

Innenausschuss
Protokoll
32. Sitzung

Bandabschrift

Öffentliche Anhörung

am 5. März 2007, 14.00 Uhr bis ca. 18.00 Uhr
10557 Berlin, Konrad-Adenauer-Str. 1

Sitzungssaal: Paul-Löbe-Haus, Raum 2 300

Vorsitz: Sebastian Edathy , MdB

Öffentliche Anhörung von Sachverständigen zur Thematik
„Modernisierung des Datenschutzes“

mit folgender inhaltlicher Strukturierung:

1. „Modernisierung des Datenschutzes“

2. „Datenschutz-Audit“

- a) Antrag der Abgeordneten Gisela Piltz, Ernst Burgbacher, Jens Ackermann, weiterer Abgeordneter und der Fraktion der FDP

Datenschutz-Audit-Verfahren und Datenschutz-Gütesiegel einheitlich regeln

BT-Drucksache 16/1169

- b) Antrag der Abgeordneten Silke Stokar von Neuforn, Kai Boris Gehring, Monika Lazar, weiterer Abgeordneter und der Fraktion BÜNDNIS 90/DIE GRÜNEN

Datenschutzaudit umsetzen - Gütesiegel stärkt Bürgerrechte und schafft Akzeptanz für wirtschaftliche Innovationen

BT-Drucksache 16/1499

3. „Scoring und Unternehmensinformationspflicht bei Datenschutzpannen“

- a) Antrag der Abgeordneten Silke Stokar von Neuforn, Bärbel Höhn, Ulrike Höfken, weiterer Abgeordneter und der Fraktion BÜNDNIS 90/DIE GRÜNEN

Mehr Datenschutz bei so genanntem Scoring

BT-Drucksache 16/683

- b) Antrag der Abgeordneten Silke Stokar von Neuforn und der Fraktion BÜNDNIS 90/DIE GRÜNEN

Informationspflicht für Unternehmen bei Datenschutzpannen einführen

BT-Drucksache 16/1887

	<u>Seite</u>
I. Anwesenheitsliste	4
<ul style="list-style-type: none"> • Mitglieder des Deutschen Bundestages • Bundesregierung, Bundesrat, Fraktionen 	
II. Sachverständigenliste	6
III. Sprechregister der Sachverständigen und Abgeordneten	7
IV. Protokollierung der Anhörung Bandabschrift	8
V. Anlage	79
Schriftliche Stellungnahmen der Sachverständigen - Ausschussdrucksachen-Nr. - 16(4) - 176 ff. -	
Prof. Dr. Ralf Bernd Abel FH Schmalkalden - 16(4)176 -	79
Dr. Johann Bizer Unabhängiges Landeszentrum für Datenschutz, Kiel - 16(4)176 G -	90
Dr. Alexander Dix Beauftragter für Datenschutz und Informationsfreiheit, Berlin - 16(4)176 D -	94
Andreas Jaspers Geschäftsführer der Gesellschaft für Datenschutz und Datensicherung e.V., Bonn - 16(4)176 F -	102
Karsten Neumann Der Landesbeauftragte für den Datenschutz, Schwerin - 16(4)176 E -	108
Cornelia Sasse Experian Deutschland Holding GmbH, Hamburg - 16(4)176 A -	149
Peter Schaar Bundesbeauftragter für den Datenschutz und die Informationsfreiheit, Bonn - 16(4)176 B -	156
Dr. Christian Thorun Verbraucherzentrale Bundesverband e.V., Berlin - 16(4)176 C -	162
Nicht angeforderte Stellungnahme SCHUFA Holding AG - 16(4)178	167

I. Anwesenheitsliste Mitglieder des Deutschen Bundestages

Bundesregierung

Bundesrat

Fraktionen und Gruppen

II. Liste der Sachverständigen für die Öffentliche Anhörung am 5. März 2007

1. **Prof. Dr. Ralf Bernd Abel** FH Schmalkalden

2. **Dr. Johann Bizer** Unabhängiges Landeszentrum für
Datenschutz, Kiel

3. **Dr. Alexander Dix** Beauftragter für Datenschutz und
Informationsfreiheit, Berlin

4. **Andreas Jaspers** Geschäftsführer der Gesellschaft für
Datenschutz und Datensicherung e.V.,
Bonn

5. **Karsten Neumann** Der Landesbeauftragte für den
Datenschutz, Schwerin

6. **Cornelia Sasse** Experian Deutschland Holding GmbH,
Hamburg

7. **Peter Schaar** Bundesbeauftragter für den Datenschutz
und die Informationsfreiheit, Bonn

8. **Dr. Christian Thorun** Verbraucherzentrale Bundesverband
e.V., Berlin

III. Sprechregister der Sachverständigen und Abgeordneten

Sprechregister der Sachverständigen

	Seite
Prof. Dr. Ralf Bernd Abel	10, 32, 38, 54, 61, 77
Peter Schaar	11, 22, 34, 43, 49, 54, 58, 59, 75
Dr. Johann Bizer	12, 16, 25, 30, 45, 48, 50, 57, 60, 73
Dr. Alexander Dix	13, 26, 34, 48, 49, 66, 71
Karsten Neumannn	14, 29, 51, 52
Andreas Jaspers	18, 40, 57, 67, 72
Dr. Christian Thorun	20, 27, 28, 36, 37, 42, 53, 60, 69, 70, 72, 75
Cornelia Sasse	39, 42, 50, 64, 68, 69, 73

Sprechregister der Abgeordneten

Vors. Sebastian Edathy	8, 11, 18, 37, 38, 43, 49, 61, 68, 78
BE Beatrix Philipp	9, 37, 38, 49, 59, 61, 68, 70, 77
BE Gisela Piltz	15, 39, 65, 68, 70
BE Dr. Michael Bürsch	24, 44, 70
BE Silke Stokar von Neuforn	31, 52, 74
BE Jan Korte	28, 49
Abg. Jörg Tauss	56

IV. Protokollierung

Vors. **Sebastian Edathy**: Sehr geehrte Damen und Herren, liebe Kolleginnen und Kollegen, ich darf die 32. Sitzung des Innenausschusses des Deutschen Bundestages in der laufenden Wahlperiode hiermit eröffnen. Die Sitzung findet statt in Form einer öffentlichen Anhörung zu verschiedenen Aspekten des Datenschutzes. Ich darf Sie hier alle sehr herzlich begrüßen. Mein Name ist Sebastian Edathy. Ich bin der Vorsitzende des Innenausschusses und werde heute die Anhörung leiten. Ich danke insbesondere Ihnen, meine sehr verehrte Frau Sachverständige, meine Herren Sachverständigen, dass Sie unserer Einladung nachgekommen sind, um hier die Fragen der Kolleginnen und Kollegen aus dem Innenausschuss sowie aus den mitberatenden Ausschüssen zum Themenbereich „Datenschutz“ zu beantworten. Wir hatten die Sachverständigen zudem gebeten, nach Möglichkeit schriftliche Stellungnahmen zu den Fragestellungen abzugeben.

Für die eingegangenen Stellungnahmen darf ich mich im Namen des Ausschusses herzlich bedanken. Sie sind den Mitgliedern des Innenausschusses, aber auch den Sekretariaten der mitberatenden Ausschüsse übermittelt worden, die Stellungnahmen werden zudem dem Protokoll über die Anhörung beigelegt. Ich gehe davon aus, dass das Einverständnis der Sachverständigen zur Durchführung einer öffentlichen Anhörung auch die Aufnahme ihrer Stellungnahmen in eine Gesamtdrucksache zu der Anhörung umfasst. Dem ist offenkundig so, herzlichen Dank. Von der heutigen Anhörung wird eine Bandabschrift gefertigt. Das Protokoll wird den Sachverständigen mit der Bitte um Korrektur übersandt. Im Anschreiben des Ausschusses werden Ihnen weitere Details zur Behandlung des Protokollentwurfes noch mitgeteilt. Die Gesamtdrucksache - bestehend aus dem Protokoll und den schriftlichen Stellungnahmen - wird dann im Übrigen nach der Freigabe auch ins Internet eingestellt. Zum zeitlichen Ablauf der heutigen Anhörung möchte ich anmerken, dass zwischen den Fraktionen vereinbart worden ist, insgesamt 4 Stunden vorzusehen, d.h. das Ende der Anhörung wird etwa bei 18.00 Uhr liegen. Ob und wann wir eine Pause bis dahin machen, könnten wir im Verlauf der Anhörung unmittelbar entscheiden.

Zum inhaltlichen Ablauf möchte ich noch einige Hinweise geben. Wie schon in der Einladung mitgeteilt, ist vereinbart, die Anhörung in drei Themenblöcke zu gliedern. Zunächst soll es allgemein um Gesichtspunkte der „Modernisierung des Datenschutzes“ gehen, 90 Minuten bis etwa 15.30 Uhr. Dann wollen wir miteinander über die vorliegenden parlamentarischen Initiativen im Bereich „Datenschutz-Audit“ reden, auch das soll 90 Minuten lang dauern, d.h. bis 17.00 Uhr. Und dann anschließend von 17.00 bis 18.00 Uhr wollen wir uns mit dem Thema „Scoring und Unternehmensinformationspflicht bei Datenschutzpannen“ befassen. Die zuständigen Berichterstatter im Innenausschuss haben miteinander vereinbart, die Anhörung zu jedem Themenkreis jeweils mit der unmittelbaren Befragung der Sachverständigen zu beginnen. Wenn Sie damit einverstanden sind, verfahren wir so. Vielen Dank. Dann erteile ich zur Befragung der Sachverständigen für den ersten

Bereich, nämlich für den allgemeinen Themenblock „Modernisierung des Datenschutzes“ der Berichterstatterin der Unionsfraktion, der Kollegin Beatrix Philipp das Wort. Ich bitte Frau Philipp und auch die weiteren Kolleginnen und Kollegen, die hier Fragen stellen, darum, nach Möglichkeit den- oder diejenigen Sachverständigen zu benennen, dem bzw. denen die jeweilige Frage gilt. Frau Philipp, Sie haben das Wort.

Abg. **Beatrix Philipp:** Herr Vorsitzender, meine Damen und Herren, ich darf vielleicht eine einleitende Bemerkung machen, weil ich mich noch mal ausdrücklich bedanken möchte oder darauf aufmerksam machen möchte, dass wir ein Verfahren gewählt haben, das also nicht ganz selbstverständlich ist, weil Anhörungen normalerweise - wenn ich das so sagen darf - zu Anträgen und ausschließlich zu Anträgen stattfinden, und wir hier eine Strukturierung gewählt haben, nämlich „Modernisierung des Datenschutzes“ im Allgemeinen. Und das ist nicht selbstverständlich, dass das nicht nur ausgesprochen friedlich, sondern mit der Zustimmung aller Fraktionen so vereinbart worden ist. Jedenfalls haben wir uns davon versprochen, diese Debatte etwas offener und großzügiger zu gestalten und eigentlich doch auch zum Ausdruck zu bringen, was nicht immer so unterstellt wird, aber dass es einige Dinge gerade im Bereich des Datenschutzes gibt, die uns einen. Das ist spätestens dann festzustellen, wenn der Datenschutzbericht im Plenum aufgerufen wird und wir eine - bisher jedenfalls immer - gemeinsame Resolution fertig gebracht haben, einen Entschließungsantrag. Auch das ist nicht selbstverständlich. Ich will das mal vorausschicken, weil ja eigentlich immer sofort angenommen wird, dass beim Datenschutz - also spätestens beim Datenschutz - sich die Welten trennen, die Geister scheiden, wie auch immer. Das Gemeinsame, denke ich, ist ganz sicherlich der Wunsch nach mehr Transparenz. Das zieht sich durch alle Bereiche und wird auch seit einigen Jahren - wenn ich das so sagen darf - immer wieder deutlich gemacht. Und auch eine gewisse Zufriedenheit mit dem Datenschutzgesetz kann man feststellen. Aber es gibt zweifellos, und das kann man eben auch schon den vorliegenden Stellungnahmen entnehmen, einige Defizite im Bereich der Umsetzung hier oder da. Und deswegen sitzen wir u.a. hier zusammen, um zu überlegen, was verbesserungswürdig, was verbesserungsfähig ist und wie man das dann am besten gestaltet. Dass es Vollzugsdefizite gibt, merkt man spätestens dann, wenn man gezwungen ist, auf europäischer Ebene zu einem Konsens zu kommen bei der Umsetzung in den einzelnen europäischen Ländern, spätestens aber dann, wenn man versucht, Europa und die USA auf eine Linie zu bringen. Das will ich jetzt aber nicht vertiefen. Das wird ja auch im Plenum diese Woche noch mal eine Rolle spielen.

Also dieses vorausgeschickt, würde ich doch vielleicht Herrn Prof. Abel, aber auch die anderen, so sie sich verstehen als diejenigen, die etwas beizutragen haben, bitten: Diese institutionellen Vorkehrungen, die Herr Prof. Abel in seiner Stellungnahme als verbesserungswürdig ansieht wie zivilrechtliche Instrumente, die einer Verbesserung bedürfen, vielleicht könnten Sie dazu ein paar Beispiele nennen.

Dann etwas, was mich sehr interessieren würde, ob die Sanktionen ausreichend sind. Sie haben, Herr Prof. Abel, an einer Stelle „Vorsprung durch Rechtsbruch“ formuliert. Vielleicht ist auch das ein Stichwort, über das wir uns hier mal etwas näher unterhalten müssten.

Vors. **Sebastian Edathy**: Herr Prof. Abel, Sie sind direkt angesprochen worden. Ich bitte um Ihre Stellungnahme.

SV **Prof. Dr. Ralf Bernd Abel**: Vielen Dank, Frau Philipp. Meine Damen und Herren, die Fragestellungen sind außerordentlich vielseitig. Es geht darum, dass Datenschutz an so vielen Stellen wie möglich und so breit wie möglich verankert wird, um den Gefährdungen, von denen wir alle wissen, die aus Technologie und technologischer Entwicklung fließt, entgegenzutreten. Zum einen gibt es die Möglichkeiten des Datenschutzrechtes im engeren Sinne. Aber es ist ja von Anfang an bekannt, dass das klassische Datenschutzrecht, das BDSG in seiner Funktion als „Grundgesetz des Datenschutzes“, nur einen Teilaspekt, vielleicht einen Hintergrundaspekt ausleuchten kann, aber eben nur einen Teilaspekt. Ein anderer Teilaspekt ist das Thema „Vorsprung durch Rechtsbruch“. Sie haben es direkt angesprochen. Das ist ein Thema aus einem scheinbar ganz anderen Bereich, nämlich aus dem Wettbewerbsrecht. Ich komme deshalb darauf, weil ich häufiger von Unternehmen gebeten werde, gutachtlich dazu Stellung zu nehmen, was datenschutzrechtlich richtig und was nicht zulässig wäre. Und in solchen Gesprächen kommt es dann nicht selten vor, dass jemand auf Seiten eines Unternehmens sagt: Ja, wenn wir uns gesetzeskonform verhalten - neuhochdeutsch „Compliance“ genannt - wenn wir uns gesetzeskonform verhalten, dann kostet uns das auch eine ganze Menge Geld und Aufwand. Da gibt es andere, die machen es nicht. Und was passiert? Eigentlich erkennbar eher wenig. Und dann hat sich schon lange die Frage gestellt: Wie ist es dann z.B. mit dem Wettbewerbsrecht, wo ja nicht nur Unternehmen sich untereinander ggf. verklagen, sondern wie ist es, wenn auch Verbraucherschutzverbände - also autorisierte Organisationen - das Recht haben, auch Datenschutzverstöße mit wettbewerbsrechtlichen Mitteln zu verfolgen, um so diejenigen „schwarzen Schafe“, diejenigen, die sich unterhalb der gesetzlichen Norm betätigen, und damit wirtschaftliche Vorteile verbinden, in den Griff zu bekommen? Ich könnte mir also vorstellen, dass man hier vielleicht seitens des Gesetzgebers im Rahmen des UWG eine Verdeutlichung festschreibt, denn es ist bisher so, dass die Rechtsprechung der Vorstellung, dass hier ein Vorsprung durch Rechtsbruch erfolge, nicht so recht gefolgt ist. Heute muss schon Gravierendes passieren, um die Möglichkeiten des UWG wahrzunehmen. Soviel zu der einen Frage, die Sie angesprochen haben.

Zum Zweiten geht es um das Thema „Sanktionen“. Wir haben bekanntlich im BDSG und an anderer Stelle ein paar strafrechtliche Sanktionen und Ordnungswidrigkeitstatbestände. Aber wenn man sich die Größenordnung der Bußgelder anschaut und die Höhe der Strafen, dann sind das keine

Größenordnungen, die in einem angemessenen Verhältnis stehen zu einer in größerem Umfang vorkommenden Nichtübereinstimmung mit dem Gesetz. Man kann sehr leicht erhebliches Geld einsparen, und dann mögen Bußgelder, die sich ja staffeln und auch nicht immer sofort in höchster Form verhängt zu werden pflegen - wenn überhaupt - solche Bußgelder also als eher gering erscheinen. Nun mag es sein - das müsste man erforschen, darüber könnte man nachdenken -, ob die Wirksamkeit von Sanktionen nun immer von der Höhe der Strafandrohung oder vielleicht von der Dichte der Bußgeldverfolgung abhängt. Aber eine zu geringe Höhe mag auch ein Signal in die falsche Richtung sein, nämlich, dass datenschutzwidrige Verhaltensweisen oder Nichtkonformität mit den gesetzlichen Anforderungen, sehr lässliche kleine Sünden und bloßes Verwaltungsunrecht seien. Darüber - meine ich - sollte man schon an dieser Stelle nachdenken.

Vors. **Sebastian Edathy**: Herr Schaar, möchten Sie sich auch zur Thematik äußern? Und wenn es weitere Sachverständige gibt, die zu dem Bereich etwas sagen wollen, geben Sie bitte ein Handzeichen.

SV **Peter Schaar**: Vielen Dank, Herr Vorsitzender. Ich stimme Herrn Abel vollständig zu im Hinblick auf die angedachten Konsequenzen. Ich will noch mal verdeutlichen, wo hier Lücken sind. Wir haben im § 43 BDSG bestimmte Bußgeldvorschriften. Diese Bußgeldvorschriften sind allerdings nicht konsequent und sind nicht wirklich lückenlos. Es fällt z.B. auf, dass nur in wenigen Ausnahmefällen die unrechtmäßige Nutzung personenbezogener Daten sanktioniert wird. Nämlich wenn diese Daten für einen bestimmten Zweck übermittelt worden sind, und dann zu einem anderen Zweck genutzt werden. Aber in dem Fall, in dem die Daten von einer verantwortlichen Stelle, die sie erheben durfte, völlig zu Unrecht genutzt werden, fehlt jegliche Sanktionsandrohung. Das ist völlig inkonsequent, das ist auch nicht einzusehen, dass hier mit zweierlei Maß gemessen wird. Gerade durch die zweckfremde Nutzung der Daten entsteht zusätzliches Gefährdungspotential. Und es sind auch erhebliche Schäden für den Betroffenen zu befürchten. Gerade deshalb meine ich, hier muss man diese Lücke schließen.

Zweiter Punkt: Er betrifft nicht in erster Linie die Vorschriften des BDSG, sondern die Organisation der Datenschutzkontrolle, der Datenschutzaufsicht für den nichtöffentlichen Bereich. Hier wissen Sie ja, dass wir Länderzuständigkeit haben, abgesehen von den beiden Bereichen, für die ich zuständig bin, nämlich Post und Telekommunikation. Die Länderzuständigkeit hat Konsequenzen für die Ahndung von Ordnungswidrigkeiten. Des Weiteren hört man von Wirtschaftsvertretern, dass bestimmte Aufsichtsbehörden besonders streng seien und auch bereit seien, hohe Bußgelder zu verhängen, andere nicht. Ich will das jetzt nicht kommentieren. Gleichwohl ist es durchaus nicht nur plausibel, sondern es gibt Anhaltspunkte dafür, dass ein Teil der Aufsichtsbehörden besonders zurückhaltend ist, insbesondere Aufsichtsbehörden, die sich mit anderen Ministerien abzustimmen haben. D.h., wir stoßen im Düsseldorfer Kreis, in der Koordinationsinstanz der Aufsichtsbehörden,

bisweilen auf das Argument, das haben wir noch nicht mit dem Wirtschaftsministerium abgestimmt. Das kann nicht sein. Die Stärkung der Unabhängigkeit der Datenschutzaufsicht für den nichtöffentlichen Bereich hat etwas mit Vollzugsdefiziten zu tun und auch mit einer teilweisen Nicht-Ahndung von Ordnungswidrigkeiten. Ich will hier nicht pauschal sagen, alle Datenschutzaufsichtsbehörden, die bei Länderministerien sind, handeln so. Aber das Argument ist eigentlich nicht zulässig, dass ministerielle Abstimmungs-Mechanismen greifen sollen, so dass dann also Standortaspekte mit darüber entscheiden, ob eine bestimmte ordnungswidrige Handlungsweise sanktioniert wird oder nicht. Danke.

Vors. **Sebastian Edathy**: Vielen Dank, dann würde ich Herrn Dr. Bizer zunächst bitten.

SV **Dr. Johann Bizer**: Vielen Dank. Es ist ja schon mal erschütternd, dass man feststellen muss, dass es Unternehmen gibt, die mit dem Argument kommen, die Einhaltung des geltenden Rechts sei zu aufwendig. Das ist doch für einen Rechtsstaat ein sehr erschütterndes Zwischenergebnis und Zwischenfazit. Es bedeutet im Grunde genommen, dass das Vertrauen in die Integrität der rechtlichen Bestimmungen des Rechtsstaats zerbröseln, wenn sich das bewahrheitet und sich durchsetzt und fortsetzt. Da muss der Gesetzgeber also aufpassen, dass er in seiner Tätigkeit mit dem, was er verabschiedet, auch wirklich dafür sorgt, dass das, was er da macht, zur Lachnummer wird, um es etwas salopp zu formulieren. Wir kennen das Problem aus dem Umweltbereich natürlich auch. Das ist ein ganz historisches Problem. Deswegen reden wir ja auch über die Modernisierung des Datenschutzrechts, nämlich mit welchen Mechanismen es uns gelingt, dieses Vollzugsdefizit abzubauen. Und der eine Weg, der angedeutet worden ist, ist der, der sehr schnell unter dem Label „mehr Bürokratie“ läuft: Aufwertung der Aufsichtsbehörden. Und der andere Weg ist, den Herr Abel auch mit beschrieben hat, als eine, man muss versuchen, mit Hilfe von Wettbewerb, von Wettbewerbskriterien diesen vermeintlichen Vorteil in ein Nachteil umzudeuten. Beide Wege sind richtig. Über den zweiten Weg - denke ich - reden wir dann noch mal, wenn es um Datenschutz-Audit geht. Beim ersten Weg wird man mit Sicherheit darauf achten müssen, dass das, was als Vollzugskapazität da ist, auch wirklich effektiv wirksam in der Lage ist, zu arbeiten. Dazu gehört zum einen - da stimme ich Herrn Schaar völlig zu - die Unabhängigkeit der Aufsichtsbehörden, dazu gehört aber auch eine personelle Ausstattung, nicht nur quantitativ, sondern auch qualitativ, die in der Lage ist, nicht nur einfach prima facie, eine AGB-Kontrolle vorzunehmen, also im Internet zu gucken und zwar AGB-Bestimmungen gegeneinander zu halten, sondern die auch in der Lage ist, eine technische Kontrolle vor Ort vorzunehmen, um zu gucken, ob das, was behauptet wird, auch wirklich eine tatsächliche Datenverarbeitung vor Ort stattfindet. Und ich glaube, dass ich keine allzu „kessle Lippe“ riskiere, und allzu vielen Kollegen „in die Suppe spucke“, wenn ich behaupte, dass in den meisten Aufsichtsbehörden die technische Kompetenz aufgrund

mangelnder personeller Ausstattung nicht vorhanden ist, um solche aktiven Kontrollen vor Ort, auch technischen Kontrollen vor Ort, auch vorzunehmen. Und das führt dazu, dass sich Daten verarbeitende Stellen sehr leicht auch sehr sicher fühlen können, weil sie eben nicht Sorge haben müssen, da kommt dann mal eine Kontrollbehörde und guckt vorbei und sagt: Machen sie mal ihr Passwort und zeigen sie mal, was sie da haben; wir wollen mal sehen, mit welchen Programmen sie arbeiten und sozusagen dezidiert nachzuprüfen, was da eigentlich für personenbezogene Daten verarbeitet werden.

Vors. **Sebastian Edathy**: Vielen Dank. Noch zwei weitere Wortmeldungen von Sachverständigen, Herr Dr. Dix und dann Herr Neumann, bitte.

SV **Dr. Alexander Dix**: Vielen Dank, Herr Vorsitzender. Ich wollte nur noch das ergänzen, was Herr Schaar gesagt hat, den offensichtlichen Wertungswiderspruch in den Bußgeldtatbeständen, den Ordnungswidrigkeitentatbeständen. Das kann man sehr plastisch machen, wenn man den Fall eines markt- und meinungsforschungs- oder eines werbetreibenden Unternehmens nimmt, das Personen anschreibt, um Daten zu erheben. Es ist gesetzlich verpflichtet, dabei auf das Widerspruchsrecht nach § 28 BDSG hinzuweisen. Wenn es diese Pflicht verletzt, begeht es eine Ordnungswidrigkeit. Wenn es aber korrekt auf das Widerspruchsrecht hinweist und anschließend die Daten eingesammelt hat und sich über den Widerspruch hinwegsetzt, der erhoben worden ist, ist es keine Ordnungswidrigkeit. Das kann nicht sein. Dieser eklatante Widerspruch sollte schleunigst behoben werden.

Ich will aber auch noch auf eine - aus meiner Sicht - notwendige Ergänzung des Systems der Bußgeldtatbestände hinweisen, das sich aus neueren Erfahrungen ergibt, die die Aufsichtsbehörden in verstärktem Umfang machen. Es gibt immer wieder Fälle, in denen Personen im Internet öffentlich zugängliche Informationen in veränderter Form, teilweise in manipulierter zusammengesetzter Form, zu neuen Veröffentlichungen nutzen, um die abgebildeten, die diese Bilder teilweise selbst ins Internet gestellt haben, zu verleumden oder an den Pranger zu stellen - wie auch immer - schlecht aussehen zu lassen. Ein besonders eklatanter Fall war zu beobachten bei dem gescheiterten Grundstücksverkauf in Delmenhorst, wo eine Bürgerinitiative von Personen, die den Verkauf des Hotels an einen NPD-Funktionär verhindern wollte, dafür wiederum im Internet mit einer Liste in Erscheinung getreten ist und anschließend haben Rechtsradikale diese Liste genutzt, um sozusagen die politischen Gegner „an die Wand zu stellen“ und zu verleumden in übelster Weise. Das ist nur ein Beispiel, es gibt noch ganz andere, unpolitische Beispiele, die es aber meiner Ansicht nach notwendig machen, hier einen neuen Bußgeldtatbestand zu formulieren, der die Verwendung allgemein zugänglicher Daten dann mit Bußgeld bedroht, wenn die schutzwürdigen Interessen der Betroffenen offensichtlich dadurch beeinträchtigt werden. Die bestehenden zivilrechtlichen und strafrechtlichen Sanktionen, die evtl. hier auch greifen würden, sind häufig in solchen Fällen stumpf. Deshalb meine ich, sollte das Arsenal der Bußgeldtatbestände ergänzt werden.

Vielleicht noch einen ergänzenden Hinweis zu dem Gesichtspunkt des Wettbewerbs, den Herr Abel erwähnt hat. Ich erinnere daran, dass das Bundesverfassungsgericht in seiner Entscheidung zu den Berufsunfähigkeitsversicherungen vom Oktober vergangenen Jahres den Mangel an Wettbewerb um den besten Datenschutz ausdrücklich gerügt und kritisiert hat. Also, es muss auch Anliegen des Gesetzgebers sein, für einen solchen Wettbewerb zu sorgen, denn nur dann ist der einzelne Betroffene in der Lage, mit Hilfe von Einwilligung und anderen Möglichkeiten auf die Verwendung seiner persönlichen Daten steuernd Einfluss zu nehmen.

Vors. **Sebastian Edathy**: Dann abschließend in dieser Runde Herr Neumann, bitte.

SV **Karsten Neumann**: Ich wollte auf die Frage von Frau Philipp noch zwei Aspekte ergänzen. Die erste Voraussetzung - denke ich - für Wirksamkeit strafrechtlicher Sanktionen ist das Vorhandensein eines Unrechtsbewusstseins. Schon dies begegnet uns in vielen Fällen, dass das allein fehlt, sondern Datenschutz oft als lästiges bürokratisches Hindernis begriffen wird und deshalb auch die Sanktion bei Verstößen dagegen unter der Überschrift „der Amtsschimmel wiehert“ wahrgenommen wird, also die Grundrechtsrelevanz der Tätigkeit und der Aufsichtstätigkeit, die wir da ausüben, auch unterschätzt wird. Zum zweiten Aspekt. Wie wirkt die Strafandrohungshöhe? Ich habe es feststellen können in Mecklenburg-Vorpommern. Nachdem vor zwei Jahren bei uns die Aufsicht beim Landesbeauftragten für den Datenschutz zusammengeführt wurde, habe ich im Haushaltsplan als Leertitel eine Einnahmeposition für Bußgelder in den Haushalt geschrieben, damit wir überhaupt, falls die Situation mal kommt, in der Lage sind, etwas einzuziehen. Schon das hat ausgereicht in vielen Fällen. Es hat sich herumgesprochen, dass die Aufsichtsbehörde nun wohl bereit ist, dieses Mittel auch zu nutzen. Schon das wirkt. Meine zweite Beobachtung in dem Zusammenhang: Ich führe Schulungen für betriebliche Datenschutzbeauftragte durch und frage immer ganz gern: Wie kommen sie denn hierher? Und ich höre zunehmend, dass Wirtschaftsprüfer im Rahmen der Prüfung eines Unternehmens auf das finanzielle Risiko der fehlenden Bestellung eines Datenschutzbeauftragten aufmerksam machen. Und über diesen Weg die Unternehmen erfahren, dass sie Datenschutzbeauftragte zu bestellen haben. Das ist aus meiner Sicht auch ein interessanter Ansatz, der vielleicht verstärkt werden kann, umso höher tatsächlich die Strafandrohung ist. Letztendlich ist aber auch aus meiner Sicht - und das will ich gerne unterstützen - das Vollzugsdefizit natürlich in der Kalkulation mit drin. Also die Unternehmen wissen natürlich, wie leistungsfähig die Aufsichtsbehörden sind, auf welchem Weg sie überhaupt Verstöße feststellen und wie sie dann agieren. Das ist völlig transparent. Wir sind in dem Fall sehr transparent. Und damit ist auch die Höhe des Risikos leicht zu kalkulieren. Doch aus meiner Sicht fehlt leider eine Flanke in diesem Schutzmechanismus, und das ist die Justiz, das ist die Staatsanwaltschaft, bei denen ich versucht habe, in den letzten anderthalb Jahren verstärkt darauf hinzuweisen, dass wir hier in der Definition von Juristen oft als strafrechtliche

Dunkelnorm definiert Mittel in der Hand haben, um einen Bereich von wachsender Kriminalität auch entgegenzutreten, die bisher - denke ich - bei der Justiz so bekannt noch nicht sind. Auch das Strafantragsrecht des Landesbeauftragten führte erstmals dazu, dass viele Staatsanwaltschaften sich mit diesen Sanktionen überhaupt beschäftigt haben. Ich denke, auch auf dieser Schiene wäre durch die Justiz noch einiges zu leisten. Danke.

Vors. **Sebastian Edathy**: Vielen Dank. Das Fragerecht wechselt dann zur FDP-Fraktion. Das Wort hat die Kollegin Gisela Piltz.

