18. Wahlperiode

Deutscher Bundestag
Ausschuss Digitale Agenda

# Wortprotokoll
der 58. Sitzung

**Ausschuss Digitale Agenda**
Berlin, den 24. Februar 2016, 16:00 Uhr
11011 Berlin, Konrad-Adenauer-Str. 1
Sitzungssaal: PLH E.200

Vorsitz: Jens Koeppen, MdB

## Tagesordnung - Öffentliche Anhörung

**Tagesordnungspunkt 1** **Seite 08**

Öffentliches Fachgespräch zum Thema
"Europäische Datenschutzgrundverordnung"

a) **Sachverständigenliste**

**Ausschussdrucksache 18(24)SB25**

b) **Fragenkatalog**

**Ausschussdrucksache 18(24)SB26**

**Mitglieder des Ausschusses**

| | **Ordentliche Mitglieder** | **Stellvertretende Mitglieder** |
|---|---|---|
| CDU/CSU | Beermann, Maik | Hornhues, Bettina |
| | Durz, Hansjörg | Lange, Ulrich |
| | Jarzombek, Thomas | Schön (St. Wendel), Nadine |
| | Koeppen, Jens | Tauber, Dr. Peter |
| | Nick, Dr. Andreas | Wanderwitz, Marco |
| | Schipanski, Tankred | Wendt, Marian |
| | Schwarzer, Christina | Whittaker, Kai |
| SPD | Esken, Saskia | Bartol, Sören |
| | Flisek, Christian | Dörmann, Martin |
| | Klingbeil, Lars | Heidenblut, Dirk |
| | Reichenbach, Gerold | Stadler, Svenja |
| | Zimmermann, Dr. Jens | Träger, Carsten |
| DIE LINKE. | Behrens, Herbert | Korte, Jan |
| | Wawzyniak, Halina | Pau, Petra |
| BÜNDNIS 90/DIE GRÜNEN | Janecek, Dieter | Beck (Köln), Volker |
| | Notz, Dr. Konstantin von | Rößner, Tabea |

-3-

Tagungsbüro

Deutscher Bundestag

# Sitzung des Ausschusses Digitale Agenda (24. Ausschuss)
Mittwoch, 24. Februar 2016, 16:00 Uhr

## Anwesenheitsliste
gemäß § 14 Abs. 1 des Abgeordnetengesetzes

| Ordentliche Mitglieder | Unterschrift | Stellvertretende Mitglieder | Unterschrift |
|---|---|---|---|
| **CDU/CSU** | | **CDU/CSU** | |
| Beermann, Maik | | Hornhues, Bettina | |
| Durz, Hansjörg | | Lange, Ulrich | |
| Jarzombek, Thomas | | Schön (St. Wendel), Nadine | |
| Koeppen, Jens | | Tauber Dr., Peter | |
| Nick Dr., Andreas | | Wanderwitz, Marco | |
| Schipanski, Tankred | | Wendt, Marian | |
| Schwarzer, Christina | | Whittaker, Kai | |
| **SPD** | | **SPD** | |
| Esken, Saskia | | Bartol, Sören | |
| Flisek, Christian | | Dörmann, Martin | |
| Klingbeil, Lars | | Heidenblut, Dirk | |
| Reichenbach, Gerold | | Stadler, Svenja | |
| Zimmermann Dr., Jens | | Träger, Carsten | |
| **DIE LINKE.** | | **DIE LINKE.** | |
| Behrens, Herbert | | Korte, Jan | |
| Wawzyniak, Halina | | Pau, Petra | |
| **BÜNDNIS 90/DIE GRÜNEN** | | **BÜNDNIS 90/DIE GRÜNEN** | |
| Janecek, Dieter | | Beck (Köln), Volker | |
| Notz Dr., Konstantin von | | Rößner, Tabea | |

Stand: 19. Februar 2016
Referat ZT 4-Zentrale Assistenzdienste, Luisenstr. 32-34, Telefon: +49 30 227-32659, Fax: +49 30 227-36339

-4-

Tagungsbüro

**Sitzung des Ausschusses Digitale Agenda (24. Ausschuss)**
Mittwoch, 24. Februar 2016, 16:00 Uhr



| Ministerium bzw. Dienststelle (bitte in Druckschrift) | Name (bitte in Druckschrift) | Unterschrift | Amts-bezeichnung |
|---|---|---|---|
| BMWi | Dr. Krogias | | RDir. Ref. |
| BMVI | | | |
| BKM | WITZEL | | ORR |
| BMI | Eickelpasch | | RD |
| BMU | v. Knobloch | | |
| BMI | W. Veil | | Ref. |
| BMJV | SPARY | | Ref. |
| BMWi | Krüger, Philipp | | |
| IKA | Grundmann | | RDir |
| BMJV | HAYUNGS | | RD |
| BMJV | Kynast | | RD |

– 5 –

Tagungsbüro

**Sitzung des Ausschusses Digitale Agenda (24. Ausschuss)**
Mittwoch, 24. Februar 2016, 16:00 Uhr



## Bundesrat

| Land | Name (bitte in Druckschrift) | Unterschrift | Amts-bezeich-nung |
|---|---|---|---|
| Baden-Württemberg | | | |
| Bayern | | | |
| Berlin | | | |
| Brandenburg | | | |
| Bremen | | | |
| Hamburg | | | |
| Hessen | Hartwill | | BE |
| Mecklenburg-Vorpommern | | | |
| Niedersachsen | | | |
| Nordrhein-Westfalen | | | |
| Rheinland-Pfalz | | | |
| Saarland | | | |
| Sachsen | Langer | | Ref. |
| Sachsen-Anhalt | | | |
| Schleswig-Holstein | | | |
| Thüringen | | | |

Tagungsbüro

Deutscher Bundestag

**Sitzung des Ausschusses Digitale Agenda (24. Ausschuss)**
Mittwoch, 24. Februar 2016, 16:00 Uhr

| | Fraktionsvorsitz | Vertreter |
|---|---|---|
| CDU/CSU | | |
| SPD | | |
| DIE LINKE. | | |
| BÜNDNIS 90/DIE GRÜNEN | | |

**Fraktionsmitarbeiter**

| Name (Bitte in Druckschrift) | Fraktion | Unterschrift |
|---|---|---|
| SCHEELE | LINKE | |
| LIENING | CDU / CSU | |
| Piallat | Grüne | |
| Klaßeck | SPD | |
| Schröder | LINKE | |
| Leuxner | SPD | |
| Jörn Pohl | Grüne | |
| Burczyk | LINKE | |
| | | |
| | | |

**Liste der Sachverständigen**
Öffentliche Anhörung
am Mittwoch, 24. Februar 2016, 16.00 Uhr im Saal E.200 PLH

Zum Thema:
Europäische Datenschutzgrundverordnung

**Unterschriftenliste:**

| | |
|---|---|
| **Frau Andrea Voßhoff**<br>Beauftragte für den Datenschutz und die Informationsfreiheit | |
| **Herr Jan Oetjen**<br>Vorstandsmitglied Consumer Applications,<br>United Internet AG | |
| **Frau Dagmar Hartge**<br>Landesbeauftragte für den Datenschutz und<br>für das Recht auf Akteneinsicht Brandenburg | |
| **Frau Dr. Waltraut Kotschy**<br>Expertin für Datenschutz und E-Government | |
| **Herr Prof. Dr. Rossnagel**<br>Leiter des Fachgebiets Öffentliches Recht,<br>Universität Kassel | |

**Tagesordnungspunkt 1**

**Öffentliches Fachgespräch zum Thema "Europäische Datenschutzgrundverordnung"**

Der **Vorsitzende**: Liebe Kolleginnen und Kollegen, ich begrüße Sie ganz herzlich zur 58. Sitzung des Ausschusses Digitale Agenda, heute mit einer weiteren öffentlichen Anhörung zum Thema Europäische Datenschutzgrundverordnung. Ich freue mich über das große Interesse hier im Ausschusssaal und hoffe, dass das Interesse am Live-Stream auf Bundestag.de ebenso groß ist. Ich begrüße alle Zuhörer ganz herzlich. Zum heutigen Thema haben wir fünf Sachverständige eingeladen. In Abstimmung mit den Fraktionen gingen die Einladungen an Frau Andrea Voßhoff, die Beauftragte für den Datenschutz und die Informationsfreiheit, Herrn Jan Oetjen, Vorstandsmitglied Consumer Applications, United Internet AG, Frau Dagmar Hartge, Landesbeauftragte für den Datenschutz und das Recht auf Akteneinsicht in Brandenburg, Frau Dr. Waltraut Kotschy, Expertin für Datenschutz und E-Government und Herrn Prof. Dr. Rossnagel, Leiter des Fachgebiets Öffentliches Recht, Universität Kassel. Ich freue mich, dass wir diesen großen Sachverstand heute in unserem Ausschuss haben, und auf die Diskussion über die Europäische Datenschutzgrundverordnung. Bei der Europäischen Datenschutzgrundverordnung geht es darum, das Datenschutzrecht zu vereinheitlichen, damit die Bürger mehr Kontrolle über die eigenen Daten haben, und dafür Sorge zu tragen, dass wir EU-weit einen gleichen Datenschutzstandard haben. Es darf also keine Rückzugsräume mehr geben. Das ist das Ziel. Mit dem Verordnungsentwurf soll Gleichheit geschaffen werden. Es ist natürlich bei solch großen Projekten nicht überall mit Begeisterung zu rechnen. Die Kritiker sehen eine Bevormundung des Bürgers, die Befürworter loben diese Reform als einen großen Meilenstein in Sachen Verbraucherschutz und die Beseitigung des Flickenteppichs innerhalb Europas. Zu welchen Schlüssen wir hier heute kommen, ob es Änderungen gibt für die Nutzungsrechte, für die Innovation und für die Wettbewerbsbedingungen, das werden wir dann in zwei Stunden sehen. Da sind wir auf die Diskussion gespannt. Bevor wir in die Debatte einsteigen, will ich noch auf die Dinge aufmerksame machen, die wir vereinbart haben. Zuerst wird es ein fünfminütiges Eingangsstatement der Sachverständigen geben, anschließend eine Fragerunde der Fraktionen. An Redezeit für die Abgeordneten stehen jeweils 3 Minuten zur Verfügung. Dann sammeln wir die Fragen, die die Sachverständigen dann beantworten. Jeder Abgeordnete kann zwei Fragen an einen Sachverständigen oder je eine Frage an zwei Sachverständige stellen. Dann gibt es für die Beantwortung jeweils 3 Minuten. In der zweiten Runde werden die Fragen direkt beantwortet, also eine Frage, eine Antwort, jeweils 3 Minuten. Bitte benutzen Sie die Mikrofone und schalten Sie diese ein, bevor Sie reden, und danach wieder aus, damit es keine Rückkopplung gibt. Ich komme zu den Statements der Sachverständigen und erteile als erstes das Wort der Beauftragten für den Datenschutz und die Informationsfreiheit, Frau Andrea Voßhoff, bitteschön.

SVe **Andrea Voßhoff**: Vielen Dank, Herr Vorsitzender, meine Damen und Herren Abgeordnete, liebe Damen und Herren Experten, die Sie heute da sind. Ich darf mich zunächst für die Gelegenheit ganz herzlich bedanken, zu einem der, wie ich finde, datenschutzpolitisch wichtigsten Vorhaben, nämlich der Datenschutzgrundverordnung, mich heute äußern zu können und zu dürfen. Sie wissen alle, dass sich im Dezember vergangenen Jahres die Verhandlungsführer Parlament, Rat und Kommission auf den Text der Datenschutzgrundverordnung geeinigt haben. Ich meine, das war ein guter Tag für Europa und auch ein guter Tag für den Datenschutz. Ein guter Tag für Europa war es vor allen Dingen deshalb, weil es nach vierjährigen Verhandlungen gelungen ist, eines der wichtigsten Vorhaben politisch zu einem erfolgreichen Abschluss zu bringen. Das war während der Verhandlungen nicht immer anzunehmen. Schließlich waren bei einem sehr komplexen Thema 28 Regierungen der EU-Mitgliedstaaten unter einen Hut zu bringen. Dann ist es sehr erfreulich, dass das mit dem entsprechenden Willen und der Kompromissbereitschaft gelungen ist. Und wie ich meine, wird das Europäische Datenschutzrecht künftig durchaus auf hohem Niveau Geltung haben. Es war bei aller Kritik im Detail, dazu kommen wir sicherlich heute noch, ein guter Tag für den Datenschutz. Aus Sicht auch meines Hauses stellt die Datenschutzgrundverordnung im Grunde eines sicher, nämlich die Festschreibung bewähr-

