte ich ein weiteres Mal auf das Beispiel jener Staaten verweisen, die in ihren Datenschutzgesetzen deren Geltungsdauer

ausdrücklich angeben und damit die jeweiligen Parlamente explizit an den Zeitpunkt erinnern, an dem neu nachgedacht werden muss. Erst recht gilt es aber vor diesem Hintergrund zu fragen, wie lange es noch bis zur Anwendung der Verordnung dauern soll. Wenn mittlerweile von einigen Jahren die Rede ist, kommt man schwerlich umhin, sich – gerade um einen vorzeitigen Verfall der gesetzlichen Regelung möglichst zu vermeiden – zu überlegen, wie eine Technologie, die sich durch ihren ständigen und immer schnelleren Wandel auszeichnet, dann aussehen könnte.

Mein letzter Punkt: Manche Bestimmungen des Entwurfs sind völlig verfehlt. Beispielhaft dafür ist etwa die für die Wahl eines Datenschutzbeauftragten vorausgesetzte Anzahl der Beschäftigten. Nicht anders ist es bei der Haftung. Wie der Schadenersatz aussieht, bleibt unklar. Das war sicherlich auch bisher so. Nur verträgt sich eine durchaus verschiedene Interpretation nicht mit einer Verordnung. Schließlich, Konzessionen, wie sie bei der Einwilligung gemacht werden, um ihren Anwendungsbereich einzuschränken, leuchten zwar zunächst durchaus ein, reichen jedoch nicht aus. Nicht von ungefähr lässt der dem Bundestag vorliegende Gesetzesentwurf zum Arbeitnehmerdatenschutz eine Einwilligung bei der Verarbeitung der Daten von Beschäftigten nur zu, wenn sie sich auf einer einschlägigen gesetzlichen Regelung gründet. Kurzum, Alternativen zu den augenblicklichen Vorschlägen gibt es durchaus, sie sind allerdings mit einer beträchtlichen Arbeit am Entwurf verbunden.

Vors. **Wolfgang Bosbach**: Vielen Dank, Herr Prof. Dr. Simitis. Frau Dr. Sommer, Sie sind die Landesbeauftragte für Datenschutz und Informationsfreiheit in Bremen und Bremerhaven. Sie haben das Wort.

SV **Dr. Imke Sommer** (Landesbeauftragte für Datenschutz und Informationsfreiheit der Freien Hansestadt Bremen): Herzlichen Dank für die Gelegenheit zur Stellungnahme. Nicht überall da, wo Datenschutz draufsteht, ist Datenschutz auch drin. Wir sind es denjenigen, die jetzt vielleicht nicht im Saal sind, sondern die insgesamt unsere Debatte verfolgen, aber schuldig, über Datenschutz zu reden. Das Kürzel der Verordnung lautet Datenschutzgrundverordnung. Wenn wir uns den Langtext des Verordnungstitels angucken, merken wir, warum diese Erwartung nicht überall erfüllt wird. Der lautet nämlich „Verordnung zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten“ aber dann auch: „und zum freien Datenverkehr“. D. h., wir haben eine Situation, in der wir zwei Rechtsgüter haben. Das kennen wir aus dem Verfassungsrecht. Für die Fälle, in denen wir zwei Rechtsgüter haben, die wir miteinander abwägen sollen, hat uns Prof. Hesse ein wunderschönes Instrument an die Hand gegeben, das heißt praktische Konkordanz. Da geht es darum, dass beide Rechtsgüter weitestmöglich verwirklicht werden.

Hier haben wir aber eine andere Situation. Wir haben das Rechtsgut des freien Datenverkehrs und so wie es uns die Kommission vorgelegt hat, ist dieses Rechtsgut zu 100 Prozent verwirklicht. In der europäischen Logik ist es so: Wenn wir eine Verordnung haben, wenn wir nicht die Möglichkeit haben, dass Mitgliedstaaten über dieses Regelungsniveau hinausgehen, dann gelten überall in Europa exakt dieselben Regelungen. Wenn Daten fließen wollen – das ist ja die europäische Logik –, dann werden sie nicht an der Grenze aufgehalten, sondern sie können fließen. Letztlich haben wir 100 Prozent für das eine Rechtsgut. Das ist dann keine praktische Konkordanz mehr. Das liegt an der Unterschiedlichkeit dieser beiden Rechtsgüter.

Im Datenschutz ist es anders. Da hilft es nichts, wenn überall dieselben Regelungen gelten. Im Datenschutz ist nur interessant, wie hoch die Regelungen sind. Je höher das Regelungsniveau ist, desto mehr wird dieses Recht auf Datenschutz erfüllt. Deswegen ist es ganz wichtig, dass man sagt, dass man ein hohes Datenschutzniveau auf europäischer Ebene hat, aber es muss die Möglichkeit geben, dass man darüber noch hinausgeht. Gerade wenn man in einer solchen Situation ist, die wir hier alle als den Ausgangspunkt sehen, nämlich dass sich die Technik entwickelt, dass wir neue Regelungen haben müssen, müssen wir wieder neu darüber nachdenken. Dann sind wir in so einer Situation, wo sich kreative Lösungen entwickeln können. Ich komme aus Bremen, ich bin Föderalistin, ich glaube, heterogene Gruppen sind kreativ. Wenn man unterschiedliche Situationen hat, in denen man verschiedene Lösungen für neue Probleme findet, dann kommt man weiter und dann kommt man auch für den Datenschutz weiter.

Das Wichtige zu diesem Zeitpunkt ist, dass klar ist, dass man diese Logik – wir brauchen ein hohes Mindestdatenschutzniveau, worüber die Mitgliedstaaten hinausgehen können – nicht nur für den öffentlichen Bereich braucht. Die brauchen wir auch für den nicht-öffentlichen Bereich, für die Wirtschaft. Da fühlen sich die Menschen in der Tat extrem angegriffen. Da haben sie kein Vertrauen. Das sagt die Kommission auch. Den Menschen fehlt das Vertrauen, dass im Internet ihre Daten sicher sind. Deswegen liegt die europäische Online-Wirtschaft am Boden, weil die Leute das Vertrauen nicht haben. Man kann aber ein Vertrauen nur aufbauen, wenn es gerechtfertigt ist. Wir müssen ein Mindestdatenschutzniveau haben, das gerechtfertigt ist, wo sich die Menschen darauf einstellen können und dann kann es noch mehr sein. Selbst in der Logik der Kommission ist es wichtig, das zu haben und auch für den nicht-öffentlichen Bereich.

Beim öffentlichen Bereich ist es eher so, dass die Mitgliedstaaten alle dagegen halten und wollen, dass der öffentliche Bereich ausgenommen wird, und sagen, wir wollen unsere eigene Regelungen durchsetzen, wir haben unterschiedliche Verfassungsgeschichten. Da müssen wir aus Datenschutzsicht aufpassen, dass da wohlmöglich die Situation entsteht, dass da keine europäische Regelung

zustande kommt. Um es einfach zu sagen: Das, was da jetzt vorgelegt ist, ist noch nicht geeignet, Vertrauen zu schaffen.

Da sind schon ganz viele Argumente gekommen. Es fehlen die technischen Anforderungen. Dazu ist ganz viel gesagt worden. Wenn ich nicht weiß, wie die Technik beschränkt wird – das begründet auch mein Misstrauen – und wie sie begründet wird und was dazu in der Verordnung drinsteht, dann schafft das kein Vertrauen. Auch die Bindung von technischen Angaben daran, was sie kosten, schafft kein Vertrauen. Wenn ich weiß, dass die das nur machen, wenn das nicht so viel kostet, dann glaube ich nicht, dass sie es tun. Es fehlt so eine Verpflichtung, Geräte und Programme von sich aus datensparsam herzustellen, Grundeinstellungen datenschutzkonform vorzulegen. Ein datenschutzrechtlicher Hammer ist tatsächlich auch die Geschichte, dass kleine und mittlere Unternehmen von datenschutzrechtlichen Anforderungen entbunden werden. Ich kann doch als Nutzerin des Internets nicht voraussagen, wie viele Mitarbeiterinnen und Mitarbeiter die Firma, deren Anwendung ich nutze, beschäftigt. Das kann ich doch nicht wissen. Mein Vertrauen da hinein, dass das möglicherweise eine Firma ist, die groß genug ist, um diese Anforderungen gegen sich gelten lassen zu müssen, kann nicht entstehen. Der Verzicht auf Einwilligungserfordernisse baut sogar Vertrauen ab. Wenn man sich anguckt, dass die Kommission sich selbst die Befugnis nimmt, Nicht-EU-Länder als datenschutzrechtlich unbedenklich zu erklären und bei dieser Entscheidung sogar elementare Anforderungen wie Rechtstaatlichkeit nur berücksichtigen muss, schafft das auch kein Vertrauen.

Die Liste ist viel, viel länger. Das ist genau unser Problem. Es besteht die Gefahr, dass wir noch nicht alles gefunden haben. Es besteht aus Datenschutzsicht die extreme Gefahr, dass wir uns nicht durchsetzen. Genau deshalb brauchen wir jetzt einen argumentativen Kampf um diese Mindeststandards, aber dann auch einfach die Möglichkeit – um dieses Vertrauen zu schaffen, das auch die wirtschaftliche Grundlage für Unternehmen ist – einen Mindeststandard zu schaffen, auch und gerade im nicht-öffentlichen Bereich.

Vors. **Wolfgang Bosbach**: Vielen Dank, Frau Dr. Sommer. Neben mir sitzt Herr Dr. Heynckes. Er ist Mönchengladbach-Fan. Wir haben aber trotzdem eine Sachverständige aus Bremen eingeladen, was nach dem letzten Spieltag nicht selbstverständlich war. Herr Dr. Wuermeling, Sie sind Kollege aus Frankfurt am Main, Sie haben jetzt als letzter Sachverständiger das Wort.