Abg. **Gisela Piltz**: Vielen Dank, Herr Vorsitzender. Meine Kollegin Beatrix Philipp hat ja schon darauf hingewiesen, dass es gute Tradition hat, dass wir hier immer gemeinsame Beschlüsse im Bundestag fassen zum Bericht des Datenschutzbeauftragten. Aber, und das ist sicherlich etwas, was man sehr positiv sehen kann: Wenn man allerdings weiß, wie die Diskussionen laufen, wenn wir diese Beschlüsse haben, dann weiß man auch, dass sozusagen die Diskussion - je nach dem welcher Fraktion man hier angehört - doch sehr unterschiedlich verlaufen. Es ist ja auch kein Zufall, dass im Koalitionsvertrag der Datenschutz eigentlich nur als Bürokratiebegleiterscheinung erwähnt wird. Sie können sich vorstellen, dass die FDP das anders sieht. Gerade in der letzten Woche hat insbesondere der CDU-Innenminister bei einer Veranstaltung gesagt: „Wir brauchen einen Paradigmenwechsel, es muss nicht mehr geregelt werden, ob Daten erhoben werden, sondern nur noch, wer Zugriff haben soll.“ Das finde ich schon sehr interessant, und bringt mich dann zu einigen Fragen. Wie ich eben gesagt habe, Datenschutz ist für uns mehr als nur ein lapidares Recht. Datenschutz ist für uns aber zugleich sicherlich auch eine technische Herausforderung. Das ist ja immer mehr erkennbar. Und ich bitte daher jetzt die Sachverständigen Herrn Dr. Bizer, Herrn Jaspers und Herrn Schaar zum einen zu erläutern, welche Meinung sie vertreten, welche Möglichkeiten es gibt, den technischen Datenschutz zu verbessern, was der Gesetzgeber hierzu beitragen kann und welche Regelungsdefizite es aus ihrer Sicht im Bereich des Datenschutzes bei der polizeilichen und justiziellen Zusammenarbeit gibt. Datenschutz in der dritten Säule ist dabei sicherlich ein klassisches Stichwort.

Dann habe ich noch eine Frage an Herrn Jaspers alleine. Und das ist ein Thema, was Herr Schaar eben auch schon angesprochen hat, nämlich die Frage, wie man die Datenschutzaufsicht im nichtöffentlichen Bereich verbessern könnte und ob es da ein gangbarer Weg wäre, die Aufsicht auf private Dritte zu übertragen? Es ist schwierig, aber es geht ja darum, dass wir neue Wege suchen. Und es ist auch gerade darauf hingewiesen worden auf das Thema im Zusammenhang mit den Wirtschaftsprüfern. Ich weiß, dass wir darüber auch schon mal in der Partei nachgedacht haben, ob es nicht Sinn machen könnte im Zusammenhang mit dem Prüfbericht, einfach eine Verpflichtung sozusagen hineinzuschreiben, was den

Datenschutz angeht, weil man sich vorstellen könnte, dass das dann weitere Folgen automatisch mit sich bringt.

Dann habe ich eine Frage auch noch mal an Herrn Dr. Bizer. Wir kommen zwar nachher im Zusammenhang mit dem Datenschutz-Audit dazu, aber das ist ja nicht das einzige, denke ich, was marktwirtschaftliche Anreize schaffen könnte im Datenschutz. Ob Sie noch andere Vorschläge haben, Stichwort „privacy sells“, weil ich mir vorstellen könnte, dass das dann eben marktwirtschaftlich geregelt wird, das ist immer besser als staatliche Regelung. Aber das sehen andere natürlich auch wieder anders.

Und zum Schluss habe ich eine Frage noch mal an Herrn Jaspers und auch an Herrn Thorun. Datenschutz ist ja auch - das wurde auch schon angesprochen - eine gesellschaftliche Aufgabe. Erschreckend ist ja, wie viele Menschen bereit sind, für 3 Prozent über ihre Payback-Karte oder einfach nur über die Teilnahme an Preisausschreiben ihre Daten preis zu geben. Ob Sie da Möglichkeiten sehen, wie man einfach das Bewusstsein von Verbrauchern dafür schärfen kann, dass eben die eigene Datensparsamkeit der erste Schritt zum besseren Datenschutz ist. Vielen Dank.

Vors. **Sebastian Edathy**: Es sind also angesprochen - teilweise zu mehreren Fragen - Herr Dr. Bizer, Herr Jaspers, Herr Dr. Thorun und Herr Schaar. Wollen wir in der Reihenfolge vorgehen? Herr Dr. Bizer, bitte.

SV **Dr. Johann Bizer**: Zur ersten Frage zum technischen Datenschutz. Ich will mit einem Beispiel anfangen. Als das Internet anfang hat der Gesetzgeber aus guten Gründen, beraten durch verschiedene Expertengremien, ich erinnere an den Forschungsrat, damals war Herr Rüttgers Forschungsminister, das Thema des Selbstdatenschutzes auf seine „Fahnen“ geschrieben. Und zwar deswegen, weil man sich darüber im Klaren war, dass man die neuen Medien nur nutzen kann, wenn es auch Akzeptanz gibt. Und die Akzeptanz ist gefährdet, so die Vermutung - die gesicherte Vermutung mittlerweile -, wenn die Betroffenen das Gefühl haben, dass die Daten ihrer elektronischen Kommunikation von Dritten erfasst werden, sich sozusagen von ihnen entfernen und sie nicht einmal die Verfügbarkeitskontrolle über ihre Daten haben. Deswegen hatte der Gesetzgeber damals das Teledienstschutzgesetz formuliert, sozusagen pro-aktives Datenschutzmodell. Und über dieses Gesetz ist auch das erste Mal eine Vorschrift formuliert worden, Datenschutz durch Technik - eine Zielformulierung, die es den verantwortlichen Stellen aufgibt, Daten sparsamer, datenvermeidende Technologien zu implementieren. Das ist die Bestimmung, die später im Rahmen der BDSG-Novelle in § 3a Eingang gefunden hat. Das ist ein ganz grundlegender Paradigmenwechsel, weil es nämlich bedeutet, dass die datenverarbeitenden Stellen nicht nur auf der Ebene von Rechtschutz, also AGBs formulieren, sondern auf der Ebene von technischen Konzepten Daten sparsam arbeiten und wirken sollen, sozusagen auch im eigenen Interesse. Die Diskussion „poppt“ wieder auf im Zusammenhang bspw.

mit der Vorratsdatenspeicherung. Wenn das eine oder andere Unternehmen sagt: Warum sollen wir denn hier eigentlich Daten übermäßig speichern, es ist aus unserer Perspektive aus Kostengesichtspunkten viel günstiger, die Daten vorzeitig wieder zu löschen, weil wir sie gar nicht brauchen. Also Datensparsamkeit liegt im ureigenen Interesse des Unternehmens und im ureigensten Interesse der jeweiligen Betroffenen.

Jetzt ist die Frage, wie kann man diesen Datenschutz durch Technik implementieren? Man kann ihn auf der einen Seite implementieren nicht durch Rechtsbestimmung, sondern durch eine Form von pro-aktiver Forschungs- und Entwicklungspolitik. Das ist eine Frage der Innovation. Ich will mal ein Beispiel nennen: Aus einem europäischen Fördertopf arbeiten wir derzeit mit einem kleinen mittelständischen TK-Unternehmen in Kiel zusammen und entwickeln einen Spam-Filter für Voice over IP. Das ist sozusagen pro-aktiver technischer Datenschutz. Spam kennen wir über e-Mail. Es ist absehbar, dass es bald bei Voice over IP unheimlich billig ist, dass es auch Spam geben wird. Also muss man technische Vorsorge dazu schaffen. Oder zweites Beispiel: Wir alle merken in der praktischen Arbeit, insbesondere mit Forschungseinrichtungen, mit Forschungslabors, wenn es um medizinische Daten geht, dass Pseudonymitätskonzepte einen unheimlich hohen Stellenwert in der Praxis haben. Auf der einen Seite geht es darum, Datenverarbeitung zu ermöglichen, aber auf der anderen Seite will man auch die Risiken möglichst minimieren. Das kann man durch intelligente Pseudonymitätskonzepte machen. Man muss nur sicherstellen, dass es eindeutige Verwendungsverbote gibt. Dass es Regeln gibt, die unterbinden, dass die Identifikationsdaten nicht unbefugt zusammengeführt werden mit den pseudonymisierten Daten. Dass man Johann Bizer nicht der Nummer 211 zufügen kann. Unter 211 sind dann alle meine personenbezogenen medizinischen Daten gespeichert. Das ist ein Punkt, an dem der Gesetzgeber es bisher versäumt hat, eine klare ausdrückliche Regelung zum Schutz von Pseudonymitätskonzepten zu schaffen. Wenn man Datenschutz durch Technik nach vorne bringen will, dann muss man auf der einen Seite sehen, das hat auch etwas zu tun mit Technik, technischer Innovation, mit der Förderung von dieser modernen datensparsamen Technologie. Aber es hat auf der anderen Seite mit Datenschutzrecht zu tun, nämlich dann, wenn es darum geht, Pseudonymitätskonzepte auch rechtlich abzusichern. Und da sind wir an einer Schnittmenge, wo ich den Teilbereich Ihrer zweiten Frage aufgreifen kann. Wenn man nämlich Pseudonymitätskonzepte hat, ist die nächste Frage, wer darf denn auf diese Pseudonymitätskonzepte zugreifen? Klar, erst einmal bspw. der Universitätsforscher, der mit den Daten arbeiten will. Aber wir wissen natürlich auch sofort, dass im Hintergrund auch schon die Begehrlichkeiten der Behörden der Inneren Sicherheit aufflackern, wenn man solche Pseudonymitätskonzepte realisiert hat. Das ist ein ganz kritischer Punkt, weil er in dem Moment, wo man diesen Begehrlichkeiten nachgibt, wiederum das Vertrauen der Betroffenen in die Integrität dieser Pseudonymitätskonzepte automatisch „mitschwingt“.

Zu Ihrer nächsten Frage: Audit. Also gibt es noch „privacy sells“? Gibt es noch andere Instrumente um dieses „privacy sells“ zu befördern? Ja, es gibt sie. Es gibt sie auf der einen Seite durch klare Transparenzregelungen, die Verpflichtung zur Transparenz nach außen. Wir haben den § 4 Abs. 3 BDSG, der die einzelnen Unternehmen verpflichtet zu sagen, wer sie sind, zu welchen Zwecken sie personengebundene Daten verarbeiten und an welche Kategorien an Empfängern sie diese Daten vermitteln. Man könnte diesen Katalog durchaus noch erweitern, um weitere Informationspflichten, um auf diese Art und Weise dem Betroffenen zu vermitteln, was im Einzelnen, wer jeweils verantwortlich ist. Z.B. könnte man diesen Informationskatalog erweitern um die Information, wer der betriebliche Datenschutzbeauftragte ist. Man könnte „privacy sells“ auch erweitern, indem man - da nehme ich einen Aspekt von Herrn Abel auf, den wir nicht weiter erörtert haben - indem man dieses Problem des Wettbewerbsvorsprungs durch Rechtsbruch, dadurch versucht, zu nivellieren, dass man ein Verbandsklagerecht einführt. Dass man die Möglichkeit eröffnet, dass Verbraucherdatenschutzverbände ebenfalls, so ähnlich wie es im Wettbewerbsrecht Gang und Gebe ist, sozusagen den Verstoß gegen datenschutzrechtliche Vorschriften sanktioniert. „Privacy sells“ hat nach unserer Erfahrung überall dort eine besondere Bedeutung, wo die einzelnen Unternehmen eine hohe Kundenaffinität haben. Also bspw. im Telekommunikationsbereich, im Internetsektor, so etwa wie im Versandhandel, wo es wirklich darum geht, Geschäfte zu generieren durch Kundenkontakte. Solche „privacy sells“-Konzepte durch Transparenz wirken überall da nicht, wo wir es sozusagen mit einer Grauzone, mit einem Dunkelbereich an Datenverarbeitung zu tun haben. Dazu gehört insbesondere der Bereich der Auskunfteien oder des Adresshandels, die von ihrem Geschäftsmodell her schon kein Interesse daran haben, eine offene Kommunikation mit ihren Verbrauchern und Kunden zu führen. Der Kunde der Auskunftei ist ja nicht der Betroffene, von dem er eigentlich die Daten hat, sondern der Kunde, der Auskunftei ist der Händler, der die Daten kauft. Demgegenüber will er transparent sein, aber nicht gegenüber dem Betroffenen. Bei diesem Graubereich der Daten verarbeitenden Stellen, da reichen - glaube ich - einfache Konzepte von „privacy sells“ nicht aus. Da wird man auch mit klaren rechtlichen Vorschriften wie § 9 BDSG und klaren Sanktionen nur nach vorne kommen können.

Vors. **Sebastian Edathy**: Vielen Dank, Herr Dr. Bizer. Ich möchte grundsätzlich darum bitten, wenn es sich irgendwie einrichten lässt, wegen unseres zeitlichen Rahmens, die Beantwortung der Fragen möglichst knapp zu halten, ohne dass es natürlich zu Lasten der Inhalte gehen soll. Herr Jaspers.

SV **Andreas Jaspers**: Zur ersten Frage: Datenschutz durch Technik. Ein Blick ins bestehende Bundesdatenschutzgesetz, das die größten Bereiche des Datenschutzes abdeckt, zeigt, es hat wenige Normen, die sich mit dem Thema „Datenschutz durch Technik“ beschäftigen, nämlich den § 9 und seine Anlage. Dieser ist maßnahmeorientiert. Er hat praktisch noch den technologischen Hintergrund der

Großrechnerwelt der 70er Jahre, ist überhaupt nicht mehr zeitgemäß. D.h., wenn wir fragen, was muss der Gesetzgeber sofort tun, so gehört der § 9 und Anlage in dieser Form abgeschafft, abgeändert. Das ganze muss zielorientiert sein. D.h. die klassischen Ziele der IT-Sicherheit - Verfügbarkeit, Vertraulichkeit, Integrität von Daten - müssen letzten Endes als Sicherheitsziel formuliert werden. Landesdatenschutzgesetze sind da sicherlich vorbildlicher gewesen. Datenschutz durch Technik bedeutet auch Pseudonymisierungskonzepte. Dies setzt aber voraus, dass man sich das Thema „Pseudonymität“ einmal genauer im Gesetz anschaut. Auch hier gibt es im BDSG unsaubere Lösungen, denn das Thema „Pseudonymisierung“ ist so definiert, dass es weiterhin personenbezogene Daten sind, d.h. sämtliche Schutzkonzepte ziehen im Grunde genommen nicht, weil die volle Anwendungspraxis des BDSG auch bei Pseudonymen gilt. Hier ist zu klären, wo sind die Zuordnungsmerkmale, und auch hier gibt es Vorbilder in den Landesdatenschutzgesetzen, z.B. Nordrhein-Westfalen, da müssen wir auch etwas tun.

Dann zum Thema „Datenschutzbeauftragter in der betrieblichen Selbstkontrolle“. Das ist ein „Leib- und Magenthema“ der Gesellschaft für Datenschutz und Datensicherung. Wir haben zwar Unternehmensmitglieder, aber unsere Ansprechpartner sind die Datenschutzbeauftragten. Der Datenschutzbeauftragte ist unmittelbar an die Unternehmensleitung angebunden. Er berichtet dorthin und er soll auch einiges anregen. Die praktische Wirklichkeit zeigt aber, Datenschutzbeauftragte haben nicht genug Zeit, um diese Aufgabe zu erfüllen. Das ist ein Vollzugsdefizit. Wenn aber der Gesetzgeber zum Datenschutzbeauftragten schreibt, er braucht Räume und Mittel und Geräte, dann soll auch der Zeitfaktor im Gesetz verankert werden, damit man sich darüber klar wird, dass das letzten Endes auch ein wichtiger Faktor ist, den man regeln muss. Da gibt es einiges in diesem Bereich zu tun.

Zweiter Aspekt zum Datenschutzbeauftragten: Bürokratie. Ist der Datenschutzbeauftragte Bürokratie? Aus Sicht der GDD, aus meiner Sicht, überhaupt nicht, denn die Unternehmen müssen Datenschutz einhalten. Einer muss sich sowieso um das Thema kümmern. Insofern ist die letzte gesetzliche Entwicklung, die wir gehabt haben, den Datenschutzbeauftragten unter den Maßstab der Bürokratie zu stellen in Artikel 1 des Gesetzes zum Abbau der Bürokratie, sicherlich ein falsches Signal. Wo man Bürokratie abbauen kann, ist bei der Bestellung des Datenschutzbeauftragten in Konzernen. Hier sagen wir, dass ein Konzerndatenschutzbeauftragter unter erleichterten Voraussetzungen zu bestellen ist. Da kann man Bürokratie abschaffen mit einer Bestellung für den Konzern mit Rechtswirkung auf die gesamten verbundenen Unternehmen. Was wir auch regeln müssen ist: Der Datenschutzbeauftragte und seine Kontrolle der Mitarbeitervertretung. Wir haben nach der Entscheidung des Bundesarbeitsgerichts vom 11. November 1997 - als Rheinländer kann man sich den Termin 11.11. immer gut merken - kontrollfreie Zonen im Unternehmen. Der Datenschutzbeauftragte darf den Betriebsrat nicht kontrollieren auf der einen Seite, gleichzeitig ist das gesamte Unternehmen inklusive Betriebsrat für den Datenschutz verantwortlich. Man hat das

Thema immer wieder verschoben, hat gesagt, das kommt demnächst in ein Arbeitnehmerdatenschutzgesetz. Das ist aber nicht ersichtlich. Also muss diese Kontrolllücke geschlossen werden, hier muss die Kompetenz des Datenschutzbeauftragten erweitert werden, jedenfalls ihn soweit zu kontrollieren, auch in Anerkennung der Unabhängigkeit des Betriebsrats, wenn es um die Wahrung der Betroffenenrechte geht. Hier müssen wir etwas für den Datenschutzbeauftragten tun.

Das nächste Thema, was Sie angeschnitten haben, war die Fragestellung: Kann man das Thema „Datenschutzkontrolle“ privatisieren? Wir haben ja schon, wenn man sich die Datenschutzkontrolle anschaut, drei Prinzipien: Der Betroffene selber soll sich kümmern. Es gibt die betriebliche Selbstkontrolle, die wichtig ist. Ein Datenschutzbeauftragter hat im Unternehmen diese Kontrollfunktionen und muss den Datenschutz „anstoßen“. Natürlich gehört der „Datenschutz“ zum Thema „Compliance“. Automatisch müssen die Wirtschaftsprüfer sich mit dem Thema beschäftigen. Das kommt auch in ihren Prüfbericht hinein. Das bekommt man in verstärktem Maß „unter die Nase gerieben“. Vor Jahren war es wirklich ein kleines Thema in der Ecke, heute ist es ein Thema, was auch in den Berichten von internen Revisionen behandelt wird, aber auch von Wirtschaftsprüfern. Insoweit ist das - meine ich - der richtige Weg. Und was die Fremdkontrolle anbetrifft durch den Staat selber, das kann man nicht privatisieren. Hier geht es auch letzten Endes darum, Bußgelder zu verhängen, also staatlich einzugreifen. Insofern sehe ich hier keinen direkten Regulierungsbedarf.

Das weitere Thema, was Sie angeschnitten haben: Thema „Payback-Karte“. Was muss man da machen? Nun, ich stehe vor 14 Tagen beim Kaufhof an der Kasse und man fragt eine ältere Dame, die vor mir stand: Haben Sie die Payback-Karte? Nee, nee, sagt die Dame, ich weiß nicht, was Ihr mit meinen Daten macht. Das Beispiel zeigt, es gibt schon eine gewisse Transparenz. Es ist natürlich die Frage: Wer macht die Transparenz, welche Meinungen gibt es hierzu? Ich will das Payback-Verfahren gar nicht hinterfragen. Im Grunde genommen zeigt es aber die Richtung, worauf es hinausläuft. Entscheidend ist natürlich, ob die Transparenzanforderungen sauber gelöst werden. Ob man alles von einer Einwilligung abhängig machen sollte, ist so eine Frage. Gut, beim Payback-Verfahren konkret ist die Einwilligung sicherlich notwendig, und die Transparenz muss hinreichend deutlich gemacht werden. Ich denke aber, die Gerichte haben schon den Weg gezeigt, wie die Transparenz aussehen muss, die haben ja schon manches gestoppt. Eine andere Frage ist, „opt-in“ oder „opt-out“. Ich denke, hier gibt es jedenfalls - soweit im ersten Schritt erkennbar - keinen unmittelbaren regulatorischen Regelungsbedarf. Ich denke, das waren die Punkte, die Sie mich gefragt haben.

Vors. **Sebastian Edathy**: Vielen Dank. Herr Dr. Thorun, bitte.

SV **Dr. Christian Thorun**: Erst einmal vielen Dank. Sie haben natürlich Recht, effizienter Datenschutz basiert darauf, dass man gute Gesetze hat und dann auch

durch einen vernünftigen Vollzug dafür Sorge getragen wird, dass diese eingehalten werden. Aber am Anfang steht - gerade was die Datenerhebung durch private Stellen angeht - auch der Verbraucher, das Individuum selbst, und das Prinzip der Datensparsamkeit. Also, wie geht jeder selbst mit seinen Daten um. In der Tat ist es so, dass man sich da manchmal fragen muss, ist denn der Verbraucher in der Regel oder häufig sehr naiv, wenn man sich die Zahl der Kundenkarten anguckt oder die Bereitschaft an e-Mail-Systemen teilzunehmen, die umsonst sind, aber wo dann eben die ganzen Daten durchforstet werden. Allerdings das eine, was man sicherlich machen muss, ist die Bewusstseinsbildung. Aber diese Bewusstseinsbildung - und das ist unsere Erfahrung, die wir in den letzten Jahren gemacht haben - die geht voran, weil der Einzelne immer stärker realisiert, wie er negativ dadurch beeinträchtigt wird, dass seine Daten in vielfältiger Weise zur Verfügung stehen. Wir werden gleich das Thema „Scoring“ ansprechen, aber es sind auch vermehrt Verbraucher, die sich bei uns melden und sagen: Wie kann es eigentlich sein, dass wir angerufen werden, belästigt werden durch Telefonwerbung. Und die Fragen, die uns diese Leute stellen, sind zutreffend. Woher haben diese Leute die ganzen Informationen? Das, was wir also sehen, ist, dass es durchaus einen Bewusstseinswandel bei den einzelnen Verbrauchern gibt, der dazu führt, dass vielleicht ein Umgang mit personenbezogenen Daten sparsamer und präventiver erfolgt. Die andere Frage ist natürlich: Wie leicht machen wir es den einzelnen Verbrauchern, tatsächlich präventiv tätig zu werden? Hier sehe ich einen großen Handlungsbedarf. Wenn wir uns z.B. das Prinzip der Einwilligung angucken, Herr Jaspers hat soeben gesagt, dass er da nicht unbedingt Handlungsbedarf sieht. Aber wie die Gerichtsurteile im Moment zeigen, besteht dort ein Handlungsbedarf. Das Grundprinzip ist das, wenn Daten erhoben werden, dann muss es dafür eine rechtliche Grundlage geben. Daten müssen für ein bestimmtes Vertragsverhältnis erhoben werden oder diese Daten müssen aufgrund einer freiwilligen Einwilligung erfolgen. Wie sieht es bei der Einwilligung aus? Nehmen wir das ganz konkrete Beispiel von Payback: Häufig ist es so, dass in Beitrittserklärungen das Kästchen schon im Vorfeld ausgefüllt ist, wo dahinter steht: Ich willige dazu ein, dass meine Daten auch für Werbezwecke weiterverarbeitet werden. Natürlich hat der Verbraucher die Möglichkeit, dieses Kreuz durch ein so genanntes „Opt-out“ auszukreuzen, also diese Einwilligung zu widerrufen und dann das Formular auszufüllen. Aber das tun die wenigsten Verbraucher. Und jetzt könnte man sagen, „Opt-in“, „Opt-out“, das sind irgendwie philosophische Diskussionen, die keine große Praxisrelevanz haben. Studien zeigen allerdings, wenn man Verbraucher fragt: Willigen Sie ein, dass Ihre Daten für Werbemarketingzwecke weiterverwendet werden? Dann tun das 20 Prozent. Sagt man allerdings Verbrauchern: Wenn ihr nicht wollt, dass diese Daten erhoben werden, dann kreuzt das einfach aus, benutzt das „Opt-out“. Dann tun das auch nur 20 Prozent. Was ist das Ergebnis? In dem einen Fall geben 20 Prozent die Einwilligung, in dem anderen Fall 80 Prozent. Also, es geht hier nicht um irgendwelche sprachlichen Nuancen, sondern es geht hier um grundlegende Prinzipien der Einwilligung, und ich denke, dass wir hier, falls wir von

den Gerichten nicht Klärung bekommen, dass wir das gesetzgeberisch brauchen. Die andere Frage ist, eine Einwilligung sollte freiwillig erfolgen. Was bedeutet denn „Freiwilligkeit“? Wenn ich heute einen Kredit haben möchte, dann ist die SCHUFA-Anfrage ein Standardverfahren geworden. Oder ein anderes Beispiel: Nehmen wir Ebay. Um bei Ebay teilnehmen zu können, muss ich bei der Registrierung einwilligen, dass meine Daten auch für Werbe- und Marketingzwecke verwendet werden. Natürlich kann ich dann verklausuliert diese Einwilligung wieder rückgängig machen; wer macht das aber schon. Ich denke, dass hier ein eindeutiger Verstoß gegen das Prinzip der Freiwilligkeit vorliegt. Wir brauchen hier Klärung. Das Dritte ist: Gerade bei technologischen Entwicklungen, nehmen wir das Beispiel RFID. Das ist eine Technologie, die auch für den Verbraucher durchaus Vorteile bringt, und die Technologie wird von Seiten der Bundesregierung und auch auf europäischer Ebene stark gefördert. Was wir dort allerdings brauchen ist ein größeres Verständnis dafür, dass Verbraucherbelange, dass Datenschutzbelange schon in die Technologie eingearbeitet werden. Die Herausforderung der Technik besteht darin, dass die RFID-Chips kontaktlos und prinzipiell unsichtbar miteinander kommunizieren. Wie sieht also die Verwendung von RFID-Chips im Einzelhandel aus? Wenn diese Chips unbemerkt kommunizieren, was ist dann mit dem Gebot der Transparenz? Wie sieht es aus mit der Einwilligung, wenn diese Chips tatsächlich kommen? Ich denke, dass hier ernstzunehmender Gesprächsbedarf besteht, der nicht unbedingt darauf hinauslaufen muss, dass ein RFID-Gesetz geschaffen wird. Aber ich denke, dass wir hier einige Grundfragen klären müssen, nämlich, wie gehen wir mit personenbeziehbaren Daten bei neuen Techniken um? Und es ist die Frage, welche Anforderungen stellen wir hier auch an die Industrie, an die Selbstverpflichtungserklärung.

Der letzte Punkt, und den haben Herr Abel und Herr Bizer angesprochen: Ich denke, dass in der öffentlichen Diskussion der Datenschutz tatsächlich häufig als Bremse wahrgenommen wird. Er wird auch als ein Grund gesehen, dass man Terrorismus nicht so gut bekämpfen kann. Und ich denke, dass wir hier auch in der öffentlichen Diskussion sehr viel vorsichtiger damit sein müssen, dass wir auch das entstehende Bewusstsein bei Verbrauchern für den Datenschutz nicht dadurch konterkarieren, dass wir leichtfertig den Datenschutz über die „Klippe springen“ lassen. Deswegen brauchen wir auch, gerade was die Verbraucherschutzorganisation angeht, mehr Rechte, um den Datenschutz zu Gehör zu bringen.

Vors. **Sebastian Edathy**: Abschließend bitte Herr Schaar.

SV **Peter Schaar**: Zum Thema „Technologischer Datenschutz“ ist ja hier schon einiges gesagt worden. Die Frage ist ja, inwieweit das Datenschutzrecht seine Steuerungsfunktion in Bezug auf die technologische Entwicklung noch besitzt. Es hat einmal, vor allem im Hinblick auf § 9 BDSG durchaus eine gewisse Steuerungsfunktion ausgeübt. Diese Vorschrift, die den technisch-organisatorischen Schutz der personenbezogenen Daten normiert, hat ganz maßgeblich dazu geführt,

dass heute Datenverarbeitungen ohne jeden Zugriffsschutz - Ausnahmen bestätigen die Regel - kaum noch denkbar sind. Nur, dies greift zu kurz in einer Welt, wo „Ubiquitous Computing“ stattfindet, wenn Datenverarbeitung allgegenwärtig wird. Und das bedeutet, dass Daten quasi beiläufig anfallen als Nebenprodukte von technischen Prozessen. Da sind wir erst am Anfang. Es ist ja nicht nur das Handy, über das Verbindungsdaten - oder Verkehrsdaten sagt man neuerdings - entstehen, sondern in Zukunft wird es der Kühlschrank sein, und das Auto sammelt Daten in verschiedenen Datenspeichern, die dann von Werkstätten ausgelesen werden oder über Funk übertragen werden können. Wir werden hier eine weitere Zunahme der Datenmengen in unglaublichen Dimensionen erleben. Die Frage ist: Wie kann man den § 3a BDSG, das Gebot der Datensparsamkeit, so umsetzen, dass diese Regelung auch tatsächlich gestaltend wirkt. Im Augenblick ist es ein reiner Programmsatz, d.h. üblicherweise hat er kaum Konsequenzen. Ich habe bisher keine Ausschreibung gesehen, die ausdrücklich forderte: die Datensysteme, die angeboten werden, sollen so gestaltet werden, dass so wenig personenbezogene Daten wie möglich entstehen. Ich würde auf einen solchen Mangel natürlich hinweisen, aber mir werden die Konzepte nicht in der Ausschreibungsphase, sondern erst deutlich später vorgelegt. Und dann sind im Grunde die wesentlichen Gestaltungsparameter schon gesetzt. Den Datenschutz technologisch zu unterstützen, heißt auch, ihn sehr frühzeitig in Planungen mit einzubeziehen. Was spricht denn dagegen, z.B. in Ausschreibungen der Verwaltung entsprechende standardmäßige Formulierungen aufzunehmen? Dazu gehört natürlich auch ein politischer Wille. Und die Botschaft, die häufig im Augenblick öffentlich ankommt, ist, dass gar nicht gewollt ist, dass möglichst wenig personenbezogene Daten entstehen, sondern dass es aus verschiedenen Gründen eher gewollt ist, dass personenbezogene Daten entstehen. Der Technologierat hatte 1996 angeregt, auch anonyme Nutzungsvorgänge bei elektronischen Diensten vorzusehen. Dies hat ja dann auch Eingang gefunden in das Datenschutzrecht. Im Augenblick geht die Entwicklung bekanntlich genau in die andere Richtung. Wir haben derzeit zu tun mit einem Gesetzentwurf des Bundesjustizministeriums, der sich - meines Erachtens zu Unrecht - auf eine Europäische Richtlinie beruft, wonach eine Identifikationspflicht für e-Mail-Kunden eingeführt werden soll, d.h. jeder, der eine e-Mail-Adresse beantragt, muss Name und Anschrift nennen. Und da ist dann natürlich logisch, dass man nicht „Mickymaus“ und „Disneyland“ angeben darf, sondern dass man seine echte Anschrift nennt und für die Zwecke der Rückverfolgung ist es sogar wichtig, dass man dann nicht nur eine Identifikationspflicht einführt, sondern eine Verifikationspflicht, sonst bringt das Ganze überhaupt nichts. Damit würden zusätzliche Datenmengen generiert. Ich trete dafür ein, dass sich stattdessen eine Kultur der Datensparsamkeit durchsetzt. Dazu könnte auch beitragen, dass wie in anderen Bereichen von Ministerien Wettbewerbe initiiert werden, bei denen z.B. möglichst datenschutzfreundliche Technologien prämiert werden. Warum soll es solche Wettbewerbe nicht geben? Die zentrale Botschaft könnte darin bestehen: Datensparsamkeit ist ein ganz wichtiger Aspekt für

Erfolg und für eine ethisch angemessene Datenverarbeitung. Dieser Aspekt ist noch nicht so tief verankert, wie ich es mir wünschen würde.