ter Prinzipien des grundrechtsorientierten Datenschutzrechts. Grundlage des Datenschutzrechts ist und bleibt das informationelle Selbstbestimmungsrecht des Einzelnen. Auch das Verbotsprinzip, das beibehalten wurde, ist zu begrüßen. Das gleiche gilt für die weiteren Prinzipien, insbesondere, gerade auch in der Entwicklung der digitalen Welt der Datensparsamkeit, der Erforderlichkeit, der Angemessenheit, der Transparenz und auch der Zweckbindung. Bei aller Kritik im Detail, auch die Gewährleistung der Datensicherheit ist in der Datenschutzgrundverordnung zu finden. Das ist zu begrüßen. Ich denke, dass diese Datenschutzgrundverordnung wirtschaftliche Entwicklung nicht hemmt, sondern eher Anlass und Ansätze gibt für innovative und intelligente Geschäftsmodelle, die sich dann auch durch guten Datenschutz auszeichnen. Demzufolge können sie auch ein Qualitätsmerkmal der europäischen Wirtschaft sein. Sie wissen, die Datenschutzgrundverordnung wird erst ab Mitte 2018 zur Anwendung kommen. Und auch das, das wird sicherlich die Aussprache und das werden die Statements heute zeigen, ist sehr ambitioniert. Es gilt nun, in dieser Zeit die notwendigen Anpassungsregelungen durch die nationalen Gesetzgeber erfolgen zu lassen. Die Öffnungsklauseln, ob wir sie nun gut finden oder nicht, sie sind leider Gottes zum Teil da. Sie müssen mit Leben gefüllt werden. Was dieses mit Leben füllen heißt, auch aus nationaler Sicht, ist zum einen die Frage. Wir haben als einer der wenigen europäischen Mitglieder eine föderale Struktur der Datenschutzaufsichtsbehörden, so dass wir national zu regeln haben, wie und in welcher Weise diese Aufsichtsbehörden in dem künftigen, wichtigen europäischen Datenschutzausschuss vertreten sein werden. Nach meiner Auffassung sollte als ordentliches Mitglied durchaus auch die BfDI per gesetzlicher Regelung in Betracht gezogen werden. Da wir aber eine föderale Struktur haben, sollte sie selbstverständlich auch föderal aufgebaut sein. Die Datenschutzgrundverordnung gewährt die Möglichkeit, einen Stellvertreter für das ordentliche Mitglied zu gewähren. Da wäre zu überlegen, ob dies durch einen Ländervertreter wahrgenommen werden sollte, damit sich diese föderale Struktur widerspiegelt. Ganz wichtig ist mir auch die Möglichkeit, per Öffnungsklausel für die nationalen Mitgliedstaaten, in diesem Falle Deutschland, die verbindliche Bestellung betrieblicher Datenschutzbeauftragter zu ermöglichen. Hier lässt es die Datenschutzgrundverordnung, die dies nicht dem Grunde nach regelt, weil kein Konsens zu erzielen war, zu, dass dieMitgliedstaaten das verbindlich regeln. Es wäre außerordentlich begrüßens-und wünschenswert, wenn der nationale Gesetzgeber die bisherige verbindliche Regelung in Deutschland auch beibehalten würde, nämlich das sogenannte Zweisäulenmodell des Datenschutzes, bestehend aus Datenschutzaufsicht der Behörde, aber eben auch aus dem betrieblichen oder behördlichen Datenschutzbeauftragten. Das hat sich in der Vergangenheit nicht nur bewährt, sondern ist auch im Interesse der Unternehmen und des Datenschutzes aufrechtzuerhalten. Noch einen Punkt, den ich in besonderer Weise erwähnen möchte: Die Datenschutzgrundverordnung gibt den nationalen Mitgliedstaaten die Möglichkeit, den Beschäftigtendatenschutz weiter auszubauen. Auch das ist ein Punkt, den es zu erwähnen gilt und der bei der nationalen Umsetzung einen hohen Stellenwert einnehmen sollte.

Der **Vorsitzende**: Vielen Dank. Herr Oetjen, Sie haben das Wort, bitteschön.

SV **Jan Oetjen**: Herzlichen Dank für die Einladung und die Möglichkeit, in diesem Rahmen zu der Datenschutzgrundverordnung Stellung zu nehmen. Die Datenschutzgrundverordnung ist für uns einer der zentralen Pfeiler eines digitalen Binnenmarktes, den wir dringend brauchen. Ein einheitlicher Datenschutz, oder unsere Erwartung an einen einheitlichen Datenschutz, basiert auf vier Prinzipien. Wir brauchen unbedingt eine Gleichheit, also eine Beendigung des aktuellen Zustands, in dem im gleichen Absatzmarkt unterschiedliche Gesetzesvorschriften gelten, je nachdem, wo der Anbieter seinen Sitz hat. Wir brauchen eine Klarheit, eine Verständlichkeit in der Regelung. Wir brauchen eine Sicherheit, die Vertrauen bei dem Verbraucher schafft. Vor allem brauchen wir die Möglichkeit, digitale datengetriebene Mehrwerte nicht nur zu ermöglichen, sondern auch zu fördern, damit wir zukünftig Innovationen in Europa nicht mehr importieren müssen, sondern direkt hier in Europa entwickeln können. Die Datenschutzgrundverordnung ist ein wichtiger Schritt in die richtige Richtung. Gerade

das Marktortsprinzip ist ein wichtiger Pfeiler für die Gleichheit. Es dürften keine Datenschutzoasen entstehen. Wir haben bei der Steuergesetzgebung gesehen, was entstehen kann, wenn man nationale Lücken lässt oder wenn der Wettkampf einzelner Mitgliedstaaten um die Attraktivität des Standorts entfacht. Deswegen sehen wir diese Öffnungsklauseln, wie gerade im Eingangsstatement erwähnt, sehr kritisch. Man wäre gut beraten, diese klarer zu fassen oder so mit Leben zu füllen, dass solche Hintertüren nicht geöffnet werden. Genauso wichtig ist die gleiche Umsetzung und Durchsetzung des Datenschutzes. Wenn man in Deutschland sieht, dass nach letzter Zählung etwa 500 Datenschutzbeauftragte in der deutschen Industrie, in deutschen Start-ups und in wahrscheinlich ungefähr ein gutes Dutzend mittelständischen Internetunternehmen beschäftigt sind, in Irland aber der gesamten Silicon Valley-Dependance von Europa gerade einmal 50 Datenschützer gegenüberstehen, ist relativ klar, dass wir so keine Gleichheit bei der Durchsetzung in Europa erzielen werden. Es geht nicht um einen sogenannten „Race to the Top“, also wer den stärksten Datenschutz in der Durchsetzung in Europa erzielt hat, hat den besten Standortvorteil. Es geht darum, ein Level Playing Field zu erzielen und dass in jedem Staat auch die gleiche Durchsetzung der Vorschriften erfolgt. Wir denken, eine zentrale Rolle wird hier dem Datenschutzausschuss zukommen. Man wäre gut beraten, diesen mit den entsprechenden Kompetenzen und Ressourcen auszustatten, um für eine Gleichordnung, Gleichrichtung der einzelnen Datenschutzorgane in Europa zu sorgen. Weiter für sehr begrüßenswert halten wir das Einwilligungs- und Transparenzprinzip, das in dem Gesetz umgesetzt ist. Wir möchten aber davor warnen, dass dieses Prinzip überspannt wird. Wenn man für alles ein Opt-In braucht, wird das zwei Effekte haben. Zum einen wird es eine sogenannte Opt-In-Inflation geben. Wenn Sie auf jeder Seite erstmal sechs OKs abklicken müssen, bevor Sie die Seite benutzen können, ist es wenig hilfreich und der Nutzer wird irgendwann zum blinden Abklicken übergehen.Die nächste Innovation in dem Markt wäre eine Brower-Extention oder eine App, die dieses Abklicken für den Nutzer automatisch übernimmt. Im Gegensatz dazu brauchen wir einen Anreiz, um die Pseudonymisierung von Daten voranzutreiben. Wenn für die Verarbeitung von pseudonymisierten Daten die gleichen rechtlichen Voraussetzung an Opt-Ins wie bei derVerarbeitung von Klardaten geknüft werden, wird es logischerweise dazu kommen, dass die Firmen dazu tendieren, sich ein volles Opt-In für die Verarbeitung von Klardaten zu besorgen, und eben nicht mit den für den Verbraucher deutlich besser geschützten pseudonymisierten Daten zu arbeiten. Hier sehen wir Nachbesserungs-, vor allen Dingen Klarstellungsbedarf, wie mit pseudonymisierten Daten umgegangen werden darf. Letzter Pfeiler in dem gesamten digitalen Konstrukt für Europa ist, dass die Datenschutzgrundverordnung sicherlich der zentrale Pfeiler ist. Er ist aber nicht der alleinige Pfeiler. Die Datenschutzgrundverordnung allein wird nicht dazu führen, dass wir unter Datenschutzgesichtspunkten den gewünschten Zustand in Europa haben oder die Wettbewerbssituation in Europa sich vereinfacht. Wir werden parallel dazu dringend eine Regulierung der Plattform brauchen, allen voran der Betriebssysteme, denn hier eröffnet das Opt-In-Prinzip einen ganz gefährlichen Vector. Die Opt-Ins einzusammeln wird einer Plattform deutlich einfacher gelingen als einzelnen Playern, die nur Applikationen zur Verfügung haben. Wenn ich einen Player habe, der eine Suchmaschine, einen Email-Dienst, eine Cloud beherrscht, wird es dem deutlich einfacher sein, Opt-Ins einzukassieren. Wir werden die aktuelle Machtsituation in Europa eher manifestieren als auflösen. Wichtig ist, dass die Datenschutzgrundverordnung nicht als Monolith gesehen wird, sondern als ein Baustein des digitalen Marktes, und dass wir die Plattformneutralität in Europa entsprechend umsetzen. Vielen Dank.

Der **Vorsitzende**: Vielen Dank, Herr Oetjen. Frau Hartge, Sie haben das Wort, bitteschön.

SVe **Dagmar Hartge**: Vielen Dank, Herr Vorsitzender. Meine Damen und Herren, ich bedanke mich ganz herzlich für die Einladung. Auch von mir bekommen Sie zunächst den Hinweis, dass diese Datenschutzgrundverordnung durchaus ein Erfolg geworden ist. Sie mag Mängel haben, sie mag noch Probleme in der Praxis aufwerfen. Aber sich nach vier Jahren auf einen einheitlichen Datenschutz für ganz Europa verständigt zu haben, halte ich für eine große Leistung. Mir ist es wichtig, Ihnen zu sagen, dass hier die Bürgerrechte und

die Wirtschaft in einen Ausgleich gebracht worden sind, der recht fair gelungen ist. Wichtiges Anliegen der Datenschutzgrundverordnung ist aus meiner Sicht im technischen Bereich, Innovationen zu schaffen. Wir haben hier Punkte, wie Privacy by Design, durchaus ein wichtigen Faktor, um der Wirtschaft Möglichkeiten zu geben, sich nach vorne zu entwickeln. Wir haben im Bereich der Technik Anforderungen, wie Pseudonymisierung, Anonymisierung, die sicherlich für innovative Entwicklungen ein wichtiger Gesichtspunkt sind. Wir haben auf der anderen Seite für die Bürgerinnen und Bürger eine Stärkung ihrer Transparenzrechte, die sich aus meiner Sicht als sehr wichtig erweisen. In der Vergangenheit hat sich gezeigt, dass die Transparenz häufig mangelhaft war. Transparenz ist eine Grundlage für ein informationelles Selbstbestimmungsrecht. Ohne Wissen kann man sich nicht entscheiden. Die Datenschutzgrundverordnung führt das One-Stop-Shop-Prinzip ein, was der Wirtschaft auch einen großen Vorteil bringt, weil sie in Zukunft nur noch mit einer einzigen Aufsichtsbehörde zu tun hat. Damit wird ein massiver Kritikpunkt beseitigt, den gerade wir Aufsichtsbehörden in der Vergangenheit immer wieder gehört haben. Sehr wichtig ist auch das Marktortprinzip. Mit dem Marktortprinzip schaffen wir es erstmals, auch US-amerikanische Unternehmen sowie Unternehmen aus Drittstaaten an das europäische Datenschutzrecht zu binden. Bisher war das nicht der Fall. Bisher waren wir darauf angewiesen, mit Unternehmen zu verhandeln und uns zu bemühen, dass sie sich an europäisches Recht halten. Das ist jetzt anders. Das bedeutet, dass die Unternehmen in einem Wettbewerb stehen, der angemessen und fair ist und der gestützt wird durch Sanktionen, die erstmals in dieser Grundverordnung in einem Ausmaß verhängbar sind, wie wir es bisher in Europa nicht gekannt haben. Wir haben Öffnungsklausueln, was man durchaus kritisch sehen kann. Die Grundverordnung ist damit angetreten, dass sie im privaten Bereich, im Bereich für die Wirtschaft, gesagt hat: Wir wollen einen komplett einheitlichen Datenschutz. Das ist sicherlich nicht ganz gelungen und das hat auch gute Gründe. Es ist in den Verhandlungen sichtbar geworden, dass es eben nicht möglich ist, alles komplett einheitlich zu machen. Ich hoffe sehr, dass man die Öffnungsklauseln, die geschaffen worden sind, so nutzen kann, dass die Einheitlichkeit möglichst weitgehend erhalten bleibt. Wir haben etwas erhalten, was aus deutscher Sicht sicherlich auch zu begrüßen ist. Im öffentlichen Bereich ist es weiterhin möglich, öffentlich-rechtliche Vorschriften zu haben. Hier wird es darum gehen, dass wir einen Abgleich mit der Grundverordnung haben, um uns mit den öffentlich-rechtlichen Vorschriften im Rahmen der Grundverordnung zu bewegen. Ein ganz wichtiger Punkt sind die Aufsichtsbehörden. Gerade Deutschland ist als föderales Land anders aufgestellt als ein dezentraler Staat wie Frankreich. In Deutschland wird es darum gehen, dass wir die Aufsicht so aufstellen, dass sie den Vorschriften der Grundverordnung entsprechend zügig und effektiv funktioniert. Ich halte das für sehr gut machbar. Wir haben mit der Konferenz der Datenschutzbehörden und der Länder ein Gremium, das bereits geübt und sehr gut dafür geschaffen ist, für eine effiziente Umsetzung der Regelungen zu sorgen. Und dieses Gremium wird auch dafür sorgen, dass die nötigen Abstimmungsprozesse in einer großen Geschwindigkeit erfolgen. Zum Schluss würde ich auch gerne den Hinweis geben, welche Vorschrift mir als Öffnungsklausel sehr wichtig ist. Wir haben immer noch Bedarf daran, den Beschäftigtendatenschutz selbst zu regeln. Da die Grundverordnung das nicht mit Standards gemacht hat, würde ich mir wünschen, dass diese Öffnungsklausel vom deutschen Gesetzgeber genutzt wird. Vielen Dank.