SV **Dr. Ulrich Wuermeling** (Rechtsanwalt, Latham & Watkins LLP, Frankfurt am Main): Vielen Dank, Herr Bosbach. Ich werde die Gelegenheit wahrnehmen, zwei Punkte anzusprechen. Erst einmal eine grundsätzliche Frage und dann etwas hinsichtlich der praktischen Anwendung dieser Verordnung. Die grundsätzliche Frage: Was müssen wir überhaupt europäisch regeln? Der Grundsatz ist die Subsidiarität. Das bedeutet, dass alles besser national geregelt ist, es sei denn, es

gibt gute Gründe, es anders zu tun. Das Misstrauen gegenüber der Europäischen Kommission, von dem wir hören, spricht vielleicht auch ein bisschen dafür. Es gibt im öffentlichen Bereich auf der Ebene der EU dafür Vorschriften. Es gibt den Vertrag von Lissabon, Art. 8 der Grundrechtecharta, der den Datenschutz regelt und Art. 16 des Vertrages über die Arbeitsweise der Europäischen Union. Diese Regelungen sehen vor, dass europäisch nur geregelt werden soll, was auch einen europarechtlichen Bezug hat. Die Regelung im öffentlichen Bereich, wie sie jetzt vorgeschlagen ist, die praktisch für jede Schule gelten würde, die wir hier in Deutschland betreiben, ist meiner Ansicht nach davon nicht gedeckt. Meiner Ansicht nach muss man die Fragen der Subsidiarität jetzt im Gesetzgebungsverfahren geltend machen und sicherstellen, dass hier die Grenzen klar gezogen werden, denn von alleine wird es nachher nicht funktionieren. Ein Beispiel dafür: Wenn Sie eine Schule betreiben, dann würde die Europäische Kommission über delegierte Rechtsakte festlegen, welche technischen Sicherheitseinrichtungen diese Schule für ihre Datenverarbeitung haben muss. Das ist etwas, was auf keinen Fall auf europäischer Ebene gemacht werden muss und damit ist es auch nicht notwendig, es dort zu tun. Das zweite Thema, auf das ich eingehen will, ist die Frage, ob eigentlich alltägliche und wenig riskante Datenverarbeitungen europäisch geregelt werden müssen. Das sind Datenverarbeitungen, die weder überraschend noch in irgendeiner Form beunruhigend sind. Dazu will ich Sie durch eine ganz kurze „Sightseeing-Tour“ durch die Verordnung mitnehmen. Wenn Sie irgendein Beispiel nehmen: Wir nehmen jetzt einen Landwirt, der Eigenvertrieb macht. Er sammelt E-Mail-Adressen und Anschriften seiner Kunden und möchte eben damit Eigenvertrieb betreiben und diese Kunden bewerben und ihnen sagen, wenn es eine Neuschlachtung oder Ähnliches gab. Er muss sich mit dieser Verordnung beschäftigen. Es fängt damit an, dass er sich die Frage stellen muss, ob die Datenverarbeitung dem Grundsatz nach Treu und Glauben entspricht. Ich weiß nicht, zu welchem Ergebnis er kommt. Dann muss er die Datenverarbeitungen, die er durchführt, in einer Weise durchführen, dass sie für den Betroffenen nachvollziehbar ist. Wenn er Cloud-Computing-Dienste oder Ähnliches verwendet, kann auch das schon wieder fraglich sein. Dann muss er die Zwecke dieser Verarbeitungen genau festlegen. Ich weiß nicht, in welcher Form er das dann tun würde, aber wir nehmen einmal an, dass es nur zu Werbezwecken ist. Dann würde es ihm gelingen. Dann müssen die Daten, die er dort speichert, für die Zwecke angemessen und sachlich relevant sein. Das ist auch eine Prüfung, die er durchführen muss, vielleicht bei den E-Mail-Adressen und bei den Anschriften noch einfach, bei weiteren Daten sicher schwierig. Sie müssen sachlich richtig und auf dem neuesten Stand sein. Das muss er über die Zeit auch sicherstellen, was er beispielsweise, wenn sich die Adresse ändert, beim Meldeamt nicht mehr nachfragen kann, weil die Daten zu Werbezwecken verwendet werden sollen – jedenfalls dann, wenn sich die Forderungen des Bundesrates durchsetzen. Dann

muss er die Daten in einer Form speichern, dass die Person identifizierbar ist. Wenn er nur die E-Mail-Adresse hat, ist das schon nicht mehr gewährleistet. Außerdem muss er eine Interessenabwägung vornehmen, d. h. die berechtigten Interessen gegen die schutzwürdigen Interessen abwägen und überlegen, ob er zu Werbezwecken diese Daten hier verarbeiten darf. Das dürfte noch einigermaßen einfach sein. Er muss sich aber bei Zweckänderungen, d. h., wenn jemand einmal eine Bestellung aufgegeben hat und er die Daten jetzt zu Werbezwecken verwenden will, überlegen, ob das eigentlich mit dem ursprünglichen Zweck noch vereinbar ist oder nicht. Auch da kann man zu unterschiedlichen Ansichten kommen. Meiner Ansicht nach ist es vereinbar. Hier gibt es aber auch andere Ansichten, was diese Zweckbindungsregelung bedeuten soll. Er muss aufpassen, wenn er Daten von einem Kind bekommt, das unter 13 Jahre alt ist. Wenn er von dem eine E-Mail-Adresse bekommt und ihm Werbung schickt, dann wäre das auch unter der Verordnung verboten, es sei denn, man kommt zum Ergebnis, dass er keine Dienste der Informationsgesellschaft anbietet. In solche Detailprüfungen muss er einsteigen und sich fragen, ob seine Webseite, die Informationen über seinen landwirtschaftlichen Betrieb gibt, dann ein Dienst der Informationsgesellschaft ist. Dann möchte er bei bestimmten Personen vorhalten, wo er es eben weiß, dass diese bestimmte Fleischsorten beispielsweise nicht essen. Wenn er sich dann merkt, dass jemand Moslem ist und deshalb kein Schweinefleisch isst, dann kommt er in die Regelung für besondere Kategorien von Daten. Da eröffnet sich dann ein ganzer Prüfungskatalog, der damit im Zusammenhang steht. Er muss eine Richtlinie vorsehen, eine Policy, die jedermann leicht zugänglich ist und seine Datenstrategie enthält. Er muss ein elektronisches Verfahren schaffen, damit man sein Recht auf Auskunft und Berichtigung geltend machen kann. Dann muss er die Betroffenen informieren, und zwar mit dem ganzen Katalog von Informationen. Seine eigenen Kontaktdaten, den Zweck der Verarbeitung, die Dauer, d. h. er muss sich überlegen, wie lange er diese E-Mail-Adressen speichert. Er muss über das Auskunftsrecht informieren, über die Adresse der Datenschutzaufsichtsbehörde. Er muss darüber informieren, wenn die Daten möglicherweise in ein Drittland exportiert werden, das wäre möglicherweise der Fall, wenn er einen Cloud-Anbieter nutzt. Dann muss er noch über sonstige Informationen berichten, die später irgendwann die Europäische Kommission in irgendwelchen delegierten Rechtsakten festlegt. Falls er die Daten nicht von der Person erhebt, die sie betreffen, dann geht es noch weiter, d. h. wenn ich ihm beispielsweise die E-Mail-Adresse meiner Frau geben würde, dann müsste er all diese Informationen auch erst einmal meiner Frau entsprechend zusenden. Dann kommt etwas, was meines Erachtens richtig ist: Es gibt ein Widerspruchsrecht gegen Werbenutzung und darauf muss er hinweisen. Jetzt geht es weiter mit technisch-organisatorischen Maßnahmen. Die muss er nämlich einhalten und diese werden später auch von der Europäischen Kommission festgelegt. D. h. er muss dann wahrscheinlich in



delegierte Rechtsakte auf der Webseite der Europäischen Kommission schauen, um zu sehen, welche technisch-organisatorischen Maßnahmen hier einzuhalten sind. Wenn er einen technische Dienstleister nutzt, kommt er in einen riesigen Regelungsbereich über Auftragsdatenverarbeitung, den er auch noch einhalten muss. Dann gibt es noch Sicherheitsanforderungen, die die Europäische Kommission festlegen kann. Da muss er dann wieder auf die Webseite der Europäischen Kommission schauen. Und weil er Gesundheitsdaten mit dabei hat, kommt er möglicherweise in eine Folgenabschätzungsregelung, die auch wieder einiges mit sich bringt. Wenn man sich das alles überlegt, muss man sich doch an irgendeiner Stelle die Frage stellen, ob wir wirklich alle Regelungen, die wir hier haben, auf jede Art Datenverarbeitung anwenden müssen. Meiner Ansicht nach ist das bei alltäglichen und wenig riskanten Datenverarbeitungen nicht der Fall. Das sind meiner Ansicht nach mindestens 90 Prozent aller Datenverarbeitungen, die wir haben. Für diese würde es ausreichen, wenn man wenige Grundregeln zur Sicherheit, zum Auskunftsrecht, zur Berichtigung und zum Werbewiderspruch hat. Ich finde die Idee richtig, sich darauf zu konzentrieren, Datenschutz dort zu regeln, wo Risiken bestehen und sie dort aus meiner Sicht angemessen streng zu regeln, aber sich eben stärker darauf zu konzentrieren, diese Bereiche zu regeln. Das wäre es von meiner Seite an dieser Stelle.

Vors. **Wolfgang Bosbach**: Vielen Dank, Herr Dr. Wuermeling. Wir kommen jetzt zur Fragerunde der Berichterstatterinnen und Berichterstatter der Fraktionen. Ich darf darum bitten, nicht nur die Frage zu formulieren, sondern sie auch an die Sachverständigen zu adressieren. Herr Kollege Mayer, bitte.