Zum Thema „polizeiliche Zusammenarbeit in der dritten Säule“ denke ich, dass wir uns im Augenblick in einer entscheidenden Phase befinden. Die Europäische Kommission hat einen Entwurf für eine Datenschutzregelung für diesen Bereich vorgelegt. Diese Regelung ist allerdings bei verschiedenen EU-Mitgliedstaaten auf Bedenken gestoßen und eine Vielzahl von Einwänden ist dann erst mal zu Protokoll genommen worden, die jetzt unter der deutschen Ratspräsidentschaft abgearbeitet werden. Was mir Sorge bereitet, ist, dass nicht die Datenschutzexperten damit beauftragt worden sind, sondern eine Arbeitsgruppe, die sich im Wesentlichen mit polizeilichen Aufgaben beschäftigt. Hier würde ich mir wünschen, dass z.B. die deutsche Ratspräsidentschaft auch die Expertengruppe für den Datenschutz im Bereich der Dritten Säule stärker einbezieht in die Formulierung der entsprechenden Richtlinie. Die deutsche Ratspräsidentschaft hat ja dazu die Möglichkeit. Was letztlich daraus wird, wird man natürlich sehen. Wichtig ist für mich, dass es auch in den Bereichen Polizei und Justiz eine allgemeine Datenschutzregelung gibt, die einen hohen Datenschutzstandard gewährleistet. Das wäre auch eine Voraussetzung dafür, dass Informationen zwischen den Mitgliedstaaten ungehindert fließen können, und es ist - so hoffe ich - auch eine gemeinsame Auffassung der Regierungen und der Datenschützer, dass man hier zu einem Ausgleich kommt. Wenn man es nicht schafft, den Datenschutz auf ein hohes Niveau auch in dem Bereich der polizeilichen justiziellen Zusammenarbeit zu heben, dann wird es hier auch keinen freien Datenaustausch geben oder darf es jedenfalls von Verfassung wegen so nicht geben. Deshalb würde ich mir wünschen, dass man bald zum Abschluss kommt.

Vors. **Sebastian Edathy**: Vielen Dank. Für die SPD-Fraktion hat das Wort der Kollege Dr. Michael Bürsch.

Abg. **Dr. Michael Bürsch**: Herzlichen Dank. Ich beginne mit einem Dank an die Sachverständigen. Sie haben sich der Mühe unterzogen, gerade auch zu dem allgemeinen Komplex „Modernisierung des Datenschutzes“ etwas aufzuschreiben, wenn ich das richtig sehe, unentgeltlich, ehrenamtlich, ohne dass sie dafür honoriert werden können. Das ist auch nicht mehr selbstverständlich und das gibt schon eine ganze Menge Stoff, den wir berücksichtigen können. Wir haben für die ersten zwei Fragesteller eine Stunde gebraucht, deshalb glaube ich, können wir jetzt nur nach dem Prinzip „Freiwillige Selbstkontrolle“ arbeiten. Ich beschränke mich auf eine Grundsatzfrage: Zu dem Gesamtkomplex „Modernisierung“, über den man abendfüllend reden könnte, da ist das Thema, was alle Ihre Stellungnahmen durchzieht, die rasante technische Entwicklung. Als Gesetzgeber hinken wir ja im Grunde immer hinterher. Wenn wir „Gesundheitsreform“ machen ist die Entwicklung im Grunde schon weiter, wenn wir „Rente mit 67“ beschließen, brauchte man vielleicht schon die mit 70. Aber nirgendwo geht es so rasant zu wie auf dem Gebiet, über das wir heute reden. Und jetzt frage ich mich als Gesetzgeber und Jurist - was

ich mal gelernt habe - wie kann denn da Gesetzgebung wirklich aussehen? Soll das eine Generalklausel sein, die das erfasst, dass wir im Grunde schon in einem halben Jahr, in einem dreiviertel Jahr Meilen weiter sind? Wie kann eine solche Gesetzgebung für diesen wirklich verdammt schnellen Bereich aussehen, die auf der einen Seite, das die Frage an Herrn Bizer, die Akzeptanz des Datenschutzes aufrechterhält, und die z.B. auch in Rechnung stellt, was die Betroffenen wollen. Wir reden manchmal - habe ich den Eindruck - ein bisschen über die Köpfe hinweg. Im Bereich „Sicherheit“ sind - glaube ich - inzwischen viele Privatmenschen bereit, mehr an Datenschutz aufzugeben, als es denn der allgemeinen Sicherheit dient. Das ist eine Entwicklung, wenn wir das geschützte Rechtsgut Datenschutz betrachten, wie weit decken wir das noch ab, was die Betroffenen wirklich wollen?

Und an Herrn Dix die Frage, das finde ich einen interessanten Ansatz, der Gedanke der Risikoadäquanz oder, wie Sie das nennen, der „abgestufte Datenschutz“. Wie kann sich das in einer Gesetzgebung auswirken, bei der wir auch die Fachwelt mit einbeziehen müssen? Wir sind die Gesetzgeber, aber wir wissen wenig, hier sitzen vielleicht sechs, sieben Abgeordnete, die sich um das Thema kümmern. Da können Sie sich ausrechnen, das sind 1 Prozent der 614 Abgeordneten des Deutschen Bundestages. Also, wie kann man so viel Sachverstand hineinbringen, der aber wiederum nicht voreingenommen ist, sondern wirklich und objektiv auf dem Laufenden hält? Und die letzte Frage - etwas am Rande - an Herrn Thorun. Er hat so etwas bombastisch gesagt, er wende sich bei der Modernisierung des Datenschutzes gegen die ausufernde Begehrlichkeit des Staates, die solle begrenzt werden. Da würde ich gerne mal wissen, wo die noch vorhanden ist und wie man sie mit einem modernen Datenschutz begrenzen kann.

Vors. **Sebastian Edathy**: Dann bitte zunächst zur Beantwortung Herr Dr. Bizer.

SV **Dr. Johann Bizer**: Es ist interessant, dass uns die Diskussion zur Modernisierung immer wieder auf das Thema „Audit“ drängt. Es war vorhin schon so, als es um die Frage „Wettbewerb“ ging. Aber im Grunde genommen ist das meine Antwort auf Ihre Frage nach dem „wie bekommt man dieses Akzeptanzproblem in den Griff“: Wenn ich meine Daten nicht mehr unter der Kontrolle habe und mir unsicher bin, wie meine personengebundenen Daten in ubiquitären Verhältnissen verarbeitet werden. Also bspw., ich gehe durch den Sophienhof in Kiel, das ist eine Einkaufspassage, und wir stellen uns vor, dass überall an den Schaufenstern, an den Türen Lesegeräte, Scanner aufgestellt sind, die betrieben werden von den einzelnen Kaufhäusern, und die funken jetzt die Etikette an meinem Sakko, an meiner Hose, an meinen Schuhen jeweils an und versuchen auf diese Art und Weise diese Daten aus den RFID-Chips auszulesen und dann in Verbindung - soweit sie bereits gespeichert sind - mit meiner Kundenkarte oder meiner Kreditkarte zusammenzufassen. Wenn man sich das jetzt als Szenarium vorstellt - und wir sagen gleichzeitig, wir wollen aber in den Sophienhof gehen, weil er so schön ist, weil man so schön einkaufen kann, und wir wollen nicht darauf verzichten, durch den Sophienhof zu gehen - dann

ist die einzige Möglichkeit, das Problem durch Auditierung zu lösen, dass ein vertrauenswürdiger Dritter mir als Betroffenen bestätigt, dass Peek & Cloppenburg - oder wer auch immer - meine Daten nur zweckbezogen und nur in dem Rahmen, dem ich vorher zugestimmt habe, erhebt und verarbeitet. Wenn ich eine Datenverarbeitung selbst nicht mehr kontrollieren kann, brauche ich einen vertrauenswürdigen Dritten, der mir das eben bestätigt. Das ist sozusagen die erste Antwort auf Ihre Frage. Die zweite Antwort ist, wie kann der Gesetzgeber überblicken, wie schnell die Entwicklung ist. Da kann ich nur sagen, so schlecht sind Sie ja gar nicht beraten gewesen in letzter Zeit. Wenn man den ersten Bericht zur Informationsgesellschaft 1998 heranzieht, dann sind da im Grunde genommen die grundlegenden Probleme, vor denen wir heute stehen, schon dort beschrieben. Der Bundestag hat dort mit seinen Experten quasi ein Handbuch erarbeitet, mit dem er heute schon arbeiten kann. Das nächste ist, Sie haben das Gutachten von Rossnagel, von Garska und von Pfitzmann zur Modernisierung des Datenschutzrechts. Da sind eine ganze Reihe von Problembereichen der neuen Technologien und Lösungen kurz und knapp beschrieben. Da sind Sie sozusagen gut beraten, mit diesem Handwerkszeug auch zu arbeiten. Wenn man an die ganzen Ausschüsse und Gremien denkt, die im Bereich der Konvergenz, also der Integration der unterschiedlichen Medien, den Deutschen Bundestag beim TDSG, bei den Telemedien, beim TKG beraten haben, glaube ich auch nicht, dass Sie so weit hinter der technologischen Entwicklung hinterher hängen. Woran es einfach nur fehlt ist, den Mut, die eine oder andere Regelung auch mal konsequent bis zu Ende zu denken und auch zu ermöglichen, wie z.B. im Bereich „Audit“ oder wie im Bereich der „Selbstregulierung“.

Vors. **Sebastian Edathy**: Vielen Dank. Herr Dr. Dix, bitte.

SV **Dr. Alexander Dix**: Vielen Dank. Zur Frage nach einem Regelungskonzept der Risikoadäquanz oder für einen abgestuften Datenschutz würde ich auch noch mal auf das zurückgehen, was Herr Bizer gerade schon erwähnt hat. Wir führen ja die Diskussion nicht „auf der grünen Wiese“, es hat in der Tat schon sehr durchdachte Konzepte gegeben zu einer grundlegenden Modernisierung des Datenschutzes. Und eines dieser Konzepte haben die Professoren Rossnagel, Pfitzmann und Garstka 2001 dem Bundesinnenministerium vorgelegt, als sie vorgeschlagen haben, zwischen einer gezielten und einer ungezielten personenbezogenen Datenverarbeitung zu unterscheiden. Noch mal zur Erinnerung: Gerade vor dem Hintergrund einer Entwicklung wie sie Herr Schaar vorhin beschrieben hat, dass wir immer mehr in eine rechnerorientierte Umwelt hineingeraten. Die Europäische Kommission spricht von einer halsbrecherischen Entwicklung. Das ist vielleicht sehr drastisch beschrieben, damit war vor allem das Internet gemeint, aber das beschreibt die gesamte Entwicklung der Informationstechnik. Wenn wir an Entwicklungen im Bereich der Nanotechnologie denken. Dass wir über kurz oder lang auch mit „schlauem“ Staub uns auseinandersetzen müssen. Also staubkorngroße RFID-

Etiketten oder andere Rechner, dann können wir überhaupt nicht mehr mit den Konzepten des herkömmlichen Datenschutzes an diese Umwelt herangehen. Es ist illusorisch, dann noch mit informierter Einwilligung oder dergleichen zu arbeiten. Also, wir müssen sicherstellen, dass wir an bestimmten Stellen möglicherweise die Anforderungen des Datenschutzrechts etwas lockern unter der Voraussetzung aber - und das ist nun entscheidend - dass technisch sichergestellt wird, dass in bestimmten Prozessen eben keine personenbezogenen Daten über längere Zeit vorhanden bleiben. Es muss sich wirklich um flüchtige Datenverarbeitungsprozesse handeln und das muss überprüfbar sein. Das ist entscheidend. Und nur dort, wo Daten erkennbar wahrnehmbare Zeitabschnitte hinweg gespeichert waren, da muss das Datenschutzrecht möglicherweise auch verschärft werden. Dieses Gedankenpaar würde ich noch mal in Erinnerung rufen. Es gibt Instrumente der Technikfolgenabschätzung, die stärker wieder ins Bewusstsein geholt werden sollten. Auch der Gesetzgeber - um mal einen ganz praktischen Vorschlag zu machen, der in Berlin bereits im Landesrecht enthalten ist, oder die Bundesregierung, wenn sie Gesetzentwürfe vorlegt - sollte nicht nur über die haushaltsrechtlichen Auswirkungen Auskünfte geben im Vorblatt des Gesetzentwurfs, sondern jedes Gesetzgebungsvorhaben auf den Datenschutz. Warum ist das so fernliegend, darüber wenigstens einen Satz zu verlieren. Entweder es gibt keine Auswirkungen oder es gibt erhebliche Auswirkungen. Jedenfalls würde das die Gesetzesautoren dazu veranlassen, überhaupt mal in diese Richtung nachzudenken. Das vielleicht hierzu.

Vors. **Sebastian Edathy**: Vielen Dank. Dann zur Frage des tatsächlich oder vermeintlich datenhungrigen Staates, Herr Dr. Thorun.

SV **Dr. Christian Thorun**: Sie hatten gefragt, wo denn die Begehrlichkeit zum Ausdruck kommt. Wir sehen es u.a. in der jetzt geplanten Vorratsdatenspeicherung. Aber es sind auch die politischen Debatten, die geführt werden: wie werden die Maut-Daten benutzt und weiterverwendet. Wahrscheinlich haben Sie Recht, dass in der Öffentlichkeit durchaus nach dem 11. September eine größere Bereitschaft auch dafür vorhanden ist, dass die Behörden größeren Zugriff auf Daten haben. Die Frage ist bloß: Wo sind hier die Grenzen? Und ist alles das erlaubt, was technisch möglich ist? Und genau das ist unsere Frage, was z.B. die Vorratsdatenspeicherung angeht. Ist dort tatsächlich der Maßstab der, wie kann die Arbeit der Behörden verbessert werden? Oder wird einfach das gefordert, was technisch mit mehr oder weniger Aufwand möglich ist? Und hier haben wir ganz eindeutig den Eindruck, dass das Zweite der Fall ist. Da ist natürlich der Gesetzgeber in der Verantwortung zu sehen, dass die Verhältnismäßigkeit gewahrt ist. Und das sehen wir nicht in jedem Fall als gegeben.

Vors. **Sebastian Edathy**: Dann hat jetzt das Wort der Sprecher der Fraktion DIE LINKE., Jan Korte.

Abg. **Jan Korte**: Ich würde gerne zwei Sachen ansprechen - auch die Kollegin Piltz hat dies tangiert - es ist natürlich auch eine Frage für uns, die sich mit dieser Thematik politisch beschäftigen. Die Frage ist: In welchem gesellschaftlichen Raum findet das ganze statt? Das Beispiel der kämpferischen Rentnerin an der Kaufhofkasse ist eher die Ausnahme, nicht die Regel, würde ich mal annehmen. Deswegen stellt sich mir die Frage - und das ist ja eine spannende Frage - wie man dann sozusagen Aufklärung im klassischen Sinne betreiben kann. Deswegen würde ich sagen, es ist auch ein Stückweit eine soziale Frage, was die Wahrnehmung von Datenschutz angeht für die große Mehrheit der Bevölkerung. Deswegen, an Herrn Thorun noch mal die Frage wie bei meinen Gesprächen z.B. mit der Verbraucherschutzzentrale in Magdeburg: können Sie relativ klar benennen, welche Personenkreise und Schichten bereit sind, ohne Ende Daten bei Preisausschreiben, Payback etc. herauszugeben. Das finde ich, ist schon eine entscheidende Frage, die natürlich eine gesellschaftspolitische Frage ist. Vielleicht können Sie dazu noch ein bisschen was sagen. Wie können wir letztendlich die Frage des Datenschutzes in der Gesellschaft verankern und inwieweit korrespondiert sie natürlich mit der sozialen Frage?

Die zweite Frage geht auch in diesen Zusammenhang: Inwieweit durch die Politik und insbesondere zzt. die Mehrheitspolitik - Sie haben die Beispiele gerade genannt: Vorratsdatenspeicherung, wir hatten viele andere Fragen, über die wir uns kräftig gestritten haben, Anti-Terror-Datei, aktuell Onlineuntersuchung oder sonst was - massivste eklatante Eingriffe stattfinden im Namen des Kampfes gegen den Terror. Und das ist natürlich auch eine Frage, inwieweit hier die Politik ein Datenschutzbewusstsein konterkariert bzw. das Gegenteil bewirkt. Und in dem Zusammenhang dann die Frage an Herrn Neumann: Müsste man, wenn man insgesamt diese ganze Entwicklung zusammenfasst, also die ganzen Fragen, die früher mal eine Selbstverständlichkeit gewesen sind, Trennungsgebot, Transparenzgebot etc., muss man dann nicht auch datenschutzrechtlich eine völlig von unten nach oben aufgebaute datenschutzrechtliche Konzeptionen sowohl rechtlich als auch politisch eigentlich angehen? Dritte und letzte Frage, vielleicht auch noch mal an Herrn Bizer: Können Sie Beispiele nennen, wo es konkret um Datenverzicht gegangen sind, wo Institutionen sowohl politisch-öffentliche als auch ökonomisch-wirtschaftliche Betriebe gesagt haben, wir verzichten auf die Erfassung von Daten. Gibt es da konkrete Erkenntnisse?

Vors. **Sebastian Edathy**: Vielen Dank. Dann zunächst zur ersten Frage des Kollegen Korte, Herr Dr. Thorun.

SV **Dr. Christian Thorun**: Vielen Dank. Die eine Frage war ja sozusagen, was können wir machen, damit die Aufklärung überhaupt fruchtet und dass wir die Verbraucher mitnehmen können. Das habe ich ja eben schon gerade versucht zu skizzieren. Ich denke, dass eine Grundvoraussetzung ist, dass wir klare und

einfache, verständliche Regeln haben, also dass klar ist, was eigentlich die Rechte des Einzelnen sind und worauf er sich berufen kann und womit er rechnen kann. Und da ist in der Tat Nachbesserungsbedarf. Es gibt eine Vielzahl von Regeln in unterschiedlichen Bereichen und da muss es eine Vereinfachung und eine Vereinheitlichung auf hohem Niveau geben. Das andere ist natürlich, dass es eine öffentliche Wertschätzung des Datenschutzes gibt, und das ist wiederum der Punkt, den ich eben gerade versucht habe anzusprechen. Dass ich da meine Zweifel habe, dass dort wirklich in der Öffentlichkeit das Bewusstsein dafür gefördert wird, dass der Datenschutz wirklich im Verbraucherinteresse ist, weil die Daten gegen ihn missbraucht werden könnten. Die andere Frage, die Sie aufgeworfen haben nach der sozialen Frage: Wer macht eigentlich mit, wer gibt wie leichtfertig seine Daten preis? Ich habe dazu keine verlässlichen Zahlen, allerdings mögen Sie damit Recht haben, dass natürlich gerade Verbraucher aus unteren Einkommensschichten oder mit einem relativ geringen Bildungsgrad an diesen vermeintlichen Preisausschreiben teilnehmen. Aber ich glaube, das ist ein viel breiteres Problem. Es gibt über 70 Mio. Rabattkarten in Deutschland. Das sind nicht nur die ärmeren oder so stark gebildeten Leute. Allerdings wo Sie Recht haben, die davon maßgeblich Betroffenen, von der Nutzung dieser Daten, das sind im Wesentlichen tatsächlich die, die nicht so viel Geld haben, die dann diskriminiert werden, wenn es um den Versand geht, wo die Straße vielleicht Rückschlüsse erlaubt, wo er wohnt usw.. Wem mangelt es an einem Problembewusstsein? Ich glaube, das ist ein größeres Massenphänomen und nicht begrenzt auf irgendeine Schicht oder Klasse. Allerdings wer die Betroffenen, und da spitzt es sich dann eher zu, wer bekommt die negative Seite dort zu spüren.

Vors. **Sebastian Edathy**: Vielen Dank. Herr Neumann dann bitte.

SV **Karsten Neumann**: Ich will vielleicht so anfangen. Ich glaube, dass ich nicht der einzige der Sachverständigen bin, dem es so ging, der bei der Erarbeitung der Stellungnahme zu dem Thema „Modernisierung des Datenschutzes“ gedacht hat: Um Gotteswillen, wie soll das aussehen? Und wenn man in so einer Situation ist - denke ich - muss man sich als erste Frage stellen, wo wollen wir hin, was ist denn das Ziel. Und ich finde der Bundesinnenminister hat in dem Punkt mir auf die Sprünge geholfen, indem er mal gesagt hat: Wir müssen endlich weg von diesem Volkszählungsurteil. Ich denke, genau das ist es nicht. Deshalb habe ich das auch an den Beginn meiner Stellungnahme gesetzt. Das Volkszählungsurteil ist aus meiner Sicht auch weiterhin der Anknüpfungspunkt, also die Zielvorstellung. Denn das geschützte Rechtsgut ist ja nicht das Datenschutzrecht oder der Datenschutz, sondern geschütztes Rechtsgut ist das Recht auf informationelle Selbstbestimmung der Bürgerinnen und Bürger. Das ist es, worum es geht, die Möglichkeit der freien Entfaltung unter den Bedingungen der modernen technischen Entwicklung. Deshalb geht es aus meiner Sicht ganz klar auch um eine Ethik der Informationsgesellschaft. Und ich will mal - wenn es auch ein bisschen platt ist und ich gebe es auch zu, geklaut - ein Vergleichsbild geben. Zu den Zeiten, wo die Autos noch 30 km/h fahren

und nur von einer gehobenen Klasse benutzt worden sind, brauchte man noch keine Straßenverkehrsordnung. Aber je schneller der Verkehr wird, und je mehr die Infrastruktur in dieser Informationsgesellschaft tatsächlich die Infrastruktur unseres gesamten gesellschaftlichen Lebens ist, des wirtschaftlichen, des privaten Lebens, in der Situation, wo wir Autobahnen haben, wo Autos mit 200 km/h fahren, wo also die Gefährdung des Einzelnen wächst, umso mehr brauchen wir klare Regelungen, hier brauchen wir eine klare Straßenverkehrsordnung. Da weiß dann jeder, wenn ich auf die Straße gehe, begeben mich in Gefahr, auch wenn es nur 3 Prozent sind, aber ich begeben mich in Gefahr. Das weiß dann jeder. Und wir brauchen neben der klaren und einfachen Straßenverkehrsordnung - wie gesagt: wir fahren rechts lang, außer einige wenige Länder - wir haben Ampeln, wir haben Vorfahrtsregelungen. Dann brauchen auch einen TÜV, der sagt, das Auto darf die Straße benutzen, und wir können grundsätzlich darauf vertrauen, dass es auch fährt. Denn je ausgefeilter und je differenzierter - und das habe ich versucht in der Stellungnahme aus Sicht des Arbeitskreises „Technik“ der Datenschutzbeauftragten deutlich zu machen - je ausgefeilter und moderner die Technik wird, umso mehr ist es nicht mehr leistbar, tatsächlich alles zu wissen, bei jeder Einwilligung tatsächlich zu wissen, worin man einwilligt. Und deshalb - das denke ich - muss der Ansatz sein, wenn man über eine Neukonzeption nachdenkt, darüber nachzudenken, wie wir das Recht auf informationelle Selbstbestimmung, so wie es das Bundesverfassungsgericht verstanden hat, unter diesen modernen Bedingungen gewährleisten können. Danke.

Vors. **Sebastian Edathy**: Dann abschließend bitte Herr Dr. Bizer.

SV **Dr. Johann Bizer**: Es gibt eine ganze Reihe von Beispielen, wo Unternehmen oder öffentliche Stellen auf Datenerhebung und -verarbeitung und -nutzung nach einem intensiven Beratungsgespräch auch verzichten, wo man die Grenzen von „Compliance“, das Stichwort von Herrn Abel vorhin, erfolgreich aufzeigt. Häufig stellt man dann fest, dass es Unwissenheit ist bei den datenverarbeitenden Stellen, oder auch nur falsche Vorstellungen von den Möglichkeiten, die ihnen das Datenschutzrecht gibt. Das fängt an bei so Beispielen wie Erhebung von Daten mit einer Videokamera in einem Einkaufsumfeld oder der Nachbar, der mit der Videokamera versucht, seinen Nachbarn zu beobachten, obwohl er doch nur seine Gartenpforte im Blick behalten oder angeblich seine Vögel beobachten will, aber auch gleichzeitig die Kamera die Beobachtung des Nachbarhauses ermöglicht. Das geht bis hin zur Kundendatenverarbeitung auf den Ebenen: welche Daten werden erhoben, wie lange werden sie eigentlich wirklich gebraucht? Also brauche ich, z.B. im Rahmen der Erhebung von Kundendaten das Geburtsdatum auch wirklich, wenn es letztendlich nur um die Bonität geht. Wie lange werden die Daten eigentlich gespeichert, bis hin zu ganz schwierigen und diffizilen Fragen bei der Protokollierung. Wer hat wann auf welches System zugegriffen? Wie lange muss man solche Daten für Zwecke der Datenschutzkontrolle aufheben oder darf man die dann auch für andere Zwecke weiterverwenden? Ich könnte Ihnen eine Fülle von Beispielen sowohl

aus eGovernment als auch aus dem Wirtschaftsbereich sagen, wo man feststellt, aber immer erst nach intensiver Beratung und nach deutlichen Hinweisen, dass dann der Umfang der Datenerhebung deutlich zurückgefahren wird. Dass jetzt Unternehmen von sich aus sagen, wir haben hier ein datensparsames Verfahren, das begegnet uns allenfalls dann, wenn ein Hersteller zu uns kommt und sagt, wir interessieren uns für ein Datenschutzgütesiegel. Und dann stellt sich die Frage, ob es wirklich datensparsam ist.

Vors. **Sebastian Edathy**: Vielen Dank. Dann zum Abschluss der ersten Berichterstatterunde hat Frau Silke Stokar von Neuforn für die Fraktion BÜNDNIS 90/DIE GRÜNEN das Wort.

Abg. **Silke Stokar von Neuforn**: Herr Vorsitzender, meine Damen und Herren, ich möchte auch damit beginnen, dass ich mich bei allen Referenten hier bedanke, insbesondere für den ersten Teil Ihrer schriftlichen Stellungnahmen. Sie haben sich erneut herangemacht an das Thema „Modernisierung des Datenschutzes“, und ich möchte im Vorfeld aus dem politischen Bereich sagen - und das gilt nicht nur für den Datenschutz - es hilft nicht der Verweis auf Gutachten in den Schubladen. Das gilt auch für die Kenntnis, dass die Eisberge schmelzen und dem Eisbären die Scholle „unterm Hintern“ wegtaut. Diese Gutachten hatten wir auch schon vor 15 Jahren, und dennoch ist heute der Klimawandel das Thema. Meine erste Frage geht dann auch vielleicht etwas provozierend in die Richtung, weil ich weiß, es mangelt uns nicht an Wissen: Brauchen wir im Bereich des Datenschutzes eine neue Strategie, um dieses große politische Vorhaben „Modernisierung des Datenschutzgesetzes“, das sich drei Koalitionen nacheinander vorgenommen haben, ganz gleich, ob Schwarz-Gelb, Rot-Grün oder die große Koalition. Sie hat es sich - glaube ich - noch nicht mal vorgenommen in den Koalitionsvereinbarung. Letztendlich braucht der politische Bereich - und Datenschutz kann sich nur aus dem Parlament heraus entwickeln, das hat die gesamte Geschichte der Datenschutzgesetzgebung in Deutschland gezeigt - braucht der politische Bereich auch noch einmal eine Debatte über erfolgreiche Strategien im Bereich des Datenschutzes. Da wir die Fragen an bestimmte Sachverständige stellen sollen, wähle ich jetzt einfach mal Herrn Prof. Dr. Abel aus zu dieser Frage und Herrn Dr. Dix.

Eine konkrete Frage zu Modernisierung des Datenschutzes, der Datenschutzgesetze möchte ich an Herrn Schaar richten, und zwar können Sie uns vielleicht noch mal einen Hinweis geben, wie wir dieses Spannungsfeld im Datenschutzrecht lösen: einerseits soll das Datenschutzrecht technikneutral sein, ich halte den Grundsatz des technikneutralen Rechts nach wie vor für einen richtigen, weil sich die Technik so rasant entwickelt, dass man für jedes Verfahren eine spezielle gesetzliche Regelung finden kann, aber andererseits sehen wir an bestimmten Techniken - ich möchte hier mal die RFID benennen, aber auch Scoringverfahren - dass allgemeine Grundsätze des Bundesdatenschutzgesetzes eben genau nicht klar greifen in diesem Technikbereich, weil wir mittlerweile sogar eine Unterscheidung brauchen zwischen

„personenbezogenen Daten“ und „Daten, die sich auf Personen beziehen lassen“, also ganz neue Begrifflichkeiten.

Und an Herrn Dr. Thorun habe ich die Frage: Müssen wir Datenschutz heute nicht weiter sehen? Wir sind den Schritt gegangen zu sagen, wir haben auf der einen Seite den Datenschutz und haben zusätzlich hinzubekommen, mit dem Informationsfreiheitsgesetz Datenschutz und Informationsfreiheit in ein Verhältnis zu setzen. Aber ich glaube, dass wir auch die Kombination Datenschutz und Verbraucherschutz brauchen. Wie kann man diese beiden bisher parallel laufenden Bereiche stärker zusammenbringen. Meine letzte Frage geht an Herrn Dr. Abel. Sie beziehen sich in Ihrem Statement mehrfach auf den Begriff der „Selbstregulierung“. Ich befasse mich nun seit einigen Jahren mit dem Begriff der „Selbstregulierung“ im Datenschutzbereich. Mir ist es bis heute nicht gelungen, auch nur ein positives Beispiel hier zu finden. Gerade im Bereich der RFID-Chips habe ich das Gefühl, dass die Wirtschaft hier das Angebot der Selbstregulierung hat und seit zwei Jahren weder bereit noch in der Lage ist, dieses Angebot mit Inhalten zu füllen. Wie können wir den Druck erweitern? Das Instrument finde ich ja gut, dass Selbstregulierung auch tatsächlich von der Wirtschaft verlässlich, verbindlich als ein Instrument genutzt wird.

Vors. **Sebastian Edathy**: Es sind vier Sachverständige angesprochen. Zunächst Herr Prof. Abel, bitte.

SV **Prof. Dr. Ralf Bernd Abel**: Zunächst zur Frage, ob wir eine neue Strategie brauchen? Ich denke, im Grunde sind die Fragen, mit denen wir zu tun haben, die alten Fragen, nicht anders als 1970, 1974, 1977, auch die Grundlage ist dieselbe. Es ist die verfassungsrechtliche Spannung zwischen einerseits dem freien Umgang mit Informationen, also das, was wir in Art. 5 GG garantiert und gewährleistet finden. Auf der anderen Seite steht das gleichwertige Grundrecht auf informationelle Selbstbestimmung. Da kann ich Herrn Neumann Recht geben, das muss und kann nur unser Ausgangspunkt sein. Es ist eine fundamentale Aussage für eine demokratische und moderne Informationsgesellschaft, anders geht es nicht. Dieses Spannungsverhältnis, diese Themen sind, wenn man in den Diskussionsstand der vergangenen 30 Jahre hineinschaut, eigentlich gleich geblieben. Aber was sich verändert hat, ist die Technologie und damit auch der Grad von Gefährdung einfach durch die Dimension, die man früher in dieser Form so nicht kannte. Ob es aber deshalb einen neuen Strategiebedarf geben sollte, halte ich für zweifelhaft. Eigentlich müssen die alten Strategien, die ja so schlecht nicht waren, weil sie uns im Vergleich zum Rest der Welt einen durchaus passablen Datenschutz beschert haben, nur angepasst und fortgeschrieben werden. Beispiel: Die schon genannte „RFID-Technik“ könnte man möglicherweise so ähnlich regeln wie das Thema „Videoüberwachung“, dass also für diesen Bereich der Technologie zwar eine Regel eingeführt wird, aber nicht so, dass man nun eine völlig neue Bestimmung schafft, sondern indem man sich an das gegebene Konzept anpasst. Zweiter Teil der Strategie ist einerseits eine behördliche Kontrolle, die aber schon aus

Haushaltsgründen nicht mit riesigen Kontroll- und Überwachungsorganen ausgestattet sein kann, sondern die andererseits unterfüttert ist mit einem Stück Selbstkontrolle, nämlich der Einrichtung der betrieblichen und dann behördlichen Datenschutzbeauftragten. Die wurde anfangs zwar verlacht. Seinerzeit wurde befürchtet, das sei so ähnlich wie bei der Freiwilligen Film-Selbstkontrolle, eine unglaubliche Alibiveranstaltung. So war die Befürchtung zu Beginn und das übrigens auch in anderen Ländern. Frankreich hat den betrieblichen Datenschutzbeauftragten mittlerweile übernommen. In Holland gibt es Ähnliches, auch in Großbritannien gibt es entsprechende Überlegungen. Diese Implementierung durch betriebliche Datenschutzbeauftragte ist von außerordentlicher Bedeutung, weil nur eine solche durchaus auch privatwirtschaftlich angesiedelte Form der Umsetzung so in die Breite geht, wie es anders nicht möglich wäre. Womit ich nicht sagen will, dass es bereits perfektioniert wäre. Wir sind erst auf dem Wege. Aber aus langjähriger Befassung mit der Frage weiß ich, dass die Umsetzung des Datenschutzes, wenn es diese Einrichtung so nicht gäbe, sehr viel schwieriger wäre. Ich weiß aus anderen europäischen Ländern, die sprachlich manchmal gar nicht so weit weg von uns sind, dass, eben weil es betriebliche Datenschutzbeauftragte nicht gibt, Vollzugsdefizite in sehr viel größerem Umfang vorhanden sind als das bei uns der Fall ist. Das muss man auch im Blick haben. D.h., wir brauchen auch hier keine neue Strategie, sondern sollten die vorhandene Strategie verbessern.