Der **Vorsitzende**: Vielen Dank, Frau Hartge. Frau Dr. Kotschy, Sie sind die Nächste.

SVe **Dr. Waltraut Kotschy**: Vielen Dank für die Erteilung des Wortes und vielen Dank für die Einladung. Meine Funktion ist vielleicht ein bisschen die österreichische Sichtweise einzubringen, die naturgemäß etwas verschieden ist. Sie werden sicher wissen, dass die österreichische Regierung mit der Grundverordnung nicht ganz so glücklich war. Ich bin aber der Meinung, man sollte Unglück nicht weiter pflegen, sondern zur Tagesordnung übergehen. Wir werden damit leben und das Beste daraus machen. Für uns ist zunächst einmal zweifellos die Schaffung des Marktortprinzips, wie Sie das nennen, eine ganz große Errungenschaft, weil es endlich die Unterschiedlichkeit in den Regeln für verschiedene Marktteilnehmer beseitigt. Das ist meiner Meinung nach eine wirklich

große Errungenschaft. An sich ist das Ziel, den europäischen Datenschutz zu vereinheitlichen, zu begrüßen. Woran wir etwas weniger glauben ist, dass das so schnell geht. Es erscheint uns doch eher so, als dass Datenschutz als Querschnittsmaterie zunächst erst einmal relativ abstrakt formulierte Prinzipien haben kann. Dementsprechend braucht das Herunterbrechen auf die Probleme der einzelnen Materie ein bisschen Zeit und Mühe, damit man Datenschutz auch wirklich praktisch anwenden kann. Wir müssen ein bisschen Geduld haben in Europa, wenn wir diese abstrakten Regeln tatsächlich für die einzelnen Use Case, mit entsprechenden Safeguards anfüllen. Das dauert. Das ist Knochenarbeit. Da muss man sich hinsetzen und diese Use Cases wirklich herausarbeiten. In diesem Sinne sind wir jetzt ein bisschen unglücklich darüber, dass für den privaten Bereich nationale Regelungen gewissermaßen weggeschoben werden. Weil, es ist natürlich schwierig sich vorzustellen, wie jetzt im Bereich des traditionellen Marketings in Österreich bewährte Regelungen plötzlich nicht mehr gelten sollen. Wir müssen noch nachdenken, wie man das lösen kann. Meiner Meinung nach ist es besser, diese Regeln zu haben, als keine Regeln zu haben, solange wir keine gemeinsamen Regeln haben. Nun, man wird sehen, wie man damit umgeht. Gewisse Nachteile sehen wir in Art. 6 f, wo es um die legitimen Interessen des Auftraggebers oder eines Dritten geht. Hier haben wir in Österreich eine strengere Regelung. Sie werden mich fragen, wie gibt es das. Ja, das gibt es, weil wir das immer so hatten und bei der Umsetzung der Richtlinien nicht gezwungen waren, einen niedrigeren Datenschutz einzuführen. Das muss jetzt endgültig aufgegeben werden. Das ist für uns eine ganz entscheidende Regelung. Wir sind sehr dafür, dass eine Risikofolgenabschätzung betrieben wird. Das Problem wird sein, dass in der praktischen Durchführung seitens der Aufsichtsbehörden großer Aufwand, große Kenntnis, großer Einfallsreichtum gefordert ist. Und ich hoffe, wir sind alle so aufgestellt, dass diesem Anspruch genügt werden kann. Das ist ein hoher Anspruch an die Aufsichtsbehörden. Transparenz, da bin ich vollkommen der Meinung meiner Vorrednerin ist wesentlich besser verwirklicht als bisher. Ich finde vor allem die Idee, dass Icons eingesetzt werden können, wirklich interessant und hoffentlich zukunftsweisend. Insgesamt sage ich, trotz einer grundsätzlich etwas negativen Haltung, dass wir voranschreiten müssen. Wir müssen schauen, wie wir die Chancen der Grundverordnung nutzen können. Ich sehe vor allem, dass unendlich viel Arbeit von den Aufsichtsbehörden und vom Europäischen Datenschutzausschuss geleistet werden muss, und die Mitgliedstaaten aufgerufen sind, die Voraussetzungen dafür zu schaffen. Danke.

Der **Vorsitzende**: Danke Ihnen, Frau Dr. Kotschy. Jetzt hat Prof. Dr. Rossnagel das Wort für sein Eingangsstatement. Bitteschön.

SV **Prof. Dr. Alexander Roßnagel:** Vielen Dank für die Einladung. Bitte erlauben Sie, dass ich eine etwas andere Perspektive einnehme. Ich will mein Statement in fünf Thesen gliedern: 1. Der Entwurf einer Datenschutzgrundverordnung ist enttäuschend. Sie führt in Deutschland zu einer Absenkung des Datenschutzes. Sie wird den künftigen Herausforderungen wie zum Beispiel Big Data, Cloud Computing und datenzentrierten Geschäftsmodellen nicht gerecht. Man versucht sie nicht einmal zu adressieren. 2. Die Verordnung leidet vor allem an der Unterkomplexität ihrer Regelungen. Sie will in 45 Artikeln des materiellen Datenschutzes die gleichen Probleme behandeln, die im deutschen Datenschutzrecht in tausenden von Vorschriften geregelt werden. Wird unterstellt, dass nicht alle deutschen Regelungen übertrieben sind, wird deutlich, welches Defizit die Datenschutzgrundverordnung aufweisen muss. Wer meint, diese vielfältigen gesetzlichen Regelungen durch wenige generelle und abstrakte Regelungen ersetzen zu können, unterschätzt nicht nur die Regelungsaufgabe gewaltig, sondern übersieht auch die negativen Auswirkungen, die dadurch entstehen, dass er die Vielfalt und Differenzierung bestehender Regelungen beseitigt und gewaltige Lücken in der Rechtssicherheit schafft. 3. Die Verordnung leidet an einer übertriebenen Technikneutralität. Sie übertreibt den sinnvollen Ansatz, keine Regelung zu erlassen, die Technikentwicklungen verhindert, in dem sie auch die spezifischen Risiken ignoriert, die zum Beispiel Big Data, Ubiquitous Computing, Cloud Computing und datenzentrierte Geschäftsmodelle verursachen. Die gleichen Regelungen wie für die Datenverarbeitung beim Bäcker um die Ecke sollen auch für diese risikoreichen Datenverarbeitungsformen

gelten. Durch solche Regelungen werden nicht nur die spezifischen Grundrechtsrisiken übersehen, sondern bleiben auch Interessengerechtigkeit und Rechtssicherheit unberücksichtigt. 4. Die Verordnung verfehlt das ursprüngliche Ziel, ein unionsweit einheitliches Datenschutzrecht zu schaffen, das für einen einheitlichen Grundrechtschutz und für Wettbewerbsgleichheit sorgt. Das liegt zum einen daran, dass die Verordnung nur Anwendungsvorrang und keinen Geltungsvorrang vor dem nationalen Recht genießt. Dadurch gelten die Regeln der Mitgliedstaaten weiter. Nur wenn die Verordnung und die nationale Regelung in der Anwendung zu unterschiedlichen Ergebnissen führen, ist die Verordnung vorrangig anzuwenden. Dies führt dazu, dass das künftige Datenschutzrecht aus einem unübersichtlichen Konglomerat von Unionsrecht und nationalem Recht besteht. Große Unsicherheit entsteht darüber, welche nationale Vorschrift künftig noch anwendbar ist. Ein einheitliches Datenschutzrecht wird aber auch durch die Verordnung selbst verfehlt. Da der Unionsgesetzgeber selbst gemerkt hat, dass seine Regelungen unterkomplex sind, gibt die Verordnung in etwa 60 Regelungen den Mitgliedstaaten Regelungsaufträge oder gewährt ihnen Regelungsspielräume. Dies führt dazu, dass alleine deshalb die meisten der deutschen Datenschutzvorschriften weiter anwendbar sind. Dies gilt zum Beispiel für das gesamte öffentliche Datenschutzrecht, für alle Regelungen, die Pflichten zur Datenverarbeitung begründen, zum Beispiel für die Bereiche des Arbeitsrechts, des Medienrechts, der Forschung, der Statistik, der Berufsgeheimnisse, des Umgangs mit medizinischen Daten und für viele weitere Bereiche. Ein einheitlich praktiziertes Datenschutzrecht wird schließlich durch den hohen Abstraktionsgrad der Regelungen verhindert. Nehmen wir als Beispiel den Erlaubnistatbestand der berechtigten Interessen, die mit den schutzwürdigen Interessen der betroffenen Person abzuwägen sind. Diese Abwägung wird in jedem Mitgliedstaat nach der bisherigen Datenschutzkultur unterschiedlich erfolgen. Bei gleichem Wortlaut wird die Abwägung zum Beispiel für die Videoüberwachung in Großbritannien an der bisher sehr großzügigen Praxis orientiert, in Deutschland hingegen an der Abwägung, der Paragraph 6 b) BDSG zugrunde liegt. Weil einzelne Technikanwendungen von der Verordnung ignoriert werden, wird diese wichtigste Verarbeitungserlaubnis für jede Technikanwendung in jedem Mitgliedstaat praktisch einen anderen Inhalt haben. Wettbewerbsgleichheit ist so nicht zu erreichen.
5. Die schwer durchschaubare Gemengelage von Unionsrecht und deutschem Recht erfordert eine Anpassung des deutschen Datenschutzrechts, insbesondere des Bundesdatenschutzgesetzes, vor allem für die nichtöffentliche Datenverarbeitung. Notwendig sind Regelungen, die die Verordnung erst vollzugsfähig machen. Erforderlich sind außerdem Festlegungen zu den Spielräumen des deutschen Gesetzgebers, mit welcher Zielrichtung er davon Gebrauch machen will. Um Umstellungskosten zu minimieren würde ich empfehlen, sich ziemlich weit an den geltenden Regelungen zu orientieren. Ich denke, wir werden über diesen Regelungsbedarf noch sprechen. Vielen Dank.

Der **Vorsitzende**: Meine Damen und Herren Sachverständige, ich bedanke mich für die ersten Ausführungen und darf die Debatte eröffnen. Als erstes gebe ich das Wort dem Abgeordneten Marian Wendt für die CDU/CSU-Fraktion.

Abg. **Marian Wendt** (CDU/CSU): Vielen Dank, Herr Vorsitzender, meine Damen und Herren Sachverständigen. Wir sind auch froh, dass wir nach vier Jahren derVerhandlungen auf EU-Ebene nun einen Vorschlag zu einem einheitlichen Datenschutzniveau und Recht in Europa haben. Dass das noch nicht perfekt ist, haben Sie herausgestellt. Das wissen wir auch.Wir müssen das stetig verbessern und verändern. Deswegen haben wir heute das Gespräch mit Ihnen als Experten. Meine Frage geht zunächst an Herrn Oetjen. Wie bewerten Sie im Zusammenhang mit der Datenschutzgrundverordnung und bezogen auf Cloud Computing, Big Data und andere datenzentrierte Geschäftsmodelle die getroffene Regelung bei der Weiterverarbeitung und Pseudonymisierung? Sind diese Anwendungsmodelle, diese Geschäftsmodelle, weiterhin möglich?.Werden sich diese erschwerend oder erleichternd auswirken? Frau Voßhoff, meine Frage an Sie als Datenschutzbeauftragte lautet: Wie können wir eine Situation herbeiführen, die es weiterhin zulässt, Anonymisierung und Pseudonymisierung für einen hohen Stellenwert zu generieren und auch Big Data, Open Data einfacher zu ermöglichen?

Der **Vorsitzende**: Als nächstes die Kollegin Wawzyniak für die Fraktion DIE LINKE.

Abg. **Halina Wawzyniak** (DIE LINKE.): Ich will in der ersten Runde je eine Frage an Frau Kotschy und Herrn Roßnagel stellen. Diese beziehen sich im Wesentlichen auf etwas, was schriftlich vorgetragen worden ist. Frau Kotschy, Sie haben auf Seite 2 geschrieben: „(…) wesentliche Aspekte der seit 1995 doch erheblich geänderten Datenverarbeitungsgewohnheiten unserer Gesellschaft sind jedoch unberücksichtigt geblieben. Damit meine ich vor allem Änderungen in der Rollenverteilung der wesentlichen Akteure, betroffener, verantwortlicher Dienstleister.“ Ich habe das ähnlich gelesen bei Herrn Prof. Roßnagel. Er hat das meines Erachtens in der These 3 auch so angedeutet. Zumindest bei dem Punkt Cloud Computing auf der Seite 3, wo Sie das Thema ansprechen, dass sozusagen „(…) personenbezogene Daten Dritter übertragen werden, dem Einflussbereich und der Kontrolle der Verantwortlichen entzogen werden.“ Ich würde gerne von Frau Kotschy hören, was diese geänderten Rollenverteilungen sind. Gibt es da einen Lösungsansatz? Herrn Prof. Roßnagel würde ich gerne zu einer schriftlichen Aussagen befragen. Er schrieb, dass spezifische Regelungen des Modells der Auftragsdatenverarbeitung notwendig sind unddass diese modifiziert werden müssen. Beinhaltet das, dass die Rollenverteilung von betroffenen, verantwortlichen Dienstleister nochmal anders definiert werden müssten?