BE **Stephan Mayer (Altötting)** (CDU/CSU): Vielen Dank. Ich habe an zwei Sachverständige Fragen, an Herrn Dr. Wuermeling und Herrn Dr. Abel. Zunächst einmal meine Frage an Herrn Dr. Wuermeling: Ich darf gleich an Ihre zuletzt gemachten Ausführungen anknüpfen. Der Grundsatz der Kommission ist die Einwilligung. Art. 7 Abs. 1: Die Datenverarbeitung ist nur dann zulässig, wenn eine Einwilligung der betroffenen Person vorliegt. Nun ist dies ein diametraler Widerspruch zu dem bisherigen deutschen Datenschutzrecht. Die Frage, die sich meines Erachtens stellt, ist: Wie wird mit Altfällen verfahren, gesetzt den Fall, die Verordnung tritt im Jahre 2015 in Kraft? Müssen dann alle Unternehmen bei all ihren bisherigen Kunden, deren Daten sie natürlich in ihren Informationssystemen haben und bisher auch verarbeiten, legal verarbeiten, dann neu erheben, sprich von all ihren Kunden eine neue Einwilligung einholen oder drängt sich nicht die Notwendigkeit auf, dass eine Übergangsregelung für die Fälle gefasst wird, die bisher nach legalen Gesichtspunkten der Datenverarbeitung unterliegen? Die zweite Frage bzgl. der Einwilligung bezieht sich auf den Art. 7 Abs. 4, der die individuelle Einwilligung für den Fall, dass zwischen den Vertragspartnern ein erhebliches Ungleichgewicht besteht, ausschließt. Sehen Sie hier nicht die Gefahr,

dass dieser Artikel unwägbar formuliert ist? Es stellt sich die Frage: Wann besteht zwischen Vertragspartnern ein erhebliches Ungleichgewicht? Besteht auch zwischen Facebook und Google und der jeweiligen Einzelperson ein erhebliches Ungleichgewicht oder nicht? Sehen Sie hier die Notwendigkeit einer Konkretisierung des Art. 7 Abs. 4? Eine weitere Frage an Sie, Herr Dr. Wurmeling: Es ist jetzt schon diverse Male von den Sachverständigen angesprochen worden, dass diese praktische Konkordanz zwischen den Persönlichkeitsrechten auf der einen Seite und den Rechten des Binnenmarktes und den Wirtschaftsrechten auf der anderen Seite, möglicherweise in dieser Verordnung, in diesem Entwurf nur unzutreffend vorgenommen wurde, insbesondere auch was kleinere Unternehmen anbelangt. Nun sieht der Art. 28 Abs. 4 eine Ausnahme für kleinere Unternehmen vor, was die Dokumentationspflichten anbelangt. Sehen Sie die Notwendigkeit – Sie haben auf einige Auskunfts- und Informationspflichten hingewiesen, Art. 14 und 15 –, dass eine ähnliche Ausnahme auch für Auskunfts- und Informationspflichten nach den Art. 14 und 15 vorgenommen wird, insbesondere für kleinere und mittelständische Unternehmen und – Sie haben sehr anschaulich einen Fall geschildert – diese, was die Risikoadäquanz anbelangt, nicht zur Gefahr geneigt sind wie andere Unternehmen, wie möglicherweise Facebook oder Google. Lieber Dr. Abel, an Sie die Frage gerichtet, wie mit diesen delegierten Rechtsakten umzugehen ist? Wir haben von einigen Sachverständigen schon diese deutliche Kritik vernommen, dass die Anzahl der delegierten Rechtsakte zu groß ist und sich da natürlich die Frage anschließt, auch insbesondere unter verfassungsrechtlichen Gesichtspunkten, wie Sie diese Vorgabe der Kommission einschätzen, dass hier in nahezu 50 Fällen die konkrete Ausgestaltung des geltenden Datenschutzrechtes der Kommission ohne jegliche Einflussmöglichkeit von dem Europäischen Parlament oder auch von nationalen Parlamenten überlassen bleibt? Durchaus aber auch diese Frage im Zusammenhang mit der rasanten Entwicklung des Datenschutzrechtes, insbesondere aufgrund der rasanten Entwicklung unserer Informations- und Kommunikationstechnologie. Wenn man sich vor Augen hält, dass die Richtlinie aus dem Jahre 1995 stammt, aus der Zeit, als das Internet noch in den Kinderschuhen stand, natürlich auch verbunden mit dem partikularen Verständnis dafür, dass aufgrund dieser rasanten technologischen Entwicklung auch ein gewisser Spielraum für die Kommission überlassen bleiben muss, insbesondere im Rahmen des technischen Datenschutzes, auch auf diese sich veränderten Gegebenheiten einzugehen und diesen Rechnung zu tragen. Die letzte Frage bezieht sich auf die Art. 57ff., sprich auf das vorgesehene Kohärenzverfahren: Wie schätzen Sie unter verfassungsrechtlichen Gesichtspunkten diese Möglichkeit der Kommission ein, dass diese Befugnisse der nationalen Datenschutzaufsichtsbehörden ausgehöhlt werden und doch hier eine Allgemeinzuständigkeit über die Gefahr der Allgemeinzuständigkeit des europäischen Datenschutzbeauftragten aufbringt?

Vors. **Wolfgang Bosbach**: Vielen Dank. Herr Dr. Wuermeling, bitte.

SV **Dr. Ulrich Wuermeling** (Rechtsanwalt, Latham & Watkins LLP, Frankfurt am Main): Erst einmal zur Rolle der Einwilligung. Es ist natürlich so, dass in dem Vorschlag der Verordnung auch eine ganze Reihe anderer Rechtsgrundlagen außer der Einwilligung enthalten sind. Es ist aber meines Erachtens von der Wertung her – da gebe ich Ihnen Recht – sicher so, dass die Einwilligung eine stärkere Bedeutung haben soll. Das liegt daran, dass man erstens den Zweckbindungsgrundsatz verstärkt hat, es liegt zweitens aber auch daran, dass die so genannte Interessenabwägungsklausel, die wir sonst häufig benutzen, in Zukunft von der Kommission ausgestaltet werden soll und auf diese Weise natürlich eine zusätzliche Beschränkung, die wir heute in diesem Bereich noch nicht haben, hinzukommen könnte, die dazu führt, dass man stärker auf eine Einwilligung abstellt. Die Einwilligung selber ist in einigen Situationen sicherlich ein wichtiges und auch richtiges Instrument. Man muss nur aufpassen, dass man die Einwilligung wirklich nur für Fälle verwendet und sie auch nur für Fälle anwendbar macht, bei denen große Gefahren für die betroffenen Personen bestehen. Wenn man das nicht tut, dann verbraucht sie sich. Wenn man bei jeder Stelle eine Einwilligung einholen muss, dann achten die Beteiligten nicht mehr darauf. Die Warnfunktion geht verloren, d. h. wir entledigen uns mit der Ausweitung des Anwendungsbereichs der Einwilligung eines ganz wichtigen Instruments des Datenschutzes. Die Einwilligung selbst, so wie sie geregelt ist, hat tatsächlich das ein oder andere Problem. Eine Übergangsregelung ist sicherlich eine Frage, die sich stellt. Was passiert mit alten Einwilligungen? Bisher gibt es keine Übergangsregelungen. Insofern gebe ich Ihnen Recht, dass man an dieser Stelle darüber nachdenken sollte. Was die Tatsache anbelangt, dass die Europäische Kommission sagt, dass, wenn ein Ungleichgewicht besteht, die Einwilligung dann nicht wirksam sein soll, führt zu einer ganz erheblichen Rechtsunsicherheit, denn Sie wissen weder im Arbeitsverhältnis noch beispielsweise im Verhältnis von einer großen Versicherung zu ihrem Kunden oder auch in anderen Konstellationen nicht mehr, ob Sie eigentlich diese Grenze überschritten haben oder nicht. Einerseits versucht man die Einwilligung als Instrument stärker zu etablieren, andererseits macht man ihre Anwendung aber sehr unsicher und schafft damit eine Rechtsunsicherheit, die man vermeiden könnte. Ich glaube, dass der Gesetzgeber an dieser Stelle besser beraten ist, die Verkehrsregel vorzugeben, statt dieses Thema immer auf die Einwilligung zu verschieben. Zum Thema der Dokumentationspflichten und der praktischen Umsetzung im Bereich der kleinen und mittleren Unternehmen: Das Beispiel, was ich gesagt habe, zeigt deutlich, dass es Bereiche gibt, wo tatsächlich für kleine Unternehmen die Einhaltung unzumutbar ist und im Grunde genommen gar kein so großes Schutzinteresse besteht, dass all diese Verpflichtungen Sinn machen. Insofern ist es richtig, darüber nachzudenken. Ich glaube aber auch, dass es vielleicht nicht die Anzahl

der Mitarbeiter ist, die entscheidend ist, sondern eher die Frage, wie riskant das ist, mit dem ich umgehe. Sie können mit drei Leuten eine sehr riskante Datenbank betreiben. Sie können auch mit 2.000 Mitarbeitern Datenverarbeitung machen, die im Grunde genommen fast gar nicht reguliert werden müsste, weil sie so einfach und alltäglich ist, dass hier mein Kriterium von Beunruhigung und Überraschung gar keine Anwendung findet. Danke!

Vors. **Wolfgang Bosbach**: Herr Dr. Abel, bitte.