Und dann kann ich gleich auf Ihren letzten Punkt eingehen, nämlich die Frage der „Selbstregulierung“. Der Ansatz ist gut gedacht, er steht in § 38a BDSG. Wir haben die Möglichkeit, aber sie wird nicht genutzt. Das kann natürlich unterschiedliche Ursachen haben. Ich habe selber in einem Fall miterlebt, dass eine Selbstregulierung bei einem Verband zwar gegen § 38a durchgeführt worden ist. Ganz einfach, weil die vom Gesetzgeber vorgesehene Möglichkeit, dass die Aufsichtsbehörde eine Konformitätserklärung abgibt, nicht genutzt wurde, weil die Aufsichtsbehörden dann so lange nach einem hineinzunehmenden „Mehrwert“ gefragt haben, bis der Verband sagte, jetzt wollen wir nicht zusätzlich „Mehrwert“ schaffen, der im Gesetz nicht steht, sondern irgendwo muss Schluss sein. Wir machen es jetzt so, wie wir es uns gedacht haben. Wir setzen unser Konzept der Selbstregulierung um, aber wir verzichten auf den Behördenstempel, weil die immer neuen Anforderungen, die von Behördenseite gestellt werden, zu weit gehen. Das ist eine persönliche Erfahrung, die ich gemacht habe. Ich habe sie von anderer Stelle in ähnlicher Form bestätigt gehört. Man sollte solchen Erfahrungen nachgehen und sich fragen, warum wird § 38a nicht genutzt? Ich halte es für eine sinnvolle Regelung und wäre sehr froh, wenn eine breite Selbstregulierung käme. Und ich meine etwas, was wir in den USA ansatzweise feststellen können, dass es immer mehr „Datenschutz-Policies“ gibt, deren Einhaltung über Klagemöglichkeiten, meist Zivilklagen, auch auf Schadensersatz gewährleistet wird. Dort wird also etwas geschaffen, was nicht auf öffentlich-rechtlichen Bestimmungen beruht, sondern auf Selbstverpflichtungen. Und gerade was das Thema Scoring angeht, meine ich, dass man den Weg der Selbstverpflichtung durchaus versuchen sollte. Nur dann, wenn es nicht funktioniert,

müsste der Gesetzgeber tatsächlich eingreifen. Es gibt bisher keine Angebote. Aber in die Richtung Selbstverpflichtung zu gehen, halte ich für gut. Und wir müssten vielleicht gemeinsam darüber nachdenken, warum die bestehenden Regelungen noch nicht funktionieren.

Vors. **Sebastian Edathy**: Vielen Dank. Herr Dr. Dix, bitte.

SV **Dr. Alexander Dix**: Ich kann dem zustimmen, was bereits mehrfach gesagt wurde. Es ist die Frage nach der evtl. notwendigen neuen Strategie. Der verfassungsrechtliche Rahmen ist nach wie vor gut, und er ist maßgeblich und er sollte auch - und muss auch - für uns Richtschnur bleiben. Es ist allerdings bedauerlich, dass der Gesetzgeber gerade in den letzten Jahren wiederholt erst vom Bundesverfassungsgericht daran erinnert werden muss, dass der gilt. Das Verfassungsgericht hat mehrfach diesen Rahmen auch noch mal expliziter formuliert, wenn es etwa von einem absolut geschützten Persönlichkeitskern gesprochen hat. Ich will nur darauf hinweisen, dass eigentlich politisch überall Einvernehmen darüber zu bestehen scheint, dass niemand in Deutschland eine Überwachungsgesellschaft will, so wie sie etwa in Großbritannien unbestreitbar bereits zu beobachten ist. Dennoch bewegen wir uns auf einer schiefen Ebene, das lässt sich nicht bestreiten. Wir sind auf einer Entwicklung in eine solche Überwachungsgesellschaft, die offenbar niemand will, und ich sage bewusst „Gesellschaft“ und nicht „Überwachungsstaat“. Dann, und das ist vielleicht ein Moment, wo man über eine durchaus grundlegende Änderung im Regelungskonzept nachdenken müsste, sollten wir uns verabschieden von der Dichotomie zwischen Datenschutz für den staatlichen Bereich und den privatwirtschaftlichen Bereich. Was nicht heißt, dass es Sonderregeln für jeweils beide Bereiche nicht auch in Zukunft geben muss. Aber die starre Unterscheidung zwischen Datenschutz für die staatliche oder kommunale Verwaltung einerseits und Datenschutz für die Privatwirtschaft andererseits, die ist überholt, und die muss verabschiedet werden. Es muss auch um eine Gesamtsicht der Überwachungsintensität gehen, der der Bürger - ganz egal von welcher Seite - zunehmend ausgesetzt ist.

Vors. **Sebastian Edathy**: Vielen Dank. Herr Schaar, bitte.

SV **Peter Schaar**: Sie haben nach der Möglichkeit gefragt, Technologie zu regulieren. Es ist in der Tat eigentlich die Aufgabe des Datenschutzes, mit Technologie umzugehen, den Umgang mit Technologie zu steuern. Jetzt stellt sich allerdings die Frage, ob man neben die Instrumente, die das Bundesdatenschutzgesetz bisher bereitstellt, weitere Mechanismen stellen kann, die ggf. effektiver sind, oder die gesetzlichen Mechanismen in der Weise ergänzen, dass sie wirksam werden können. Ich denke, der wesentliche Ansatz wird nicht sein, spezifische, auf einzelne Technologien abstellende Regelungen zu formulieren. Ein „RFID-Gesetz“, oder ein „RFID-Paragraph“, ein „Biometrie-Paragraph“, und für „local-

base-services“ ein weiterer Paragraph, der ins allgemeine Datenschutzgesetz eingehen könnte - das kann es eigentlich nicht sein. Es kann bestimmte Bereiche geben, wo es sinnvoll ist, auch technologische Regelungen in Spezialgesetze einzufügen, wie es z.B. bei der elektronischen Gesundheitskarte erfolgt ist. Das - finde ich - ist ein relativ gutes Beispiel, bei dem man versucht hat, technologische Aspekte in ein Gesamtkonzept einzubetten, möglichst frühzeitig, wo auch der Gesetzgeber dafür Sorge getragen hat, dass bestimmte Sicherungen eingebaut werden. Eine solche Regelung nimmt mir vielleicht nicht die Sorge, dass auf Dauer mit diesen Daten auch mal etwas Unrechtmäßiges geschieht, aber es verringert diese Sorge zumindest sehr stark. Wichtig ist, dass man bestimmte Mechanismen ausfindig macht, die vielleicht teilweise sogar schon im Datenschutzrecht stehen, die genau diese Steuerungsfunktionen entfalten könnten, aber es bisher nicht tun. Ich denke hier bspw. an die Vorschrift zur Vorabkontrolle. Dieses Instrument gibt es seit der Europäischen Datenschutzrichtlinie von 1995. Es ist so ein bisschen versteckt dann auch bei uns ins Datenschutzgesetz übernommen worden. Diese Vorschrift mit Leben zu erfüllen wäre z.B. ein sinnvoller Ansatzpunkt. Oder auch die Frage der Gütesiegel; die ja angesprochen worden ist im Zusammenhang mit „Datenschutz-Audit“ - wir werden das auch später vertiefen. Es ist auch ein wichtiger Aspekt, Datenschutz über Verfahren zu realisieren. Das „Privacy-Impact-Assessment“ ist angesprochen worden. Diese Datenschutzfolgeabschätzung, die im Übrigen nicht nur in Berlin - also im Land Berlin -, sondern auch auf europäischer Ebene mittlerweile verbindlich ist. Die Europäische Kommission hat sich verpflichtet, stets ein „Privacy-Impact-Assessment“ vorzunehmen, wenn ein datenschutz-relevantes Thema angepackt wird, sei es ein technologisches Projekt, oder eben eine Regulierung. Ich denke, daran kann man sich auch in Deutschland durchaus orientieren, dass man solche verfahrensmäßigen Sicherungen für die weitere Steuerung von Technologie schafft. Darüber hinaus, denke ich, dass der Aspekt der Transparenzsteigerung wichtig ist. Da können auch neue Instrumente hilfreich sein. Das werden wir nachher noch mal aufgreifen im Hinblick auf den „Security Breach Information Act“. Es ist aber auch die Frage einer fairen Praxis. Das knüpft ein bisschen an die Strategiediskussion von vorhin an: Was ist eigentlich ein fairer Umgang mit personenbezogenen Daten? Prof. Abel hat das ja angesprochen bei seinem letzten Beitrag. Hier könnte man durchaus auch im Hinblick auf technologische Steuerungsmechanismen Fortschritte erreichen, wobei es dann nicht damit getan ist, dass man von den Unternehmen fordert, Datenschutzerklärungen abzugeben, in denen der Umfang der Datenverarbeitung dargestellt wird, sondern dass auch Sanktionsmechanismen wirklich greifen, auch solche zivilrechtlicher Natur. Lassen Sie mich abschließend einen Aspekt hier nennen, der mir ganz wichtig ist, auch im Hinblick auf das Gesamtprojekt „Modernisierung des Datenschutzes“. Sie haben ja die Geschichte angesprochen. Ein Nachteil des Verfahrens, das man damals gewählt hat, war, dass man die Vorstellung hatte, man kann eine Rundumerneuerung des Datenschutzrechtes in einem Schritt vornehmen, und dann ist es getan. Diese Vorstellung war ein bisschen naiv, glaube ich. Es geht nicht, dass

man in einer sich ständig verändernden und sich weiterentwickelnden Informationsgesellschaft einen Endstand erreicht, sondern es muss im Prinzip immer wieder gefragt werden: Gibt es Fehlentwicklungen, müssen wir hier nachsteuern? Ich meine, hier helfen manchmal kleine Schritte weiter. Man muss nicht die Riesenreform des Bundesdatenschutzgesetzes haben, sondern denkbar wäre es auch, dass man an bestimmten wichtigen „Baustellen“ arbeitet und dort entsprechend dann zu neuen, besseren Regelungen kommt. Ein ganz wichtiger Aspekt ist dabei die Verständlichkeit von Datenschutzvorschriften. Wir sollen hier zumindest in einen Prozess eintreten, in dem man schaut, welche Datenschutznormen gibt es? Und vielleicht könnte man dort auch zu einer Zusammenfassung gelangen. Das ist vom Bundesinnenministerium wiederholt zugesagt worden, aber bisher habe ich kein Resultat gesehen. Vielleicht bewirkt ja diese Anhörung, dass jetzt mehr Arbeit in dieses Projekt hineinfließt, dass dann auch ein Output zu erwarten ist.

Zur Frage der personenbezogenen Daten: Sie ist auch wichtig bei einer technologischen Regulierung - RFID-Chips sind angesprochen worden und „Scoring“. Wir müssen hinterfragen, greifen die Datenschutzregeln hier überhaupt? Was ist personenbezogen, was ist nicht personenbezogen? Wo ist das Schutzgut, das Recht auf informationelle Selbstbestimmung, möglicherweise auch betroffen, selbst wenn die Daten noch nicht personenbezogen sind? Das Datenschutzrecht reguliert das bisher nicht befriedigend. Hier gibt es vielleicht Möglichkeiten über „Fair Informations-Practices“, also über den Verbraucherschutz, auch zu Instrumenten weiter zu kommen, die über den klassischen Regelungsbereich des Datenschutzes hinausgehen.

Vors. **Sebastian Edathy**: Abschließend Herr Dr. Thorun, bitte.

SV **Dr. Christian Thorun**: Frau Stokar, vielen Dank für diese grundsätzliche Frage zum Verhältnis zwischen Datenschutz und Verbraucherschutz. Grundsätzlich ist festzustellen, dass Datenschutz mit Verbraucherschutz nicht zwingend etwas zu tun haben muss. Allerdings sollte Verbraucherschutz dann etwas mit Datenschutz zu tun haben, wenn die Interessen der Bürger in ihrer Rolle als Verbraucher beeinträchtigt sind. Und da sehen wir genau die Entwicklung, die ich eben gerade auch versucht habe zu skizzieren. Dass nämlich die Privatsphäre der Verbraucher heute in erheblichem Maße durch die privaten Stellen bedroht ist. Was muss getan werden? Ja, das eine ist natürlich Bewusstseinswandel, wobei ich da auch nicht das Gefühl habe, dass wir da noch unbedingt viel machen müssen. Die Verbraucher zeigen ein erhöhtes Problembewusstsein. Dass wir jetzt hier in solcher Anhörung als Verbraucherschutzorganisation eingeladen sind, ist auch ein Indiz dafür, dass sozusagen dieser Nexus zwischen Datenschutz und Verbraucherschutz eine andere Anerkennung erfährt. In Diskussionen über Rabattkarten, -programme oder RFID-Technologie usw. sind wir immer stärker repräsentiert. Das, was wir allerdings brauchen, das haben hier auch verschiedene Redner angesprochen, ist eine Modernisierung des Datenschutzes, die genau das reflektiert, dass Datenschutz nicht

im Wesentlichen Schutz vor dem Staat ist, sondern im weiten Maße auch vor privaten Stellen. Es ist auch so, was wir schon angesprochen haben, dass Verbraucherschutzorganisationen dann konsequenterweise auch mehr Rechte brauchen und nicht nur über AGB-Verfahren den Datenschutz einzuklagen, sondern auch über andere Verfahren. Das Dritte ist, dass bei Fragen der technologischen Gestaltung - Herr Schaar hatte es schon angesprochen - natürlich die Datenschützer nicht immer erst nachher befragt werden sollen, was haltet ihr jetzt von unserer Technologie, sondern dass genauso wie die Datenschützer die Verbraucherschützer schon im Vorfeld „ins Boot“ geholt werden. Ich denke, dass hier die RFID-Technologie ein gutes Beispiel ist. Es gibt auch diesen Diskussionsprozess gerade im BMWI zu der großen Konferenz im Juni zum Thema „RFID“. Ich denke, dass es hier auch gerade von Seiten der Bundesregierung geboten wäre, klarzustellen, dass man Datenschutz als Verbraucherschutz ernst nimmt. Ich habe da häufig aus der Praxis den Eindruck, dass dieses Bewusstsein dort fehlt. Ich würde mir wünschen, dass durchaus von Seiten der Exekutive da oder der Legislative mehr kommt.

Vors. **Sebastian Edathy**: Vielen Dank. Wir können gemeinsam feststellen, dass die Sachverständigen sehr auskunftsfreudig sind. Das ist ja auch grundsätzlich ganz gut. Ich entnehme dem Zeitplan, dass wir gerade mal die erste Berichterstatterrunde geschafft haben. Deswegen würde ich mit Blick auf die zweite und die dritte Runde, in die wir nachher einsteigen, bitten, dass die Fragesteller sich vielleicht auf zwei Sachverständige nach Möglichkeit erst mal konzentrieren und wir dann noch die Möglichkeit nach der Berichterstatterrunde haben, entweder einen zweiten Durchlauf zu machen oder anderen Kolleginnen und Kollegen die Möglichkeit zu geben, Fragen zu stellen. Ich darf jetzt vielleicht fragen, ob es noch zu dem ersten Block allgemein „Modernisierung des Datenschutzes“ Fragebedarf gibt. Das ist der Fall bei der Kollegin Philipp, bitte.

Abg. **Beatrix Philipp**: Ich hätte gerne an Herrn Dr. Thorun die Frage gestellt: Wie viele Menschen wenden sich an Sie? Sie haben eben mal so zwischendurch gesagt, die fragen telefonisch an, wie kommen die an meine Daten oder irgend so was. Können Sie mal sagen, wie viele sich wegen der Problematik aus dem Datenschutz an Sie wenden, so mal über den Daumen gepeilt? Und mit welchen Beschwerden?

SV **Dr. Christian Thorun**: Ich kann Ihnen jetzt leider keine Zahl nennen. Das, was die Art der Beschwerden ist, sind a) die, die fragen: Wie kommt es dazu, dass ich angerufen werde, wie kommen die an meine Daten? Die fragen mich ja Fragen, und die sind so gezielt, dass ich mich wundere, wie diese überhaupt dazu kommen, mich diese Dinge zu fragen. Und dann sind es diese Geschichten: Warum bekomme ich jetzt nicht den Kredit, den ich mir wünschen würde aufgrund meiner Stellung, aufgrund meines Jobs. Wie kann das denn eigentlich sein? Oder Versicherungsabschlüsse, wo man sich plötzlich fragt: Warum komme ich in diese Versicherung nicht hinein oder zu dem Tarif oder nicht bei dem Anbieter?

Vors. **Sebastian Edathy**: Vielen Dank. Sofern keine Pause gewünscht ist - was nicht der Fall ist - kommen wir jetzt zum zweiten Block, zum Thema „Datenschutz-Audit“. Zeit ist bis 17.00 Uhr dafür vorgesehen. Es gibt dazu zwei Anträge, einmal der FDP-Fraktion, einmal der Fraktion BÜNDNIS 90/DIE GRÜNEN. Wir machen weiter in Form einer neuen Berichterstatterrunde, d.h. das Wort hat die Kollegin Beatrix Philipp.

Abg. **Beatrix Philipp**: Herr Vorsitzender, meine Damen und Herren, die CDU/CSU-Fraktion hat sich immer sehr kritisch mit dem „Datenschutz-Audit“ befasst, das wissen Sie. Ich überschreibe das mal so, das geht ja auch aus der einen oder anderen Stellungnahme hervor: Es geht eigentlich um das Gütesiegel für die Einhaltung des geltenden Rechts. Ich will das nur mal so oben drüberstellen und deswegen die Frage jetzt an Herrn Prof. Abel, aber auch an Frau Sasse: Wer käme denn für die Festlegung der Kriterien und die Durchführung Ihrer Meinung nach in Frage? Sehen Sie einen oder keinen Konflikt, wenn das die Aufsichtsbehörden machen, wie das ja hier oder da angeklungen ist? Und schließlich die Frage, wenn ich das gerade richtig verstanden habe: Ein Gesetz oder eine Rechtsverordnung oder ist es eine Sache, die auf Länderebene abgehandelt werden würde?

Vors. **Sebastian Edathy**: Vielen Dank. Herr Prof. Abel, bitte.

SV **Prof. Dr. Ralf Bernd Abel**: Vielleicht darf ich zunächst auf die dritte Frage eingehen. Es gibt Zuständigkeiten teilweise bei den Ländern, teilweise beim Bund. Wenn wir hier beim Bund sind, wo sicherlich die Auditierung über das Recht der Wirtschaft - als Annex-Kompetenz - geregelt werden könnte, zumindest für den nichtöffentlichen Bereich, da stelle ich mir schon die Frage: Muss man alles wirklich durch Parlamentsgesetz regeln? Vielleicht geht das ein bisschen weit. Schleswig-Holstein oder Mecklenburg-Vorpommern haben diese Frage mit einer Rechtsverordnung gut in den Griff bekommen. Das halte ich persönlich für leichter, denn wenn es irgendwo eine Veränderung gäbe, oder Veränderungsanpassungsbedarf, muss nicht immer der Bundestag die gesamte Gesetzgebungsmaschinerie anwerfen, evtl. noch mit Hilfe des Bundesrates. Das ist schon sehr viel Aufwand. Insoweit erscheint mir eine Rechtsverordnung eigentlich wie bei der Straßenverkehrsordnung mit zahlreichen kleinen Änderungen - falls nötig - sinnvoller. Natürlich kann man bestimmte Sachverhalte durchaus per Bundesgesetz regeln, auch im BDSG. Zum Beispiel die Frage der Zuständigkeit. Wer soll etwa als „Wurzelninstanz“ - wie es manchmal so schön heißt - in Frage kommen? Sollen es nicht vielleicht am besten die Aufsichtsbehörden sein? Aber damit habe ich eine gewisse Schwierigkeit. Zum einen gibt es mit sechzehn plus einer eine große Zahl von Aufsichtsbehörden, was sicherlich Regelungen schwierig macht. Zum anderen sind Aufsichtsbehörden natürlich nicht nur Unterstützungs-, sondern auch Kontrollinstanzen. Daher sollte eine saubere Trennung - jedenfalls was den

nichtöffentlichen Bereich angeht, nicht was den öffentlichen Bereich auf Länderebene angeht, da sieht es anders aus - im nichtöffentlichen Bereich bundesweit zwischen Aufsicht Auditierung stattfinden, denn dadurch wäre auch eine Kontrolle besser gewährleistet. Mir persönlich ist es der angenehmere Gedanke, dass hier eine staatliche Stelle schon über das wacht und das kontrolliert, was an anderer Stelle gewährleistet wird, denn hier ist ja schon oft das Wort „Vertrauen“ angesprochen worden. Vertrauen in das Funktionieren der Mechanismen. Und da meine ich, dass es gut ist, wenn wir gewissermaßen ein „Vier-Augen-Prinzip“ einführen, so dass einerseits eine andere Behörde als die Aufsichtsbehörden zuständig ist für Sachverständigenwesen und Zulassung und andererseits die Aufsichtsbehörden immer noch unabhängig einen Blick darauf werfen. Wer käme in Betracht? Also mir persönlich erscheint das BSI sinnvoll. Herr Schaar, Sie haben mit dem BSI bereits in einigen Bereichen zusammengearbeitet. Das BSI als eine Bundesbehörde, die ganz erhebliche und hervorragende Kompetenzen vereinigt, ist durchaus eine sinnvolle Überlegung. Eine andere Überlegung wären die Organisationen der Industrie- und Handelskammern, die schon gesagt haben, dass sie zu einer solchen Aufgabe bereit wären. Das ist sicherlich etwas, über das man noch nachdenken kann, ob da z.B. auch für den Bereich der Banken die BAFin die richtige wäre. Auch darüber könnte man nachdenken. Ich denke aber, dass vor allen Dingen beim BSI entsprechende Kompetenzen vorhanden sind. Aber gut, das ist Diskussionssache, das würde ich jetzt hier auch nicht abschließen. Da müsste man in einem eigenen Verfahren die Positiva - Negativa entsprechend bewerten.

Vors. **Sebastian Edathy**: Vielen Dank. Dann Frau Sasse, bitte.

SV **Cornelia Sasse**: Vielen Dank, Frau Philipp. Die Frage, Herr Dr. Abel, ich kann mich den Worten meines Vorredners nur anschließen in dem Vorschlag, zu entzerren, und zwar die Verantwortung den Aufsichtsbehörden aufzuerlegen. Wenn ich mir vorstelle, die Aufsichtsbehörde solle uns als Unternehmen kontrollieren, dann sehe ich hier die Schwierigkeit, wenn diese Behörde uns auch auditiert. Insofern das Vertrauen z.B. dem BSI auf alle Fälle, aber auch den Industrie- und Handelskammern zu schenken, sehe ich als außerordentlich praktikabel an. Viel wichtiger, aber vielleicht kommen wir noch dazu, und vielleicht kommt die Fragestellung auf, ist zu klären, was zu prüfen ist und was zu auditieren ist.

Vors. **Sebastian Edathy**: Vielen Dank. Dann hat als nächste Kollegin das Wort Frau Piltz von der FDP-Fraktion.

Abg. **Gisela Piltz**: Vielen Dank. Ich habe manchmal das Gefühl, wenn es um „Datenschutz-Audit“ geht, ist es ein bisschen wie beim Informationsfreiheitsgesetz. Man glaubt immer, wenn es eingeführt ist, geht die Welt unter und irgendwie dreht sie sich weiter, ohne dass es größere Kollateralschäden gibt. So denke ich das manchmal auch beim „Datenschutz-Audit“. Ich finde es sehr spannend, es gibt doch

mehrere staatlich verordnete Gütesiegel. Die gibt es auch, ohne dass ich gemerkt hätte, dass da wirklich größere Schäden einhergegangen wären. Wenn einem von Ihnen größere Schäden bei anderen Siegeln bekannt sind, wäre ich sehr dankbar, wenn Sie uns das mitteilen könnten, weil ich glaube, auch die Erfahrung mit anderen Bereichen macht ja vielleicht Sinn für eine Art „Datenschutzsiegel“. Darum geht es ja mehr oder weniger. Meine Fragen gehen an Frau Sasse, Herrn Jaspers und an Herrn Thorun. Sie haben ja eben schon zu Recht darauf angespielt, welcher Gegenstand oder was soll die Auditierung eigentlich behandeln? Da ist eine Überlegung, ob man das Unternehmen insgesamt auditiert oder ob man einzelne Produkte oder einzelne Dienstleistungen auditiert, und ob Sie der Ansicht sind, einzelne Dienstleistungen z.B. würden ausreichen oder ob es das gesamte Unternehmen sein soll. Und für die Verbraucher besteht dann das Problem, wenn es innerhalb eines Unternehmens sozusagen kundenfreundliche Produkte und andere nichtkundenfreundliche Produkte gibt. Aber vielleicht haben Sie eine Meinung dazu. Dann ist natürlich eine Frage bzw. geht es um den Maßstab der Auditierung, ob es sinnvoll ist, dass allein die Erfüllung datenschutzrechtlicher Vorschriften Gegenstand dieser Auditierung ist? Hält es dann nicht sozusagen die Unternehmen davon ab, sich ein bisschen mehr zu bemühen? Es könnte ja auch Sinn der Sache sein, dass man einen Wettbewerb nach oben offen lässt, also erste, zweite Güte, keine Ahnung. Wenn ich nur sage, wer die Vorschriften erfüllt, der bekommt eins, dann habe ich aber als Unternehmen kaum noch einen Anreiz zu sagen: Ich bin aber noch besser. Das Problem ist, ich kann es zwar sagen heute im Internet, wenn ich da selber im Internet bezahle. Natürlich werben die alle mit Sicherheit. Aber ich kann es nicht überprüfen, die Chance habe ich nicht als Verbraucher, weil ich keine Vergleichbarkeit habe. Und so gesehen habe ich natürlich, wenn einer sagt, wir sind aber noch besser, als Verbraucher auch wenig Vergleichsmöglichkeiten. Zur Zuständigkeit, wer die Zertifizierung macht, ist ja hier schon verschiedentlich gesprochen worden. Meine Zusatzfrage dazu ist nur, ob Sie sich vorstellen könnten, dass es eben die Wirtschaft selber macht, die IHKS haben Sie schon genannt. Ob Ihnen da vielleicht noch eine andere Möglichkeit einfällt, weil, wir suchen ja auch nach der besten Lösung. Und meine letzte Frage ist, ob Sie im Bereich der Auditierung internationale Beispiele kennen, wo die Welt sich weitergedreht hatte, nachdem man das eingeführt hat, und wo wir nicht glauben, dass das alles untergeht. Herzlichen Dank.

Vors. **Sebastian Edathy**: Angesprochen sind, wenn ich es richtig verstanden habe, drei Sachverständige. Dann zunächst Herr Jaspers, bitte.

SV **Andreas Jaspers**: Was soll Gegenstand des Audit sein? Im Grunde genommen kann man eigentlich froh sein, dass nicht sofort, nachdem der § 9 BDSG verabschiedet worden ist, ein Gesetz ergangen ist, dann wären „Daten verarbeitende Stellen“ Gegenstand des Audits geworden. Und ob das sinnvoll ist, ein gesamtes Unternehmen mit all seinen Verfahren zu auditieren, war letztendlich als ein

Hauptproblem von Seiten der Wirtschaft gesehen worden. Wenn ein bisschen „Wasser den Rhein hinabgeflossen“ ist, ist man weitsichtiger geworden. Sicherlich hat man durch die Erfahrungen des ULD gesehen, in welche Richtung es so gehen könnte, was man auditieren soll. Auditieren sollte man auf jeden Fall, das haben wir auch gesagt. Datenschutz durch Technik bedeutet eben auch, Anreize dafür zu schaffen. Ich habe ja nichts davon, datenschutzfreundliche Technologien zu machen. Ich muss auf den Markt gucken. Es müssen Anreize geschaffen werden, und hier ist das Audit eine der entscheidendsten Weichenstellungen. Am Rande dazu, wer soll auditiert werden? Nun, wir sehen insbesondere das Audit dort, wo es einen Vorteil für das Unternehmen bringt. Insbesondere Dienstleister möchten gerne ihre Dienstleistung zertifizieren lassen auf Datenschutzkonformität. Und dies ist auch branchenübergreifend, das ist auch unternehmensgrößenübergreifend. Selbst kleine Unternehmen sagen, wir sind topp Archivierer, wir können es, wir möchten das gerne der Welt zeigen. Insbesondere deswegen, weil im BDSG praktisch die Regelüberprüfung weggefallen ist. Da gibt es sicherlich entsprechende Bedürfnisse und Interessen, die wir deutlich wahrgenommen haben. Was soll Maßstab der Auditierung sein? Sie sprachen die Frage an, „soll es nicht ein bisschen mehr sein?“ Die Frage ist, was ist gesetzliche Übererfüllung für ein Gütesiegel: plus 10 Prozent, plus 20 Prozent? Ich denke, ein vernünftiges Datenschutzkonzept, das letzten Endes technikorientiert ist, das auch dem Prinzip der Datenvermeidung und der Datensparsamkeit genügt. Wenn das vorhanden ist, ist das ausreichend. Wenn ich 10 Prozent mehr fordere, kosten 10 Prozent viel Geld und ohne erkennbaren Nutzwert. Und wenn es dann weiter hochgestaffelt ist, muss man sich fragen, welche Folgewirkung entsteht daraus. Letzten Endes muss man auch an die Frage der Bürokratie und der Kosten denken. Ein vernünftiges Datenschutzkonzept kann auditiert werden. Ich denke, im Grunde genommen wird auch keine Scharlatanerie betrieben werden, wenn man entsprechend auditiert. Wer soll es machen? Wir sagen, bei den Datenschutzaufsichtsbehörden gibt es Inkompatibilitäten. Das wurde bereits ausgeführt, dem kann ich mich nur anschließen. Man sollte natürlich auch hier Bürokratie vermeiden und bestehende Strukturen nehmen. BSI und BFDI haben ja schon Schutzprofile entwickelt, in diese Richtung schon gearbeitet. Da letzten Endes der Schwerpunkt der Auditierung die Technik ist, ist das BSI im Spiel. Die legen den Zertifizierungsrahmen fest. Und wer soll es praktisch machen? Auch da setzen wir auf bestehende Strukturen, da sagen wir nämlich, dass soll letztendlich die IHK-Organisation machen.