Der **Vorsitzende**: Vielen Dank. Für die SPD-Fraktion der Kollege Reichenbach.

Abg. **Gerold Reichenbach** (SPD): Ich habe zunächst eine Frage an Frau Voßhoff. Sie schreiben in Ihrer Stellungnahme bei der Frage, wie die künftige Vertretungsregelung ausgestaltet werden soll - hat mich auch nicht überrascht, dass alle Kompetenzen möglichst bei Ihnen liegen sollen bzw. einheitlich bei der BfDI zu regeln sei. Jetzt entnehme ich aber der Antwort von Herrn Prof. Roßnagel, unter Verweis auf Art. 23 Abs. 4) und 5) Grundgesetz, dass bei einer grundsätzlichen Einbindung der Länder der öffentliche Bereich im Länderbereich bleiben würde. Vor diesem Hintergrund frage ich Sie, was halten Sie von der Regelung, die die bayerische Seite vorgeschlagen hat, nämlich dies im Rahmen der bestehenden Datenschutzkonferenz der Landesdatenschutzbeauftragten zu regeln. Die zweite Frage geht an Frau Hartge. Es ging über die Ticker, dass Großbritannien für sich in Anspruch nimmt, dass sich das Vereinigte Königreich vom Anwendungsbereich desArtikels 43 a), da geht es um die Weitergabe von Daten europäischer Bürger an Strafverfolgungsbehörden oder Sicherheitsdiensten anderer Länder (Snowden, NSA), ausgenommen fühlt. Welche Konsequenz hätte das für einen einheitlichen Datenschutz innerhalb Europas? Welche Auswirkungen hätte das auf Daten, die innerhalb der Europäischen Datenschutzgrundverordnung nach Großbritannien transferiert würden?

Der **Vorsitzende**: Für die Fraktion BÜNDNIS 90/DIE GRÜNEN Dr. Konstantin von Notz, bitteschön.

Abg. **Dr. Konstantin von Notz** (BÜNDNIS 90/DIE GRÜNEN): Meine Damen und Herren Sachverständigen, herzlichen Dank für diese interessanten Einführungen. Ich glaube, es wird deutlich, dass die schwierigen Operationen der Umsetzung noch vor uns liegen. Ich möchte zwei Fragen an Herrn Prof. Roßnagel stellen. Zum einen, wo wird die Aufsicht zukünftig stattfinden und wie schafft man es, eine flächendeckende Datenschutzaufsicht und -kontrolle im Hinblick auf das, in der Verordnung verankerte, One-Stop-Shop-Verfahren zu gewährleisten? Kann es tatsächlich darin liegen, die Kontrolle in Brüssel zu zentrieren oder brauchen wir diese föderale Struktur, die wir haben. Die zweite Frage bezieht sich flankierend auf das, was wir jetzt erleben. Wir wissen um die Probleme bei den Geheimdiensten und Sicherheitsbehörden, bei Massenüberwachung und ähnlichem. Da stellt sich die Frage, wie man die Dinge flankiert. Die Europäische Datenschutzgrundverordnung, würde ich jetzt einmal zuspitzen, ist wenig wert, wenn wir den Status quo bei dieser Massenüberwachung, die wir haben, behalten. Deshalb die Frage im Hinblick auf das Privacy Shield, das nur vor dem Hintergrund der Snowden-Veröffentlichung zu erklären ist, und die EuGH-Entscheidung. Was muss hier passieren? Reicht das aus, was wir jetzt als lockere Zusagen

hören, oder wie kann man eigentlich diese Diskussion Nachfolgeabkommen Safe Harbor verbinden mit der Frage Europäische Datenschutzverordnung, um am Ende zu einem effektiven Grundrechtschutz der Bürgerinnen und Bürger zu kommen, der in unser aller Interesse liegen sollte.

Der **Vorsitzende**: Vielen Dank für die Fragen. Kommen wir zu deren Beantwortung. Die Fragen vom Kollegen Wendt beantworten bitte Herr Oetjen und Frau Voßhoff. Herr Oetjen, Sie haben als erster das Wort.

SV **Jan Oetjen**: Vielen Dank. Wie der Name Big Data vermuten lässt, folgen Big Data-Geschäftsmodelle der einfachen Formel Datenmenge mal Datenqualität. Man braucht möglichst viele Daten möglichst guter Qualität, um in diesem Sektor Erfolg zu haben. Das Unternehmen, dem das am erfolgreichsten gelingt, wird das beste und schnellste Geschäft aufbauen. Jetzt hat das deutsche Datenschutzgesetz nicht gerade den schlechtesten Ruf, sowohl in Deutschland als auch international. Es erlaubt aktuell die Verarbeitung von pseudonymisierten Daten ohne explizite Opt-Ins aller Nutzer einholen zu müssen. Jetzt mag man auf den ersten Blick denken, das zusätzliche Opt-Ins für die Verarbeitung jeglicher Form von pseudonymisierten Daten würden das Datenschutzniveau heben. Wie im Eingangsstatement aber erörtert, befürchten wir, dass das Gegenteil der Fall ist - wie man heute schon an diesen klassischen Cookie Opt-In-Laschen, die auf jeder Seite herunterfahren und sagen, Achtung, diese Seite setzt Cookies, sehen kann. Das führt einfach dazu, dass der Nutzer gegenüber Opt-Ins buchstäblich abstumpft und irgendwann alles abklicken wird, was man ihm vorsetzt. Von daher wird es hier nicht zu einer Anhebung des Datenschutzniveaus kommen. Im Gegenteil führt dies zu einer Inflation von Opt-Ins und dem großen Risiko, dass der Nutzer nicht mehr unterscheidet, wo sind wirklich kritische Daten, die ich freigebe, und wo geht es einfach nur um pseudonymisierte Verarbeitung. Der zweite Effekt wird sein, dass Unternehmen keinen Anreiz haben, Daten zu pseudonymisieren. Denn, wenn ich die gleichen Anforderungen für Klardaten wie für pseudonyme Daten habe, wird das Unternehmen dazu übergehen, gleich Klardaten zur Verarbeitung abzufragen, was unter Datenschutzgesichtspunkten schlechter ist, als wenn man mit pseudonymisierten Daten arbeiten darf. Dritter Punkt und das ist ein sehr gefährlicher. Natürlich manifestiert es die aktuellen Machtverhältnisse in Europa. Die Plattformen, die Betriebssysteme haben die besten Chancen Opt-Ins einzukassieren und werden dementsprechend die großen Vorteilsnehmer dieser Regelung sein, wenn für jedwede pseudonymisierten Daten Opt-In-Verfahren eingeführt werden müssen. Dann wird derjenige sie erzielen, der die höchste Nutzungsintensität und die stärkste Nähe zum Nutzer hat. Das sind naturgemäß die großen Plattformen, allen voran die Betriebssysteme. Ich glaube an diesen Punkt, um Ihre Frage klar zu beantworten. So wie es heute geregelt ist, sehen wir ein Risiko für Big Data-Geschäftsmodelle in Europa, aber auch für Innovationen, die nicht nur von Großkonzernen betrieben werden, sondern von Jung- und Kleinunternehmen, denen wir in Europa eine Chance geben wollen.

SVe **Andrea Voßhoff**: Vielen Dank für die Frage. Ich will auf die letzten Worte von Herr Oetjen eingehen, dass er ein Risiko für Big Data-Anwendungen sieht und damit auch für Innovationen in Europa. Ich halte dagegen. Ich denke, Big Data-Anwendungen sind auch unter der Datenschutzgrundverordnung anwendbar. Ich werbe sehr dafür, diese Technologien der Anonymisierung und Pseudonymisierung nachhaltig zu fördern. Ich glaube, das ist eine Möglichkeit, Innovationen in diesem Bereich zu forcieren, die in der Vergangenheit nach meiner Auffassung viel zu kurz gekommen sind Das heißt für mich, dass wir bewusst auf datenschutzfreundliche Produkte und Anwendungen setzen. Ich meine, dass das möglich ist. Ich darf ergänzend noch erwähnen, durch die Datenschutzgrundverordnung zieht sich in vielen Bereichen, auch was die technologische Entwicklung betrifft, für die Unternehmen das Thema der sogenannten Zertifizierung. Es ist wichtig, dass bestimmte Modelle, die für innovative Entwicklung denkbar sind, auch zertifizierbar sind. Das heißt datenschutzkonform ausgestaltet und mit einer entsprechenden Zertifizierung versehen werden können. Ich kann die Wettbewerbsvorteile oder -nachteile - ich bin kein Wirtschaftspolitiker - letztendlich nicht abschließend bewer-

ten. Ich sehe aber gerade in Deutschland den Aspekt, datenschutzfreundliche Technologien im Bereich anonymisieren oder pseudonymisieren zu fördern, als zu wenig berücksichtigt an. Da würde ich mir mehr politischen Willen wünschen.

Der **Vorsitzende**: Die Fragen von der Kollegin Wawzyniak gingen an Frau Dr. Kotschy und Herrn Prof. Roßnagel.

SVe **Dr. Waltraut Kotschy**: Danke vielmals. Wenn man die Definitionen im Art. 4 der Grundverordnung ansieht, erkennt man, dass sich im Text seit 1995 nichts geändert hat, obwohl sich in der Wirklichkeit gerade beim Betroffenen meiner Meinung nach doch sehr Wesentliches geändert hat. Seit 1995 ist die Privatperson durch die Erreichbarkeit und Verfügbarkeit des Internets in eine völlig andere Position gelangt, was ihre Fähigkeit betrifft, Daten zu verarbeiten- seien es die eignen oder seien es die Daten von anderen. Ein Kritikpunkt ist, dass man diese Änderung, die für unser gesellschaftliches Leben ungeheuer stark ist, in der Definition nicht reflektiert sieht. Man sieht sie eigentlich nur im Recht auf Datenportabilität reflektiert. Das ist der einzige Punkt, wo auf diese Frage eingegangen wird. Die an mich gestellte Frage lautete, ob man hier etwas ändern müsste. Das ist natürlich im gegenwärtigen Zeitpunkt eine Frage, die ich lieber mit Nein beantworten würde, weil sie sonst ganz hoffnungslos ist. Es geht eher darum, ob es uns möglich wäre, bei der Interpretation dieser Bestimmungen darauf einzugehen, dass der Betroffene heute in zwei Varianten vorkommt: einmal als echtes „Opfer der Datenverarbeitung“ und einmal als „Täter“, weil er selbst Daten zur Verarbeitung einbringt und sich dazu Plattformen bedient, die ihm angeboten werden. Dieses Verhältnis, dass der Betroffene gleichzeitig auch Verantwortlicher ist, der sich eines Auftragsverarbeiters bedient, müsste in der Interpretation etwas stärker herausgearbeitet werden, weil er extreme Folgen hat. Er macht ganz klar, wer eigentlich über die Daten, die man hier aufnimmt auf einem Band, wenn man läuft etc., verfügungsberechtigt ist. Wer ist eigentlich der Verantwortliche für die Verarbeitung dieser Daten? Der Betroffene. Man muss durch eine solche Sichtweise viel klarer machen, wo die Verfügungsgewalt liegt, die im Zusammenhang mit Ubiquiteous Computing noch alle ermittelt werden. Ich glaube, hier würde eine genauere Definition der Interpretation erforderlich sein.