SV **Professor Dr. Ralf Abel** (Rechtsanwalt, PRA Legal, Hamburg): Zur ersten Frage, meine Einschätzung der delegierten Rechtsakte. Ich denke, dass mit der Zahl und auch dem Gegenstand dieser delegierten Rechtsakte ein Verstoß gegen die Gewaltenteilung naheliegt. Die Gefahr besteht, und sie besteht nicht nur hier. Ich habe das Gefühl, dass mit dieser Verordnung Grenzen überschritten bzw. Grenzen eingeebnet werden, die aus gutem Grund in einer langen, demokratischen Entwicklung eigentlich erst erkämpft worden sind. Hier wird sehr schnell die Grenze zwischen den Möglichkeiten der Kommission und den Möglichkeiten des europäischen Gesetzgebers verwischt. In diesem Fall haben wir wirklich mit der Verordnung eine echte europäische Gesetzgebung vorliegen. Man fragt sich, wenn man sich die einzelnen Bestimmungen anschaut, wo denn eigentlich noch das Europäische Parlament oder wo noch die nationalen Parlamente, sprich auch der Deutsche Bundestag, die Möglichkeit hat bzw. haben, einzugreifen? Natürlich gibt es die Möglichkeit – ich weiß, da wird man sofort sagen, dass das die Kommission so vorschreibt, man kann das Ganze kassieren. Wenn man aber mal von den Praktikabilitätsgesichtspunkten ausgeht, wann wird dann ein komplettes Recht, einen delegierten Rechtsakt zu erlassen oder ein delegierter Rechtsakt in toto kassiert; nur, wenn man sich über einige Einzelbestimmungen Gedanken macht und die nicht für richtig hält. Es ist ein sehr holzschnittartiges Verfahren, was dort eingeführt werden soll und was in der Praxis wohl kaum dazu führen wird, dass sich im Europäischen Parlament Mehrheiten bilden, die sagen, dass sie das alles nicht wollen und selber machen. Das ist ein erheblicher Webfehler. Wenn ich noch einmal das Beispiel aufgreifen darf: Wo darf denn die Kommission tätig werden, z. B. im Bereich der Zertifizierungen, also in einem Bereich, in dem normativ durchaus materielles Recht gesetzt werden kann, auch wenn man nur Gegenstand, Umfang, Inhalt und Voraussetzungen eines Zertifizierungsmechanismus vorgibt. Faktisch kann ich über Zertifizierungen eine ganze Menge Normen vorgeben. Ich weiß, wovon ich rede, denn ich bin selbst ein akkreditierter Gutachter beim ULD und bekomme dort mit, wie Vorgaben für Zertifizierungen schon in den Markt und in die Märkte hineinwirken und wie man sich natürlich nach diesen Vorgaben richtet. Das wäre in einem völlig anderen Maße und weitaus stärker der Fall, wenn man diese delegierten Rechtsakte zuließe. Wie sieht es aus mit dem Spielraum? Natürlich braucht man einen

Spielraum, aber hier wird ein Webfehler sehr deutlich sichtbar, indem nämlich für den Spielraum versucht wird, ein administratives Verfahren und eine Einflussnahme der Exekutive zu schaffen, während in Wirklichkeit die Flexibilität in der Struktur der Gesetzgebung liegen müsste. Die Gesetzgebung dürfte sich nicht auf eine bestimmte Technologie beschränken oder beziehen. Die Gesetzgebung – und da gebe ich Herrn Dr. Simitis völlig Recht – muss von vorneherein eine Offenheit und eine Flexibilität zulassen. Das ist das, was hier auch nicht passiert. Hier soll im Grunde eine „Lex Facebook“ gemacht werden, die dann einheitlich auf sämtliche denkbaren Verarbeitungen von Informationen angewandt wird. Dieser Webfehler hat die vielen Folgen, die wir eben hier am Tisch gehört haben. Flexibilität ja, aber nicht dadurch, dass eine Exekutivbehörde, welche die Kommission nach wie vor ist, oder ein Teil der Exekutiven in der Lage ist, Gesetzgebung durchzuführen. Beim Kohärenzverfahren sieht es ähnlich aus. Beim Kohärenzverfahren kann ich zwar sehr gut nachvollziehen, warum man das macht, damit nämlich nicht wieder diese Unterschiede, die wir jetzt auch schon haben, und die auch schon stark zu Lasten der deutschen Wirtschaft gehen, in Europa herrschen, sondern dass man schon zu einheitlichen Bestimmungen kommt. So wie es hier vorgesehen ist, mit dem Letztentscheidungsrecht der Kommission einerseits und mit der Zeitdauer, die ein solches Kohärenzverfahren in Anspruch nimmt, andererseits, fürchte ich, dass das nicht zu einer Rechtsvereinheitlichung führt, sondern nur zu Unterschieden oder zu Recht zweierlei Art; nämlich die einen, die etwas machen, die sich diesem Verfahren erst einmal nicht unterwerfen und bei denen im Augenblick nichts passiert, weil die Aufsichtsbehörden viel zu schwach besetzt sind, um wirklich den Hunderttausenden von Unternehmen in ihrer Tätigkeit nachgehen zu können und die anderen, die sich dem unterwerfen müssen, vielleicht monatelang oder jetzt, wenn man so die Erfahrungen in Deutschland betrachtet mit dem innerdeutschen Kohärenzverfahren des Düsseldorfer Kreises. Da muss man auch manchmal sehr lange Zeiträume abwarten, bis es dort eine Meinungsbildung gibt – wenn überhaupt. Ein solches Verfahren ist so langwierig und ich kann mir nicht vorstellen – angesichts der kurzen Innovationszyklen, die es in der Wirtschaft gibt – dass diese kurzen Innovationszyklen da überhaupt noch abgebildet werden können, und das gilt nicht nur für die Wirtschaft, sondern das gilt auch für den privaten Bereich. Wenn man sich überlegt, wie viel sich für Privatbenutzer etwa von Smartphones geändert hat innerhalb von wenigen Jahren. Seit wann gibt es denn das iPhone oder Ähnliches, das sind doch nur ein paar Jahre. Damit haben sich das Verhalten und die Möglichkeiten, nicht nur der Wirtschaft und nicht nur der Selbständigen und Freiberufler, sondern auch der einzelnen Bürger, massiv verändert. Einzelnes zu dürfen und drei Jahre zu warten, oder zwei Jahre, bis ein Kohärenzverfahren funktioniert, halte ich für einen Bürokratismus, der so nicht funktionieren kann. Genau dasselbe übrigens, wenn ich das noch hinzufügen darf, zum Thema Einwilligung. Einwilligung ist zwar wünschenswert in einer Reihe von Fällen, aber

die Einwilligung ist, weil sie sich auf festgelegte Sachverhalte beziehen muss, starr. Die Einwilligung kann nur starr sein. Ich muss vorher wissen, in was ich einwillige, sonst wäre die Einwilligung nach deutschem Recht unzulässig bzw. nichtig. Wenn ich aber vorher alles genau wissen muss, dann habe ich einen starren Mechanismus und es kann derjenige, der die Einwilligung hat, mit den Daten nicht mehr frei weit weggehen von der Einwilligung. Damit haben wir eine Erstarrung, die genau das Gegenteil dessen ist, was wir überall haben, nämlich dynamische Prozesse.

Vors. **Wolfgang Bosbach**: Herr Dr. Konstantin von Notz, bitte. Ich halte den Verkehr nicht auf.

BE **Dr. Konstantin von Notz**: Sie sind das nicht, Herr Vorsitzender, an Sie würde sich das auf gar keinen Fall wenden. Die Zeit läuft davon und ich sehe, dass ich nicht mehr drankomme. Deswegen würde ich sehr darum bitten, dass etwas zu komprimieren, wenn wir nur zwei Stunden für so eine wichtige Reform nehmen, dann muss das meiner Ansicht nach etwas komprimierter ablaufen.

Vors. **Wolfgang Bosbach**: Herr Kollege Gerold Reichenbach ist Spezialist für kurze, knackige Formulierungen. Wenn die Sachverständigen, Frau Piltz, auch kurz und knackig antworten.

BE **Gerold Reichenbach** (SPD): Den Gefallen kann ich Ihnen jetzt nicht tun. Das wäre neu, dass die Redezeit der CDU/CSU auf die Redezeit der SPD angerechnet wird. Ich habe zunächst zwei Fragen an Herrn Prof. Dr. Simitis und Frau Dr. Sommer. Da geht es einmal um das angesprochene Verhältnis zwischen dem Datenschutz als ein Teil des Grundrechtsschutzes und dem Prinzip der Freiheit im Wirtschaftsbereich, das auch bei Prof. Härting oder auch bei Prof. Abel angesprochen worden ist. Meine Frage ist, ob das gleichwertige Abwägungsgrundsätze sind, oder gibt die allgemeine Grundsatzrechtsprechung ein Abwägungsgefälle her, insbesondere wenn es um enge persönliche Daten geht? Daran anschließend auch die Frage an Prof. Härting: Sie haben gesagt, dass Sie gerne Alltagskommunikation ausnehmen würden. Da würde ich gerne einmal wissen, wenn Sie Alltagskommunikationen ausnehmen, was dann von der Kommunikation – Herr Neumann hat das angedeutet, was an persönlichen Daten, Fotos, aufgespeichert und genutzt wird – im Bereich des Datenschutzes in der jetzigen Situation, wie sie international oder auch national, im Internet oder auch bei sonstigen Diensten an Daten anfällt, erfasst wird? Die nächste Frage an Herrn Prof. Simitis: Sie haben darauf hingewiesen, dass das immer eine nachholende Arbeit gegenüber der Technik des Datenschutzes sei. Deswegen meine Frage: Bei einem Umkehrungsverbotprinzip, wie es von einem Teil abgelehnt wurde, u. a. von Frau Dr. Sommer oder von Herrn Prof. Dr. Hornung, aber wenn ich es richtig

verstanden habe, von den Herren Dr. Wuermeling und Dr. Abel gefordert wurde, wäre im Grunde genommen nur das verboten, was ausdrücklich verboten ist, alles andere ist erlaubt. Ist denn Datenschutz in der modernen, technischen Welt überhaupt noch herstellbar oder würde es sofort nach Inkrafttreten der Gesetzgebung eine ganze Menge an Umgehungstatbeständen erleben, die den Datenschutz wieder aushebeln? Dritte Frage an Herrn Dr. Wuermeling: Ich glaube übrigens, dass das, was Sie dargestellt haben, weniger ein Mangel an Praktikabilität für den kleinen Handwerksmeister ist, als eher eine sinnbildliche Darstellung der juristischen Sprache. Die Formulierung „... des Wurfputs durch Fassen des Stils, der sich als Fortsatz in dem Wurfblatt darstellt, und den festlegenden Wurf- und Gleithand in Richtung des Zieles zu befördern hat, die Gleithand entlang des Stils zur Wurfhand zu führen und das Wurfputz in Wurfrichtung zu befördern“, steht nämlich in einer Richtlinie, in dem Fall kein Gesetz, aber aus dem Bereich des Arbeitsschutzes drin, was nichts anderes heißt als Schippen. Diese Formulierung führt jetzt nicht dazu, dass der deutsche Handwerker im Bauverkehr dadurch behindert würde, dass er ständig die Gleithand, den Stil, die Wurfrichtung, das Wurfputz, die Wurfschaufel und den Wurfvorgang zu definieren hat, sondern das passiert automatisch, wenn ein Handwerker die Daten speichert, um seine Kunden zu informieren. Beim Fensterbau ist der Zweck schon festgelegt. Deswegen meine Frage: Inwieweit ist das nicht eher eine juristische Aufblähung, was den Handwerksmeister wirklich betrifft? Welche der von Ihnen beschriebenen Vorgänge sind über Art. 28 Abs. 4 ohnehin ausgenommen?