Nur ein abschließendes Wort. Brauchen wir ein gesetzliches „Datenschutz-Audit“? Wir brauchen es, denn die bisherigen Initiativen seitens der Wirtschaft, hier mal selber Gütesiegel zu entwickeln, sind alle bisher nicht zielführend gewesen. Die Gewerkschaften haben es probiert, allen voran die Deutsche Postgewerkschaft. Dieses Gütesiegel ist entwickelt worden und wird überhaupt nicht benutzt. Der TÜV hat es probiert, damit aber keinen Markt gesehen. Die DEKRA hat es probiert, hat damit auch keinen Markt gesehen. Wir waren überall in ihren Arbeitskreisen vertreten. Man hat sich da Mühe und Gedanken gemacht. Offensichtlich scheint man

auf den „Adler“ zu warten, von daher sollte man das Audit offensichtlich staatlich „aufhängen“. Wir brauchen es deswegen, weil es ein sinnvolles Mittel ist zur datenschutzfreundlichen Technik. Danke schön.

Vors. **Sebastian Edathy**: Vielen Dank. Frau Sasse, bitte.

SV **Cornelia Sasse**: Vielen Dank, Frau Piltz. Herr Jaspers hat es bereits erwähnt, was soll geprüft werden? Auch hier kann ich nur sagen aus Unternehmenserfahrung sagen, es kann sich hauptsächlich auf die technischen und organisatorischen Pflichten beziehen. Es wird z.B. sehr schwierig sein in allen größeren Unternehmen, die wie wir Auftragsdatenverarbeiter sind. Es ändern sich täglich die Herausforderungen an unsere Verfahren. Es ändern sich täglich und mit unseren Kunden mit den verschiedenen Aufträgen die Herausforderungen an die einzelnen Prozesse der Datenverarbeitung. Es ändert sich nie die Herausforderung an das Selbstverständnis, an den Datenschutz für ein Unternehmen. Ich gehe dabei von jedem Unternehmen aus. Es kann nicht die Rechtschaffenheit eines Unternehmers in Frage gestellt werden, wenn es sich nicht zertifizieren lässt. Dann ist da die Frage nach dem Wettbewerb: Ist ein Wettbewerb nötig, was ein Audit betrifft? Ich möchte sagen, dass dies gefährlich sein könnte, denn es würde evtl. ein Unternehmen in der Öffentlichkeit in Frage stellen, welches sich nicht datenschutzrechtlich auditieren lässt. Vielleicht nicht weil es nicht den Datenschutz einhält, sondern weil es nicht wirtschaftlich in der Lage ist, das zu tun, das zu finanzieren. Es steht bis dato noch nicht einmal fest, welchen verwaltungstechnischen Aufwandes es bedarf, noch dazu welcher Kosten es bedarf, das durchzuführen. Es kann nicht sein, dass ein Unternehmen deshalb als „Schwarzes Schaf“ dargestellt wird, wenn es kein Audit-Gütesiegel hat. Es muss schon eine Möglichkeit gefunden werden, hier eine Balance zu finden. Und zu der Frage, ob es internationale Erfahrungen gibt, dazu kann ich sagen, es wird sie geben in den Ländern, in denen es kein einheitlich und rechtlich geregeltes Datenschutzniveau gibt. Da muss es das geben, und ich denke, das gibt es. Ich kann dort nicht aus der Erfahrung von Audit berichten, aber ich kann mir das gut vorstellen.

Vors. **Sebastian Edathy**: Vielen Dank. Herr Dr. Thorun, bitte.

SV **Dr. Christian Thorun**: Ich möchte zuerst auf die letzte Frage eingehen: Geht die Welt unter? Dieses Argument kann ich in keinsten Weise nachvollziehen, denn es handelt sich hierbei um ein marktwirtschaftliches, freiwilliges Instrument. Also die Unternehmen, die daran teilnehmen, erhoffen sich dadurch einen marktwirtschaftlichen Vorteil. Und von daher gibt es auch gar keinen Zwang für andere Unternehmen, da unbedingt mitzumachen, es sei denn, dass sie sich auch über diese Produkteigenschaft mit „ins Spiel“ bringen wollen. Natürlich wird das dann zusätzliche Kosten für diese Unternehmen verursachen, aber dann auch hoffentlich mit dem eintretenden Mehrerlös, indem man das Produkt mit dieser Eigenschaft

verkaufen kann. Die Herausforderung im Datenschutz liegt darin begründet, dass es sich um unsichtbare Produkteigenschaften handelt. Datenschutz ist ja nicht so wie die Datenrate bei dem DSL von 6.000 auf 16.000. Diesen Unterschied spüre ich. Deshalb muss der Datenschutz irgendwie sichtbar gemacht werden durch Labels. Und was sind da die Grundvoraussetzungen, die wir bei diesem Label immer sehen? Diese Labels müssen glaubwürdig sein. Deswegen ist es auch so wichtig, dass diese Labels durch eine glaubwürdige Instanz geprüft werden und Kriterien geprüft werden, die klar definiert sind, so dass auch tatsächlich, wenn ich ein Label sehe und sichergehen kann, okay, die bestimmten Kriterien sind eingehalten und es wurde von einer unabhängigen Instanz überprüft. Von daher kann ich das Argument „geht die Welt unter“ nicht nachvollziehen. Ich glaube, der Datenschutz bereichert einfach nur den Wettbewerb um eine neue Komponente, nämlich die Komponente des Wettbewerbs um den Datenschutz, um einen möglichst guten Datenschutz. Gegenstand der Auditierung: Der Verbraucher schaut häufig nicht unbedingt danach, ob jetzt ein Unternehmen X, Y Mitglied ist oder sich bestimmten Regelungen insgesamt unterwirft, sondern meist wird es am Produkt selbst sichtbar. Er kauft ein Produkt, eine Dienstleistung und möchte dann am besten durch ein Label sehen, unter welchen Bedingungen dieses Produkt erzeugt worden ist. Von daher würde ich dafür plädieren, dass tatsächlich dieses Siegel am Produkt sichtbar macht, dass sozusagen der Datenschutz hier eingehalten wird. Die Frage des Maßstabs, also sozusagen das Minimum oder ob man nach oben den Wettbewerb offen lassen soll, da würde ich natürlich sagen: Wettbewerb sollte nach oben offen gelassen werden. Dann sollte man sich darüber Gedanken machen, dass es vielleicht ein Bronze-, Silber-, Gold-Siegel gibt. Das Bronzesiegel stellt sicher, dass das gesetzliche Niveau dort eingehalten wird und nach obenhin sollte es offen sein, denn das ist ja der Wettbewerb. Der Wettbewerb soll ja ein Wettbewerb um die besten Ideen sein und von daher nach oben offen sein. Mit internationalen Beispielen kann ich jetzt nicht dienen, aber ich möchte verweisen auf andere Bereiche, wo Siegel durchaus große Marktkraft entfaltet haben: es handelt sich um die Eierkennzeichnung. Ich denke, die Auditierung ist ein ergänzendes Instrument, um diesen Vollzugsdefiziten, die wir im ersten Teil der Anhörung besprochen haben, mit entgegenzuwirken.

Vors. **Sebastian Edathy**: Sind die Kolleginnen und Kollegen damit einverstanden, wenn sich Sachverständige äußern, die gar nicht gefragt worden sind? Dann macht das jetzt ausnahmsweise Herr Schaar. Bitte.

SV **Peter Schaar**: Ja, danke für diese Ausnahme, Herr Vorsitzender. Zum Thema „internationale Erfahrung“: Es gibt internationale Erfahrungen von Unternehmen, die selbst von Gütesiegelvergabe leben. Insbesondere US-Unternehmen haben solche Gütesiegel entwickelt. Diese Gütesiegel sind aber, wenn man sich das genau anschaut, häufig sehr unbefriedigend, weil sie nur sagen, dass die Praxis eines Unternehmens mit seinen Zusicherungen übereinstimmt. Ob die Praxis gut oder schlecht ist, wird damit gar nicht zertifiziert, so dass die Aussagekraft zumindest

beschränkt ist und dem Einzelnen nicht unbedingt sehr viel weiterhilft. Wenn ein Verstoß stattfindet, kann es zu Sanktionen durch die Federal Trade Commission oder eine andere entsprechende Aufsichtsbehörde bis hin zu erheblichen Bußgeldern kommen. Zweite Erfahrung - auch aus den USA - sind die Safe-Harbour-Auditierungen. Safe-Harbour ist ein Abkommen, das die Europäische Union mit den Vereinigten Staaten getroffen hat. In diesem Abkommen ist eine Auditierung durch unabhängige Wirtschaftsprüfer vorgesehen. Diese Erfahrungen sind sehr positiv. Die Kriterien sind im Safe-Harbour-Abkommen selbst definiert. Es handelt sich in der Tat um Unternehmensauditierung, nicht um Produktauditierung, und dies wird als sehr erfolgreich wahrgenommen. Insofern würde ich das nicht vollständig von der Hand weisen. Drittes internationales Beispiel sind die so genannten Common Criteria, die aus der IT-Sicherheit kommen. Dabei geht es um internationale Standards für die Zertifizierung von Produkten anhand formaler Kriterien. Einige Anwendungen sind hier ja schon genannt worden. Herr Jaspers hat etwa auf Schutzprofile hingewiesen, die der Bundesdatenschutzbeauftragte in Zusammenarbeit mit dem BSI und privaten Unternehmen entworfen hat, z.B. für Videosysteme. Damit wird eine technische Eigenschaft überprüft, die es ermöglicht, Datenschutzerfordernungen einzuhalten. Ob der Einsatz dann auch datenschutzgerecht ist, ist eine andere Frage.

Vors. **Sebastian Edathy**: Vielen Dank für die Ergänzung. Das Wort hat nun Herr Dr. Bürsch für die SPD-Fraktion.

Abg. **Dr. Michael Bürsch**: Mit einem gewissen Stolz schaue ich als Schleswig-Holsteiner auf mein Heimatland. Von Schleswig-Holstein lernen, heißt Audit begreifen. Können Sie, Herr Bizer, uns mal von den Erfahrungen seit 2003 mit 35 Gütesiegeln sagen, was können wir davon lernen? Was sind die Vorgaben, die Sie aus diesen vier Jahren Erfahrung an uns weitergeben können? Die Frage auch: Brauchen wir, wenn das in Schleswig-Holstein so wunderbar funktioniert, dies dann auf nationaler Ebene? Und wenn ja, warum? Was ist mit dem ersten Produkt von Microsoft, was jetzt im Februar 2007 zum ersten Mal an einen ausländischen Hersteller vergeben worden ist. Wie waren da die Bedingungen? Und an Herrn Dix, der es in seiner Ausführung herausgehoben hat, die Frage: welche wirtschaftlichen Anreize kann man denn setzen? Denn - anders als Frau Philipp, die vielleicht ein großer Anhänger von Sanktionen ist - glaube ich, Sanktionen verleiten leicht dazu, dass man Wege sucht, zu vermeiden, was an Sanktionen aufgestellt ist, wären Anreize besser, die das Positive betonen. Also, welche wirtschaftlichen Anreize kann es denn für ein Audit geben? An Herrn Schaar die Frage: Es wird ja immer gesagt, das ist ja wunderbar, die Großen können sich das erlauben. Wir werben ja gerne - ich auch - für den wirtschaftlichen Wettbewerbsvorteil Audit. Aber die Kleinen können sich das nicht erlauben. Wie ist es mit dem Mittelstand? Wie kann man vermeiden, dass es für den Mittelstand Wettbewerbsnachteile durch Audit gibt, oder soll man ein Zweiklassenrecht einführen, also die vereinfachte Variante für die Klein- und mittelständischen Unternehmen. Was kann man da machen?

Vors. **Sebastian Edathy**: Vielen Dank. Zunächst Herr Dr. Bizer, bitte.

SV **Dr. Johann Bizer**: Vielen Dank für die Frage, Herr Bürsch. Schleswig-Holstein hat in der Tat sowohl große Erfahrungen mit Gütesiegeln als auch mit Auditverfahren. Unter Gütesiegeln versteht unser Recht die Siegelung von Produkten, von Audit sprechen wir, wenn es um Verfahren automatisierter Datenverarbeitung geht. Im Bereich des Gütesiegels haben wir bisher 35 Zertifizierungen zu Ende geführt. Zahlreiche Produkte sind bereits zertifiziert, d.h. der Zertifizierungszeitraum von drei Jahren war abgelaufen und die Antragsteller, die Hersteller haben ihre Produkte neu eingereicht. Wie funktioniert das bei uns? Es ist ein zweistufiges Verfahren. Beim ULD prüfen nach Fach- und Sachkunde akkreditierte Gutachter aufgrund eines privatwirtschaftlichen Vertrages mit dem Hersteller das Produkt nach allgemeinen von uns veröffentlichten Kriterien, legen das Gutachten dem ULD vor und dann wird von uns von einer eigenen Zertifizierungsabteilung dieses Gutachten geprüft, ggf. werden Nachforderungen gestellt, so dass das Produkt verbessert werden muss oder die Dokumentation verbessert werden muss. Wenn wir dann zufrieden sind, dann verlangen wir dieses Gütesiegel als ein Zertifikat, als eine Bescheinigung für die Datenkonformität dieses Produktes. Der Hersteller bezahlt das Gutachten, also bezahlt seinen Gutachter. Im Regelfall schreiben die Hersteller das Gutachten aus und wählen sich dann den günstigsten oder den lokal nächsten - wie auch immer - der dann eben für sie das Gutachten erstellt. Für das ULD gibt es eine Gebührenordnung, sie steht im Internet. Da bewegen sich die Entgelte nach Tagessätzen, ein Tagessatz kostet bei uns 560 €. Sie können davon ausgehen, dass die Prüfung eines Gutachtens so im Durchschnitt etwa 2 Tage dauert; bei größeren Verfahren wie Microsoft dauerte es ein bisschen länger, weil es ein erheblich komplizierteres Verfahren war, wo mehr Unterlagen zu prüfen waren. Wie teuer das Gutachten für den einzelnen Hersteller ist, wissen wir nicht, weil es ein rein privatwirtschaftliches Verhältnis ist. Das ist übrigens auch nicht anders als bei den Sicherheitszertifizierungen, die das BSI, das Bundesamt für die Sicherheit in der Informationstechnik, vornimmt, oder die nach anderen international gebräuchlichen Standards, wie z.B. BS 1799, der ein britischer Standard ist, oder der CobIT, das ist ein amerikanischer Standard, auch durchgeführt werden. Warum ist das Verfahren bei uns zweistufig? Es ist deswegen zweistufig, weil wir auf diese Art und Weise als ULD eine Qualitätssicherung vornehmen. Wir haben ja unterschiedliche Gutachter, die diese Produkte prüfen. Und man muss jetzt aufpassen, dass der Hersteller, der sein Gutachten quasi kauft, auf diese Art und Weise ein Dumping über Marktpreise, ein Qualitätsdumping einleitet. Deswegen diese Zweistufigkeit, dass wir als ULD noch mal auf das Gutachten gucken. Wir wissen aus den Gesprächen mit unseren Herstellern, die sich das Produkt bei uns haben zertifiziert lassen, dass sie genau aus diesem Grund sich auch auf das Gütesiegel eingelassen haben, weil sie mit dem ULD eine öffentliche unabhängige Einrichtung haben, die die letzte Qualitätssicherung übernimmt. Das ist übrigens

auch explizit - können Sie auch entsprechend nachfragen - der Grund, warum sich Microsoft nach langem Suchen auf dem internationalen Markt für das Gütesiegel in Schleswig-Holstein entschieden hat. Wie gesagt, wir wollen letztendlich ein Zertifikat von einer öffentlichen und unabhängigen anerkannten Stelle. Nun kam das Argument von Ihnen u.a. Herr Abel, dass es doch ein bisschen anrühlich wäre, wenn die Aufsichtsbehörde gleichzeitig auch eine solche Zertifizierung vornimmt. Da möchte ich Sie erst mal darauf hinweisen, dass in § 38 BDSG selber eine Beratungsaufgabe der Aufsichtsbehörde drinsteht. Die Aufsichtsbehörde muss beraten. Wir haben das Instrument der Vorabkontrolle, insbesondere im behördlichen Bereich. Da habe ich noch nie gehört, dass im Rahmen der Vorabkontrolle sich die Datenaufsichtsbehörde möglicherweise selbst gebunden hätte. Wir haben im Bereich der Selbstregulierung in § 38 a BDSG, wo sozusagen selbstregulative Mechanismen vorgelegt werden, das Gleiche auch im internationalen Datentransfer, die ebenfalls von der Aufsichtsbehörde gebilligt werden müssen, da ist auch noch keiner auf die Idee gekommen, das zu kritisieren. Im Gegenteil, die Selbstbindung ist ja gerade gewünscht, weil sie auf diese Art und Weise auch Rechtssicherheit verschafft. Im Regelfall stoßen wir auf eine Zweitprüfung eines Gütesiegels immer dann, wenn ein gütegesiegeltes Produkt im Realeinsatz in eine bestimmte Systemumgebung implementiert wird. Wenn ein Ratsinformationssystem als Produkt ein Gütesiegel hat, und in der Gemeinde Norderstedt dann eingesetzt wird, dann prüfen wir natürlich die Implementierung dieses Produkts: Sind Sicherheitseinstellungen verändert worden, ist die Administration so, wie es im Handbuch vorgesehen ist, usw., das ist der entscheidende Punkt.

Daneben gibt es bei uns auch eine Auditierung von Verfahren, aber nur aus Rechtsgründen im behördlichen Bereich. Wir sind nicht in der Lage, aus Rechtsgründen anders zu auditieren als Behörden. Da auditieren wir Datenschutzmanagement und Verfahren. Das reicht vom kommunalen Bereich, z.B. an Internetanbindung bis hin zur Personaldatenverarbeitung bis hin zu unserem Landesnetz in Schleswig-Holstein, was wir auditiert haben. Oder jetzt als ein laufendes Auditverfahren, um Ihnen nur eine Größenordnung zu geben, das Rechenzentrum unseres Dienstleisters Dataport, eine Anstalt des öffentlichen Rechts mit ungefähr 1.300 Mitarbeitern, die die Governmentverfahren für Schleswig-Holstein, Hamburg und Bremen betreuen. Darüber hinaus haben wir ein laufendes Auditverfahren, in dem landwirtschaftliche Subventionen nach EU-Anforderungen vergeben werden. Da geht es um die Größenordnung von 600 Mio. €, die jedes Jahr darüber ausgeschüttet werden. Auch da sind wir bereits in einem umfassenden Datenschutz- und Sicherheitsauditprozess drin.

Die Frage nach den Maßstäben, die gestellt worden sind. Bei Auditverfahren, da sagte ich bereits, Kernpunkt ist das Datenschutzmanagement. Es muss definierte Zuständigkeiten und Prozesse geben bei Sicherheits- und Datenschutzvorfällen in Verbindung mit allen konkreten Verfahren, sonst macht das keinen Sinn. Ich glaube nicht, dass die Frage so „kriegsentscheidend“ ist, ob man eine nach oben offene

Richterskala braucht und es eine Datenschutzskala gibt. Ich glaube, das kann man dem Wettbewerb überlassen. Das wird sich von selbst ergeben.

Sorgen haben die Unternehmen, die auditieren wollen, die bei uns anfragen, aber die wir wieder nach Hause schicken müssen. Nur als Beispiel: Ein Unternehmen, das Scoringverfahren anbietet, hat uns gefragt, ob wir das nicht auditieren können. Können wir nicht, aus Rechtsgründen. Eine Partnerschaftsbörse im Internet - klar, dass es da besondere Vertraulichkeitserwartung gibt - hätte ganz gerne ihr Produkt auditiert. Können wir aus Rechtsgründen nicht, weil das kein Behördenbereich, sondern privatwirtschaftlicher Bereich ist. Die Frage: Wer soll jetzt auditieren? Ich sagte bereits, dass eine Menge guter Gründe dafür sprechen, dass es die jeweiligen Datenschutzinstanzen machen, weil sie die größte Autorität auch nach außen gegenüber dem jeweiligen Betroffenen haben. Und dass das auch das Kernargument ist, warum sich Microsoft auf das umständliche und langwierige Zertifizierungsverfahren beim ULD letztendlich auch eingelassen hat. Wenn Modelle diskutiert werden, wie Industrie- und Handelskammern oder das BSI, dann möchte ich nur den knappen Hinweis geben, dass der Bundesgesetzgeber nicht die Verwaltungskompetenz hat, sondern die Verwaltungskompetenz liegt bei den Ländern. Der Bund sollte eine Regelung treffen, damit Auditverfahren auch für den privatwirtschaftlichen Bereich auf freiwilliger Basis möglich und zulässig sind. Der Bund könnte auch Entlastung schaffen, indem er allgemeine Akkreditierungsregeln für die Gutachter, ihre Sach- und Fachkunde, schafft, weil das Berufsausübungsregelung nach Art. 12 GG ist. Das sollte man auch nicht in einer Verordnung machen, das sollte man sauber in einem Gesetz machen, damit man auch dem einen oder anderen Gutachter die Akkreditierung entziehen kann, wenn es notwendig ist. Ist bei uns zwar noch nicht vorgekommen, könnte aber mal der Fall sein. Aber die Ausführung, wer dann die jeweiligen Institutionen sind, das muss man den Ländern überlassen. Jetzt haben wir das Problem, so viel Gütesiegelverfahren gibt es ja gar nicht. Wir haben jetzt 35. Alles Produkte, die in der Schleswig-Holsteinischen Landesverwaltung eingesetzt werden können. Wenn man jetzt anfängt, das in die Fläche auszurollen, und 16 Länder auffordert, entsprechende Institutionen vorzusehen. Ich glaube, das könnte leicht zu einer Überforderung oder zu einer Überbürokratisierung führen. Ich denke, dass der richtige Weg wäre, wenn der Bund sich an dieser Stelle heraushält, er aber die Länder auffordert, im Wege einer Ländervereinbarung, Staatsvertrag, Verwaltungsabkommen - müsste man noch prüfen - festzulegen, ob diese Rolle nicht von einzelnen Ländern für andere übernommen wird. Das ULD für den Norden, Saarland oder Bayern für den Süden, was auch immer, kann man sich als Modell so vorstellen. So wie in anderen Bereichen auch kooperativ Verwaltungsaufgaben übernommen und geleistet werden, so wäre das in diesem Bereich durchaus möglich.

Vors. **Sebastian Edathy**: Vielen Dank. Als nächster Sachverständiger hat das Wort Herr Dr. Dix, nein. Herr Dr. Bizer noch mal:

SV Dr. Johann Bizer: Microsoft ist ein Produkt, Windows Update Server haben die als Gütesiegel. Wir haben nicht Microsoft als Unternehmen, sondern wir haben ein spezifisch definiertes Produkt von Microsoft zertifiziert. Update Server, von dem regelmäßig die Updates eingespielt werden zwischen ihrem Rechner und dem Server, wo die Kommunikation läuft. Zertifiziert worden ist dieser Mechanismus des Updates. Dass da nichts passiert, was der Betroffene nicht weiß oder was mit den geltenden Datenschutzbestimmungen nicht in Einklang steht. Das passiert dadurch, dass Microsoft gegenüber den Gutachtern die Dokumentation ihres Verfahrens aufgedeckt hat und diese in einem Langgutachten uns gegenüber beschrieben haben und die Datenschutzkonformität technisch und rechtlich geprüft haben. Und wir dann als Zertifizierungsstelle, wie in anderen internationalen Standards übrigens auch, wir dann eine Plausibilitätskontrolle vorgenommen haben nach den geltenden Datenschutzbestimmungen. Wir machen keine Skalierung zwischen sehr gut oder ausreichend, sondern es gibt das Gütesiegel oder es gibt es nicht.

Vors. **Sebastian Edathy:** Vielen Dank. Jetzt hat in der Tat das Wort Herr Dr. Dix.

SV Dr. Alexander Dix: Herr Bürsch, Sie haben nach den wirtschaftlichen Anreizen gefragt. Die sind aus meiner Sicht der entscheidende wirtschaftliche Anreiz, den der Gesetzgeber geben sollte. Es ist in der Tat eine bevorzugte Auftragsvergabe an Unternehmen, die Produkte mit Siegeln oder möglicherweise auch Dienstleistungen mit Gütesiegeln anbieten. Vorbild für eine solche Regelung könnte das brandenburgische Datenschutzgesetz sein, das ausdrücklich vorsieht, dass Produkte und Verfahren, deren Vereinbarkeit mit den Regeln des Datenschutzrechts in einem förmlichen Verfahren geprüft und positiv bewertet worden sind, vorrangig berücksichtigt werden sollen. Ich bin nicht sicher, ob es eine ähnliche Regelung in Schleswig-Holstein auch gibt. Es ist wohl so. Also diese beiden Länder haben es vorgemacht. Ich meine, eine solche Bevorzugung ist wettbewerbs- als auch vergaberechtlich unproblematisch, wenn sichergestellt ist, dass es nicht so verstanden wird, der teure Anbieter mit einem guten Datenschutzkonzept seinen Preisnachteil wettmachen könnte. Datenschutz kann immer nur ein positiver Faktor sein in einer Gesamtauftragsvergabe - wie etwa auch im Bereich der Gleichstellung der Geschlechter oder in anderen gesellschaftlich gewünschten Entwicklungen hat der Gesetzgeber entsprechende Konzepte auch schon verfolgt. Das sollte der Bundesgesetzgeber aber, wenn er ein Auditgesetz verabschiedet, durch eine Änderung des § 9a Bundesdatenschutzgesetz ausdrücklich vorsehen, damit dieser Anreiz für die Unternehmen auch deutlich wird. Damit sie sich nicht auf etwas einlassen, von dem sie gar nicht wissen, was es ihnen bringt.

Vors. **Sebastian Edathy:** Frau Philipp, wenn es Nachfragen gibt, dann melden Sie sich auch, sonst ist das alles nicht im Protokoll. Frau Philipp habe ich jetzt so verstanden, dass Sie eine Nachfrage haben. Ist das so, dann stellen Sie sie bitte.

Abg. **Beatrix Philipp**: (...) meine erste Bemerkung nicht widerlegt zu sein scheint, das geht eigentlich nur darum - deswegen auch der Zwischenruf, ich bitte um Entschuldigung, das Einhalten der Gesetze zu bestätigen. Ist das richtig?

Vors. **Sebastian Edathy**: Herr Dr. Dix.

SV **Dr. Alexander Dix**: Das ist richtig, das ist der zentrale Schritt, den kann man sich bestätigen lassen durch ein Gütesiegel, ohne dass die Aufsichtsbehörde vorher erst einmal prüfen muss.

Vors. **Sebastian Edathy**: Dann hat jetzt das Wort der Bundesdatenschutzbeauftragte.

SV **Peter Schaar**: An mich war die Frage gerichtet: Wie sieht es aus mit den kleinen und mittleren Unternehmen? Das schleswig-holsteinische Beispiel belegt durchaus, dass gerade kleine und mittlere Unternehmen im Datenschutzgütesiegel eine Chance sehen in einem Wettbewerb, bei dem ansonsten die großen sehr viele Vorteile haben, kein Alleinstellungsmerkmal zu gewinnen. Wenn jetzt so große wie Microsoft - und das sind ja sozusagen die Größten, was den Bereich der Software angeht - auch aufspringen, dann geht dieser Vorteil möglicherweise ein wenig verloren, aber im Sinne des Datenschutzes. Grundsätzlich denke ich, dass kleine und mittlere Unternehmen hier durchaus eine Chance haben. Die Frage ist häufig damit verbunden: Wie hoch sind die Kosten, die durch Audit verursacht werden? Ich denke, da muss man natürlich immer die verschiedenen Produkte anschauen oder die Arten der Gütesiegel, die dann vergeben werden. Jedes Verfahren oder Produkt muss unabhängig begutachtet werden, und die Begutachtung gibt es nicht umsonst, d.h. einen gewissen Preis müssen diese Audits auch haben. Geschenkt wäre ein solches Gütesiegel nichts wert. Wie man dann den Prozess ausgestalten kann, darüber kann man ggf. noch sprechen, aber das ist nicht Ihre Frage gewesen.

Vors. **Sebastian Edathy**: Vielen Dank. Dann hat als nächstes das Wort für die Fraktion BÜNDNIS 90/DIE GRÜNEN Frau Stokar von Neuforn. Nein, tut mir leid, Herr Korte hat das Wort für die Fraktion DIE LINKE..

Abg. **Jan Korte**: Wir sind größer und stärker, da möchte ich doch drauf bestehen. Ich habe drei ganz kurze Fragen. Zum einen noch mal die Frage an Frau Sasse, was Sie eben in Ihren Ausführungen meinten, da sind Sie recht vage geblieben im Hinblick auf die Kosten, insbesondere für kleine und mittlere Unternehmen. Da sprachen Sie darüber, man müsste eine Balance herstellen. Das würde ich gerne etwas konkreter wissen, was Sie damit meinen. Mit der zweiten Frage würde ich mich noch mal an Herrn Bizer wenden. Es würde mich interessieren - ich finde es auch sehr gut, und da herrscht hier ja offensichtlich Einigkeit, wie in Schleswig-Holstein verfahren wird - ob Sie Erfahrung haben, wie es in anderen Ländern gehandhabt wird, ob es da einen

Bezug auf Schleswig-Holstein gibt. Und wenn es den gibt, wird er offenbar negativ sein, sonst hätten ja alle anderen Länder das übernommen, würde ich logischerweise annehmen. Da würden mich die Argumente interessieren, die dort vorgebracht werden. Wenn Sie das kurz berichten könnten. Und dritte und letzte Frage an Herrn Neumann. Mich würde noch interessieren, wie weit die Überlegungen in Mecklenburg-Vorpommern sind, insbesondere was die Akkreditierungsverfahren für Gutachter und Produkte angeht. Da gab es ja reichlich Überlegungen und Vorschläge, wie weit ist das gediehen?

Vors. **Sebastian Edathy**: Dann zunächst Frau Sasse, bitte.

SV **Cornelia Sasse**: Herr Korte, vielen Dank für die Frage. Es tut mir leid, dass ich mich missverständlich ausgedrückt habe. Ich möchte einfach anregen, dass man zumindest zu definieren hat, welchen Umfang dieses Datenschutz-Audit zu haben hat: Produkt, Verfahren, Prozesse, ganze Unternehmen. Insofern sehe ich dort eine Gefahr, dass kleine und mittlere Unternehmen ins Hintertreffen geraten, wenn sie sich den Kostenfaktor nicht leisten können, den vielleicht der Anspruch an ein Audit an sich hat, wenn nicht klar definiert ist, was es zu auditieren gilt. Ist Ihre Frage damit beantwortet?

Vors. **Sebastian Edathy**: Sehr schön, dann Herr Dr. Bizer, bitte.

SV **Dr. Johann Bizer**: Wie verhalten sich andere Länder dazu? Die Schweiz hat gerade eine eigene gesetzliche Regelung geschaffen und hat unseren Gütesiegel-Anforderungskatalog mit unserer Zustimmung wortwörtlich übernommen. In Japan gibt es Auditregelungen, gibt es übrigens auch in deutschsprachiger Auflage von der von mir herausgegebenen Zeitschrift „Datenschutz und Datensicherheit“, die ich Ihnen gerne zur Verfügung stellen kann. Herr Prof. Rossnagel hat vor zwei oder drei Jahren dort einen längeren Forschungsaufenthalt gehabt und hat das dokumentiert. Wir haben vor kurzem einen japanischen Kollegen bei uns gehabt, der seine Erfahrung mit unserem Verfahren abgeglichen hat. Und als Drittes: Die Europäische Kommission hat Schleswig-Holstein für dieses Konzept von Gütesiegel und Audit im Jahr 2004 einen Innovationspreis verliehen. Die Europäische Kommission hat uns gebeten, einen Antrag zu stellen und Partner zu suchen, um im Rahmen eines so genannten Itemprojektes die Europäisierung dieses Datenschutz-Gütesiegel-Produktes voranzutreiben. Item bedeutet, das sind aus der Perspektive der Kommission Verfahren oder Produkte, die es wert sind, auch in andere Länder exportiert zu werden, möglicherweise mit bestimmten Anpassungen. Dieses Projekt „Europrice“ genannt, wird am 1. Mai starten. Es sind beteiligt Partner aus Schweden, aus Frankreich, aus Spanien, aus Italien und anderen Ländern. Sie sehen daran, dass der Datenschutz-Audit-Zug rollt. Und mit dem Microsoft-Gütesiegel, um das auch noch mal klar zu sagen, können Sie das Rad sowieso nicht mehr zurückdrehen. Es gibt es einfach. Und derjenige der anfängt, an den Standards von Schleswig-

Holstein rumzukritisieren, der muss sich ja die Frage stellen, was man aus dem Standortvorteil, den man jetzt gerade errungen hat, dass Microsoft nach Deutschland kommt und sagt, wir wollen in Deutschland ein Gütesiegel nach den in Deutschland gebräuchlichen europäischen Datenschutzregeln haben, wie man mit diesem Standortvorteil umgeht. Da kann ich nur sagen: Bitte hegen und pflegen, aber nicht zertrümmern.