SV **Prof. Dr. Alexander Roßnagel:** Zum Thema Cloud Computing denke ich, dass die Datenschutzgrundverordnung uns in eine Situation gebracht hat, die eine große Rechtsunsicherheit nach sich zieht. Wir haben nicht mehr die Definition im § 3 Abs. 7, nach der die Auftragsdatenverarbeiter Teil der Stelle sind. Die werden jetzt mit eigener Verantwortung behandelt. Das heißt, Datenübermittlung an diese ist jetzt eine Datenübermittlung, die zu rechtfertigen ist. Vorher war das nicht der Fall. Als Rechtfertigungsgrund, als Erlaubnistatbestand haben wir nur Art. 6 Abs. 1f, die Interessenabwägung. Das wird in vielen Fällen dazu führen, dass die Schutzwürdigkeit des Betroffenen höher zu gewichten ist als die berechtigten Interessen derer, die die Daten ins Cloud Computing geben wollen. Die Beauftragung als Datenauftragsverarbeiter setzt voraus, dass dieser Auftragsverarbeiter sorgfältig ausgewählt ist, dass er Weisungen bekommt, dass er entsprechend kontrolliert wird. Das überfordert den normalen Cloud Computing-Nutzer gewaltig. Das kann der nicht. Und der Cloud Computing-Anbieter kann auch nicht realisieren, dass das stattfindet. Wir haben Anforderungen, die so nicht erfüllbar sind. Wir müssten Regelungen finden, wo eine Fremdkontrolle möglich ist. Eine Zertifizierung, die die Grundlage dafür bietet, dass jemand Cloud Computing anbieten darf. Aber das fehlt. Wir müssen jetzt überlegen, ob wir das mit den deutschen Spielräumen, die wir haben, nachholen. Dann haben wir in Deutschland aber andere Regeln als in anderen Mitgliedstaaten. Zweite Frage, zur Effektivierung der Aufsicht. Ich denke, hier kommt man in ein ganz schwieriges Dilemma. Denn einerseits ist die jeweilige Aufsichtsstelle unabhängig, ausdrücklich unabhängig. Andererseits muss die Aufsicht in Europa irgendwie koordiniert werden. Wie man das hinbekommt, wie man die dezentrale Unabhängigkeit und eine zentrale, gemeinsame Sichtweise von Aufsichtsbehörden realisiert, das wird ganz schwierig sein. Da sind die Regelungen, noch nicht ausgereift. Dritter Punkt war die Frage, bewirkt das, was wir inzwischen über das Privacy Shield wissen - es ist sehr wenig - dass eine angemessene Datenverarbeitung in den USA angenommen werden kann. Wenn man das

vergleicht mit den Vorgaben des EuGH vom 6. Oktober 2015, muss man zu dem Ergebnis kommen, dass weder die Reduzierung staatlicher Überwachung auf das absolut Notwendige noch einen ausreichenden Rechtsschutz in den USA realisiert oder garantiert wird.

Der **Vorsitzende**: Vielen Dank. Die Fragen vom Kollegen Reichenbach beantworten bitte Frau Voßhoff und Frau Hartge.

SVe **Andrea Voßhoff**: Herr Abg. Reichenbach, die Datenschutzgrundverordnung schreibt vor, dass Mitgliedstaaten, die föderale Aufsichtsstrukturen haben, einen gemeinsamen Vertreter in den Ausschuss entsenden sollen. Es gibt einige Länder, die haben kleinere föderale Strukturen. Aber im Grunde hat nur Deutschland eine so ausgeprägte und, wie ich finde, bewährte föderale Aufsichtsstruktur,. Deshalb muss sich selbstverständlich in diesem Ausschuss die föderale Struktur widerspiegeln. Ich hatte mit meinen Antworten darauf hingewiesen, dass wir in dem Ausschuss ein ordentliches Mitglied zu benennen haben und in der Datenschutzgrundverordnung ist enthalten, dass dieses ordentliche Mitglied einen Vertreter hat. Meine Argumentation war, dass ich der Auffassung bin, ein Bundesgesetz sollte die Vertretung regeln. Ich halte das für notwendig und geboten, weil der Bund auch eine Einstandspflicht hat bezüglich der Einhaltung der Grundverordnung und damit des europäischen Rechts. Deshalb hielte ich die Regelung durch ein Bundesgesetz für sinnvoll. Ich könnte mir die Regelung so vorstellen, wie in meinem Eingangsstatement gesagt, damit sich die föderale Struktur widerspiegelt, dass die BfDI das ordentliche Mitglied ist und der Stellvertreter von den Ländern entsprechend nominiert und dort gesetzt ist. Sie haben Recht, dass die Themen,die im Europäischen Datenschutzausschuss auch als rechtsverbindliche Entscheidungen getroffen werden können, in vielen Fällen Bereiche tangieren, die in die Länderkompetenz gehören. Deshalb werden sich in dieser Konstruktion das ordentliche Mitglied und der Stellvertreter auch abzustimmen haben. Nicht dass das ordentliche Mitglied abstimmen kann, wie es für richtig hält, sondern dass es nicht nur mit dem Stellvertreter eine enge Abstimmung gibt. Denn - und das ist der zweite Punkt, den man hier in diesem Zusammenhang noch erwähnen muss und soll - durch unsere föderale Struktur sind wir auch gehalten, eine einheitliche Meinungsbildung der Datenschutzaufsichtsbehörde in Deutschland herbeizuführen. So eine enge Koordinierung wird uns vor grundsätzliche Herausforderungen stellen. Ich finde, dass diese enge Koordinierung und die Abstimmung dazu sehr wohl über die Datenschutzkonferenz nicht nur erfolgen kann, sondern erfolgen soll. Es geht aber um die Frage, wer die Bundesrepublik dort vertritt. Deshalb habe ich vorgeschlagen, aufgrund der Einstandspflicht des Bundes, daß die Bundesbeauftragte das ordentliche Mitglied sein sollte. Aber damit die Interessen der Länder gewahrt sind, auch ein Ländervertreter gesetzlich vorgesehen wird. Die beiden stimmen sich ab und beide müssen sich eng an die Vorgaben der deutschen Datenschutzaufsichtsbehörden, die ihre Meinung entsprechend zu koordinieren haben, anlehnen. Ich will nicht unbedingt von imperativen Mandaten sprechen, aber es geht darum, die deutschen Interessen mit einer Stimme zu vertreten.

Abg. **Gerold Reichenbach** (SPD): (Nachfrage) Die Bayern schlagen vor, das so zu machen, aber das jeweils die Datenschutzkonferenz per Wahl festlegt, wer Vertreter und wer Stellvertreter ist, so dass nicht automatisch die BfDI Vertreter ist.

SVe **Andrea Voßhoff**: Wenn man das einem Gremium wie der Datenschutzkonferenz überlassen würde, sehe ich das Problem, dass damit der Bund seiner Einstandspflicht nicht unbedingt nachkommen kann. Denn, je nachdem, wäre er von der, im Gremium getroffenen, Entscheidung abhängig. Wenn diese nicht getroffen würde, wäre Deutschland nicht repräsentiert. Deshalb hielte ich es für sinnvoller und zielführender, durch ein Bundesgesetz diese Vertretungsregelung zu fixieren. Dies schließt nach meiner Auffassung die Interessenlage der Länder in keinem Falle aus. Ähnlich strukturiert wie - das kennen wir auf der Bundesebene in der föderalen Struktur - Bund und Bundesländer sich in europäischen Fragen bei gemeinsamen Zuständigkeiten einigen müssen.

SVe **Dagmar Hartge**: Vielen Dank, Herr Abg. Reichenbach. Ihre Frage zielt darauf ab, was wäre, wenn es möglich ist, sich aus § 43 a) tatsächlich zu verabschieden. So, wie Großbritannien das ganz offensichtlich erklärt hat. Wenn es möglich wäre, sich zu verabschieden, dann würde das bedeuten, dass Staaten, die sagen, wir müssen uns an diese Vorgabe nicht halten, auch keine Vorgabe haben in Bezug auf die Frage, ob sie bei Anfragen von Gerichten aus Drittstaaten Daten übermitteln dürfen. Man muss für Großbritannien ganz klar sehen, dass es dort viele Unternehmen gibt, die Daten deutscher Bürgerinnen und Bürger verarbeiten. D.h., es beträfe uns als Bürgerinnen und Bürger unmittelbar. Wenn das andere Mitgliedstaaten auch machen würden, wäre diese Schutzvorschrift, die es letztendlich werden sollte, ausgehebelt. Ich hoffe sehr, dass am Ende durch Prüfungen feststellt wird, dass ein Vorbehalt nicht geht. Die Regelung ist ein bisschen schwierig, weil sie tatsächlich justizielle Hintergründe berührt und sich mitten in der Grundverordnung wiederfindet. Dass man mit einer Klausel der Einwilligung sagen kann, ich halte mich nicht daran, kann ich der Grundverordnung nicht entnehmen. Das hat auch mich schon überrascht. Am Ende bleibt zu hoffen, dass nach nochmaliger Prüfung festgestellt wird, dass dies gar nicht möglich ist und Großbritannien zurückgeholt werden kann.

Der **Vorsitzende**: Alle Fragen wurden nun beantwortet. Dann kommen wir zur zweiten Runde. In der zweiten Runde hat der Kollege Schipanski das Wort für die CDU/CSU-Fraktion. Und es wird gleich im Anschluss geantwortet.

Abg. **Tankred Schipanski** (CDU/CSU): Vielen Dank, Herr Vorsitzender. Ich darf erstmal feststellen,dass der Kollege Dr. von Notz jetzt leider nicht mehr da ist. Wir haben weder irgendwo eine Massenüberwachung festgestellt noch ist der Privacy Shield Ausfluss der Snowden-Enthüllungen. Ich denke, das haben wir hier und auch in anderen Ausschüssen festgestellt. Dementsprechend bedarf es einer Berichtigung dieser Aussage des Herrn Kollegen. Ich habe eine Frage an Frau Voßhoff. Es geht nochmal um die pseudonymisierten Daten. Wir im deutschen Recht kennen diesen Begriff. In der Datenschutzgrundverordnung ist das für die anderen Mitgliedstaaten eine neue Kategorie, die wir einführen. Er wird zu einem offenen Rechtsbegriff, der entsprechend ausgelegt werden muss. Welche Gefahren sehen Sie in diesem Zusammenhang? Können wir uns mit unserem deutschen Verständnis ein Stück durchsetzen oder bedarf das einer langen justiziellen Klärung? Meine zweite Frage geht an Frau Hartge. Es betrifft ebenfalls diese Verfahren der Anonymisierung, Pseudonymisierung, die wir kennen. Uns, als Deutsche, liegt sehr daran, diesen beiden Verfahren einen höheren Stellenwert zu geben. Aus Ihrer Erfahrung, was können Sie uns politisch empfehlen, um beiden Verfahren einen höheren Stellenwert zu geben? In den anderen Mitgliedstaaten oder auch in der Anwendung der Datenschutzgrundverordnung ist das eine neue Kategorie. Und wir wollen mehr dafür werben. Es war sehr aufwendig von deutscher Seite, diese neue Kategorie überhaupt hineinzubringen.

SVe **Andrea Voßhoff**: Ja, wir haben in der Datenschutzgrundverordnung eine Vielzahl von unbestimmten Rechtsbegriffen, die der Interpretation bedürfen. Wir kennen in Deutschland eine Definition der pseudonymisierten Daten in Abgrenzung zur Anonymisierung. Das ist für uns auch Grundlage und Basis. Die Gefahren langer justizieller Klärungen würde ich in dem Bereich eher weniger sehen. Bei anderen Rechtsbegriffen bedarf es einer justiziellen Klärung. Im Bereich der pseudonymisierten Daten würde ich meinen, eher weniger. Künftig wird dem Europäischen Datenschutzausschuss und den nationalen Parlamenten, sofern sie Gestaltungsspielraum haben, in allen anderen Fällen dem Datenschutzausschuss die hohe und wichtige Funktion zukommen, solche Begrifflichkeiten durch Leitlinien und Vorgaben zu definieren. Es gibt andere Rechtsbegriffe, bei denen das Risiko erheblich größer ist.

SVe **Dagmar Hartge**: Die pseudonymisierten Daten sind in der Datenschutzgrundverordnung auch definiert. Wir haben in Art. 3 Nr. 3a) die Definition, so dass wir europäisch von den gleichen Begrifflichkeiten ausgehen werden. Ich denke, dass der Europäische Datenschutzausschuss ein gutes Gremium ist, um für die Pseudonymisierung für alle Mitgliedstaaten gleiche Anwendungsfelder zu entwickeln. Der Ausschuss hat, wie man in den Regelungen sieht, die zentrale Funktion, für eine

Einheitlichkeit der Rechtsanwendung zu sorgen, so dass er sich auch Themen annehmen kann, die praktisch bedeutungsvoll werden können. Ich denke schon, dass der Pseudonymisierung hier im Datenschutzrecht eine hohe Bedeutung zukommt. Wir haben die anonymisierten Daten. Das ist für Datenschützer immer perfekt, aber man kann mit denen nicht immer arbeiten. Das ist die deutsche Erfahrung. Ich glaube, dass die Anwendungsfelder gefunden und festgelegt werden können, so dass wir alle profitieren könnten.

Abg. **Halina Wawzyniak** (DIE LINKE.): Nochmal eine Frage an Frau Kotschy und Herrn Roßnagel. Diesmal zum Thema Profiling. Das wird unter bestimmten Bedingungen in der Datenschutzgrundverordnung zugelassen, darf aber nicht zu automatisierten Entscheidungen führen. Zumindest wir haben es so gelesen, dass es durch die Datenschutzgrundversorgung keine Ausdehnung der Möglichkeit des Profiling gibt - im Vergleich zur bisherigen Regelung in Deutschland, dass es aber die Möglichkeit gibt, dass der nationale Gesetzgeber restriktivere Einschränkung des Profiling vornehmen kann. So haben wir das gelesen. Die Fragen an Frau Kotschy und Herrn Roßnagel wären, ob Sie restriktivere Regelungen im Hinblick auf Profiling sinnvoll finden. Wenn Sie die sinnvoll finden, was könnten Sie sich vorstellen?