Vors. **Wolfgang Bosbach**: Prof. Dr. Simitis, bitte.

SV **Professor Dr. Dres. h. c. Spiros Simitis** (Goethe-Universität, Frankfurt am Main): In genau dem Absatz der Entscheidung des Bundesverfassungsgerichts zur Volkszählung, in dem die informationelle Selbstbestimmung als Grundrecht anerkannt wird, stellt das Gericht ebenso klar wie nachdrücklich fest, dass sie zu den elementaren Funktionsbedingungen einer demokratischen Gesellschaft zählt. Nur wenn der Einzelne weiß, was mit seinen Daten geschieht, also auch und gerade gewährleistet ist, dass die Daten in einem bestimmten Kontext verarbeitet werden und sich ihre Verwendung deshalb genauso überprüfen wie berichtigen lässt, hat er zugleich die Chance, in der Gesellschaft mitzuwirken. Konsequenterweise muss bei jeder Reflexion über Anforderungen an den Datenschutz bedacht werden, ob die Möglichkeit gesichert ist, sich zu vergewissern, was mit den Daten geschieht und, soweit es sich als nötig erweisen sollte, korrigierend einzugreifen.

Wenn ich zudem die immer häufigeren Vorschläge höre, es nicht bei generell anwendbaren Erwartungen an die Verwendung personenbezogener Daten zu belassen, vielmehr die Notwendigkeit einer Regelung sowohl an der Bedeutung als auch an den Folgen der Verarbeitung zu messen, fühle ich mich an die

Frühzeit des Datenschutzes erinnert. Ganz in diesem Sinne hatte z. B. Frankreich den Regelungsakzent zuvörderst auf sensitive Daten gesetzt. Differenzierungen mögen sicherlich erwägenswert sein. Die vergangenen Jahrzehnte haben freilich eines wieder und wieder bestätigt. Einen effizienten, in seiner konstitutiven Bedeutung für die Struktur der Gesellschaft gesehenen und beurteilten Datenschutz kann es nur geben, soweit sämtliche personenbezogene Angaben einbezogen werden. Variationen im Umgang mit den verschiedenen Daten mögen daher erforderlich sein. Sie rechtfertigen jedoch keineswegs eine Beschränkung gesetzlicher Verarbeitungsvorgaben auf wie immer ausgewählte Angaben.

Vors. **Wolfgang Bosbach**: Vielen Dank. Frau Dr. Sommer, bitte.

SV **Dr. Imke Sommer** (Landesbeauftragte für Datenschutz und Informationsfreiheit der Freien Hansestadt Bremen): Das Datum „Esse ich Schweinefleisch oder nicht“ kann eben aus dem Kontext heraus, aus dem ich es erhoben habe, ganz, ganz extreme Wirkungen haben. Das kennen wir aus der Fluggastdatendebatte. Verhältnis freier Datenverkehr und Datenschutzrecht, europäisch gesehen: Ich kann in diesem Zusammenhang nur darauf hinweisen, dass wir eine europäische Grundrechtecharta haben, in der dieses Grundrecht auf Datenschutz normiert ist. Wir haben im Grunde dort einen Punkt, der etwas mit dem freien Datenverkehr zu tun hat. Das ist die unternehmerische Freiheit, aber die wird anders formuliert. Da wird gesagt, dass das, was sich in den Mitgliedstaaten entwickelt hat, zur Kenntnis genommen wird. Die Schlüsse daraus können Sie selber ziehen. Ich finde bloß, dass wir in dem, was wir hier diskutieren, eine eindeutige Meinungsäußerung Richtung Datenschutzgrundrecht finden müssen.

Am 9./10. Oktober 2012 gab es in Brüssel eine Veranstaltung, in der sich ein Vertreter von Microsoft die ganze Zeit hingestellt und gesagt hat „C'est fantastique!“ Er freut sich über das, was da passiert ist, weil die das schon immer mit Google gefordert haben. Nach der Street View Geschichte nervte sie, dass wir so viele sind und dass wir so unterschiedliche Auffassungen vertreten und sie wollen jetzt endlich mal alles einheitlich haben. Die haben sich 100-prozentig durchgesetzt. Das müssen wir einfach im Kopf behalten. Das andere ist nicht 100-prozentig durchgesetzt. Das sehen wir hier. Das Datenschutzgrundrecht hat sich da noch nicht genügend artikulieren lassen. Dabei ist es doch Anspruch der europäischen Ebene, das Vertrauen für die Menschen zu schaffen.

Die Datenschutzgrundverordnung ist in die digitale Agenda eingebettet. Das ist ein Gesetzesvorhaben von 31 in der digitalen Agenda. Es geht darum, Vertrauen zu schaffen, dass die Menschen wirklich das, was da angeboten und für sie interessant ist, auch tatsächlich nutzen können. Dafür brauchen sie Vertrauen. Und die Menschen in Europa sind nicht dumm. Die merken, wenn das nur ein Etikettenschwindel ist. So wie wir das jetzt diskutieren, kann man große Probleme



mit dem haben, was dabei herauskommt. Da steht dann Datenschutzgrundverordnung drauf und in Wirklichkeit ist freier Datenverkehr drin.

Vors. **Wolfgang Bosbach**: Vielen Dank. Herr Härting, bitte.

SV **Professor Niko Härting** (Rechtsanwalt, Berlin): Ich weise nur darauf hin, dass wir in der Grundrechtecharta selbstverständlich auch die Kommunikationsfreiheit als Freiheit geschützt haben, selbstverständlich auch die Berufsfreiheit und die Freiheit der unternehmerischen Betätigung. Es gehört wohl zu den Webfehlern der Grundverordnung, dass im Art. 1 immer noch so getan wird, als gebe es eine Abwägung zwischen dem Datenschutz und den Persönlichkeitsrechten auf der einen Seite und dem Datenverkehr auf der anderen Seite. Das ist das beste Beispiel dafür, dass die Entwurfsverfasser im Jahr 1995 stehen geblieben sind, denn damals hieß der Datenverkehr physische Grenzüberschreitung. Die gibt es heute doch kaum noch. Insofern stammt das aus einer Vorstellungswelt, die aus der Vor-Internetzeit stammt. In der heutigen Zeit sind die Bezugsgrößen, also das, woran sich das Datenschutzrecht im privaten Bereich orientieren muss, auf der einen Seite die Persönlichkeitsrechte und auf der anderen Seite vielfältige – und nicht nur die wirtschaftliche Entfaltungsfreiheit, sondern auch vielfältige andere – Grundrechte, die auch betroffen sind und betroffen sein können bzw. auf der Basis von Daten ausgeübt werden. Daran anknüpfend die Bemerkung – Stichwort Microsoft –, dass ich den Eindruck habe, die, die noch vergleichsweise gut mit den Regelungen, wie jetzt vorgeschlagen, fahren könnten, sind die großen amerikanischen Unternehmen. Von denen ist so viel die Rede. Eine Reihe von Vorschriften sind exakt auf diese zugeschnitten. Das Problem ist nur, da man ja nicht Sondervorschriften für große amerikanische Unternehmen machen kann, man jetzt auch Vorschriften schaffen muss, bei denen man nicht ganz durchdacht hat, was denn eigentlich die Folgen für den Rest der Wirtschaft sind, auch die Offline-Wirtschaft darf man dort nicht vergessen, nebenbei gesagt auch für den öffentlichen Bereich. Herr Reichenbach hat mich gefragt, was man sich denn unter alltäglicher Kommunikation vorstellen darf. Ich darf nur ein Beispiel nennen: Da darf man keinem Missverständnis erliegen – auslassen heißt ja nicht, dass das unreguliert bleiben soll. Transparenz ist zum Beispiel etwas, was auch für die alltägliche Kommunikation fraglos gelten soll und von niemandem hier, glaube ich, bezweifelt wird. Nach dem jetzigen Recht ist es entweder/oder. Entweder wir haben einen Personenbezug und eine nicht nur persönliche, familiäre Nutzung, denn dann sind wir im vollen, strengen Regime des Datenschutzes. Das ist aber auch nicht ganz begreiflich, denn es gibt Bereiche auch der persönlichen, familiären Nutzung und die Graubereiche, wo man sich um den Personenbezug streitet, wo es durchaus vernünftig ist, über Transparenz zu reden, auch über Regeln des sorgsamem Umgangs mit Daten zu sprechen. Anders gesagt, durch die private datengeschützte Kommunikation können Persönlichkeitsrechte ganz

erheblich gefährdet werden. Daher ist das gar nicht mehr einzusehen, dass man diese Ausnahmen hat. Man braucht sie bloß nach dem geltenden Recht, weil es eben schwarz ist und weil das geltende Recht nur schwarz und weiß vorsieht. Entweder die strengen Regeln wie das Verbotsprinzip oder es geht überhaupt nichts. Da vermag ich nicht mehr einzusehen, dass das seine Richtigkeit hat. Deswegen finde ich es richtig, zwischen zwei unterschiedlichen Stufen der Datenkommunikation zu unterscheiden. Einmal das, was mit der Kurzformel Alltagskommunikation bezeichnet ist, wo es nicht richtig ist, mit dem Verbotsprinzip zu operieren, wo es aber wohl richtig ist, auch dort Regeln aufzustellen, da ist aus meiner Sicht Transparenz das erste Gebot, um dann Bereiche zu definieren, die wir als besonders sensibel ansehen, wie z. B. den Bereich Gesundheit, wo mit Verboten zu operieren ist.

Vors. **Wolfgang Bosbach**: Vielen Dank. Herr Dr. Wuermeling, bitte.