Vors. **Sebastian Edathy**: Herr Neumann, bitte.

SV Karsten Neumann: Ja, vielleicht das Gütesiegel auch noch ausbauen, also von den positiven Erfahrungen lernen. Wir haben den Diskussionsprozess auch in Mecklenburg-Vorpommern, also die gesetzliche Regelung - genauso wie sie Herr Dr. Dix von Brandenburg, glaube ich, zitiert hat - im Datenschutzgesetz seit 2002, dass Produkte bevorzugt berücksichtigt werden sollen, die eine solche Auditierung durchgemacht haben. Auch bei uns fehlt bis heute die Rechtsverordnung und zwar - unter Hinweis des Innenministeriums unseres Landes, dass der Bundesgesetzgeber an der Umsetzung des § 9a arbeitet - bis der Bund hier das geregelt hat, wir eine solche Regelung nicht bräuchten. Das ist schade, insbesondere deshalb, weil die IHKs es auch so sehen. Jedenfalls die IHK in Mecklenburg-Vorpommern hat entsprechende Initiativen bisher so beantwortet, dass offensichtlich ein Bedarf nicht bestünde und man deshalb unter Hinweis auf Deregulierungsbemühungen davon absehen solle. Das zeigt für mich nur, dass man sich mit dem Thema nicht beschäftigt hat. Denn Auditierung ist Deregulierung. Denn die Auditierung führt dazu - und Frau Philipp, Sie reiten aus meiner Sicht völlig zu Recht darauf herum - natürlich stellt das Audit die Kompatibilität mit den Datenschutzbestimmungen fest. Wir haben aber leider die Situation, dass in einer Stadt, - beispielsweise meiner Heimatstadt Stralsund - wenn eine Ausschreibung gemacht wird, kaum jemand tatsächlich in der Lage ist, die datenschutzrechtliche Zulässigkeit eines angebotenen Produktes, sagen wir mal für ein Krankenhausinformationssystem, zu bewerten. Niemand kann es ohne eine externe Beratung oder ohne die Einbeziehung eines Externen. Und das, was das Unternehmen, das dieses Produkt anbietet, in Mecklenburg-Vorpommern 35 Mal machen müsste - ich glaube so viele Krankenhäuser haben wir noch - macht es dann nur einmal und bekommt für diese einmalige Prüfung die Bestätigung der Aufsichtsbehörde, dass sie diese Einschätzung auch teilt. Und diese Bestätigung wirkt natürlich auch gegenüber allen anderen Anwendern. Das Interessante daran ist, dass Unternehmen bei mir anfragen. Die Unternehmen brauchen oder suchen genau diese Bestätigung der Aufsichtsbehörde, weil bspw. der Anbieter einer Arztsoftware zu mir sinngemäß sagt: „Jeder Arzt, zu dem ich gehe und mein Produkt anbiete, fragt mich: 'Ist das zulässig, was du hier tust?' Und jeder muss sich gegenwärtig auf mein Wort verlassen. Wenn sie es mal geprüft haben, kann ich doch dieses Siegel jedes Mal verwenden.“ Insofern trägt die Auditierung auch zu einer vielfachen Potenzierung der Prüftätigkeit der Datenschutzbeauftragten bei. Wir könnten endlich sozusagen aus einer Stunde

Arbeit 1000 Stunden für Datenschutz machen, zumal ein Produkt vielleicht 1000 Mal verkauft wird und nur einmal geprüft werden müsste, von uns. Deshalb bin auch ich ein starker Verfechter des Verfahrens, wobei wir uns an die Erfahrung Schleswig-Holsteins angelehnt haben. Bei uns ist es gegenwärtig so, auf die Frage von Herrn Dr. Bürsch, dass unsere Unternehmen jetzt nach Schleswig-Holstein gehen und sich dort zertifizieren lassen, weil der Effekt der gleiche ist. Zu dem Problem, was Prof. Abel ansprach: auch darüber haben wir intensiv diskutiert. Natürlich, es sind 16 plus 1 Aufsichtsbehörden. Gerade deshalb - denke ich - brauchen wir einen bundeseinheitlichen Rahmen. Aber wer kann es sich leisten, die teilweise schwierige Frage zu beantworten, ob ein Produkt nicht nur in Schleswig-Holstein zulässig ist, sondern auch in Bayern oder in Nordrhein-Westfalen? Wer soll das besser können als die Aufsichtsbehörden in diesen Ländern, die nämlich die landesrechtlichen Unterschiede, die sich manchmal auch technisch auswirken können, am besten kennen. Beispielsweise ist Auftragsdatenverarbeitung in Bayern, in bayerischen Krankenhäusern, gesetzlich nicht zulässig. Wer sollte so eine Arbeit leisten können, wenn nicht die Aufsichtsbehörden. Ich rede jetzt davon, dafür zu sorgen, dass der Kriterienkatalog tatsächlich einheitlich bundesweit ist. Der Katalog, nach dem wir dann prüfen, muss von allen Aufsichtsbehörden akzeptiert werden.

Zwischenrufe (nicht rekonstruierbar)

SV **Karsten Neumann**: Genau, sonst wird es richtig bunt. Wenn wirklich der Gutachter, der letztendlich diese Arbeit zu leisten hätte, auch noch landesrechtliche Differenzen zu berücksichtigen hätte, würde das auch die Kosten vervielfachen.

Vors. **Sebastian Edathy**: Vielen Dank. Der Kollege Korte hat signalisiert, dass er eine Nachfrage hat. Hat sich erledigt. Dann hat jetzt nun doch die Kollegin Stokar das Wort. Bitte.

Abg. **Silke Stokar von Neuforn**: Ich danke. Zwei Vorbemerkungen: Ich habe schon während der ganzen Regierungszeit unter Rot-Grün nicht verstanden, warum es gegen das Datenschutz-Audit und gegen die Schaffung von Datenschutzütesiegel so eine unglaubliche Blockade gibt. Die Entwicklung, die darauf hin eingesetzt hat im internationalen Bereich, ist eine ähnliche wie bei Feinstaub oder Dieselerusspartikel. Diese in Deutschland gut entwickelte Idee, was das UDL aus Schleswig-Holstein gesagt hat, wird von anderen europäischen Ländern übernommen. Amerika hat ein Wirtschaftsinteresse daran, mit deutschen Gütesiegeln in den deutschen IT-Markt hineinzugehen. Die Blockade der Wirtschaft ist für mich nicht nachvollziehbar. Na gut, über die Blockaden im Innenministerium bei dem Wort „Datenschutz“ müssen wir anders hinwegkommen. Meine Fragen richten sich an zwei Personen, einmal an Herrn Thorun: Können Sie noch mal darlegen, wie aus Sicht der Verbraucherinnen und Verbraucher ein Gütesiegel gestaltet sein muss, damit es zwei Dinge sicherstellt, nämlich dass tatsächlich Vertrauen in das Gütesiegel vorhanden ist und dass Transparenz gewährleistet ist zu den einzelnen Produkten. Ich möchte diese Frage auch noch an Herrn Prof. Abel stellen, weil Sie das BSI ins Gespräch gebracht

haben, auch Microsoft gehört in diese Fragestellung mit hinein. Können Sie hier wirklich noch vertreten, dass das BSI als eine Behörde fürs BKA Trojaner entwickelt, d.h. ein Eigeninteresse hat, dass es Datensicherheit nicht mehr gibt, dass sie eindringen können in private PCs. Dass die gleiche Behörde, von denen öffentlich bekannt ist, dass sie sozusagen als „Hacker“ agieren, gleichzeitig die Datensicherheit zertifizieren können. Für mich ist seit dieser Entwicklung, also der Hackersoftware, das BSI beim Thema Datensicherheit niemand mehr, dem ich vertraue; der wird mir ein Verfahren anbieten, damit er seine Trojaner leichter installieren kann. Da würde ich gerne wissen, wie da Ihre Meinung ist. An Herrn Schaar ist die Frage schon mehrfach gestellt worden: Wie muss eine bundesgesetzliche Regelung aussehen, damit wir nicht 16 unterschiedliche Regelungen haben und dazu noch 20 Anbieter aus der Wirtschaft, die alle ihre eigenen Bedingungen für ein Gütesiegel entwickeln? Danke.

Vors. **Sebastian Edathy**: Zur Beantwortung bitte zunächst Herr Dr. Thorun.

SV **Dr. Christian Thorun**: Sie haben die grundsätzliche Frage aufgeworfen, welche Kriterien muss ein Gütesiegel erfüllen, damit es dann auch tatsächlich von den Verbrauchern angenommen wird. Das eine ist, dass wir klare Regelungen brauchen und diese Regelungen dürfen nicht landesweit gelten, sondern sie müssen deutschlandweit gelten und auch am besten europaweit und vielleicht sogar weltweit. Da möchte ich den Gedanken von Herrn Bizer aufnehmen. Es geht jetzt darum, Weichen zu stellen, dass wir wirklich die guten Beispiele, die wir in Deutschland haben, und die Maßstäbe, die hier gesetzt worden sind, katapultieren und mit in den europäischen Raum hineinragen und dann halt vielleicht durchaus weltweit zum Erfolgsschlager machen. Aber das bedarf, was auch Herr Dix angeregt hat, dass wir nämlich die Nachfrageseite hier nutzen, um die Nachfrage nach diesen Gütesiegeln zu vergrößern, um die Unternehmen zu belohnen, die tatsächlich die zusätzlichen Kosten erst mal auf sich nehmen. Also klare Kriterien, die nicht nur deutschlandweit, sondern am besten europaweit oder weltweit gelten. Das zweite ist die Glaubwürdigkeit. Das, was in einem Gütesiegel ausgesagt wird, muss von einer unabhängigen Instanz nachgeprüft werden, sonst glaube ich dem ja nicht, was irgendjemand selbst über sich behauptet oder von irgendwelchen Stellen, denen ich nicht Glauben schenke, behauptet wird, also die Unabhängigkeit. Und das Dritte ist das Prinzip der Sichtbarkeit. Das haben wir auch gesehen, z.B. - es mag zwar etwas sachfremd klingen - aber dieses Beispiel der Eierkennzeichnung finde ich so wunderbar. Seitdem auf den ersten Blick erkennbar ist, welche Eier aus der Legebatterie kommen oder aus der Freilandhaltung, steigt die Nachfrage nach den biologischen oder nach Freilandeiern, weil es auf den ersten Blick ganz klar für jeden Verbraucher am Produkt erkennbar ist, woher es kommt. Und gerade wenn wir über Internetdienstleistungen reden oder technische Dienstleistungen, wie Herr Bizer das Beispiel dargestellt hatte von Microsoft. Es ist für den Verbraucher, wenn er ein Update fährt, in keinsten Weise erkennbar, was jetzt da eigentlich im Hintergrund

alles passiert, welche Daten dort ausgetauscht worden sind, welche Informationen über mein Betriebssystem, über die Programme, die dort gespeichert sind, in welcher Form übertragen werden. Und genau um diese für den Verbraucher unsichtbaren Prozesse irgendwie sichtbar zu machen, brauchen wir die Prüfung Externer, die den Sachverstand haben und überhaupt den Einblick bekommen, dieses zu überprüfen. Und deswegen ist ein Label so wichtig, weil ein Label verborgene Produkteigenschaften sichtbar macht. Ich hoffe, dass das die Frage beantwortet hat.

Vors. **Sebastian Edathy**: Vielen Dank. Dann als nächster Sachverständiger Herr Prof. Abel, bitte.

SV **Prof. Dr. Ralf Bernd Abel**: Mein Vorschlag, das BSI, betrifft natürlich vor allem die technische Kompetenz. Wenn Sie einwenden, ob es nicht vielleicht verbrannt ist, ist das sicherlich ein Argument, über das man nachdenken muss, also ob hier Verlässlichkeit, Vertrauenswürdigkeit besteht. Allerdings wenn man sich anschaut, was in der IT-Welt so abläuft, dann ist es doch so, dass an ganz vielen Stellen ehemalige Hacker sitzen - sehr erfolgreiche Hacker - die Sicherheitsberatung betreiben und dies sehr gut machen. Ich möchte nicht einer deutschen Behörde unterstellen, dass sie etwas Gesetzwidriges tut. Ich glaube auch nicht, dass Sie das unterstellt haben. Es wäre sicherlich zu überlegen, wo Grenzen sind, vielleicht werden die Hacker dadurch zu ehemaligen Hackern. Ich denke, wir müssen auf die Kompetenz schauen und auf die Vertrauenswürdigkeit. Das ist natürlich eine Frage, die Sie an dieser Stelle stellen, die ich hier nicht endgültig werde beantworten können. Man muss sicher sein können, und das ist eigentlich mein Anliegen, dass eine unabhängige Behörde als staatliche Stelle, die nicht von Wirtschaftsinteressen abhängig ist und abhängig gemacht werden kann, hierfür zuständig ist. Und soweit stimme ich mit Herrn Bizer überein - es ist vielleicht mehr die Überlegung, das zweistufige Verfahren vielleicht auf zwei Behörden zu verteilen, wobei das eine die Zertifizierung ist und das andere die Überprüfung. Ich denke dabei auch an die Tatsache, dass mit Letzterer nicht nur 16, sondern 16 plus eine Behörde zu tun haben. Erfahrungen aus dem Zusammengehen der Länder sind manchmal gut, aber nicht immer. Und ob da dann so schnell etwas daraus wird, wenn der Bundesgesetzgeber hier tätig wäre, steht dahin. Da bin ich vielleicht mehr auf der Seite des Bundesgesetzgebers, um einen verlässlichen Rahmen zu schaffen.

Vors. **Sebastian Edathy**: Das Wort hat jetzt Herr Schaar.

SV **Peter Schaar**: Was kann man tun, um eine Zersplitterung zu vermeiden? Was die Aufsichtszuständigkeiten anbelangt, haben wir ja im Datenschutz - das wird von der Wirtschaft durchaus nachvollziehbar auch beklagt - leider vielfältige Aufsichtsbehörden mit unterschiedlichen - teilweise widersprüchlichen - Ansätzen und die Frage ist: Wird das ganze ins Quadrat gehoben, wenn wir noch die Gütesiegel bekommen? Das ist natürlich eine Befürchtung, die vorhanden ist und

deshalb denke ich, muss man hier einen bundesgesetzlichen Rahmen ziehen. Der Bundesgesetzgeber sollte sich nicht raushalten - das möchte ich hier ganz ausdrücklich sagen -, sondern er sollte bestimmte Vorgaben im Hinblick auf dieses Gütesiegel schaffen, da gibt es auch kompetenzrechtlich überhaupt keine Probleme. Einmal sollte er festlegen, was überhaupt ein solches Gütesiegel ist, und er sollte Festlegungen zum Vergabeprozess treffen. Ferner sollte er etwas zu den Kriterien sagen, wobei man diese Kriterien sicherlich eher abstrakt formulieren muss, da wir eben unterschiedliche gesetzliche Regeln haben, im Bundesdatenschutzgesetz, in den Spezialnormen, dann in Bezug auf bestimmte Länderbesonderheiten, wo landesrechtliche Zuständigkeiten bestehen. Das kann sicherlich der Bundesgesetzgeber nicht im Detail abbilden, aber in abstrakter Weise kann er das sehr wohl tun.

Ggf. könnte er auch Festlegungen treffen über die Folgen der Vergabe. Soll sie überhaupt Rechtsfolgen haben und welche Rechtsfolgen könnten das sein, etwa in Bezug auf den Einsatz von Produkten in der Bundesverwaltung, auf die Landesverwaltung kann er da sicherlich keinen Einfluss nehmen. Aber er könnte z.B. mit Blick auf die Aufsichtstätigkeit der Aufsichtsbehörden bestimmte Vorgaben treffen. Schließlich könnte er auch den Akkreditierungsprozess festlegen, d.h. die Anforderungen an die Gutachter und auch bestimmte Sanktionsmechanismen für fehlerhaftes Arbeiten. Das kann alles der Bundesgesetzgeber tun. Er sollte darüber hinaus - das ist sicherlich ein Punkt, über den noch mal länger diskutiert werden muss - gewährleisten, dass diese Gütesiegel einerseits eine hohe Qualität haben und dass sie im Prinzip auch länderübergreifend anerkannt werden. Letzteres ist sicherlich mit das Schwierigste. Man könnte auch versuchen, dies über einen Staatsvertrag zu regeln, aber ich bin nicht so sicher, ob das tatsächlich der Königsweg ist. Bei einer landesgesetzlichen Regelung könnte man durchaus auch an eine Prozedur denken, die die Verwaltungskompetenz der Länder nicht berührt. Ich hätte keine besondere Sympathie dafür, als oberste Gütesiegelinstanz das BSI einzusetzen, da es eine ganz andere Aufgabenstellung hat. Auch der Bundesdatenschutzbeauftragte ist im Hinblick auf die begrenzte Aufsichtszuständigkeit sicherlich nicht unbedingt die ideale Instanz, bei der man das ansiedeln sollte. Insofern denke ich, spreche ich auch wirklich nicht pro domo. Wichtig ist allerdings, dass man die Frage beantwortet - Herr Bizer hat ja gesagt, es gäbe da keine Alternative, darüber muss vielleicht noch mal nachgedacht werden - muss es ein zweistufiges Verfahren sein? Gibt es nicht auch alternative Mechanismen, die eine entsprechende Qualität der Gütesiegel sichern? Wenn es kein zweistufiges Verfahren gäbe, würden insbesondere die Anforderungen an die Kriterien und an die Akkreditierung und möglicherweise auch die Beanstandung von Gütesiegeln durch die Aufsichtsbehörden in einer bundesgesetzlichen Regelung festzulegen sein. Wir sind uns völlig einig, dass es hier nicht einen „Down-Sizing-Prozess“ geben darf, wo letztlich auch nichts an Mehrwert für die Unternehmen übrig bleibt, wenn das Gütesiegel nicht vom Staat vergeben würde, sondern von Gutachtern. Wichtig ist - und das finde ich ganz entscheidend - dass die Gutachter

unabhängig sind. Nicht nur, dass sie qualifiziert sind, sondern dass es keinerlei wirtschaftliche oder sonstige Verquickungen gibt, muss gewährleistet sein. Ich denke, dass auch eine entsprechende Aufsicht stattfinden muss. Im Hinblick auf die Akkreditierung, insbesondere wo die Akkreditierung stattzufinden hat, gibt es sicherlich verschiedene Möglichkeiten, die dann im Gesetzgebungsverfahren noch mal vertieft zu diskutieren sind.

Vors. **Sebastian Edathy**: Vielen Dank. Es hat sich noch der Kollege Tauss gemeldet. Gibt es weitere Kolleginnen und Kollegen, die jetzt zu dem Themenbereich „Datenschutz-Audit“ Fragen haben? Das ist nicht der Fall, denn hat jetzt Herr Tauss das Wort.

Abg. **Jörg Tauss**: Danke schön. Nur eine kleine Vorbemerkung. Ausnahmsweise will ich jetzt mal was ganz Nettes sagen über das BMI. Wir haben Gespräche geführt mit Herrn PSts Peter Altmaier. Und Ergebnis dieses Gesprächs in Sachen Audit war, dass, wenn ein Bedürfnis nach einem Audit vorhanden ist - übrigens auch in der Wirtschaft seitens der Wirtschaftsverbände dies artikuliert wird - dann wolle man auch seitens des BMI dem Wunsch, wie er aus dem Parlament schon mehrfach geäußert worden ist, auch nachkommen. Die Argumente, die gegen das Audit sprechen, werden überwiegend natürlich auch von der Wirtschaft vorgetragen. Meine Fragen gehen jetzt an Herrn Jaspers, Herrn Bizer und Herrn Schaar, nämlich nach den Befürchtungen, die geäußert werden. Herr Jaspers, wir haben oft diskutiert über die Frage „betrieblicher Datenschutzbeauftragter“, Schwächung durch Audit ja oder nein. Wie müsste ein Audit aussehen, das zu einer Stärkung des betrieblichen Datenschutzbeauftragten führt, an einer Schwächung kann ja kein Mensch interessiert sein. Also gibt es Vorstellungen von Ihrer Seite. Dann die ganze Frage - wir haben es ja heute gehört - Unübersichtlichkeit des Bundesdatenschutzgesetzes, schwierige Handhabung des Bundesdatenschutzgesetzes, zum Teil auch Bürokratie durch Bundesdatenschutzgesetz, weil eben der Versuch gemacht wird, viele Sachverhalte mit einem gesetzlichen Rahmen und vielen Einzelbestimmungen zu lösen. Wo könnte uns, Herr Bizer, aus Ihren Erfahrungen heraus - und das würde ich auch Herrn Schaar schlichtweg fragen - ein Audit helfen, auch bei dem, was Herr Prof. Abel beklagt hat, nämlich das Recht wird nicht eingehalten. Das sind doch die Vorteile des Audits, dass man sowohl für die Wirtschaft und natürlich auch für die Konsumenten, die Verbraucher mehr Sicherheit bekommt. Es sind ja erhebliche Vorteile für die Wirtschaft mit dem Auditierungsverfahren verbunden. Da die Bundesregierung dafür wirbt, dass wir hier also gerade bei der Wirtschaft versuchen, Vertrauen für das Audit herbeizuführen, würde ich sagen, wäre es sinnvoll, dass wir jetzt vielleicht zum Schluss dieses Teils der Anhörung noch ein paar Argumente bekommen in diese Richtung. Herr Jaspers, was bringt uns ein Stück weit voran über das hinaus, was Sie verdienstvoller Weise auch schon schriftlich vorgelegt haben, weil dann könnten wir mit DIH, mit Bitcom und mit allen anderen in weiteren Runden diese Frage noch einmal etwas intensiver erörtern. Es will hier niemand was Böses,

sondern wir wollen den Datenschutz befördern im Zusammenhang mit Wettbewerbsvorteilen, im Zusammenhang auch mit nicht mit mehr Bürokratie, sondern mit der Chance, Datenschutz voranzubringen und bürokratische Verfahren mit Hilfe der Auditierung auch möglicherweise zu reduzieren.

Vors. **Sebastian Edathy**: Dann zunächst bitte Herr Jaspers.

SV **Andreas Jaspers**: Ja, ganz kurz. Da muss ich gar nicht überlegen auch hinsichtlich der Frage, die von Frau Philipp schon gestellt worden ist: Warum hat die Wirtschaft mit beiden Beinen auf der Bremse gestanden, als das Thema „Datenschutz-Audit“ aufgekommen ist. Das lag daran - ich wiederhole mich hier - dass im Gesetz steht, ganze datenverarbeitende Stellen werden überprüft und zwar mit Blick auf sämtliche Verfahren, auch der gesamten internen Verfahren, was gar nichts bringt. Letzten Endes wird wieder ein riesengroßer Bürokratiezirkus aufgebracht. Die Diskussion ist ja mittlerweile sehr viel weiter und deswegen sind wir ja pro Dienstleistungs-Audit und Produkt-Audit. Da gibt es ja vernünftige Argumente. Nur, das muss man erst mal langsam aus den Köpfen rauskriegen, dass nicht ganze Unternehmen auditiert werden sollen, denn dagegen haben auch die Datenschutzbeauftragten etwas gehabt. Denn wenn sie mit auditiert werden müssen, da wäre ein externer Auditor gekommen und hätte gefragt: Was tust du denn den ganzen Tag? Die Frage ist, ob das auch mit der Unabhängigkeit des Datenschutzbeauftragten zu vereinbaren wäre. Die Unabhängigkeit des Datenschutzbeauftragten wäre hier erheblich hinterfragt gewesen. Von daher haben sich die Datenschutzbeauftragten, soweit sie lobbymäßig tätig werden konnten, gegen ein solches Audit gestemmt, das sich letzten Endes auf die datenverarbeitende Stelle insgesamt und damit auf sich selber bezieht. Also wird die Frage aufgeworfen, wie kann man die betriebliche Selbstkontrolle auf der einen Seite und das Datenschutz-Audit miteinander harmonisieren. Nun, der Datenschutzbeauftragte sollte in den Prozess praktisch mit eingebunden werden. D.h. das Unternehmen entscheidet nicht gegen den Datenschutzbeauftragten, sondern mit dem Datenschutzbeauftragten für die Durchführung des jeweiligen internen Audits, des Dienstleistungsaudits. Damit wird der Datenschutzbeauftragte nicht originär selber Gegenstand der Auditierung, das würde sich mit seiner Unabhängigkeit beißen. In dem Sinne wäre die Frage gelöst.

Vors. **Sebastian Edathy**: Vielen Dank. Dann Herr Bizer und Herr Schaar.

SV **Dr. Johann Bizer**: Vielen Dank. Da bin ich durchaus einer Meinung mit Ihnen. Es geht nicht darum, ganze Unternehmen zu auditieren, und nach wie vor ist es ein freiwilliges Audit. Und das Unternehmen schneidet seinen Auditbereich zu. Ich denke aber, dass es unerlässlich ist, dass das Datenschutzmanagement auch immer mit ein Bestandteil dieses Auditverfahrens ist. Weil, nur alleine ein Verfahren, ohne dass ich einen Blick hinaufwerfe: „Habt ihr überhaupt einen betrieblichen

Datenschutzbeauftragten? Was macht ihr bei Vorfällen? Wie eskaliert ihr, wenn ihr Auftragsdatenverarbeiter seid? Habt ihr einen Weg definiert, dass es eskaliert zu eurem Auftraggeber, dass der auch Bescheid weiß, ob er seine Kunden informieren muss usw..“ Diesen Managementprozess muss ich auch mit in den Blick nehmen. Aber wie gesagt, man kann das Verfahren ansonsten elegant auch zuschneiden. Es gibt eine Reihe von deutschen Unternehmen, die bereits gute Erfahrungen mit der internen Auditierung haben. Die Telecom ist z.B. ein solches Unternehmen, da ist schon seit Jahren - weit vor dem § 9a BDSG - damit angefangen und die Erfahrung immer weiter verfeinert hat. Oder ein anderes Unternehmen, die ABB als Maschinenbau-Unternehmen. Da gibt es eine ganze Reihe von internen Auditmechanismen, die wollen wir jetzt nicht einem Pflichtaudit unterziehen. Entscheidend ist, dass das Unternehmen sagt, wir wollen definierte Verarbeitungsverfahren, weil die für uns von Bedeutung sind, z.B. im Rahmen einer Verhandlung mit dem Betriebsrat. Oder aber eine Kundendatenbank, einer Kundendatenanwendung oder einer Internetanwendung, wo Kundendaten hineingehen, die wollen wir einem Audit unterziehen. Das sind Mechanismen, die das Unternehmen selbst freiwillig zuschneidet, und dann sagt, okay, da wollen wir ein Zertifikat, um nach Außen auch aktiv im Wettbewerb mit unserer Qualität in Sachen Datenschutz werben zu können.

Noch eine letzte kurze Bemerkung zur Frage der Zweistufigkeit. Wir richten uns in unserer Europäisierung des Gütesiegels und des Auditsverfahren nach der ISO-Norm, internationale Standardnorm 27001. Und die sieht aus Qualitätssicherungsgründen eine Zweistufigkeit vor. Jetzt stellen Sie sich mal vor, dass ein Datenschutzgütesiegel in Portugal verliehen wird, und eins wird in Kiel in Schleswig-Holstein verliehen wird. Da muss ich doch irgendwie einen Mechanismus der Qualitätssicherung schaffen - und den beschreibt die ISO-Norm 27001 -, dass ich sicherstelle, dass die Portugiesen das annähernd genauso sehen wie wir, oder wir das annähernd genauso sehen wie die Portugiesen. Ich brauche immer diesen Mechanismus der Qualitätssicherung, und das ist das, was ich mit Zweistufigkeit meine. Darüber sind wir uns offenbar alle einig.

Vors. **Sebastian Edathy**: Vielen Dank. Herr Schaar.

SV **Peter Schaar**: Da hat sich ja schon ein Problem erledigt. Es geht nicht um die Zweistufigkeit in jedem Verfahren, sondern um eine Qualitätssicherung, das finde ich also dann auch in Ordnung. Zum Thema: Wo kann ein Audit helfen? Ich denke dort, wo Datenschutz eine Rolle im Markt spielt, überall dort. Das ist sicherlich zunehmend der Fall, weil bei allen möglichen Produkten personenbezogene Daten anfallen. Ich denke insbesondere an Versicherungen und an Banken, weil sie mit Informationen handeln, d.h. deren Geschäftszweck gerade der Umgang mit - zum wesentlichen Teil personenbezogenen - Daten ist. In solchen Bereichen kann es einen echten Wettbewerbsvorteil geben, wenn ein Unternehmen bescheinigt bekommt - aufgrund einer unabhängigen Begutachtung -, dass in einem bestimmten Produkt, einer

bestimmten Dienstleistung oder auch - hier möchte ich doch ein bisschen das abschwächen, was Herr Jaspers gesagt hat - auch die gesamten Unternehmensstrukturen datenschutzgerecht gestaltet sind.

Wenn ein Unternehmen nichts weiter macht, als personenbezogene Daten zu verarbeiten wie die SCHUFA, dann kann es ja eigentlich nicht nur darum gehen, allein den Scorewert zu beurteilen. Dies könnte man zwar auch machen, aber es wäre sicherlich sinnvoll, dass man dann schon den Gesamtprozess des Umgangs mit den personenbezogenen Daten einbezieht

Zwischenrufe (nicht rekonstruierbar)

SV Peter Schaar: Deshalb denke ich, das ist auch in § 9a BDSG nicht vorgesehen, dass das Audit nicht das ganze Unternehmen betreffen soll, sondern seine Datenschutzkonzepte. Und wenn es ein Datenschutzkonzept gibt, dann muss es nicht jegliche Form auch eben der Arbeitnehmerdatenverarbeitung umfassen. Das ist völlig richtig. Da kann es ein separates Siegel geben, das finde ich in Ordnung. Die Frage, wo kommt es am schnellsten zu wirtschaftlichen Vorteilen, ist auch leicht beantwortbar: Überall dort, wo elektronische Dienstleistungen erbracht werden. Überall dort, wo das Internet eine Rolle spielt, wo man ggf. auch das Gegenüber nicht kennt, kann ein Audit direkten wirtschaftlichen Vorteil bringen. Ich glaube, das ist der Punkt, wo man sehr schnell zu einem Ergebnis kommt. Mir ist aus den Reihen der Internetwirtschaft immer wieder gesagt worden: Wir wollen eigentlich so etwas haben. Und immer ist große Enttäuschung darüber ausgedrückt worden, dass das nicht vorankommt. Ich denke, dass man sicherlich hier einen Schwerpunkt haben wird und nicht etwa beim Unternehmensaudit.

Vors. **Sebastian Edathy:** Vielen Dank, Herr Schaar. Weitere Fragen hat Frau Kollegin Philipp.

Abg. **Beatrix Philipp:** Herr Dr. Bizer sagte, Microsoft als Beispiel bzw. die Unternehmen schneiden selbst zu. Mir ist das in der ersten Runde so ergangen, als Sie gesagt haben: „Wer Microsoft zertifiziert ... dieses Schnipselchen ...“ Da würde ich den Oberverbraucherschützer fragen, ob Sie das nicht vielleicht als irreführend empfinden, wie es gerade mir passiert ist. Microsoft ist zertifiziert, also würde ich dann schon annehmen, nicht nur beim Update.