SVe **Dr. Waltraut Kotschy**: Profiling ist tatsächlich eine der ungemütlichsten Datenverarbeitungen aus der Sicht des Betroffenen, weil hier tief in die Privatsphäre eingegriffen wird, um daraus Schlüsse zu ziehen. Wir sind uns einig, dass natürlich nicht solche Schlüsse gezogen werden, die Rechtsfolgen oder Folgen von ähnlicher Bedeutung haben. Wir könnten uns unter Umständen vorstellen, dass man im Marketingbereich irgendwelche sinnvollen Grenzen festlegen könnte, worauf nicht profiliert werden darf. Denn Marketing ist wahrscheinlich eine der wichtigsten Anwendungsbereiche von Profiling. Marketing ist eine jener Materien, bei der nicht behauptet werden kann, dass es nicht erlaubt ist. Es ist zweifellos eine erlaubte Tätigkeit. Aber es stehen sich legitime Interessen auf der einen Seite und Datenschutzinteressen auf der anderen Seite gleichwertig gegenüber. Es ist die Kunst des Gesetzgebers gewesen, durch Rechtsvorschriften eine Balance zwischen diesen Interessen zu erreichen, indem er Konditionen schafft, mit denen beide legitimen Interessen verwirklicht werden können. Ich glaube, in dem Bereich wäre es sogar sehr wichtig, Grenzen von Profiling festzulegen. Ich sehe noch nicht ganz, was der Gesetzgeber tun darf. Denn das ist privater Bereich und der Gesetzgeber sollte im privaten Bereich keine datenschutzrechtlichen Regelungen schaffen. Da wäre eine andere Form der Schaffung von Regeln, nämlich „The code of conducts“, sehr interessant. Ich würde noch kurz etwas aus österreichischer Erfahrung sagen wollen, ich weiß nicht, wie das in Deutschland ist. Codes of Conducts sind für uns ein Fremdkörper. Es besteht kein besonderer Enthusiasmus der Branchen in der Wirtschaft, sich hervorzutun und umfangreiche Regelwerke zu schaffen. Vielleicht muss doch wieder der Gesetzgeber eingreifen, indem er jene Grenzen festlegt, die er für Profiling, im Verhältnis zum Grundrecht auf Datenschutz, als angemessen ansieht.

Der **Vorsitzende**: Die gleiche Frage an Prof. Roßnagel.

SV **Prof. Dr. Alexander Roßnagel:** Im Art. 20 der Datenschutzgrundverordnung ist Profiling nur teilweise geregelt, nämlich nur, soweit es die Grundlage ist für automatisierte Entscheidungen. Das heißt, die Personalisierung von Diensten und Geräten zum Beispiel ist nicht erfasst. Wenn Google bei seiner Suche auf mich personalisiert, um mir bessere Auskünfte geben zu können, und deswegen ein äußerst umfassendes Personenprofil von mir erstellt, ist das von diesem Artikel gar nicht erfasst. Als Grundlage für automatisierte Entscheidungen, insbesondere für das Scoring und sowas, haben wir die Regel, dass es grundsätzlich verboten ist. Es sei denn, europäische Regeln, nationale Regeln oder die Einwilligung erlauben dies. Jetzt nichts zu regeln würde nur dazu führen, dass keine nationalen Regeln bestehen. Die Einwilligung kann trotzdem erteilt werden und die europäischen Regeln könnten trotzdem getroffen werden. Deswegen halte ich es für sinnvoll, dass der deutsche Gesetzgeber sich dieses Problems annimmt,d iesen Spielraum ausnutzt und geeignete Regeln aufstellt um, wie das dann in Abs. 1b) des Art. 20 steht, einen Ausgleich zwi-

schen den verschiedenen Interessen zu gewährleisten. Wir haben 2009 relativ gute Regeln in das BDSG hineingebracht. Das wäre eine Gelegenheit, diese beizubehalten, anzupassen oder zu verschärfen. Ich erinnere an die Regelung zur Zulässigkeit in § 28 a) und b). Die kann man jetzt weiterverwenden. Wir haben Auskunftsregeln, die in § 34 Abs. 2 und 4 BDSG einen entsprechenden Ausgleich bilden. Alle diese Regeln können genutzt werden. Und dann würde ich den Gedanken, den Sie angesprochen haben, nämlich dass es bestimmte Daten gibt, die nicht Gegenstand von Profiling sein dürfen, aufgreifen. Besonders schützenswerte Daten oder Daten, die für die Betroffenen unfair sind, wie Geo-Scoring etc., sind dann herauszunehmen.

Der **Vorsitzende**: Vielen Dank. Herr Kollege Reichenbach, bitte.

Abg. **Gerold Reichenbach** (SPD): Ich habe zwei Fragen an zwei Sachverständige. Die eine geht an Frau Hartge zu dem gleichen Thema, zu dem ich auch Frau Voßhoff gefragt habe. Frau Voßhoff hat eine zwingend eindeutige Regelung mit der Einstandspflicht des Bundes begründet. Dazu würde ich gerne die Sicht einer Landesdatenschutzbeauftragten hören. Wie kann im föderalen System die Abbildung noch adäquat stattfinden? Vielleicht können Sie auch zu dem bayerischen Vorschlag, den Sie sicher kennen, Stellung nehmen. Die zweite Frage geht an Prof. Roßnagel. Sie haben, wie Frau Hartge, in Ihrer Stellungnahme ausgeführt, dass man im Rahmen des Beschäftigtendatenschutzes die Öffnungsmöglichkeiten der Datenschutzgrundverordnung, die für den Bereich spezifische gibt, nutzen sollte. Deswegen meine Frage: Welche Konsequenzen hätte das für die höchstrichterlichen Entscheidungen, die wir jetzt schon im Arbeitsrecht haben, wenn wir dies nicht nutzen würden? Wenn man sagen würde, wir lassen es darauf ankommen, dass es im Rahmen der Datenschutzgrundverordnung geregelt ist. Wenn dies nicht ausreichend wäre, wo sehen Sie dann den dringendsten nationalen Regelungsbedarf zur Spezifizierung des Arbeitnehmerdatenschutzes?

SVe **Dagmar Hartge**: Zu der Frage, wie man es für die Vertretung im Europäischen Datenschutzausschuss auch machen könnte. Ich sehe keine Vorgabe, dass der Bund vertreten sein muss. Ich denke, im Datenschutz ist es ein bisschen anders. Wir haben gleichberechtigte Aufsichtsbehörden in einem föderalen Mitgliedstaat. Die Grundverordnung geht für föderale Mitgliedstaaten davon aus, dass diese Staaten sich festlegen müssen, wer sie vertritt. Aber das ist eine offene Frage. Klar ist es nicht ganz einfach, das in einem föderalen Staat zu entscheiden. Wir haben Bund und Länder, und da bin ich mit Frau Voßhoff einer Meinung, wir brauchen, weil wir Bund und Länder haben, in diesem Ausschuss auch einen Vertreter des Bundes und einen Vertreter der Länder. Wer aber der führender Vertreter ist, wer die Stimme am Ende abgibt, das meine ich, muss man in diesem Bereich, wo wir wirklich gleichberechtigt nebeneinander sitzen, einem Gremium der Datenschutzbeauftragten überlassen. Deswegen fände ich es richtig, wenn der Gesetzgeber den Rahmen vorgibt, dass wir als Konferenz der Datenschutzbeauftragten sicherzustellen haben, eine effektive Vertretung im Ausschuss zu gewährleisten. Es muss eine erste und eine zweite Vertretung geben. Es muss nach meiner Auffassung auch definitiv immer so sein, dass einmal Bund und einmal Land vertreten sind. Wer aber führt, das kann der Gesetzgeber nicht festlegen. Da ist es auch ganz klar, dass wir da unterschiedliche Interessen haben. Die Länder vertreten eben ihre Länderinteressen. Ich möchte auch darauf hinweisen, dass wir gerade im privaten Bereich überwiegend Befugnisse in den Ländern haben. Das heißt, auch die meisten Federführungen sind in den Ländern, so dass natürlich aus dieser Sicht auch passend ist, dass vielleicht auch mal ein Ländervertreter die Stimme in Brüssel abgibt. Eine Koordinierung wird immer nötig sein. Jemand, der in Brüssel eine Stimme für eine federführende Aufsichtsbehörde abgibt, ist daran gebunden und kann nicht einfach selbsttätig andere Entscheidungen treffen. Zum bayerischen Vorschlag: Finde ich gut, weil der letzten Endes daran ansetzt, dass die Vertretung effektiv erfolgen muss und zielführend ist. Das trifft sich mit meiner Auffassung, dass die Länder genauso wie der Bund vertreten können. Das ist im Prinzip diese Regelung.

SV **Prof. Dr. Alexander Roßnagel:** Der Beschäftig-

tendatenschutz regelt ein besonderes „Gewaltverhältnis“ zwischen dem Arbeitgeber mit seinem Direktionsrecht und dem Arbeitnehmer mit seinen Grundrechten. Und es ist zu versuchen, die beiden Dinge in Einklang zu bringen. Dafür haben wir eine jahrzehntelange Rechtsprechung der Arbeitsgerichte. Der Art. 82 ermöglicht für den Bereich des Beschäftigtendatenschutzes, dass die Mitgliedstaaten durch Gesetz oder Kollektivvereinbarungen spezifischere Regelungen treffen. Das heißt, wenn sie keine treffen, gelten die allgemeinen Regelungen, die für alles gut sind. Dann werden nämlich alle diese Fragen schlicht über die Regelung des § 6 Abs. 1b), nämlich, dass hier ein Arbeitsvertrag besteht, geregelt. Das allein gibt ein Riesenfeld von Rechtsunsicherheit. Ob unter diesen Grundsätzen dann die Rechtsprechung weiter aufrechterhalten werden kann, ist ein vollkommenes offenes Thema. Deswegen wäre es äußerst hilfreiche, wenn die Bundesrepublik diese Möglichkeit in die Hand nimmt und einen weiteren Anlauf unternimmt, ein differenzierteres Datenschutzrecht für das Beschäftigungsverhältnis zu regeln als das in § 32 BDSG.

Der **Vorsitzende**: Vielen Dank. Kollege Janecek, bitteschön.

Abg. **Dieter Janecek** (BÜNDNIS 90/DIE GRÜNEN): Eine Frage habe ich an Frau Hartge. Das betrifft den Art. 20 Abs. 1a), die Öffnungsklausel, nach der Profiling erlaube ist, wenn es in den Mitgliedstaaten die entsprechenden Rechtsvorschriften gibt. Jetzt habe ich in Ihrer Stellungnahme gelesen, das wäre eventuell möglich. DasBundesministerium für Justiz und Verbraucherschutz sagt, dass ist nur dann möglich, wenn man diese Rechtsvorschriften entsprechend erweitert oder ändert. Vielleicht können Sie nochmal Stellung nehmen, auch vor dem Hintergrund der Scoring-Diskussion. An Frau Voßhoff habe ich ebenfalls eine Frage. Es ist die Rede von bis zu 200 Verordnungen, auch Gesetzen, die im Rahmen der Europäischen Datenschutzgrundverordnung verändert und erlassen werden müssen. Wie wird der Prozess gestaltet? Gibt es Listen, die die Ministerien für sich anfertigen? Vielleicht können Sie ein bisschen aus dem Nähkästchen plaudern und gleichzeitig Ihren eigenen Ansatz schildern. Wie weit würden Sie gehen, um bestimmte Spielräume zu schaffen oder zu verhindern?

Der **Vorsitzende**: Vielen Dank. Frau Hartge und Frau Voßhoff, bitteschön.

SVe **Dagmar Hartge**: Vielen Dank für die Frage zum Profiling. Art. 20 nennt das Profiling unter diesem Gesichtspunkt automatisierte Einzelentscheidung. Zum einen muss man hier sagen, es ist natürlich bedauerlich, dass wir keine richtige Profiling-Regelung bekommen haben, die wirklich Grenzen setzt. Hier gibt es erstmal keine Einzelentscheidung. Aber, jetzt kommt Abs. 1, und das lese ich eigentlich so, dass der Gesetzgeber durchaus Regegelungen treffen kann, in denen er sagt, in diesen Fällen ist eine Form des Profilings möglich. Hier, denke ich, dass der Gesetzgeber aufgerufen ist, Regelungen, die wir derzeit haben, dann vielleicht nochmal neu zu erlassen oder zu bestätigen. Wir haben so etwas wie ein Profiling. Nehmen Sie Scoring. Was ist Scoring anderes als ein Profiling einer Person? Dass ich automatisiert geprüft und zugeordnet werde. Deswegen gehe ich schon davon aus, dass man unter Abs. 1a), b) Rechtsvorschriften für diese sensiblen Bereiche, wo es zwingend ist, dass der Gesetzgeber auch die Grenzen zieht, schafft. Eins dürfte ganz klar sein. Die Wirtschaft wird sagen, wir sind es gewohnt, dass wir Scoring-Verfahren zu unserer Rechtssicherheit durchführen und erwarten, dass es die weiter geben wird. Dann stellt sich die Frage, wie kommen wir dazu, diese Verfahren wirklich rechtmäßig durchzuführen. Da sind die Rechtsgrundlagen nun einmal das Mittel der Wahl. Die die Grundverordnung hat dies wahrscheinlich mit Absicht d offen gelassen hat. Ich rechne damit, dass diese Klausel entsprechend genutzt werden wird.