SV **Dr. Ulrich Wuermeling** (Rechtsanwalt, Latham & Watkins LLP, Frankfurt am Main): Danke für Ihre Frage, Herr Reichenbach. Sie haben natürlich Recht. Es gibt manchmal komplizierte Rechtsvorschriften, die sich im Alltag irgendwie von selber lösen, weil man ein bisschen gesunden Menschenverstand und Sorgfalt anwendet. Die Beispiele, die ich genannt habe, wird man auf diese Weise aber nicht lösen können. Das sind eine ganze Reihe von Verpflichtungen, die man nicht automatisch einhält. Die Ausnahme im Art. 28 Abs. 4, die Sie nennen, gilt nur für die Dokumentationspflicht. Deshalb habe ich die Dokumentationspflicht in meinem Beispiel gar nicht erst genannt. Alles, was ich genannt habe, sind Verpflichtungen, die für Unternehmen gelten, die weniger als 250 Mitarbeiter haben.

Vors. **Wolfgang Bosbach**: Zu der Unruhe im Sitzungssaal: Der arme Dr. Konstantin von Notz kommt nicht mehr dran. Wir machen nachher nach 13:00 Uhr den Tagesordnungspunkt: Individuelle Dialoge zwischen den Sachverständigen. Er hat Recht, nicht immer, aber in diesem Fall hat er Recht. Herr Dr. Wuermeling, lassen Sie sich nicht aufhalten und schon gar nicht von mir. Immer geradeaus! Subjekt, Prädikat, Objekt und dann geht es weiter!

SV **Dr. Ulrich Wuermeling** (Rechtsanwalt, Latham & Watkins LLP, Frankfurt am Main): Was ich auch noch einmal kurz ansprechen möchte: Der Webfehler liegt im Wesentlichen darin, dass die Verordnung versucht, den Bereich Internet, Neue Medien und Ähnliches zu regeln und dann mit lauter Vorschriften kommt, die eben im allgemeinen Leben nicht funktionieren und nicht passen. Das Tragische ist dabei – und da gebe ich Frau Dr. Sommer auch Recht –, wenn man glaubt, dass man die Verordnung unbedingt braucht, um Facebook oder Google unter Kontrolle zu bekommen; das ist nicht richtig, denn dafür bietet die Verordnung gar keine Instrumente. Die Struktur, die wir heute haben, dass z. B. für Facebook

ausschließlich die Datenschutzaufsicht in Irland zuständig ist, wird hiermit ausdrücklich festgeschrieben. Da werden Sie aus Deutschland keinen Einfluss mehr nehmen können. Insofern erreicht die Verordnung sogar an dieser Seite gar nicht das gesetzte Ziel.

Vors. **Wolfgang Bosbach**: Vielen Dank. Frau Kollegin Piltz, bitte.

BE **Gisela Piltz** (FDP): Herr Vorsitzender, vielleicht können wir für den Kollegen Dr. Konstantin von Notz noch eine Viertelstunde dranhängen.

Vors. **Wolfgang Bosbach**: Ich nicht, Sie ja.

BE **Gisela Piltz** (FDP): Irgendwer findet sich dann. Er hat ja Recht. Nehmen Sie es mir nicht übel. Zu Beginn – so viel Zeit muss sein – mein Dank an Sie alle. Eine Dame ist dieses Mal dabei, das ist für diesen Ausschuss eine wirkliche Premiere oder ein Fortschritt. Meine erste Frage geht an Herrn Dr. Wuermeling. Sie haben, auch wie der Bundesrat, die Subsidiarität gerügt und ich weiß, dass das hier im Parlament auch nicht gerade unkritisch gesehen wird. Wir haben uns aber gegen diesen formalen Akt ausgesprochen und der Juristische Dienst des Rates der Europäischen Union sieht es anders. Das mag einen nicht verwundern, aber halten Sie es rechtlich für zwingend, das auszuklammern, z. B. das in einer eigenen Richtlinie zu regeln, oder würde eine Richtlinie die selben Kompetenzprobleme schaffen? Meine nächste Frage geht an Herrn Dr. Simitis. Sie haben sich in der letzten Woche beim Kongress des BMI dahingehend geäußert, dass das Problem von Datenschutzgesetzgebung natürlich die rasante Veränderung von Technik ist. Das wissen wir alle. Mein Traum ist immer noch der von einem technikfesten Datenschutzgesetz, damit wir nicht jeder Technik eine neue Regelung hinterherwerfen müssen. Wenn Sie aber sagen, dass Sie das befristen wollen, dann ist das vielleicht auch ein gewisser Widerspruch in sich, weil man dann natürlich erst recht nicht für die Zukunft planen kann, wenn man es in manchen Bereichen, je nachdem wo man anknüpft, machen könnte. Von daher bin ich mir nicht so sicher, dass man solche Regelungen nicht finden kann. Könnten Sie nicht auch daran glauben, dass es gewisse Regelungen gibt, die einfach technikfest sein könnten? Dann bräuchte man auch keine Befristung. Meine nächste Frage geht an Herrn Härting. Sie beklagen – aus meiner Sicht auch zu Recht – den nicht hinreichenden Rechtsschutz gegen etwaige fehlerhafte Entscheidungen der Datenschutzaufsichtsbehörden. Wie müsste man das regeln? Kann man das überhaupt so regeln? Wenn ja, wie müsste man das regeln, damit es funktioniert? An all die Sachverständigen, die ich eben angesprochen habe, eine letzte Frage: In Brüssel gab es auch eine Anhörung zu diesem Thema und da wurde auch, wie von Ihnen allen kritisiert, diese hohe Anzahl von delegierten Rechtsakten angesprochen. Es konnte aber keiner sagen, welche eigentlich die

schlimmsten sind. Wir sind realistisch. Ich habe eine Ahnung. Ich weiß, dass man nicht 40 abschaffen kann, aber können Sie mir die drei schlimmsten Ihrer Meinung nach nennen?

Vors. **Wolfgang Bosbach**: Herr Dr. Wuermeling, bitte.

SV **Dr. Ulrich Wuermeling** (Rechtsanwalt, Latham & Watkins LLP, Frankfurt am Main): Frau Piltz, Sie haben das Gutachten des Rechtsdienstes der Europäischen Kommission genannt. In der DNA der Mitarbeiter des Rechtsdienstes der Europäischen Kommission kommt das Wort Subsidiarität nicht vor. Wenn Sie dort eine solche Frage stellen, dann ist die Antwort praktisch vorgegeben. Das ändert aber nichts daran, dass sich die Mitgliedstaaten aufgrund der bestehenden Verträge wehren müssen, wenn es zu weit geht. Ich meine nicht, dass es um die Frage geht, ob es eine Verordnung oder eine Richtlinie sein soll. Da bin ich ehrlich gesagt der Ansicht, dass es keine schlechte Idee ist, wenn wir gerade für die Privatwirtschaft innerhalb von Europa das Modell der Verordnung wählen. Es ist aber so, dass wir im öffentlichen Bereich aufpassen müssen und da meine ich, hat der Vertrag von Lissabon, der die Subsidiarität stärken sollte, im Art. 16 des Vertrages über die Arbeitsweise der Europäischen Union eine ganz klare Einschränkung, was den Anwendungsbereich im öffentlichen Bereich anbelangt, vorgenommen. Das bedeutet, dass es einen europäischen Bezug geben muss. Die europäische Regelung müsste sich darauf beschränken, im öffentlichen Bereich nur Sachverhalte zu regeln, die einen europäischen Bezug haben. Damit würden wir viele Probleme lösen und wir würden das Datenschutzrecht, das es in Deutschland gibt, weil es einfach viel qualitativer und vor allen Dingen detaillierter ist, im öffentlichen Bereich retten. Das persönlich würde ich jedenfalls für wichtig halten.

**[Wechsel der Sitzungsleitung von Vors. Wolfgang Bosbach an Abg. Gerold Reichenbach]**

Abg. **Gerold Reichenbach**: Ich habe das hier nicht öffentlich okkupiert aber der Kollege Bosbach hat mich gebeten, hier weiterzumachen, weil er aus dringenden Gründen weg muss. Ich hoffe, dass Sie damit einverstanden sind, weil ein regulärer Stellvertreter nicht anwesend ist. Herr Dr. Simitis, bitte.

SV **Professor Dr. Dres. h. c. Spiros Simitis** (Goethe-Universität, Frankfurt am Main): Sie haben mir zwei Fragen gestellt. Zunächst: Datenschutzbeauftragte wurden schon in den beiden ersten Gesetzen vorgesehen, dem hessischen Datenschutzgesetz von 1970 und dem drei Jahre später verabschiedeten schwedischen Gesetz. Bei der Definition der Aufgaben des Datenschutzbeauftragten wurde ausdrücklich auf seine Verpflichtung verwiesen,

sich fortlaufend mit der Entwicklung der Technologie auseinander zu setzen sowie das Parlament darüber zu informieren. Vom diesem wurde ebenso explizit erwartet, die gesetzlichen Vorgaben kontinuierlich weiterzuentwickeln. Genau diese Forderung findet sich auch in der von mir bereits erwähnten Befristung einzelner Datenschutzgesetze wieder. Die Frist begründet die Pflicht, gezielt sowohl auf den jeweiligen Technologiestand als auch und vor allem auf die Notwendigkeit legislativer Reaktionen einzugehen.

Die Europäische Kommission hat sich lange zurückgehalten. Spät, aber doch noch kam es 1995 zur ersten Regelung. Die nicht zuletzt in Anbetracht der offenkundigen Veränderungen der Technologie sowie der Erfahrungen in den Mitgliedsländern immer dringlichere Revision hat nicht genauso lange auf sich warten lassen. Der im Januar 2012 vorgelegte Verordnungsvorschlag korrigiert einzelne Verarbeitungsbedingungen und gibt zugleich mit der Verordnung einer neuen Rechtsform den Vorzug.

Nun zur zweiten Frage. Beispiele gibt es mehr als genug. So findet sich etwa am Ende der Vorschrift zu den besonderen Kategorien von Daten, den sensitiven Angaben, eine Verweisung, die kaum allgemeiner hätte ausfallen können. Durchaus vergleichbare Bestimmungen kehren bei der Folgenabschätzung oder den Aufgaben des Datenschutzbeauftragten wieder. Überall werden zunächst Grundsätze formuliert, ihre Präzisierung bleibt jedoch ausdrücklich der Kommission vorbehalten. Genau das halte ich für inakzeptabel, weil sich eben keine dieser Vorschriften mit einer Blanko-Vollmacht an die Kommission verträgt, die jeweiligen Bestimmungen schlicht nach ihren Vorstellungen auszulegen und genauso wenig dem Europäischen Parlament zuzumuten ist, eine endlose Diskussion über Anwendungseinzelheiten in Kauf zu nehmen.