Frau Sasse hat eben schon gesagt, wie schnell sich alles ändert. Ich habe große Probleme, wenn es nun selbst zugeschnitten wird. Es ändert sich schnell, d.h. ich müsste zeitlich limitiert werden. Und zwar, entweder ganz kurz, und dann habe ich wieder das Problem mit dem Gutachten. Da ist mir auch immer noch nicht ganz klar: also Ihre Firma, die zugeschnittene Teilchen zertifiziert haben möchte, sucht sich - wenn ich es richtig verstanden habe - selbst einen Gutachter, das ist gesetzeskonform. Und Sie zertifizieren aufgrund dieses Gutachtens, das man sich selbst gesucht hat. Ich kenne das übrigens aus dem medizinischen Bereich, das Bundesinstitut für Arzneimittel und Medizinprodukte hat das immer gemacht. Sie lassen irgendwo prüfen und gucken dann nur, ob geprüft worden ist - mit großen

Schwierigkeiten, wenn ich das mal so sagen darf. Dürfte ich noch mal fragen, ob ich das richtig verstanden habe?

Vors. **Sebastian Edathy**: Erst mal, gibt es noch Fragen? Dann erst mal Herr Dr. Thorun und dann Herr Dr. Bizer, bitte.

SV **Dr. Christian Thorun**: Also Frau Philipp, Sie haben natürlich recht. Die Gefahr der Irreführung besteht natürlich, und erstrebenswert wäre es in der Tat, dass ein gesamtes Unternehmen auditiert wird. Allerdings - und da sind wir vielleicht auch zu vorsichtig gewesen, das haben wir uns gar nicht gewagt zu fordern, da uns das fast ein wenig unrealistisch und ambitioniert erscheint - also haben wir gesagt, was wir zumindest brauchen, ist ein Produkt. Es muss sichtbar werden an der Gesamtdienstleistung. Und da ist Ihre Kritik durchaus angebracht. Vielleicht ist es ein Schnipselchen, nämlich des Updates reicht dort zu kurz. Wahrscheinlich müsste man wirklich sagen, als Gesamtprodukt ist die Datenschutzkonformität durch ein gültiges Gütesiegel bestätigt worden. Ich glaube, die Irreführung ist richtig. Natürlich darf man es dann nicht zu ambitioniert sehen, weil, dann würden wir es überhaupt nicht bekommen. Von daher ist ein Zwischenschritt sicherlich sinnvoll. Zumindest muss in diesem Gütesiegel klargestellt werden, worauf es sich bezieht. Wünschenswert ist, dass das gesamte Produkt, womit ich als Verbraucher dann zu tun habe, sozusagen datenschutzkonform ist, wenn dieses Siegel dort tatsächlich aufgetragen wird und vielleicht nicht das, was Sie als Schnipsel bezeichnet haben.

Vors. **Sebastian Edathy**: Herr Dr. Bizer, bitte.

SV **Dr. Johann Bizer**: Frau Philipp, bitte entschuldigen Sie, ich war vorhin einfach in der Notlage, dass ich einerseits den Wünschen des Vorsitzenden gerecht werden musste, mich kurz zu fassen, und auf der anderen Seite das Verfahren auch nicht in allen Einzelheiten beschreiben konnte. Man muss unterscheiden zwischen Gütesiegel und Audit. Beim Gütesiegel definiert der Hersteller das. Und er darf auch nur das Gütesiegel kommunizieren in Verbindung mit dem Produkt. Das ist eine explizite Gütesiegelaufgabe, die er bekommt. Die Verleihung des Gütesiegels ist ein Verwaltungsakt, da gibt es eine Auflage dazu. Und diese Auflage schreibt genau vor, dass er nur dieses Gütesiegel verwenden darf im Zusammenhang mit dem tatsächlich zertifizierten Produkt. Im Übrigen schlage ich vor - wenn ich das hier machen darf - ich würde Sie gerne alle im ULD begrüßen. Wenn Sie ins ULD kommen wollen, wir können uns aber auch gerne hier in Berlin treffen, dass ich ein oder zwei Hersteller - auch Anbieter von Auditierungen - hierher einlade, und wir es im Einzelnen Ihnen darlegen und beschreiben, wie das funktioniert. Vielleicht müssen Sie auch einfach mal einen Blick in ein Langgutachten werfen, wo wir eine Plausibilitätskontrolle machen, und in das dann schließlich veröffentlichte Kurzgutachten, in dem gegenüber der Öffentlichkeit kommuniziert wird, nach

welchen Maßstäben das Gütesiegel verliehen worden ist. Das sind alles Detailmechanismen, die ich vorhin in der Kürze der Zeit nicht ausbreiten konnte.

Vors. **Sebastian Edathy**: Vielen Dank. Es liegen keine weiteren Wortmeldungen vor, d.h. wir sind am Ende des zweiten Blocks des Bereiches „Datenschutz-Audit“. Habe ich davon auszugehen, dass immer noch keine Pause gewünscht ist? Also es soll durchgetagt werden, ja? Was ist mit den Sachverständigen, fühlen Sie sich noch fit? Wir machen mal 5 Minuten Pause. Ich weise darauf hin, dass das Rauchen auf den Fluren des Deutschen Bundestages noch erlaubt ist. Das mag sich bald ändern. Ich würde vorschlagen, in 5 Minuten hier wieder zusammenzukommen.

- Kurze Pause von 5 Minuten -

Vors. **Sebastian Edathy**: Liebe Kolleginnen und Kollegen, sehr geehrte Damen und Herren, wir setzen die Anhörung fort mit dem dritten Teil der heutigen Zusammenkunft, das ist das Thema „Scoring und Unternehmensinformationspflicht bei Datenschutzpannen“. Auch hierzu gibt es zwei Anträge, beide sind von der Fraktion BÜNDNIS 90/DIE GRÜNEN. Wir verfahren wie gehabt mit einer Runde der Berichterstatterinnen und Berichterstatter. Das Wort für Fragen hat die Kollegin Philipp von der Unionsfraktion.

Abg. **Beatrix Philipp**: Herr Vorsitzender, meine Damen und Herren. Herr Prof. Abel und Frau Sasse würde ich gerne fragen: Welche Möglichkeiten und Mittel kann man nutzen, um die Transparenz zu erhöhen? Wie beurteilen Sie die Offenlegung von Merkmalen? Wirkt sich das AGG - dieses Allgemeine Gleichbehandlungsgesetz - aus, - und welche Möglichkeiten zur Korrektur von Scoring oder Scoreergebnissen sehen Sie? Und schließlich: gibt es Erfahrungen mit Selbstverpflichtungen in Bezug auf die Erhöhung von Transparenz im Ausland?

Vors. **Sebastian Edathy**: Vielen Dank. Herr Prof. Abel, bitte.

SV **Prof. Dr. Ralf Bernd Abel**: Zunächst zur Frage der Offenlegung von Merkmalen. „Transparenz“ ist ja die Grundfrage, wobei - wie ich glaube - ganz unstrittig ist, dass in diesem Bereich Transparenz geschaffen werden muss. Daran kommt niemand vorbei, nur: der Teufel sitzt bekanntlich im Detail, und da stellt sich die Frage: Wie kann man Transparenz herstellen? Ich selbst halte es für vertretbar, wenn man die wichtigsten einfließenden Merkmale benennt, ob es jetzt drei oder ob es vier sind. Ich selbst würde dazu tendieren, zu sagen, „mindestens“ drei. Wenn es eine solche gesetzliche Regelung gäbe, wäre kein Unternehmen davon ausgeschlossen, mehr zu offenbaren, wenn es das für richtig hält. Denn Scores sind außerordentlich unterschiedlich und vielschichtig. Ich habe den Eindruck, dass es tausenderlei Varianten gibt. Bei manchen wird man Transparenz mit drei Hauptmerkmalen sehr gut herstellen können, woanders mögen es vier oder fünf sein. Wichtig ist nach

meinem Dafürhalten, dass der Betroffene, der Kunde, wenn er es denn will, z.B. im Bereich Internet, etwa durch Anklicken, oder im Bereich der Banken, im Bereich des Massenkredits, in der Lage ist, mehr oder weniger sofort einen - ich sage mal etwas pointiert - einen Ausdruck zu erhalten, auf dem für den normalen Betroffenen lesbar, verständlich und nachvollziehbar steht, was die wesentlichen Merkmale sind, die zu einem schlechten Score geführt haben. Das setzt natürlich voraus, dass der Score auch entscheidungserheblich ist. Ich bin mir dabei bewusst, dass es noch heute sehr viele Varianten gibt, wo ein Score nur ein zusätzliches Entscheidungsmerkmal ist, aber Hauptmerkmale z.B. die Merkmale sind, die - etwa im Kreditbereich - von der Bank selber erhoben werden, etwa Höhe des Einkommens oder andere kreditorische Belastungen. Aber dann, wenn es auf einen Score ankommt, oder wenn der Score dasjenige ist, was der Betroffene anfragt, dass man ihm dann einen Ausdruck gibt, etwa mit dem Inhalt: "Wir haben einen Score gebildet. Für Sie belastende Momente sind erstens Ihr Alter (18jährige haben noch keine entsprechende Krediterfahrung oder noch keine entsprechende Kredithistorie)." Ja, so könnte man es vielleicht formulieren. Das sind jetzt mal Beispiele. Leichtverständlich, nicht juristisch verklausuliert, sondern nachvollziehbar. Es scheint möglich oder sollte möglich sein, solche Formulierungen bei bestimmten Merkmalen zu standardisieren

Zwischenrufe (nicht rekonstruierbar)

SV Prof. Dr. Ralf Bernd Abel: Meines Wissens bisher noch nicht, sondern man denkt ja gerade darüber nach, wie man es machen kann oder muss. Es gibt bei der Kreditwirtschaft darüber zum Teil noch unterschiedliche Auffassungen. Neuerdings gibt es Aufklärung über Scores (in Form von Broschüren), aber ich meine, was ich persönlich für außerordentlich wichtig halte, ist das Individualisieren der entscheidenden Ablehnungsmerkmale, wenn es denn zu einer Ablehnung kommt, damit der Betroffene in zweiter Linie auch in der Lage ist, einen Korrekturprozess in Gang zu setzen, der ihm möglicherweise hilft, Fehlbeurteilungen richtig zu stellen. Denn das sind ja die entscheidenden Kritikpunkte am Scoring. Also Offenlegung in einer nachvollziehbaren Form, in einer leichtverständlichen Form.

Damit komme ich zur vierten Frage: nach der Selbstverpflichtung. Wie kann man so etwas regeln? Möglicherweise nicht perfekt durch Bundesgesetz. Ins Bundesgesetz, ins BDSG etwa, kann man doch nur abstrakte Begriffe aufnehmen. Sie müssten unterfüttert werden möglichst durch eine Selbstverpflichtung im Sinne von § 38a, wobei - wie gesagt - noch mal darüber nachgedacht werden sollte, warum bisher § 38a nicht so akzeptiert wird, wie Sie sich das als Gesetzgeber gewünscht haben, und wie es auch grundsätzlich wünschenswert ist. Auf jeden Fall halte ich es für sehr wichtig, dass man eine Selbstverpflichtung hineinbringt.

Die zweite Frage war die der Auswirkungen des AGG. Das AGG verfolgt sehr sinnvolle Ziele. Wenn man dann aber in der Praxis damit zu tun hat, hört man von vielen Unternehmen, dass es auch zu Schwierigkeiten führt. Aber Auswirkungen auf den Datenschutz, wo kann man sie festmachen? Man kann sie festmachen - und ich glaube, das ist auch der richtige Punkt - bei den schutzwürdigen

Ausschlussinteressen des Betroffenen. Wir haben im Grunde zwei Punkte, zwei Merkmale oder zwei Bereiche, in denen dieses Thema „Diskriminierung“ - gleich welcher Art - aufkommen kann. Das ist einmal bei den Merkmalen, die in Scores einfließen, und zum anderen beim Endprodukt. Ist das, was beim Scoring herauskommt, in irgendeiner Form diskriminierend? Ich halte es für sehr schwierig, Diskriminierung an Merkmalen festzumachen oder festmachen zu wollen. Welche Merkmale in Scores Trennschärfe bringen, ist etwas für Mathematiker, wo ich auch immer nur staunend davor stehe, weil ich kein Mathematiker, sondern Jurist bin. Aber wo die Mathematiker sehr erstaunliche Möglichkeiten haben, Dinge festzustellen, aus welchen Gründen und mit welchen Merkmalen auch immer - Sie kennen das ja von den Wahlen - im Grunde weiß man um 18.01 Uhr ziemlich genau, worauf es hinausläuft, wenn es nicht gerade nur noch um tausend Stimmen plus/minus geht. Aber die Richtung, die Stimmverteilung ist klar, alles aufgrund mathematisch statistischer Verfahren, das ist schon sehr bemerkenswert. Dass es ähnliches auch woanders mit einer ganz erstaunlichen Trennschärfe gibt, halte ich ebenfalls für bemerkenswert. Dort den Mathematikern, den Fachleuten, vorschreiben zu wollen, ihr dürft das und ihr dürft jenes nehmen oder nicht nehmen, kann meines Erachtens nicht Aufgabe des Bundesgesetzgebers sein. Aber Diskriminierung kann und darf selbstverständlich nicht sein. Und deshalb hat man schon jetzt im BDSG ein Korrektiv, das muss nur noch deutlicher gemacht werden, nämlich in der Abwägung mit schutzwürdigen Ausschlussinteressen, also dem, was man früher „schutzwürdige Belange“ genannt hat. Und an der Stelle kann man den Gebrauch jedweder Scores verhindern, wenn er zu einer gesellschaftlich und politisch unerwünschten, rechtlich unzulässigen und unerträglichen Diskriminierung führen würde. An dieser Stelle wäre es meines Erachtens auch richtig angebracht, so dass Auswirkungen des AGG sich in dieser Interessenabwägung dann darstellen könnten, und dort kann bei der Auslegung des BDSG das AGG mit als Auslegungsmerkmal herangezogen werden. Wobei ich sagen muss, dass diese Frage im Augenblick unter Juristen noch keineswegs geklärt ist, das kann man also hier nicht abschließend sagen, aber da wäre die Stelle, wo man sozusagen eine AGG-Regelung auf jeden Fall mit zu bedenken hat. Jetzt habe ich die dritte Frage eben nicht so akustisch ganz mitbekommen.

Selbstverpflichtung im Ausland: Im Ausland ist es so, dass vor allen Dingen in den USA, aber auch in Großbritannien, Selbstverpflichtungserklärungen eine zunehmende Rolle spielen. Gerade im amerikanischen Recht - im Zivilrecht, wo es die außerordentlich hohen Schadensersatzforderungen gibt, für uns manchmal unfassbar - aber eben nur im amerikanischen Recht ist denkbar, dass dort ein Verstoß gegen die Selbstverpflichtung fast schärfer zu ahnden ist, als hier ein Verstoß gegen gesetzliche Regelungen. Wenn ich es mal versuche, ganz pointiert auf den Punkt zu bringen: Wenn Sie in Deutschland - und das ist ja hier eben schon angesprochen worden - gegen eine gesetzliche Regelung verstoßen, die mehr als Ordnungsvorschrift verstanden wird, als datenschutzrechtlicher Verstoß, dann passiert möglicherweise nur wenig bis nichts, weil und wo Sanktionen fehlen. Wer in

den USA gegen eine Selbstverpflichtung verstößt, muss hohe Schadensersatzforderungen befürchten, und das passiert auch. Das führt wohl auch in solchen Bereichen zu einer Disziplinierung von Anwendern und Anbietern, die gesetzlich dort gar nicht geregelt sind. Diese Entwicklung wäre noch näher zu untersuchen, darüber sollte man nachdenken. Ich halte es für wichtig, dass eine Selbstverpflichtung nicht nur ein Stück Papier sein darf, das man als Alibi benutzt, sondern solche Selbstverpflichtungen müssen auch mit Durchsetzungsmechanismen verbunden sein.

Vors. **Sebastian Edathy**: Vielen Dank. Frau Sasse, bitte.

SV **Cornelia Sasse**: Vielen Dank, Frau Philipp, für Ihre Frage. Zunächst einmal möchte ich sagen, ich höre immer wieder das Wort „Diskriminierung“ und „Scoring“. Das Ziel des Scoring ist es nicht, zu diskriminieren, sondern möglichst hohe Annahmequoten in der Kreditvergabe zu erzielen bei kontrollierten Ausfallrisiken. Es ist einfach so: Die Kreditinstitute unterliegen mehr als genügend bereichsspezifischen Gesetzen und Auflagen, ihr Risiko zu minimieren, einzuschätzen und zu bewerten. Und hier gilt es doch, Rahmenbedingungen zu schaffen, die sowohl für den Verbraucher als auch für die Unternehmen und den Gesetzgeber akzeptabel sind für eine faire und verantwortungsvolle Kreditvergabe. Ich möchte sagen, Sie fragen danach, ob Merkmale offen gelegt werden können, wenn jemand eine Kreditentscheidung erhalten hat. Ich denke, es ist außer Frage, und ich würde mir alle Mathematiker und Analytiker auf den Plan rufen, und sie würden mir - wenn ich das so lax sagen darf - ins Gesicht springen, wenn es um die Offenlegung von Merkmalen in Scorekarten geht. Ich denke, das ist nicht das, was der Verbraucher möchte. Der Verbraucher möchte gern wissen, warum habe ich eine negative Entscheidung erhalten. D.h. es ist nicht ein Modell offen zu legen, sondern die scoring-basierte Entscheidung transparent zu machen. Das geht, es gibt sehr gute Ansätze und es gibt Möglichkeiten. Man kann den Verbraucher aber auch überfordern, denn es spielen so viele verschiedene Kriterien ein in die Vergabe einer Kreditentscheidung und in die Entwicklung von Scorekarten. Es gibt Scorekarten, die haben nur drei bis vier oder fünf Merkmale, es gibt welche, die haben 25 oder 40 Merkmale. Wie wollen Sie da offen legen? Viel wichtiger - und es fällt dabei nicht nur ein einziger Score in die Entscheidung einer Kreditvergabe - ist es, dem Verbraucher transparent zu machen, warum er eine bestimmte Entscheidung erhalten hat und was er tun kann. Ich möchte gleich drauf antworten, dass es Korrekturmöglichkeiten geben muss, die dann die automatisierte Einzelentscheidung aushebeln, die sagen, du hast die Möglichkeit, dich an uns zu wenden. Hier gibt es verschiedene Ansätze. Bezüglich Selbstverpflichtung im Ausland kann ich sagen, es gibt, wenn ich England als Beispiel nehmen darf - unser Unternehmen z.B. ist in England und auch in Amerika u.a. als Auskunftei tätig - dort eine ganz andere Daten- und Kreditkultur. Es gibt dort bereits seit den 90er Jahren einen Guide to Credit Scoring, dem sich alle Kreditinstitute angeschlossen haben und verpflichtet haben, nach diesem Guide to

Credit Scoring zu operieren und Transparenz auszuüben. Ein ähnlicher Guide wäre auch in Deutschland denkbar, ohne in ein festes Rahmengesetz gepresst zu werden. Es ist allerdings nicht so, dass wir Scoring generell über einen Kamm scheren können. Es gibt viele verschiedene Branchen. Wir haben nicht nur die Banken, die Kreditinstitute, es gibt die Telekommunikation, es gibt die Versandhäuser, es gibt Teleshopping. Wir haben so viele Herausforderungen, bei denen das Scoring angewandt wird. Und es kann nicht sein, dass alle Unternehmen auf gleiche Art und Weise transparent sein müssen. Das ist gar nicht möglich, denn es müssen schlanke, effiziente Prozesse da sein, die die Wirtschaft erforderlich macht. Es muss alles immer schneller passieren. Wir wollen als Verbraucher ganz schnell einen Onlinekredit haben. Es müssen schnelle Prozesse da sein. Und dann muss auch die Transparenz gewährleistet sein - sie soll nicht bedeuten, dass der Verbraucher benachteiligt wird und keine Möglichkeiten zur Auskunft hat - aber die Transparenz muss schon differenziert werden, auf welche Art und Weise auch immer. Und das muss den Unternehmen vorbehalten sein, das zu entscheiden, auf welche Art und Weise diese Transparenz stattfindet. Dass sie bestimmten Auflagen unterliegt, ja, aber es muss auch verschiedene Möglichkeiten geben, denn ich kann nicht erwarten, dass ich in einem Versandhandel anrufe und mit einer Dame im Call-Center telefoniere, die mir dann versucht, über Scoremerkmale einen Vortrag zu halten. Das kann nicht passieren. Es muss wohl die Möglichkeit geben, also Korrekturmöglichkeiten zu haben, aber es kann nicht zu einer kompletten Offenlegung kommen.

Vors. **Sebastian Edathy**: Frau Stokar, Sie haben nachher das Wort, zunächst aber hat das Wort die Kollegin Piltz von der FDP-Fraktion.

Abg. **Gisela Piltz**: Vielen Dank, Herr Vorsitzender. Zu Recht ist ja zum Schluss gesagt worden, dass es beim Scoring nicht nur um Kredite geht. Die erste Runde drehte sich ja vor allen Dingen um Kredite und die Tatsache, dass Menschen wissen, dass man sich dabei mehr oder weniger - mal abgesehen vom 1000-Eurokredit oder Onlinekredit - im Gespräch befindet und das dann ganz anders abläuft. Ich glaube, unsere Sorge ist ja zum Teil auch, dass Menschen gar nicht wissen, warum sie eigentlich abgelehnt werden. Man muss doch auch manchmal sagen, was einen hier bewegt. Warum man irgendwann mal in der Warteschleife ganz hinten landet, wenn man irgendwo anruft, warum man seine Waschmaschine nicht bekommt. Bei einer Kreditanfrage da höre ich ja vielleicht noch: Sie sind zu alt, sie sind zu jung oder sie verdienen nicht genug, sie haben keine Sicherheiten, aber in vielen Bereichen weiß ich das ja gar nicht, weil es gar nicht zu einer weiteren Kommunikation kommt. Und das ist natürlich ein Problem, mit dem wir uns hier beschäftigen müssen. Meine erste Frage an Herrn Jaspers. Natürlich haben wir hier auch ein Spannungsverhältnis bei denen, die entscheiden wollen, aber auch dem Schutz der Betriebsgeheimnisse verpflichtet sind - auch das darf man nicht vergessen - natürlich würde eine komplette Offenlegung ja Betriebsgeheimnisse betreffen. Aber könnte man das nicht

dadurch auflösen, dass man die entscheidungserheblichen Merkmale veröffentlicht. Ich kann mir gut vorstellen, dass man dann auf Anfrage die Merkmale einfach aufzählt, ohne sie zu bewerten - einfach, welche Merkmale bei der Entscheidung eine Rolle spielen. Ob es aus Ihrer Sicht eine Möglichkeit wäre, diese Interessen aufzulösen?

Meine zweite Frage geht an Herrn Dr. Thorun und an Herrn Dr. Dix. Scoring ist ja aus meiner Sicht eine Herausforderung einmal für den Datenschutz, aber sicher auch für den Verbraucherschutz. Und wie können wir diese beiden Bereiche besser zusammenführen? Und hat sich nicht womöglich die Unterscheidung zwischen Verbraucher- und Datenschutz mindestens in diesem Bereich - wenn nicht sogar darüber hinaus - bereits überholt? Meine dritte Frage geht an Frau Sasse, Herrn Jaspers und Herrn Dr. Thorun, ob Sie es für vorstellbar und wirtschaftlich vertretbar halten, wenn wir beim Scoring den umgekehrten Weg gehen, z.B., ob der Verbraucher, der einen Kredit haben will, oder ein Handy oder etwas bestellen möchte, sich selber scoren lässt? Und inwieweit halten Sie das für durchsetzbar bei Versicherungen, Banken usw.. Und eine Ergänzung zu meiner Frage, insbesondere an den Verbraucherschützer wahrscheinlich. Als ich in Amerika war, haben wir uns mit dem Thema beschäftigt, dann sieht man in den Bücherregalen eine ganze Reihe von Büchern, wo es ums Scoring geht. Aber nicht so wie das hier eben beschrieben worden ist, als Standard für die Firmen, sondern als Handlungsanleitung für den Einzelnen, wie man sich bessere Scorewerte verschaffen kann. Wen es interessiert, ich habe ein Buch davon im Büro. Nicht, weil ich es bräuchte - ich habe noch Glück gehabt bisher - aber weil ich es sehr interessant fand. Und ob Sie wissen, ob es solche Literatur in dem Umfang in Deutschland schon gibt, oder ob es mittlerweile schon eine Scoringberaterbranche gibt. Denn, wenn das eine da ist, haben wir normalerweise sofort auch das Gegenteil, nämlich Leute, die anderen Leuten dabei helfen, einen möglichst guten Scoringwert zu bekommen. Und wenn das so ist, und wenn das geht, dann muss man sich ja auch fragen, ob das mit dem Scoring so Sinn macht. Vielen Dank.

Vors. **Sebastian Edathy**: Es sind vier Sachverständige angesprochen. In alphabetischer Reihenfolge, dann bitte zunächst Herr Dr. Dix.

SV **Dr. Alexander Dix**: Vielen Dank, Frau Piltz. An mich haben Sie die Frage direkt gerichtet, ob nicht die Trennung zwischen Daten- und Verbraucherschutz in dem Punkt schon als überholt gelten kann. Sicherlich gibt es hier eine große Interessenidentität zwischen Datenschutz und Verbraucherschutz. Gerade beim Thema „Scoring“ ist das so. Ich will aber nicht ausschließen, dass es durchaus auch unterschiedliche Interessen bei Verbraucherschutz und Datenschutz geben kann. Beim Thema „Scoring“ fällt mir jetzt keine konkrete Anwendung ein, aber das hat es schon in anderen Bereichen unter Umständen gegeben. Allerdings ist völlig klar, dass wir bei dieser Frage mit dem, was etwa der Verbraucherzentrale Bundesverband immer schon vertreten hat, voll übereinstimmen. Vielleicht gestatten

Sie mir noch eine Bemerkung zum Thema „Betriebs- und Geschäftsgeheimnis“, weil Sie darauf auch so Wert gelegt haben. Ich bin der Auffassung, dass die einzelnen Kriterien, die in den Scorewert einfließen, schon begrifflich nicht zu den Betriebs- und Geschäftsgeheimnissen gezählt werden können. Ich könnte mir vorstellen, dass es ein solches schutzwürdiges Unternehmensgeheimnis gibt bei der mathematischen Formel, die den Scorewert selbst ermittelt, das muss man aber strikt voneinander trennen. Sowohl die einzelnen Kriterien, die in dieses Verfahren eingehen als auch die Wertigkeit, die Rangfolge halte ich nicht für geheimhaltungsbedürftig. Und deshalb würde ich vorschlagen, ganz konkret, dass der Bundesgesetzgeber hier dem Beispiel des Umweltinformationsgesetzes des Bundes folgt, das nämlich ausdrücklich vorsieht, dass der Zugang zu Informationen über Emissionen nicht unter Berufung auf Betriebs- und Geschäftsgeheimnisse der Unternehmen verweigert werden kann, § 9 des Umweltinformationsgesetzes. Und das sollte klarstellend auch in das neue Bundesdatenschutzgesetz eingeführt werden. Letzte Bemerkung zu Ihrem Hinweis auf die US-Literatur. Das zeigt genau, dass in den Vereinigten Staaten nach meiner Kenntnis die deutsche Debatte nur als „Geisterdebatte“ verstanden werden kann. In den USA hat jeder im Prinzip Zugang zu den Kriterien, die in seinen Scorewert Eingang finden. Und genau deshalb hat die Literatur dort Konjunktur, weil er nämlich Tipps bekommt - wie seriös sie im einzelnen sind, kann ich natürlich nicht beurteilen - wie kann er Einfluss darauf nehmen? Genau das ist eine Kultur der Transparenz, und ich kann nicht verstehen, warum die US-Kultur so grundverschieden von unserer sein soll, dass wir uns soviel Transparenz nicht leisten können.

Vors. **Sebastian Edathy**: Dann ist als nächster Sachverständiger Herr Jaspers dran.

SV **Andreas Jaspers**: Zunächst zur Frage von Frau Piltz. Zum Thema Spannungsverhältnis: auf der einen Seite Betriebs- und Geschäftsgeheimnisse, auf der anderen Seite „Transparenz“. Ja, dieses Spannungsverhältnis gilt es zu lösen, insbesondere vor dem Hintergrund der bereits bestehenden gesetzlichen Vorgabe, der so genannten automatisierten Einzelentscheidung. Hier wird automatisiert etwas vorentschieden oder weitgehend durchentschieden. Was den Betroffenen durchaus berührt, ist dann die Rechtsfolge. Nicht jedes Scoring ist transparenzwürdig, würde ich mal sagen, vorsichtig formuliert. Ob ich jetzt Werbung bekomme oder nicht, betrifft die Fragestellung, ob ich tatsächlich in meinen Rechten betroffen bin oder nicht. Das möchte ich hier schon mal hinanstellen. Spätestens aber, wenn ich in meinen Rechten betroffen bin, weil ich tatsächlich benachteiligt bin, weil der Computer automatisiert entschieden hat, haben wir wohl weitgehend die Praxis - jedenfalls zurzeit - dass dies nicht transparent gemacht wird, weil man letzten Endes auf die gesetzlichen Ausnahmenvorschriften geht. Nun, dieses gilt es aufzulösen, das ist im Ergebnis unbefriedigend und deswegen sagen wir, auf die entscheidungserheblichsten Kriterien kommt es an. Ich bin bei Prof. Abel, der sagt, wie viel das jetzt sind, das kommt auf den Einzelfall an. Dieser Wert drei, vier, fünf,

das sind Maßstäbe, da weiß der Betroffene, das sind die Punkte gewesen, stimmt wohl, oder stimmt für mich jetzt aber gar nicht. Dann im Einzelfall eine menschliche Nachentscheidung hinzubekommen, das ist das allerwichtigste, was wir erreichen wollen, Individualgerechtigkeit.

Zu Ihrer anderen Frage zum Thema des umgekehrten Weges. Das ist natürlich so eine Idee, wie man Transparenz schaffen kann. Ja, das ist natürlich sehr schön, wenn die Institutionen, die weitgehend im Scoringgeschäft tätig sind, hier Transparenz dadurch schaffen, in dem angeboten wird: Gehe mal ins Internet und gucke, wie dein Scorewert aussieht. Wobei auch eine Legende dazu muss, was der Scorewert aussagen könnte. Es soll ja durchaus solche Modelle geben, über die auch von der SCHUFA nachgedacht wird. Sicherlich, das ist ein Transparenzfaktor. Den allerdings gesetzlich zu fordern, weiß ich nicht. Die Forderung muss in den § 6a eingehen, Transparenz bei der automatisierten Einzelentscheidung hinsichtlich der wichtigsten Elemente. Alles andere ist *colorandi causa*, und sollte von denen freiwillig angeboten werden, die in besonderer Weise im Focus der Öffentlichkeit sind, was das Scoring anbetrifft.

Vors. **Sebastian Edathy**: Vielen Dank, dann Frau Sasse, bitte.

SV **Cornelia Sasse**: Um die Frage, Frau Piltz, aufzugreifen, ob es denn möglich ist, sich selbst zu scoren, wenn es darum geht, einen Kredit zu erhalten oder ein Handy zu kaufen oder eine Waschmaschine, d.h., darunter verstehen Sie Eigenauskünfte verstärkt einzuholen?

Zwischenrufe (nicht rekonstruierbar)

Vors. **Sebastian Edathy**: Das kommt alles nicht ins Protokoll, wenn Sie das Mikrofon nicht anmachen, Frau Kollegin, es ist dann nicht auf dem Band. Frau Sasse, aber Sie haben die Frage verstanden?

SV **Cornelia Sasse**: Ja, ich denke einmal, das zu diskutieren bedarf grundlegendes Verständnis über das Verfahren, über Scoringverfahren allgemein. Die Möglichkeit sich selbst zu scoren, d.h. auch vielleicht sich einem Scorsimulator auszusetzen, birgt immer wieder die Gefahr - und das auch als Antwort dazu - wie viel, oder ob Merkmale bekannt gegeben werden müssen - ist die Manipulationsmöglichkeit, die ich dann habe, den Scorewert zu beeinflussen.

Vors. **Sebastian Edathy**: Frau Piltz, nachher noch zu Ihrer Nachfrage.

Abg. **Gisela Piltz**: Nein, weil ich es einfach nicht verstehe. Score heißt ja automatisiertes Verfahren, z.B. ich wohne da oder ich wohne da nicht, entweder ich verdiene so viel oder ich verdiene nicht so viel. Dass Sie jetzt nicht für Transparenz sind, das haben Sie ja schon vorher gesagt, aber dass man das manipulieren kann, ich weiß nicht, wie das gehen soll.