SVe **Andrea Voßhoff**: Der Anpassungsbedarf für die nationalen Mitgliedstaaten mit einer Vielzahl bereichsspezifischer Regelungen ist immens. Das gilt vor allen Dingen mit Blick darauf, dass die Datenschutzgrundverordnung aller Voraussicht nach ab Mitte 2018 Anwendung finden wird. Der Zeitplan, um die notwendigen Regelungen und Anpassungsvorgaben zu treffen, ist außerordentlich ambitioniert. Nach meiner Kenntnis ist es so, dass im Innenministerium bereits daran gearbeitet

wird. Man kann sicherlich sagen, dass mit den Ländern intensive Kontakte geführt werden. Über den Sachstand kann vielleicht das Innenministerium berichten. Wir werden im Rahmen unserer Möglichkeiten diesen Anpassungsbedarf sehr nachhaltig und intensiv begleiten. Weil durch den Anpassungsbedarf auch erheblicher Gestaltungsspielraum entsteht. Sie sagten vorhin, Spielräume ausnutzen. Ja, die aus Sicht der Datenschutzaufsichtsbehörden, da sind sich Bund und Länder sicherlich einig, datenschutzfreundlichen Regelungen sollten in jeder Hinsicht ausgeschöpft werden. Regelungsmaßstab ist am Ende die Grundverordnung. Ich möchte nochmal nachhaltig unterstützen, was die Kollegin Hartge sagte. Die Regelung zum Profiling ist eines der Kernprobleme. Aus datenschutzaufsichtsrechtlicher Sicht außerordentlich bedauerlich wurde dieses Problem nur begrenzt, geregelt. Das Anlegen von Profilen wurde leider nicht regelt. Deshalb wäre nationaler Umsetzungsspielraum in dem Bereich zugunsten des Datenschutzes außerordentlich wünschenswert. Ich bin dem Ausschuss Digitale Agenda dankbar, dass er als erster der Ausschüsse dieses Thema auf die Tagesordnung gesetzt hat. Ich würde mir auch wünschen, dass das Parlament diesen Anpassungsbedarf von Anfang an sehr intensiv begleitet. Das ist eine gewaltige Aufgabe. Davon ausgehend, dass im nächsten Jahr Bundestagswahlen sind, ist der Umsetzungszeitraum begrenzt. Hier kommt es entscheidend darauf an, welche Schwerpunkte gesetzt werden. Was ist notwendig? Was jetzt geregelt werden muss, darf nicht nur gesehen, sondern muss auch entschlossen umgesetzt werden. Eine parlamentarische Beteiligung, gerade wenn ich den Ausschuss Digitale Agenda in seiner Aufgabenstruktur sehe, wäre außerordentlich wünschenswert. Das ist keine Kleinigkeit. Da gibt es viel Regelungs- und Gestaltungsbedarf, den wir gemeinsam nutzen sollten.

Der **Vorsitzende**: Vielen Dank. Kollege Jarzombek.

Abg. **Thomas Jarzombek** (CDU/CSU): Frau Voßhoff, ich bin Ihnen ausgesprochen dankbar, dass Sie das so sagen. Ich denke, das könnte nochmal deutlich an anderen Stellen artikuliert werden, dass hier durchaus Kompetenz und Interesse an diesem Thema herrschen. Möglicherweise auch in Abgrenzung zu anderen Auschüssen. Ich möchte noch zwei Fragen stellen, einmal an Herrn Oetjen, was das Thema Geschäftsmodelle und Level Playing Field, den Wettbewerb auf Augenhöhe betrifft. Wie sieht denn für Sie ganz konkret die Situation aus im Vergleich zur amerikanischen Konkurrenz. Sie betreiben E-Mail und Cloud-Dienste und beispielsweise Google platziert ähnliche Produkte. Wie unterscheidet sich Ihre Erlössituation durch die unterschiedliche Arbeit von Profiling von der Googles ?Wie können Sie einen Wettbewerb gegen diese amerikanischen Anbieter dauerhaft gewährleisten? Zweite Frage wäre an Frau Voßhoff. Wie beurteilen Sie die Situation, inwieweit man tatsächlich europäisch vorhandernes Datenschutzrecht exekutieren kann- unabhängig von der Frage des Strafmaßes oder des Ordnungsrahmens, eher orientiert an der Frage nach Personal, das vor Ort die tatsächliche Durchsetzung vornimmt, beispielsweise wie in Irland?

SV **Jan Oetjen**: Vielen Dank für die Frage. Ich glaube, Sie sprechen genau den kritischen Punkt an, den es in einer digitalen Neuordnung von Europa zu regeln gibt. Aktuell sehen wir die Situation sehr kritisch, für uns kritisch, weil sie erst 2018 in Kraft treten wird. Dass wir dieses Marktortprinzip aktuell nicht haben, führt dazu, dass amerikanische Anbieter einerseits durch die Rechtsstellung einem anderen Recht unterliegen und natürlich zum zweiten durch die Exekution in Irland einer anderen behördlichen Kontrolle unterliegen als wir in Deutschland. Das mal vorangestellt. Sie fragten nach den klaren Problemen in der Monetarisierung. Ich will es bildlich auszudrücken. Wenn Sie nicht zielgerichtete Werbung ausspielen, verdienen Sie gerade mal ein Zehntel von dem, was ein Anbieter verdienen wird, der diese Werbefläche mit Profildaten anreichern kann. Je reicher man diese Daten erheben und je besser man sie verknüpfen kann, desto höher die Monetarisierung. Neben den Größenvorteilen der großen US-Plattformspiele haben wir deren höhere Monetarisierung auf der einzelnen Internetseite. Für uns ist von essentieller Wichtigkeit, dass dieses CRR schnell in Kraft tritt. Zum Zweiten muss es auch gut umgesetzt und in allen Mitgliedstaaten gleich durchgesetzt werden. Zweiter großer Faktor, den ich vorhin schon einmal erwähnte, ist die Bündelung und Zusammenschaltung von Diensten. Gerade das Beispiel Google ist

ein sehr gutes. Vor zwei Monaten hat Google damit begonnen, die gesamten Datenprofile aus allen Diensten zusammenzuschalten. Also das, was auf dem Android-Gerät, über G-Mail und über die Suche generiert wird, sogar das, was Firmen, die Google-Analytics als Analyse-Tool einsetzen, an Daten generieren, wird zu einem Profil zusammengeschlossen-und das auf Fremdseiten, die die Nutzer gar nicht sehen. Das halte ich unter deutschen Datenschutzgesichtspunkten für sehr kritisch. Zum anderen zeigt das, wie wichtig es ist, dass wir eine Entbündelung dieser Services im Gesetzesansatz zur Plattformneutralität schaffen. Denn wir werden nationale Gleichheit über dieses Gesetz schaffen. Das ist sehr positiv. Wir werden für alle Marktteilnehmer die grundsätzliche Startvoraussetzung schaffen, sich Opt-Ins einzuholen. Aber das Kernproblem ist, dass sich dominierende Plattformen in den letzten Jahren diesen riesengroßen Vorsprungerarbeitet haben. Möglich war dies durch dieses Ungleichgewicht im nationalen Recht und das Konstrukt, über Safe Harbor in Europa mehr nach US-Recht als nach europäischem Recht zu verfahren. Das wieder aufzuholen werden Sie nur schaffen, wenn Sie gleichzeitig die Neutralität der großen dominierenden Plattformen herstellen und eine Entbündelung der Services erreichen.

SVe **Andrea Voßhoff**: Herr Abg. Jarzombek, die Frage, wie denn die künftigen Regelungen tatsächlich exekutiert werden, verstehe ich als Frage, welche Sanktionsmöglichkeiten es gibt, Verstöße gegen das künftige Recht zu ahnden. Da hat die Datenschutzgrundverordnung einen Bußgeldrahmen festgelegt, der für die Unternehmen durchaus sehr schmerzhaft sein kann. Den letzten Teil Ihrer Frage verstehe ich so, ob das Personal unter anderem in den Datenschutzaufsichtsbehörden ausreichend und dazu in der Lage ist, entsprechend Reglungen umzusetzen. Das ist ein Thema, dem sich das Parlament wird zuwenden müssen, und im Übrigen Parlament, Bund und Länder. Denn mit den Konsequenzen und Verstößen gegen Datenschutzaufsicht sind in Deutschland nicht nur die Bundesbeauftragte, sondern insbesondere auch die Länder konfrontiert. Die Stellung der Datenschutzaufsichtsbehörden ist in der Datenschutzgrundverordnung an vielen Stellen deutlich gestärkt worden, z.B. durch neue Aufgabenzuweisungen und das Sanktionsrecht. Auf Bundesebene gegenüber der BfDI wird das bedeuten, dass der Gesetzgeber auf Bundesebene die Sanktionen für die Bundesbeauftragte ebenfalls einführen muss. Bei den Ländern ist das weitgehend angesiedelt. Ich werbe sehr dafür, weil eine starke Datenschutzaufsicht kein Horrorszenario für jedes Unternehmen ist. Die neuen Aufgaben in der Datenschutzgrundverordnung haben für die Datenschutzaufsichtsbehörden eine Vielzahl von Beratungsmöglichkeiten, sie könnten sich auch als Zertifizierungsstellen akkreditieren. Aber in jedem Fall wird es sowohl auf Bundes- als auch auf Länderebene nötig sein, die Aufsichtsbehörden personell zu stärkem, um die Aufsicht effektiv zu gestalten und Verstöße zu sanktionieren. Das ist nicht nur der Ruf der Verwaltung nach immer mehr Personal. Das ist ein konkreter Ausdruck, dem Anspruch der Datenschutzgrundverordnung, dem Grundrecht auf Datenschutz, nachhaltig Wirkung zu verschaffen. Darüber hinaus gibt es noch andere Instrumente, u.a. das Thema Verbandsklagerecht, das in der Datenschutzgrundverordnung ergänzend zu den nationalen Regelungen geregelt wird. Von daher würde ich mir wünschen, dass der Gesetzgeber auf Bundes- und Landesebene die künftig starke Funktion, wie sie für die Datenschutzaufsicht angedacht ist, personell entsprechend untersetzt.

Der **Vorsitzende**: Frau Kollegin Wawzyniak, bitte.

Abg. **Halina Wawzyniak** (DIE LINKE.): Diesmal habe ich je eine Frage an Frau Voßhoff und Frau Hartge. Es geht mir um die Verarbeitung personenbezogener Daten eines Kindes. Wenn, vorsichtig formuliert,wir das richtig gelesen haben, ist es so, dass die Zustimmung des Trägers der elterlichen Verantwortung erforderlich sein soll. Datenverarbeiter sollen angemesse Anstrengungen unternehmen, um sicherzustellen, dass die Zustimmung vorliegt. Als Kind wird jemand im Alter von 13 bis 15 Jahren eingestuft. Jetzt ist zumindest meine Erfahrung, dass Kinder nicht erst mit 13 Jahren anfangen, diverse Geräte in die Hand zu nehmen. Es stellt sich die Frage, was daraus folgt. Wie kann aus Ihrer Sicht praktisch gewährleistet werden, dass vielleicht auch Kinder unter 13 Jahren erfasst werden. Das ist uns als Problem aufgefallen. Wir würden gerne wissen, gibt es ihrerseits Ideen, wie man dieses lösen könnte?

SVe **Andrea Voßhoff**: Wir müssen konkretisieren, was Sie als Problem sehen. Art. 8 schreibt vor, dass die Altersgrenze ab 13 und bis 16 zu ziehen ist. Das können die Mitgliedsstaaten individuell festlegen. Ich würde sie nicht unter 13 Jahre festlegen wollen. Eher hätte ich persönlich, denn nach deutschem Recht ist man ab 18 Jahren geschäftsfähig, die Altersgrenze angehoben. Ich verstehe die Argumentation derjenigen und die Tatsache, dass Kinder heutzutage schon früh User sind und mit Smartphones umgehen. Da müsste man möglichweise einen Kompromiss finden. Aber unter 13 Jahre sollte man nicht gehen. Dazu kommt es auch nur, wenn und soweit diese Einwilligung durch den Träger der elterlichen Verantwortung für das Kind oder mit dessen Zustimmung erteilt wird. Eine Beteiligung der Eltern ist noch gegeben. Der deutsche Gesetzgeber muss sich bei den Altersgrenzen festlegen. Bleibt er bei 13 Jahren oder geht er auf 16 Jahre hoch? Ich sehe auch ein Problem im Art. 1a), also in der Umsetzung der dortigen Normierung: „(…) der für die Verarbeitung Verantwortliche unternimmt oder berücksichtigt der Technik angemessene Anstrengungen, um in solchen Fällen nachzuprüfen, dass die Einwilligung durch den Träger der elterlichen Verantwortung für das Kind oder mit dessen Zustimmung erteilt wurde.“ Wir kennen im Netz das Thema der Anonymisierung. Wie kann oder soll der Anbieter diese Anforderungen sicherstellen? Insofern sehe ich da ein Problem, was ihm zuzumuten ist.Wie kann und will ein Anbieter das feststellen?