Abg. **Gerold Reichenbach**: Vielen Dank. Herr Härting, bitte.

SV **Professor Niko Härting** (Rechtsanwalt, Berlin): Ich erlaube mir nur ein Beispiel anzubringen, weil es besonders plastisch ist: Wir haben seit Jahren eine Diskussion unter den Datenschutzexperten, ich würde sagen seit 10 Jahren, über den Grundsatz von „Privacy by Design“, im Kern die vernünftige Vorstellung, dass man bei der Produkt- oder Dienstleistungsentwicklung zu einem möglichst frühzeitigem Zeitpunkt auch einfach an den Datenschutz denkt und möglicherweise vieles dafür spricht, dass ein solcher Ansatz Vorteile gegenüber der dann immer nachlaufenden Regulierung hat, von der Sie vorhin gesprochen haben, Herr Dr. Simitis. Diese Diskussion, die in den Facetten kompliziert ist, von der habe ich erwartet, dass man doch nach 10 Jahren Diskussion in diesem Vorschlag etwas dazu findet, was ein bisschen über den Programmansatz hinausgeht. Leider finden sich in Art. 23 Abs. 1 und 2, wo das geregelt ist, nicht mehr als Programmansätze. Ich sage es einmal mit meinen Worten: „Privacy by Design“ finden wir gut. Anschließend steht da, Abs. 3: Die Kommission wird

ermächtigt, Näheres bei delegiertem Rechtsakt zu erlassen. Abs. 4: Die Kommission kann technische Standards für die in den Abs. 1 und 2 genannten Anforderungen festlegen. Das ist natürlich ein bisschen armselig, um das auch einmal ganz deutlich zu sagen. Das ist für mich ein besonders vorstechender Punkt, wo einfach dieser Vorschlag ganz, ganz weit hinterher ist. Sie haben nach Rechtsbehelfen gefragt. In der Praxis hat man das, wenn man es mit Verfahren zu tun hat, in denen die Datenschutzaufsichtsbehörden tätig sind, oft mit dem Problem zu tun, dass es allzu lange dauert, bis dort Entscheidungen getroffen werden. Ich weiß aus Gesprächen mit Ihren Kollegen, dass das auf allen Seiten kritisch gesehen wird, weil es zu lange dauert, bis es zu Entscheidungen kommt. Warum ist das ein Problem? Bevor eine Entscheidung da ist, gibt es nichts, worüber man sich gerichtlich auseinandersetzen kann und dann kommt es zum nächsten Problem, dass wir dringend ein Gerichtsverfahren brauchen, weil, egal was am Ende dabei herauskommt, wir die Gerichte brauchen, um das zu konkretisieren, was ein Gesetz ist. Das ist nach dem heutigen Recht ein großes Problem. Wir haben zu den Kernbegriffen und Kernproblemen des Datenschutzes Jahrzehnte Meinungsstreitigkeiten, aber keine obergerichtliche Klärung. In diesem Entwurf spielt das Verfahren der Datenschutzaufsichtsbehörden, soweit es darum geht, dass die Aufsichtsbehörde Auflagen macht, Anforderungen stellt etc., eine Rolle. Es gibt dort eigentlich keine Verfahrensvorschriften und somit auch keinerlei Inzertiv, dass das schnell geht, während sich in anderen Regelungsbereichen auch sehr, sehr kleinliche Fristen oder dergleiche Regelungen finden. Es gibt auch eigentlich nur einen Absatz, der auch nur eine Banalität klarstellt, nämlich jede natürliche oder juristische Person hat das Recht auf einen gerichtlichen Rechtsbehelf gegen die sie betreffenden Entscheidungen einer Aufsichtsbehörde. Dieser Absatz würde natürlich auch dann gelten, wenn er nicht in der Verordnung stünde. Woran es einfach fehlt, sind klare Anforderungen im allseitigen Interesse, was denn für Grundsätze im Verwaltungsverfahren gelten sollen, wenn die Aufsichtsbehörde Beanstandungen hat, was sind dort die Verfahrensrechte – und Stichwort Untätigkeitsklage –, ein solches Verfahren in den gerichtlichen Rechtsschutz überführt werden kann.

Abg. **Gerold Reichenbach**: Herr Kollege Korte, ich habe die Bitte, damit auch die Fraktion BÜNDNIS 90/DIE GRÜNEN noch zum Zuge kommt – ich versuche auf der Uhr anzudeuten, wenn drei Minuten übersprungen sind, ansonsten bitte ich Sie, unabhängig davon, auch zuzugestehen, dass wir überziehen. Ich finde es nicht sonderlich fair, wenn eine Fraktion dann gar nicht mehr zum Zug kommt. Kollege Korte, bitte.

BE **Jan Korte** (DIE LINKE.): Wir müssen uns dringend in der nächsten regulären Sitzung des Innenausschusses und insbesondere auch bei den Obleutegesprächen darüber verständigen, dass so etwas wie heute nicht mehr

stattfindet. Es ist sowohl gegenüber den Sachverständigen als auch gegenüber den Abgeordneten und der interessierten Öffentlichkeit ein inakzeptables Verfahren. Das ist der Sache auch nicht angemessen und deswegen müssen wir uns alle gemeinsam dazu verständigen, dass so etwas in der Art und Weise, liebe Kollegin Piltz, nicht geht. Mich hätte interessiert, das weit ausführlicher zu machen, – wenn Sie das nicht interessiert, ist das ihr Problem – aber trotzdem muss man eine Regelung im Sinne der Sachverständigen treffen. Man kann so etwas nicht in zwei Stunden machen und schon gar nicht, dass es eingangs keine Redezeitbeschränkungen gibt und wenn nun die besonders interessanten Beiträge der Opposition kommen, dann gebeten wird, das in drei Minuten zu machen. So geht das natürlich nicht. Trotzdem will ich versuchen, auch im Sinne des Kollegen von Notz, es ganz kurz zu machen. Ich war sehr überrascht, wie detailversessen in Fragen des Datenschutz die CDU/CSU sein kann. Das ist eher selten. Deswegen will ich es politisch versuchen und ich will da in dem Fall nur an den Kollegen Neumann die Fragen stellen: Wenn wir über die Verordnung sprechen – ich habe einmal versucht, für diejenigen, die damit nicht alltäglich beschäftigt sind, ein Bild zu malen – sie sollen mir sagen, ob das zutrifft oder nicht: Man hat einen Mindeststandard und es gibt immer die Befürchtung, dass damit höhere Tarifverträge ausgehebelt werden, was nachweislich nicht so ist. Mich würde interessieren, ob das bei dieser Verordnung zustimmt – übersetzt gesagt, dass das Datenschutzniveau in Deutschland abgesenkt würde oder ob es vielleicht sogar so sein könnte, dass damit in wesentlichen Bereichen das Datenschutzniveau in Deutschland angehoben würde. Da würde mich interessieren, wie dort Ihre allgemeine Einschätzung ist. Zweite Frage zum Thema Arbeitnehmerbeschäftigtendatenschutz, geregelt in Art. 82: Dies ausgerechnet hier, in dieser wesentlichen Frage und gerade in Europa, allein einer nationalstaatlichen Regelung zu überlassen, kann allen Ernstes nicht richtig sein. Dazu würde ich von Ihnen ein, zwei ganz konkrete Sätze hören: Wie könnte man das machen, weil Deutschland gerade in diesem Bereich enormen Nachholbedarf hat.

Abg. **Gerold Reichenbach**: Herr Neumann, bitte.

SV **Karsten Neumann** (Landesbeauftragter für Datenschutz und Informationsfreiheit Mecklenburg-Vorpommern a. D.): Der Ausschussvorsitzende versprach uns, dass wir auch das noch sagen dürfen, was wir sonst noch sagen wollten. Das wird aber zeitlich kompliziert. Die Frage, ob das gegenwärtige Datenschutzniveau in Deutschland bei Umsetzung dieser Verordnung abgesenkt würde, kann man erst entscheiden, wenn man sich darüber einigt, von welchem Niveau wir ausgehen, von dem theoretischen Niveau in juristischen Fachdiskussionen, wie es Herr Dr. Wuermeling uns so schön vorgemacht hat, oder von der Datenschutzpraxis. Dazu könnte ich viel sagen. Ich verkürze es auf