SV Cornelia Sasse: Ich möchte nur sagen: Ich möchte es von mir weisen, dass ich nicht für Transparenz bin. Transparenz ist ein Gebot und es muss etwas für Transparenz getan werden. Und da möchte ich das Thema „Selbstverpflichtung“ aufgreifen, dass das etwas ist, mit dem wir weitestgehend für Transparenz sorgen können. Aber auch da mit mehr Verbraucherinformationen, d.h. der Verbraucher selbst wird nicht genügend über das Scoring überhaupt informiert. Und ich denke, das ist ein Faktor, der aufgegriffen werden sollte.

Vors. Sebastian Edathy: Frau Philipp möchte eine Nachfrage stellen, wie das aussehen könnte.

SV Cornelia Sasse: Ja, es gibt ja bereits seitens mehrerer Verbände die Broschüren und Informationsschriften über das Scoring, das dann auch für mehr Vertrauen seitens des Verbrauchers im Scoring sorgt. Ich denke, viel mehr bringt es, auch den Verbraucher darüber aufzuklären, dass er selbst sich bewusst werden muss, was bedeutet es, wenn ich einen Kredit aufnehme oder wenn ich etwas auf Rechnung kaufe. Ich muss mich vor Überschuldung schützen. Und da denke ich, ist ein großer Nachholbedarf an Informationen für den Verbraucher.

Und dann einen abschließenden Satz zur Frage, ob es denn gut sei, dass es Literatur gibt, die mich anleitet, meinen Scorewert zu verbessern. Ich denke, es sollte nicht Literatur sein, die mich anleitet, wie ich meinen Scorewert verbessere, denn das würde auch bedeuten, den Scorewert zu manipulieren. Es sollte eher bedeuten, wie kann ich meinen eigenen Status verbessern, um für mehr Kreditwürdigkeit zu sorgen. Ist damit Ihre Frage beantwortet?

Vors. Sebastian Edathy: Herr Dr. Thorun kann vielleicht auch etwas zu dieser Frage aus Sicht der Verbraucherschützer sagen.

SV Dr. Christian Thorun: Erst einmal möchte ich betonen, Frau Piltz, was Sie eingangs gesagt haben, nämlich das Scoringverfahren wird zwar häufig im Zusammenhang mit der Kreditwirtschaft diskutiert, aber es geht eigentlich viel weiter. Und ich denke, dass das wichtig ist für die Tragweite dessen, was wir hier besprechen. Es handelt sich hierbei um einen Einstieg in ein dynamisches Preissystem, was dann sehr grundlegende Veränderungen mit sich bringen würde und zur Diskriminierung führen könnte. Deswegen ist das, was wir hier besprechen, gerade in Bezug auf die Kreditwirtschaft exemplarisch zu sehen. Konkret: Scoring verdeutlicht, dass Verbraucherschutz und Datenschutz kein Widerspruch sind, sondern es eine enge Verbindung gibt. Ich denke, absolut in diesem Beispiel ja, ob es grundsätzlich immer der Fall sein muss, dafür kann es im einzelnen Widerlegungen geben, aber grundsätzlich beim Scoring - denke ich - dass das der Fall ist. Zweitens: Die Idee, warum sollten sich die Verbraucher nicht selbst scoren lassen? Auf der einen Seite hat es den Vorteil, dass ich dann sehr viel genauer weiß,

auf welcher Datengrundlage der Scorewert zustande gekommen ist, aber dann wirft sich in der Praxis die Frage auf, es gibt ja nicht nur ein Scoring, sondern es gibt eine große Vielzahl. Sollte ich denn tatsächlich zu jedem gehen und dort vielleicht sogar kostenpflichtig meine Scorewerte abrufen? Die dritte Frage ist: Natürlich hätte ich dann ja auch einen Anreiz, möglichst umfassend meine Daten preiszugeben, aber das widerspricht genau dem Grundprinzip des Datenschutzes, nämlich so sparsam wie möglich mit den personenbezogenen Daten umzugehen. Da sehe ich gravierenden Widerspruch. Von daher halte ich nicht viel von dieser Idee, dass man die Verantwortung auf die Verbraucher abschiebt.

Die nächste Frage, die Literatur - gerade in Amerika - das Indiz, dass es da so viel Literatur gibt, ist natürlich ein Zeichen dafür, dass die Verbraucher überhaupt was damit anfangen können. Denn sie haben eine Auskunft darüber, auf welcher Datengrundlage und wie diese Scores im Wesentlichen zustande kommen. Das ist natürlich eine tolle Sache. Aber es zeigt - und das haben Sie ja auch gesagt - im Übrigen führt die Methode auch ad absurdum, wenn ich denn Literatur habe, wie ich diese Scorewerte versehen kann, dass sie letztlich nichts mehr aussagen. Und das bedeutet, das gibt nur einen Rückschluss darauf: Ein Scorewert ist nicht allgemein zu verteufeln. Das tut ja auch keiner. Scorewertberechnung kann durchaus ein Element in einer Bonitätsbewertung sein. Aber es kann eben auch nur ein Element sein, und wir müssen uns auch der Schwächen dieses Verfahrens bewusst sein. Wir müssen uns hier - und das tun wir ja auch - über die Art und Weise unterhalten, wie Scoring eingesetzt wird. Also deswegen starker Appell. Die Literatur ist zwar ein gutes Indiz, aber es kann nicht die Stoßrichtung vorgeben, wo wir uns hinentwickeln müssen.

Abg. **Gisela Piltz**: Kennen Sie denn Literatur in Deutschland dazu?

SV **Dr. Christian Thorun**: Mir ist nicht bekannt, dass es hier großartig Literatur darüber gibt, wie Verbraucher den Scorewert beeinflussen können.

Vors. **Sebastian Edathy**: Okay, dann hat jetzt das Wort der Kollege Dr. Bürsch.

Abg. **Dr. Michael Bürsch**: Wenn ich die Stellungnahmen zu Scoring richtig gelesen habe, gibt es da einen Punkt, bei dem Meinungsunterschiede bestehen. Das ist die Frage, ob die Kriterien fürs Scoringgesetz begrenzt werden sollen. Für eine Begrenzung haben sich auf jeden Fall Herr Dr. Dix und Herr Dr. Thorun ausgesprochen, ich glaube auch Herr Schaar, und dagegen Herr Jaspers. Ich würde doch gerne hören, was dafür und was dagegen spricht. Und dann an Herrn Dr. Bizer die Frage, die sich nicht kurz beantworten lässt, denn die kurze Beantwortung im Anhang der Stellungnahme, die aus Schleswig-Holstein gekommen ist von Herrn Weichert, die kann ich nicht verstehen. Sie heißt: „Die Rechtmäßigkeit der Scorberechnung setzt voraus: a) die nach einem anerkannten Verfahren festgestellte wissenschaftlich-statistische Relevanz und Gewichtung der einbezogenen Daten, b) die Plausibilität der Daten für die Beurteilung der Kreditwürdigkeit und c) den

Ausschluss von Merkmalen, die einem Nutzungs- oder Diskriminierungsverbot unterliegen“. Es erschließt sich mir so tatsächlich nicht, was da alles mit gemeint ist, oder wie unter solchen Bedingungen überhaupt noch ein Scor in der Praxis möglich sein soll.

Vors. **Sebastian Edathy**: Zur Auswahl der Kriterien Herr Dr. Dix, Herr Jaspers und Herr Dr. Thorun.

SV **Dr. Alexander Dix**: Herr Dr. Bürsch, aus meiner Sicht muss hier bei der Frage, welche Kriterien überhaupt in ein Scoringverfahren einbezogen werden dürfen, in der Tat der Gesetzgeber stärkere Grenzen einziehen. Es hat bereits einen Versuch gegeben - allerdings in einem etwas anderen Rechtsgebiet, im Bereich des Kreditwesens. Hier hat der Gesetzgeber im § 10 Vorgaben für ein verwandtes Verfahren, das Verfahren des Rating, insbesondere aus Sicht des Finanzaufsichtsrechts, des Bankenaufsichtsrechts getroffen. Die Kriterien, die dort beschrieben worden sind, werden datenschutzrechtlich durchaus auch berücksichtigt. Das ist ein etwas komplizierter Zusammenhang. Sie fließen ein in die Güterabwägung nach § 28 des Bundesdatenschutzgesetzes. Aber, ich meine, der Kreis der Daten, der nach dem Kreditwesenrecht auszuschließen ist - das ist alles bezogen auf das Kreditgewerbe - ist zu eng, zumal gerade eben auch zu Recht Frau Piltz hingewiesen hat, dass wir hier darüber sprechen, dass Scoringmethoden nicht nur zur Prüfung der Zahlungsfähigkeit, der Kreditwürdigkeit herangezogen werden, sondern darüber hinaus zur Vertragswürdigkeit ganz grundsätzlich. Also zur Fähigkeit, am Wirtschaftsleben teilzunehmen. Und da ist es aus meiner Sicht in der Tat nicht hinzunehmen, dass die Entscheidung eines Menschen, z.B. zu heiraten, eine Lebenspartnerschaft einzugehen oder das nicht zu tun, statistisch und nach Anwendung von Scoreverfahren dazu führt, dass er von bestimmten Entfaltungschancen praktisch ausgeschlossen wird, informationell diskriminiert wird. So würde ich das nennen. Deshalb halte ich die Begrenzung, die der Gesetzgeber im Kreditwesengesetz vorgenommen hat, für unzureichend. Wir sollten ernsthaft prüfen, ob hier nicht engere Grenzen gezogen werden, z.B., dass alle die Daten, die das Bundesdatenschutzgesetz schon selbst als besonders schutzwürdig ansieht im § 3 Abs. 9, also Informationen über rassische, ethnische Herkunft, Gewerkschaftszugehörigkeit - ist bei Scoring eher etwas fern liegend - aber sexuelle Orientierung, Sexualleben, medizinische Informationen - ganz wichtig - dass alle diese Informationen definitiv nicht ins Scoreverfahren einfließen dürfen. Frau Philipp hat vorhin das AGG erwähnt. Beim Alter kommen wir schon in einen hochstreitigen Bereich, Nationalität ist ein anderes Kriterium. Aber bei all diesen Daten sollte man ernsthaft mal darüber nachdenken, ob es hier nicht Grenzen geben muss, die der Gesetzgeber präziser fassen sollte. Ich meine nicht, dass es hier ausreicht, sich auf die allgemeine Abwägungsklausel in der Generalklausel des § 28 zurückzuziehen. Das ist nicht trennscharf genug. Und gerade das Beispiel mit den besonders schutzwürdigen Daten zeigt auf, dass der Gesetzgeber des

Bundesdatenschutzgesetzes hier schon im allgemeinen Teil besondere Schutzwürdigkeit gesehen hat. Die Aufsichtsbehörden vertreten auch einheitlich die Auffassung, dass solche Daten nicht ins Scoreverfahren einfließen dürfen. Aber ich denke, das ist doch durchaus eine Klarstellung durch den Gesetzgeber wert.

Vors. **Sebastian Edathy**: Herr Jaspers, bitte.

SV **Andreas Jaspers**: Ist es sinnvoll, per Gesetz gewisse Daten einfach so auszuschließen? Es kommt immer auf den Zweck an, den man damit verfolgt. Ich meine, in dem Gutachten von Prof. Abel gibt es ein Beispiel: Wen bewerbe ich jetzt mit Schweinefleisch? Dass ich das eben sinnvollerweise nicht mache, wenn ich weiß, dass ich niemanden bewerbe, der islamischen Glaubens ist, weil er damit gar nichts anfangen kann. Das sind solche Beispiele, wo man sagen kann, es gibt durchaus denkbare Verwendungsmöglichkeiten, die auch sinnvoll sind, noch nicht einmal einen diskriminierenden Charakter haben. Insofern wären Radikalkuren, bestimmte Merkmale per Gesetz auszuschließen, nicht zielbringend. Entscheidend wird doch sein, dass man sich darauf abstützt und sagt, auf der einen Seite die allgemeinen Abwägungsklauseln, die natürlich münden müssen in statistische Methoden, was letzten Endes auch dahinter steckt bei der Bewertung dieser ganzen Sachverhalte. Die AGG-Merkmale einfach so zu nehmen und zu sagen, das geht gar nicht ins Scoring rein, das widerspricht ja schon dem AGG selber, dass es die Merkmale seinerseits unter Vorbehalte stellt. Ich kann sie verwenden, wenn es hierfür aus verschiedenen Gesichtspunkten denkbare vernünftige Gründe gibt. Also, die Frage ist, ob man dem Scoring nicht zu sehr zu Leibe rückt, wenn man tatsächlich so einen gesetzlichen Ausschluss vornimmt. Ich meine, da müsste man doch besser die Abwägungsklauseln und die Berücksichtigung auch der AGG-Merkmale im Rahmen des AGG - also mit den zusätzlichen Erlaubnistatbeständen - berücksichtigen, dort wo jedenfalls keine Diskriminierung in der Sache erfolgt und statistisch auch entsprechend erwiesen ist, dass man die Daten auch benutzen kann.

Vors. **Sebastian Edathy**: Vielen Dank. Herr Dr. Thorun.

SV **Dr. Christian Thorun**: Da die Zeit knapp ist und ich mich im Wesentlichen inhaltlich Herrn Dr. Dix anschließen kann, beschränke ich mich und ergänze nur diesen einen Punkt, dass es natürlich nicht angehen kann, was bis vor kurzem noch gängige Praxis - zumindest bei der SCHUFA war - nämlich, dass die Kreditanfragen negativ als ein Merkmal eingeflossen sind, das zu einer Verschlechterung des Bonitätswerts geführt hat. Zwar hat die SCHUFA hier Abhilfe geschaffen, und jetzt differenziert sie zwischen Konditionsabfragen und Kreditanfragen. Also Konditionsabfragen, die im Vorfeld gestellt werden, und Kreditanfragen, wenn es tatsächlich zum Vertragsabschluss kommt. Allerdings ist die gängige Praxis bei Banken immer noch so, dass in den häufigsten Fällen Kreditanfragen gestellt werden. Da es keine festen Zinssätze mehr gibt, sondern nur noch Bestzinssätze,

sollten Verbraucher Preise vergleichen. Dass sie durch das beschriebene Verfahren sanktioniert und bestraft werden, ist natürlich eine Absurdität. Das muss natürlich geändert werden. Was die Ausführungen von Herrn Jaspers angeht: Also ich stimme ihm nicht zu. Mir ist nicht ersichtlich, warum Daten z.B. über die sexuelle Neigung in einen Score einfließen sollten. Wir müssen hier unterscheiden. Es geht hier nicht um Adressdaten, Banken oder so, sondern es geht hier um Scorewertberechnung. Da bin ich mir über den Zweck, der solche Informationen erfüllen soll, würde ich gerne wissen, wann das notwendig ist.

Vors. **Sebastian Edathy**: Frau Sasse, Sie möchten etwas dazu sagen?

SV **Cornelia Sasse**: Ja, dazu möchte ich einen Erfahrungsbericht kurz nennen. Wir als Scorekartenentwickler seit über 30 Jahren haben noch keine Karte entwickelt, in der sexuelle Ausrichtung oder Religion oder sonstiges festgelegt wurden als Kriterien. Noch dazu unterliegen Scorekarten und die Scorekartenentwicklung den Genehmigungen der Aufsichtsbehörden, wie z.B. der BAFin. Sie können davon ausgehen, dass derartige Sachen nicht gemacht werden. Wohingegen z.B. das Kriterium „Alter“ bis jetzt als abzuschaffen betrachtet wurde, was für viele Branchen ganz wichtig ist, denn sie können davon ausgehen, dass ein 18jähriger nicht so finanzstark ist, wenn er noch kein festes Einkommen hat, um auf Kredit oder auf Rechnung einzukaufen, d.h., da ist das Alter signifikant. Es geht wirklich um eine Abwägung, um alle Branchen zu berücksichtigen, auch um alle Bedürfnisse zu befriedigen und in erster Linie das Bedürfnis des Verbrauchers aber nicht einhergehend mit Unternehmensbeschneidungen. Es wird für die rechtschaffenen Unternehmen kein Problem sein, ihre Transparenz darzustellen und somit auf die nicht rechtschaffenen somit erhöhten Druck auszuüben, dies ebenfalls zu tun. Danke schön.

Vors. **Sebastian Edathy**: Vielen Dank für die ergänzenden Informationen. Eine weitere Frage des Kollegen Bürsch hatte sich an Herrn Dr. Bizer gerichtet.

SV **Dr. Johann Bizer**: Ich kann es auch ganz kurz machen. Also die Rechtmäßigkeitsvoraussetzung für die Verarbeitung von personenbezogenen Daten, aus dem ein Score sich ergibt, aus dem die Negativentscheidung folgen kann, oder auch, das ist ein Aspekt, der in der Diskussion vernachlässigt worden ist, auch ein unterschiedliches Pricing, das ist in der Praxis noch mal sehr viel bedeutender. Bekomme ich 0,5 % mehr als mein Nachbar, der die gleichen Voraussetzungen hat, oder muss ich 1 % weniger bezahlen? Das wird dann die Frage. Und jetzt übersetzt in drei kurze Beispiele: Erstens: Die festgestellte wissenschaftlich-statistische Relevanz ist ein Kriterium, das die Scoringanbieter selbst von sich behaupten. Sie sagen, ihre Merkmale hätten das, also sollen sie es auch nachweisen. Kurz gesagt: Verbot der Kaffeesatzleserei. Zweitens: Die Plausibilität, es muss einen Zusammenhang geben zwischen dem was man für einen Kredit haben will, z.B. ist

es von Relevanz, das wäre jetzt die Frage, für einen Telekommunikationsvertrag, einen Handyvertrag, dass ich ein BMW-Fahrer oder Polofahrer bin, oder dass ich geschieden bin, alles Plausibilität? Und das Dritte ist, das haben wir jetzt groß diskutiert: „Indianer“ oder „Schwule“ zahlen 0,5 % oder 1 % mehr, das soll eben verboten werden.

Vors. **Sebastian Edathy**: Vielen Dank. Die Fraktion DIE LINKE. hat sich verabschiedet, Herr Kollege Korte ist nicht mehr im Saal. Das Wort hat Frau Stokar.

Abg. **Silke Stokar von Neuforn**: Meine Damen und Herren, ich möchte mindestens noch drei konkrete Fragen zu diesem Scoring stellen. Ich merke auch, dass mich das Thema immer mehr aufbringt. Ich möchte einfach mal ein Beispiel aus dem eigenen Erleben schildern, aus dem sich dann auch eine Frage ergibt: Bei der Beantragung eines Kredites war die Mitarbeiterin einer Bank nicht in der Lage, den Zinssatz zu genehmigen, den sie der Kundin, die sie seit 30 Jahren kannte, genehmigen wollte, weil der Computer diesen Zinssatz einfach nicht angenommen hat. Hintergrund war, diese Kundin wohnte in einem multikulturellen Stadtteil - und da sind wir in dem gesellschaftspolitischen Bereich, dass hier normiertes und Lifestyle-Verhalten belohnt wird, oder wirtschaftlich bestraft wird, das war vermutlich eine grünahe Person - sie hat keinen Führerschein, und fährt kein Auto, sie hat weder einen BMW noch VW gekauft, sondern nur ein Fahrrad. Das floss aber nicht ein, das war auch ein teures Fahrrad, das spielte keine Rolle. Zudem aus Klimaschutzgründen fliegt sie nicht in Urlaub. Sie macht gerne Urlaub in der Natur, wohnt nicht in teuren Hotels, hat ein sehr gutes Einkommen, eine hohe Bonität und der Computer verweigerte einen bestimmten Zinssatz. Und die Mitarbeiterin saß davor und sagte: Ich weiß nicht, warum, sie haben saumäßige Scorewerte, und holt aus der Schublade einen alten Kreditantrag, füllte ihn per Hand aus und ließ ihn vom Chef unterschreiben und sagte: Eigentlich darf ich das gar nicht. Das ist die automatisierte Welt, die automatisierte Scorewelt. Und meine Frage an Herrn Schaar, soweit ich mich erinnere, wir haben ein Verbot der automatisierten Einzelfallentscheidung. Das wird in diesen Bereichen massenhaft unterlaufen. Wo bleibt hier die Kontrolle? Wo bleiben hier die Sanktionen? Wo bleibt hier der Überblick? Und eine Frage an Herrn Thorun. In den USA ist das selbstverständlich, ich bekomme einmal im Jahr kostenlos von den Auskunfteien eine Information über Merkmale und Daten, die dort förmlich gespeichert sind. Wie kann ich als Verbraucherin meine Auskunftsrechte in Deutschland durchsetzen, wenn 50 unterschiedliche kommerzielle Unternehmen mit völlig diffusen Scorewerten anfangen, über mich irgendwelche Profile zu erstellen, die massiv in meine wirtschaftliche Handlungsfreiheit eingreifen. Wo ist da überhaupt noch Verbraucherschutz, und was muss erfüllt werden, dass Verbraucherschutz hier wieder greift?

Ich würde Herrn Schaar bitten, da wir ja am Ende sind, ganz kurz einzugehen auf unseren Antrag - Stichwort „California Act“, der, als wir ihn geschrieben haben, nur in Kalifornien galt, mittlerweile gilt er in 33 US-Bundesstaaten -, auf die Offenlegung von

Datenschutzpannen, die Themen Datenschutzpannen und Datenschutz-Audit und auch Transparenz und Offenlegung - und ich will nicht Ihre Broschüren, da kann ich mein Büro mit pflastern -, sondern ich möchte die Offenlegung der Merkmale. Das ist Transparenz.

Vors. **Sebastian Edathy**: Vielen Dank, dann schlage ich vor, dass zunächst Herr Dr. Thorun antwortet.

SV Dr. Christian Thorun: Wo bleibt hier beim Scoring noch der Verbraucherschutz? In der Tat, was Sie jetzt explizit beschrieben haben, die Praxis in der Bank, wo da nicht abgewichen werden konnte von dem Scorewert, das ist auch das, was uns berichtet wird. Die Eingabemaske sieht es einfach gar nicht mehr vor, dass man abweichen kann. Und das ist natürlich ein klarer Verstoß gegen § 6a BDSG. Das Zweite ist, dass die Grundvoraussetzung dafür ist, dass die Bank und der Verbraucher eine Korrektur vornehmen können, welche Daten zugrunde gelegt worden sind, wie sie für die Scorewertberechnung gewichtet worden sind. Da sagen wir, das ist die Maximalposition, alle diese Daten und die Gewichtung müssen klar erkennbar sein, so dass überhaupt die Korrekturmöglichkeit gegeben ist. Und das beantwortet zum Teil auch die Frage in diesem Dickicht von unterschiedlichen Scoringanbietern: Wie soll man denn da noch den Überblick behalten? Wir brauchen an den Orten, wo Scoringverfahren verwendet werden, diese Transparenz, und wir brauchen auch eine klarere Übersicht darüber, was eigentlich dann Versandhäuser und andere machen, ob die überhaupt ihre Scorewerte einhalten. So etwas muss auch von diesen Versandhäusern klar publiziert werden, damit ich überhaupt die Möglichkeit dieser Kontrolle habe. Und ich muss - was Sie auch schon angeregt haben - per Anklicken, wenn es im Internet ist, diese Werte bekommen. Wie wichtig das auch ist, nicht nur die Gewichtung zu bekommen, sondern auch die Datengrundlage, das zeigt eine Untersuchung von Börse Online. 32 Testpersonen haben einfach die Datenbasis angefragt und dabei ist herausgekommen, bei 11 war es zutreffend, bei 13 war es in mindestens einem Punkt nicht der Fall und bei 8 war es gravierend unvollständig. Das zeigt ja schon mal, dass diese Scorewertberechnung auf einem löchrigen Grund basiert und dass da auch für den Verbraucher Vorsicht geboten ist.

Vors. **Sebastian Edathy**: Dann hat das Wort der Bundesdatenschutzbeauftragte.

SV Peter Schaar: Ich denke, das ist tatsächlich eine automatisierte Einzelfallentscheidung, wenn der Sachbearbeiter nicht über diese Vorgabe hinweggehen kann, wenn das Programm entsprechend ausgestaltet ist. Dann handelt es sich aus meiner Sicht um eine unzulässige automatisierte Einzelfallentscheidung. Ich hoffe, dass die betroffene Person sich an die zuständige Datenschutzaufsichtsbehörde gewandt hat. Und ich wäre auch daran interessiert zu erfahren, was dann aus dem Fall geworden ist. Wir haben, weil uns verschiedene

Beschwerden aus diesem Bereich vorliegen, eine Prüfung des Telekommunikationssektors eingeleitet, und eine Vielzahl von Unternehmen aufgefordert, uns die Art, wie dort gescort wird, zu offenbaren. Die Rückläufe sind jetzt teilweise da. Und auch dort bestätigt sich der erste Eindruck, dass teilweise auch automatisierte Ablehnungsprozeduren laufen. D.h. wenn eine Vielzahl von Daten aus unterschiedlichen Auskunftssystemen zusammengeführt werden, und wenn eine Negativnachricht da ist, dann bekommt der Betreffende keinen Vertrag. Da guckt gar kein Sachbearbeiter mehr drauf. Solche Rückmeldungen habe ich bekommen. Eigentlich skandalös ist, dass teilweise nicht einmal die Ablehnungsgründe genannt werden, sondern allgemein verbrämt werden mit Formulierungen wie: „Aus betrieblichen Gründen“. Und erst auf hartnäckiges Nachfragen von Betroffenen wird dann teilweise gesagt: „Das liegt daran, dass Sie in einem Haus wohnen, wo wir schon mal einen Fall hatten, dass jemand seine Rechnung nicht bezahlt hat“. So etwas ist natürlich aus meiner Sicht nicht hinnehmbar. Ich habe in meinem Zuständigkeitsbereich eine breit angelegte Untersuchung gestartet, und ich denke, ich werde nach ihrem Abschluss auch über die Ergebnisse berichten.

Zum Thema „California Security Breach Information Act“: Ich habe in meiner Stellungnahme schon erwähnt, dass das nicht auf Kalifornien beschränkt ist und dass es jetzt auch auf US-Bundesebene entsprechende Überlegungen gibt, eine solche Offenbarungspflicht für Datenschutzverletzungen einzuführen. Ich weiß auch, dass die Europäische Kommission darüber nachdenkt, im Rahmen der Weiterentwicklung der Datenschutzrichtlinie genau solche Informationspflichten zu verstärken. Das muss sich nicht 100-prozentig orientieren an dem, was in Amerika jetzt schon weitgehend Gesetz ist. Ich denke, es ist ein sehr interessanter, ein guter Ansatz, den auch der Bundesgesetzgeber zumindest erwägen sollte als ein Verfahrensmechanismus, der die Rechte der Betroffenen stärkt: Wenn Daten außer Kontrolle geraten, dass dann die verantwortliche Stelle verpflichtet ist, die davon betroffenen Personen bzw. die möglicherweise davon betroffenen Personen in Kenntnis zu setzen. Das hätte mindestens zwei Konsequenzen: Die erste ist, dass die Person Schutzmaßnahmen treffen kann. Das - finde ich - ist ein ganz wichtiger Punkt. Wenn ich weiß, meine Kreditkarten-Nr. ist missbraucht worden oder ist außer Kontrolle geraten, dann schaue ich mir die Rechnung dreimal an, die ich von dem Kreditunternehmen bekomme. Wenn ich das nicht weiß, tue ich das vielleicht nicht mit der gleichen Sorgfalt. Der zweite Punkt ist: Durch das Bekanntwerden von solchen Datenschutzverstößen oder Sicherheitsverstößen wird ein indirekter Druck auf die Unternehmen ausgeübt, entsprechend mehr für die Sicherheit zu tun, um solchen Verstößen vorzubeugen. Das ist in den USA sehr gut erkennbar. Und ich denke, dass man sich in diesem Punkt durchaus ein Beispiel nehmen kann. Es stimmt nicht, dass die USA generell einen schlechten Datenschutz haben. Sie haben einen anderen Datenschutz. In bestimmten Bereichen ist er sogar besser und manche Mechanismen sind hier wirkungsvoller. Vielen Dank.

Vors. **Sebastian Edathy**: Vielen Dank. Gibt es weitere Wortmeldungen? Frau Kollegin Philipp.

Abg. **Beatrix Philipp**: Bei „Pannenhilfe“, da würde ich Herrn Prof. Abel doch noch mal fragen. Sie haben ja ausgeführt, warum es nicht übertragbar wäre. Könnten Sie das eben noch kurz erläutern, im Hinblick auf die Uhr auch wirklich kurz?

Vors. **Sebastian Edathy**: Herr Prof. Abel.

SV **Prof. Dr. Ralf Bernd Abel**: Ich will versuchen, es ganz kurz zu machen. Es ist auf jeden Fall ein wichtiger Anstoß, dass man überlegt, was passiert bei Datenschutzpannen, wie kann man damit umgehen? Jetzt haben wir im amerikanischen Recht sehr unterschiedliche Situationen, vor allem, wenn man reinguckt, auf was sich das Kalifornische Gesetz bezieht. Das sind nicht sämtliche Daten, sondern das ist vor allem eine Kombination von Daten, um die es dort geht, die dort ausdrücklich genannt sind. Diese Kombination bedeutet keine allgemeine Datenverarbeitung. D.h., man muss schon gucken, worum geht es eigentlich, um was oder welche Informationen? Oder anders gesagt, über den Verlust welcher Informationen soll wem Mitteilung gemacht werden? Das müsste man noch sehr genau betrachten, auch vor dem amerikanischen Hintergrund, dass eben andere Datenschutzgesetze in der Schärfe, jedenfalls in der formalen Schärfe, wie wir sie haben, dort nicht existieren, sondern dass auch zivilrechtlich andere Anspruchsgrundlagen benötigt werden, als es zum Teil bei uns der Fall ist. Denn wir haben im BDSG eine zivilrechtliche Anspruchsgrundlage auf Schadensersatz. Das muss man prüfen. Das können wir hier, schon wegen der gebotenen Kürze, nicht abschließend machen, aber darüber nachzudenken, ist wichtig. Auch nur über den Teil der Daten und Datenkombinationen, die das US-Recht meint, denn sonst könnte es dazu kommen - und das wird in der öffentlichen Diskussion bereits befürchtet -, dass man sagt, wenn irgendwo ein PC wegkommt, auf dem hunderttausende von personenbezogenen Daten sind oder eine Festplatte, soll man denn alle Betroffenen informieren, vor allen Dingen, wenn man gar nicht mehr weiß, wer das überhaupt gewesen war. Das kann es sicherlich nicht sein, sondern hier geht es um vertragliche Schutzpflichten, vertragliche Nebenpflichten. Möglicherweise lässt sich das BGB entsprechend ergänzen. Oder es ließe sich durch eine entsprechende BDSG-Regelung weiterkommen? Darüber muss noch intensiv nachgedacht werden, vor allem, wenn man beachtet, dass die Verstöße materiell in den amerikanischen Gesetzen relativ stark eingeschränkt sind auf ganz bestimmte Kombinationen und auch Daten, die es bei uns so gar nicht gibt, denn die Sozialversicherungs-Nr., das ist etwas, was in den USA so etwas wie eine allgemeine Personenkennziffer darstellt, wenn ich da richtig informiert bin, die es bei uns aus gutem Grunde so nicht gibt und nicht geben darf. Dies muss überdacht werden. Ich hoffe, dass ich jetzt in der Kürze die Frage beantworten konnte.

Vors. **Sebastian Edathy**: Vielen Dank. Gibt es weitere Wortmeldungen seitens der Kolleginnen und Kollegen? Das ist nicht der Fall, dann sind wir am Ende der Anhörung angelangt. Ich darf mich insbesondere im Namen der Abgeordneten bei den Sachverständigen bedanken für die patenten Auskünfte. Ich wünsche Ihnen und uns allen ein gutes Nachhausekommen oder anderenfalls einen angenehmen Arbeitsabend. Die Sitzung ist beendet.

Ende der Sitzung: 18.15 Uhr