SVe **Dagmar Hartge**: Ich kann das versuchen zu ergänzen. Dem Gesetzgeber ist eine Ermessensspanne mitgegeben worden, weil die Mitgliedstaaten im Hinblick auf Jugendliche unterschiedlich denken. Wir haben in der Vergangenheit in Deutschland in anderen Fällen als bei den sozialen Netzwerken immer gesagt, dass Jugendliche ab einem bestimmten Alter ihre Selbstbestimmungsrechte selbst ausüben können. Das variierte bei uns Datenschutzbeauftragten sicher immer so ein bisschen, aber galt meist ab 14 Jahren. Da haben wir sie dann letzten Endes freigelassen. Ich denke, es ist wichtig, sich festzulegen. Nicht angemessen wäre eine Grenze bei 16 Jahren, weil das der Situation, wie Jugendliche heute sind und was Jugendliche machen, nicht mehr entspricht. Die Eltern sind dann in der Pflicht. Frau Voßhoff hat das richtigerweise auch gesagt, das wird ein Problem sein. Wie sollen die Anbieter überprüfen, dass das alles ordnungsgemäß nachgewiesen worden ist. Was sollen die sich das belegen lassen? Das könnte zu einem Datenwust ohne Ende führen. Ich glaube, dass wir insgesamt sensibel mit Jugendlichen umgehen und vielleicht gucken müssen, dass wir, über eine Abstimmung in Europa, Anforderungen für Jugendliche formulieren. Aber die Regelung ist hier eindeutig. Es wird ganz klar gesagt, ab einem bestimmten Alter bin ich für mich selbst verantwortlich, auch im Hinblick auf mein Selbstbestimmungsrecht. Daran werden wir am Ende nicht vorbeikommen.

Abg. **Gerold Reichenbach** (SPD): Ich habe eine Frage an zwei Sachverständige, Frau Hartge und Herrn Oetjen. Sie haben nach meiner Einschätzung treffend ausgeführt, dass es mit der Datenschutzgrundverordnung auch eine Chance gibt, endlich ein einheitliches Level Playing Field hinzubekommen. Voraussetzung ist natürlich, dass wir die Verordnung auch durchsetzen. Ich habe eine Frage, die eher das Zukunftsmodell Big Data betrifft. Wir hören immer wieder, dass das in der Datenschutzgrundverordnung festgeschriebene Prinzip der Datensparsamkeit und Big Data ein Widerspruch ist. Das passe nicht zusammen. Hört sich erstmal relativ plausibel an. Allerdings bezieht sich Datensparsamkeit nur auf personenbezogene Daten. Deswegen würde ich gerne Ihre Einschätzung hören, ob das tatsächlich ein Widerspruch ist und die Verordnung uns wieder einen internationalen Konkurrenznachteil beschert, oder ob es auch Chancen gibt. Wie ist dieser Widerspruch überhaupt zu bewerten, wenn er überhaupt besteht ?

SVe **Dagmar Hartge**: Ich glaube gar nicht, dass es so ein großer Widerspruch ist. Natürlich sagen alle zunächst, Big Data und Datenschutz sind doch gar nicht vereinbar. Wie sollen wir denn an die Daten kommen? Ich selber habe in meiner Stellungnahme betont, wie wichtig mir persönlich die Transparenz ist. Ich glaube, wir haben in der Vergangenheit das Problem gehabt, dass häufig nicht erklärt worden ist, was gemacht wird. Wirhaben uns überfrachtet. Immer dann, wenn wir als Aufsicht Erklärungen abgegeben oder sie eingefordert haben, sind diese fünf Seiten lang

ausgefallen und keiner hat wirklich verstanden, was drin steht. Die Folgen sehen wir heute, tagtäglich, wenn Google uns auffordert, Opt-Ins zu erklären. Es liest doch gar keiner. Es wird einfach geklickt. In dem Moment, wo wir an diesen Mechanismen arbeiten, glaube ich, dass Bürgerinnen und Bürger Dinge freiwillig mitmachen würden. Eine Voraussetzung ist, dass die Datensicherheitsstandards wirklich sehr gut sind. Da erwarte ich auch, dass nur auf dem richtig regulären Weg Freigaben für Datenverarbeitung erfolgen könnten. Das hat uns die Datenschutzgrundverordnung mitgegeben, Lösungen zu finden, wie ich datenschutzgerecht sparsam und auf eine Weise arbeiten kann, die sicher ist. Anonymisierung ist ein Thema. Diese wird nicht sicher genug bleiben. Ich habe auf Veranstaltungen schon lernen dürfen, dass Anonymisierung, wenn ich große Datenmengen habe, zu hohen Prozentzahlen knackbar sind. Das, was heute noch eine schöne Lösung ist, die wir anbieten können, wird morgen keine mehr sein. Also kann man nur sagen, die Wissenschaft muss mitmachen und mitentwickeln. Klar ist, jedes neue Konzept hat den Datenschutz eigentlich schon mitzubringen. Dann denke ich mal, sind wir gut aufgestellt. Denn jetzt trifft es nicht mehr nur europäische Unternehmen. Jetzt betrifft es auch die Unternehmen aus Drittstaaten, das ist nicht nur die USA, das ist auch der asiatische Raum.

SV **Jan Oetjen**: Vielen Dank. Ich kann Frau Hartges Darstellungen zur Opt-In-Flut und der aktuellen Gestaltung nur zustimmen. Keinem Nutzer, selbst einem studierten Juristen, kann man zumuten, dass er 15 Seiten Datenschutzerklärungen durchliest und versteht, was er für Daten überträgt oder was ihm abverlangt wird. Zur Frage nach der Widersprüchlichkeit von Datensparsamkeit und Big Data. Es hängt davon ab, wie man Datensparsamkeit interpretiert. Ich glaube, wenn man da ansetzt und sagt, wir verbieten das generelle Erheben von bestimmten Arten von Daten, die aus heutiger Sicht nicht zwingend notwendig für die Leistungen der Dienste sind, dann interpretiert man das falsch und hemmt sicherlich eine Big Data-Entwicklung. Die Datensparsamkeit sollte dahingehend interpretiert werden, dass wir ein abstraktes Level für anonymisierte und pseudonymisierte Daten schaffen. Für Klardaten sollte diese Interpretation so umkehrt werden, dass da, wo eine Pseudonymisierung möglich ist, ein Anreiz besteht. Dann ist es ein durchaus sinnvolles Prinzip. Dieses schafft einen Anreiz für die Industrie, mit pseudonymisierten statt mit Klardaten zu arbeiten, und sich nicht den Entwicklungen verschließt. Denn dieses Gesetz, das wir heute machen, das 2018 in Kraft tritt, hat der Innovationsgeschwindigkeit der Industrie zu folgen, die im Faktor 10 bis 20 zu allen Innovationszyklen heute voranschreitet. Eigentlich macht man ein Gesetz aus alten Zyklen für in 20 Jahren, welches im Jahre 2030 oder 2035 erst in Kraft treten würde. Von daher wäre man gut bedient, die Manschetten, gerade was die inhaltlichen Regelungen angeht, nicht zu eng anzulegen.

Der **Vorsitzende**: Kollege Janecek, bitte.

Abg. **Dieter Janecek** (BÜNDNIS 90/DIE GRÜNEN): Bei dem Punkt Pseudonymisierung, Anonymisierung würde ich gerne nochmal bei Frau Harge und Herr Oetjen nachhaken. Ich war vor kurzem bei der Telekom-Innovation Lab und die sagen, sie setzen sehr stark auf Pseudonymisierung und haben dadurch eine Big Data-Lösung im Rahmen der bestehenden Regelungen, so dass Big Data möglich ist. Das wäre erstmal ein Ansatz, der einen Ausgleich schafft zwischen dem stattfindenden Kampf, den wir auf der Lobbyebene seit zwei Jahren und länger mit der Begründung erleben,dass aufgrund der Datenschutzbestimmungen bestimmte Geschäftsmodelle nicht gehen. Besser wäre es, wenn sie gehen und die Wirtschaft das auch kommunizieren kann. Vielleicht können Sie in diesem Spannungsfeld einen Einblick geben, was wirklich passiert.

SVe **Dagmar Hartge**: Sie haben das zu Recht gesagt. Die Telekom hat auf Vorträgen, die ich gehört habe, durchaus auch eingeräumt, dass Anonymisierungen letzten Endes gar nicht mehr so richtig funktionieren. Das müssen wir lernen. Pseudonymisierung ist schon deutlich weniger als die Anonymisierung. Es bedeutet, wenn man es ernst nimmt, dass die Daten wieder zusammengeführt und personenbezogen gemacht werden können. Das ist ein geschützter Zwischenschritt. Wir alle kennen ihn aus den ärztlichen Abrechnungsstellen. Ich glaube, dass wir erkennen müssen,

dass man mit beiden Punkten nicht auf Dauer wird arbeiten können. Das Datenschutzproblem wird sich verlagern. Es ist schon heute auf dem Weg dahin und wir werden kreativ neue Lösungen finden müssen. Heute kann man damit noch einiges gestalten. Bezüglich neuer Lösungen bin auch ich überfragt und sehr gespannt, mit welcher Geschwindigkeit diese entwickelt werden. Nur, genau das ist die Vorgabe der Grundverordnung. Wir müssen an den Ausgleich denken. Wir brauchen Geschäftsmodelle, wollen aber gleichzeitig den Schutz des Bürgers. Wir wollen die Betroffenenrechte. Das genau ist die Herausforderung bei diesen ganzen Modellen. Ich glaube, dass Modelle kippen, wenn man die Bürgerrechte ausklammert, um im Geschäftsbereich sehr erfolgreich zu sein. Das würde irgendwann nicht mehr akzeptiert werden.

SV **Jan Oetjen**: Vielen Dank. Ich glaube, Sie haben die Debatte sehr gut zusammengefasst. Bei der Diskussion um pseudonymisierte Daten, für oder wider, muss man die Alternativen betrachten. Die eine Alternative ist, wir erheben gar keine Daten. Dann braucht man keine wissenschaftliche Debatte, um festzustellen, dass es Big Data nicht geben wird. Die andere Alternative, die entstehen wird, wenn gleiche Anforderungen an pseudonymisierte Daten und Klardaten gestellt werden, ist, dass die Industrie direkt mit Klardaten arbeitet. So sehr wir uns immer eine ideale Welt wünschen, in der nichts zu entschlüsseln ist, ist der einzige Kompromiss, den man hier finden kann, der Umgang mit pseudonymisierten Daten. Hieran muss man hohe Anforderungen stellen. Das ist keine Frage. In dem Gesetz ist von einer Kombination aus Pseudonymisierung und Verschlüsselung die Rede. Ich glaube, das ist ein sehr wichtiger Aspekt, wie man diese Pseudonymisierung in Zukunft betreibt. Ich glaube, dass das der einzig gangbare Weg ist. Denn wenn man es so regelt oder keine Regelung schafft, dann schafft man nur das Ausschalten und Abhängen Europas von zukünftigen Entwicklungen. Wenn man die gleichen Anforderungen bei der Verarbeitung von Klardaten stellt, wird jedes Unternehmen aus einfachen wirtschaftlichen Erwägungen immer nach der höchsten Form der Verarbeitungsform streben. Da werden Sie nichtmals das Schutzniveau von pseudonymisierten Daten in Europa schaffen, sondern den Austausch von direkten Klardaten fördern, für den sich Unternehmen, Behörden und die sonstigen Datenverarbeitungsstellen die Opt-Ins holen werden.

Der **Vorsitzende**: Gibt es weitere Wortmeldungen seitens der Abgeordneten? Das ist nicht der Fall. Gibt es Ergänzungen von den Sachverständigen? Frau Dr. Kotschy, bitteschön.

SVe **Dr. Waltraut Kotschy**: Danke, Herr Vorsitzender. Ich wollte zu dem Thema der pseudonymisierten Daten noch etwas hinzufügen. Im österreichischen Recht haben wir pseudonymisierte Daten seit der Umsetzung der Richtlinie, die heißen nur indirekt personenbezogene Daten. Wir haben für pseudonymisierte Daten ein vollständiges Privileg eingeführt. Die Weitergabe von Daten an einen anderen Verantwortlichen ist dann ohne Beschränkungen zulässig, wenn die Daten sicher pseudonymisiert sind, so dass der Empfänger mit menschenmöglichen Mitteln nicht im Stande ist, die Daten zu re-identifizieren. Das hat sich einerseits, vor allem in der medizinischen Forschung sehr bewährt. Aber, und deswegen wollte ich noch einen Satz sagen, es gibt da ein Problem. Pseudonymisieren ist nicht so einfach. Pseudonymisieren ist eine Mühsal, kostet Geld und man muss es können. Daher muss man versuchen, Institutionen zu schaffen, die mit Vertrauen ausgestattet sind, um die Pseudonymisierung durchzuführen. Damit man die Daten dann in pseudonymisierter Form weitergeben kann. Bei den Institutionen, die die Echtdaten haben, ist das Problem, dass man sich in der Regel die Mühe nicht machen will. Im reinen Businessbereich ist das etwas anderes. Aber zum Beispiel im gesamten Krankenhausbereich, für die medizinische Forschung usw., da geschieht es nicht, weil man sich die Mühe nicht macht. Ich möchte diese Idee, dass man sich bemüht, solche Institutionen zu fördern, in den Raum stellen.

Der **Vorsitzende**: Da mir keine weiteren Wortmeldungen vorliegen, liebe Frau Dr. Kotschy, war das nicht das Schlusswort zu diesem Thema, aber für den heutigen Tag in dieser Debatte. Ich darf mich ganz herzlich bei den Damen und Herren Sachverständigen für die wertvollen und wirklich sehr informativen Beiträge zu diesem Thema bedanken.

Sie werden sicherlich in unsere Arbeit einfließen. Dafür herzlichen Dank. Ich bedanke mich bei den Abgeordneten für die Fragen. Ich schließe die Sitzung und berufe die nächste Sitzung des Ausschusses Digitale Agenda auf den 16. März in diesem Raum ein.

Schluss der Sitzung: 17:47 Uhr

Jens Koeppen, MdB
**Vorsitzender**