die Formel: Schauen Sie bitte in die Tätigkeitsberichte der Datenschutzbeauftragten. Wir tun hier so, als hätten wir nur juristische Auslegungsprobleme von Verfassungsrang. Wir haben aber vor allem praktische Probleme. Wir haben Unternehmen, die mit den Daten ihrer Kunden machen, was sie wollen. Wir haben die Situation, dass die Kunden kein Vertrauen mehr haben, weil ihre Daten aus ihrer Sicht zu anderen Zwecken missbraucht werden. Für Unternehmen ist das in der Regel Alltagsdatenverarbeitung und völlig selbstverständlich. Das darf man nicht aus dem Auge lassen. Im theoretischen Diskussionsniveau gibt es eine Reihe von Punkten, die hier nicht in der europäischen Datenschutzgrundverordnung auftauchen. Auch ich hätte mir gewünscht, dass das Papier der Konferenz der Datenschutzbeauftragten unter der Überschrift „Modernisierung des Datenschutzrechtes“ Berücksichtigung gefunden hätte. Es gibt viele gute Ideen, die auch umsetzungswürdig wären. Ich glaube aber, dass zum gegenwärtigen Zeitpunkt die Verordnung schon ein ganz deutlicher Schritt ist. Art. 82 regelt leider nicht den Arbeitnehmerdatenschutz, sondern der Artikel sagt, dass die Mitgliedstaaten ihn regeln dürfen. Das Positive daran ist vielleicht, dass er eine Aufforderungsfunktion hat, also: „Mitgliedstaaten kümmert Euch einmal um diesen speziellen Bereich“ aber ohne es tatsächlich selber zu tun. Da geraten wir in die Schwierigkeit, wenn wir von einem Über-/Unterordnungsverhältnis sprechen, dass dann der Einwilligung der Boden entzogen wird. Aus meiner Sicht ist das im Arbeitnehmerverhältnis ganz klar der Fall, weil der Arbeitnehmer überhaupt nicht mehr wissen und einschätzen kann, wie seine Daten letztendlich verarbeitet werden. Dasselbe gilt selbstverständlich auch für den kleinen und mittelständischen Unternehmer, sobald er sich Technologien bedient, die er überhaupt nicht mehr einschätzen kann. Wer weiß denn von uns tatsächlich und würde schwören, dass er weiß, was mit seinen Daten auf dem iPhone passiert? Es kann von uns niemand, auch die Hersteller und selbst die Aufsichtsbehörden nicht, diese Fragen beantworten. Sehr schön, gerade wieder in Kiel erlebt, wo ein Vertreter eines solchen Unternehmens immer sagte, dass er alle Fragen beantworten werde, aber er hat keine einzige beantwortet, denn er hat nur behauptet, dass er das tut. Das ist, glaube ich, das Problem, weshalb ich noch einmal unterstreichen will, was Frau Dr. Sommer sagt; dass es auch um das Interesse der Unternehmen und der wachsenden Industrie geht, Vertrauen zu schaffen. Vertrauen kann nur auf Information beruhen und Information kann nur auf tatsächlich informierter Einwilligung beruhen, wenn diese Einwilligung dann noch ein geeigneter Maßstab sein kann. Ich hoffe, dass es nicht erst der Klage und eines Gerichtsverfahrens bedarf. Ich halte diese Klagemöglichkeiten für ein wenig problematisch, weil sie vielleicht drohen, die Aufsichtsbehörden noch langsamer werden zu lassen, weil sie dann ein Klageverfahren für sich selbst befürchten. Aber vor allem stellt sich die Frage, ob die Mitgliedstaaten denn bereit sind, wenn diese Regelungen kommen, die Aufsichtsbehörden so auszustatten, dass sie zukünftig in der Lage sind, all diese



Aufgaben zu erfüllen, die hier schon enthalten sind. Das, glaube ich, wird auch noch einmal eine gewaltige Anstrengung werden, auch hier in Deutschland. Um noch einmal zu der Frage zurückzukommen: Ganz klar, auch im öffentlichen Bereich, auch hier in Deutschland, bringt diese Datenschutzgrundverordnung, wenn sie dann für den öffentlichen Bereich auch gilt, ein Mehr an Datenschutz, wenn wir z. B. die Regelungen auf Landesebene zur Bestellungspflicht von Datenschutzbeauftragten sehen – es gibt heute noch eine ganze Reihe von Ländern, die das Modell nicht kennen oder freiwillig machen oder die öffentlichen Verwaltungen bei der normalen Bürokommunikation freigestellt haben vom Datenschutz, was sozusagen ein Verständnis aus den 70er Jahren ist, das sich da noch niederschlägt.

Abg. **Gerold Reichenbach**: Herr Prof. Dr. Simitis, Sie wollten noch etwas ergänzen?

SV **Professor Dr. Dres. h. c. Spiros Simitis** (Goethe-Universität, Frankfurt am Main): Eine kurze Bemerkung zu Ihrer Frage: 1980 hat sich die Kommission für ein erstes Konzept zum Arbeitnehmerdatenschutz entschieden. Parallel dazu wurde in der Bundesrepublik, ebenfalls 1980, erstmalig eine gesetzliche Regelung des Arbeitnehmerdatenschutzes vorgeschlagen. Beide Ansätze sind gescheitert. Zweiunddreißig Jahre später, im Dezember 2010, hat die Bundesregierung den Entwurf eines Gesetzes zur Regelung des Beschäftigtendatenschutzes vorgelegt. Dessen weiteres Schicksal ist freilich nur schwer einzuschätzen, obgleich es die Verordnung den Mitgliedsländern ausdrücklich überlässt, die Verwendung von Arbeitnehmerdaten zu regeln, allerdings unter Berücksichtigung der in der Verordnung vorgeschriebenen Verarbeitungsgrundsätze. So gesehen kann das nächste Stadium nur eine entsprechende Überarbeitung des Entwurfs sein.

Abg. **Gerold Reichenbach**: Kollege von Notz, bitte.

BE **Dr. Konstantin von Notz** (BÜNDNIS 90/DIE GRÜNEN): Vielen Dank, Herr Vorsitzender. Zunächst einmal möchte ich mich den Ausführungen über die Form und den Ablauf des Kollegen Korte anschließen. Es ist keine Stilfrage, sondern es ist einfach unparlamentarisch, wenn das jetzt hier am Ende so oft knapp ist, wenn man auf der letzten Kante sitzt. Ich darf kurz auf die Einleitung von Herrn Prof. Dr. Abel eingehen, der nun sagte, dass die Daten das „Öl der Wissensgesellschaft“ sind. Um diese Metapher einmal ein bisschen transatlantisch zu bemühen, kann, wenn das so ist, unsere Antwort nicht „Drill, Baby, Drill“ sein. Es geht hier um einen hoch grundrechtsrelevanten Bereich und insofern erstaunt mich schon ein bisschen der Sound von Vielen, der in so eine Fundamentalopposition zu diesem Ansatz geht. Denn die Frage, die sich eigentlich stellt, ist doch, was passiert, wenn diese Verordnung nicht kommt? Ist das der

Weg, den wir wollen? Das halte ich im Rückschluss für falsch. Wir haben hier einen eigenen Antrag als Bundestagsfraktion BÜNDNIS 90/DIE GRÜNEN gestellt, um in die Textarbeit zu kommen und um zu besprechen, was man an dieser Vorlage verbessern kann. Das hat hier doch in den letzten zwei Stunden sehr wenig stattgefunden, sondern man hat irgendwie nur bemängelt. Aber die Frage ist, was die Alternative dazu ist. Zwei Fragen an Herrn Prof. Dr. Hornung: Ich möchte noch einmal – das haben Sie im Gutachten erwähnt, aber vielleicht in der Vorstellung keine Zeit dafür gehabt –, dass Sie die positiven Ansätze, die in der Verordnung sind, kurz benennen. Vielleicht bezugnehmend auf meine Einladung: Was machen wir denn nun mit den Themen „Big Data“, „Cloud-Computing“, soziale Netzwerke, der ganze Cross-Border-Datenverkehr, der augenblicklich stattfindet, wenn diese Verordnung nicht kommt? Was ist denn dann?

Abg. **Gerold Reichenbach**: Herr Dr. Hornung, Sie haben das Wort.

SV **Professor Dr. Gerrit Hornung** (Universität Passau): Vielen Dank für die Frage. Ich werde die nächsten zwei Stunden darüber reden, was man in dieser Verordnung noch alles besser machen kann und was passieren würde, wenn sie nicht kommt. Sie haben aber mit Cloud-Computing und transnationalen, insbesondere transatlantischen Datenflüssen zwei Grundprobleme angesprochen, um die es hier geht. Zum ersten Punkt: Positive Ansätze. Es liegt natürlich ein bisschen in der Natur der Sache, wenn man hier eingeladen wird, dass man sich immer die Frage stellt, was man besser machen oder was man kritisieren könnte. Ich habe eingangs schon gesagt, dass ich durchaus positive Ansätze sehe. Das wird klar, wenn man sich die nationalen Diskussionen anschaut: Das Modernisierungsgutachten von 2001, das für das BMI angefertigt worden ist, ist ebenso hoch gelobt wie praktisch komplett ignoriert worden. Auch da finden sich z. B. einige Ansätze für die heute diskutierten Probleme, etwa für bestimmte Verarbeitungskategorien, die weniger bedeutsam sind. Insofern würde ich nachdrücklich unterstreichen, dass wir hier positive Ansätze haben, und ich würde auch sagen, dass die Schlagworte da sind. Ich habe die Regelung zur Datenschutzrechtstechnik kritisiert – aber das Thema ist enthalten. Ich habe die Regelung zum Datenschutzaudit und Datenschutzgütesiegel kritisiert – aber das Thema ist enthalten. Wir haben die Datenschutzfolgenabschätzungen. Ich würde sagen, dass die Themen in dem Entwurf enthalten sind. Es käme darauf an, aus diesen Vorschlägen sinnvollere, bessere Regelungen zu machen, als es im Moment der Fall ist. Dazu habe ich einige Vorschläge gemacht und vieles von dem, was heute diskutiert worden ist, ist auch angeklungen. Worüber wir fast gar nicht gesprochen haben, ist tatsächlich der transatlantische Datenverkehr, der ein Problem ist: Microsoft und Google sind vielfach genannt worden und sind natürlich auch große Probleme. Auch die Regelung zur internationalen Anwendbarkeit ist aus meiner Sicht überarbeitungs- oder zumindest präzisierungsbedürftig. Was

würde passieren, wenn der Entwurf nicht kommt: Ich greife ein Beispiel heraus, nämlich das Cloud-Computing, weil das gerade angesprochen worden ist. Ich würde sagen, dass vieles von dem, was gegenwärtig vorgeschlagen ist, tatsächlich die Probleme des Cloud-Computings nicht lösen würde. Ein großes Problem des Cloud-Computings ist das Thema Auftragsdatenverarbeitung. Das Schlagwort ist heute noch gar nicht gefallen, und da hält die Regelung doch relativ stark an dem fest, was wir heute bereits im Bereich der Auftragsdatenverarbeitung haben, so dass ich sagen würde, dass die Probleme vor- und hinterher dieselben wären. Wir müssen im Bereich der Auftragsdatenverarbeitung etwas tun. Das müssten wir sowohl auf Basis des geltenden Rechts als auch auf der Basis dieses Entwurfs tun.

Abg. **Gerold Reichenbach**: Ich bedanke mich. Wir sind mit etwas Verzug am Ende der Anhörung. Ich darf mich bei den Sachverständigen noch einmal bedanken. Ich wünsche Ihnen einen guten Weg nach Hause. Sie sind aber natürlich auch gerne eingeladen, sich den zweiten Teil zur Richtlinie, mit dem wir um 14:00 Uhr beginnen, anzuhören. Ich wünsche allen einen guten Appetit.

**Ende der Sitzung: 13:06 Uhr**