Deutscher Bundestag
Ausschuss Digitale Agenda

Ausschussdrucksache
18(24)052

Die Bundesbeauftragte für den Datenschutz und die Informationsfreiheit

Öffentliches Fachgespräch „Startups, Mittelstand und Datenschutz in der digitalen Welt“ des Ausschusses Digitale Agenda des Deutschen Bundestags, 4. März 2015

Beantwortung der vorab vom Ausschuss vorgelegten Fragen

Vorab weise ich darauf hin, dass mir aufgrund der späten Übersendung nur eine erste Einschätzung zu den durchaus komplexen Fragen möglich war.

Frage 1

Welche regulatorischen Rahmenbedingungen im Bereich des Datenschutzes müssen aus Ihrer Sicht gegeben sein, um der Wirtschaft – insbesondere kleinen (wie Startups) und mittleren Unternehmen im Bereich der digitalen Wirtschaft – ein möglichst hohes Maß an Rechtssicherheit bei möglichst geringem bürokratischen Aufwand zu ermöglichen, und gleichzeitig das Recht auf informationelle Selbstbestimmung der Bürgerinnen und Bürger sicherzustellen? Gibt es konkrete bürokratische Hindernisse und ggf. hohe Bürokratiekosten, die abgebaut werden müssten, zum Beispiel um Innovationen nicht im Wege zu stehen?

Es bedarf klarer, verständlicher und gleichzeitig hinreichend abstrakter Regelungen, um den Unternehmen unabhängig von ihrer Größe ein möglichst hohes Maß an Rechtssicherheit über ihre Möglichkeiten und ihre Pflichten zu geben. Angesichts der bewährten Struktur des Datenschutzrechts ist es notwendig, dass ein Unternehmen, das ein neues Geschäftsmodell auf den Markt bringen will, sich klarmacht, dass die Verarbeitung personenbezogener Daten einen Eingriff in Persönlichkeitsrechte ihrer Kunden darstellt. Dieser bedarf immer einer Rechtfertigung in Form einer Willensbekundung des Betroffenen (durch Einwilligung, im Rahmen eines Vertrages) oder einer Rechtsgrundlage im Datenschutzrecht. Dabei muss sich ein Unternehmen folgende Fragen stellen:

- Werden für das Geschäftsmodell überhaupt personenbezogene Daten benötigt oder kann der Geschäftszweck auch ohne personenbezogene Daten erreicht werden?
- Wenn ja, welche Daten werden benötigt?
- Für welche konkreten Zwecke werden genau welche Daten benötigt?
- Wie lange werden die Daten benötigt, d. h. wann sind sie zu löschen?
- Ist eine frühzeitige Pseudonymisierung oder gar Anonymisierung möglich?
- Auf welcher rechtlichen Grundlage werden Daten erhoben, verarbeitet oder genutzt?

  - Liegt eine wirksame Einwilligung vor (Stichworte: Transparenz, Informiertheit, Freiwilligkeit)?
  - Ist ein Vertrag mit dem Betroffenen geschlossen?
  - Kann ein berechtigtes Interesse des datenerhebenden oder –verarbeitenden Unternehmens bei Abwägung mit den schutzwürdigen Interessen der Betroffenen angenommen werden?
- Sollen erhobene Daten (später) für andere Zwecke genutzt werden? Gibt es dafür wiederum eine rechtliche Basis und welche?
- Werden Daten in Drittländer übermittelt?

Darüber hinaus muss sich ein Unternehmen Gedanken darüber machen, in welcher Weise es den Transparenzanforderungen des Datenschutzrechts (Informations- und Auskunftspflichten) Rechnung trägt. Diese rechtlich bedingten Vorfragen werden flankiert von den technischen und organisatorischen Anforderungen des Datenschutzrechts, einschließlich der Fragen, ob bspw. eine Vorabkontrolle durchzuführen ist oder ein betrieblicher Datenschutzbeauftragter zu bestellen ist.

All diese Pflichten, die sich nach geltendem Recht aus dem BDSG ergeben, bringen selbstverständlich auch einen gewissen bürokratischen Aufwand mit sich. Es handelt sich jedoch um den Mindestaufwand, der zur Grundrechtssicherung unabdingbar ist und nicht abgebaut werden kann. Im Hinblick auf bürokratische Hürden ist das deutsche Datenschutzrecht aber im Vergleich zu anderen Datenschutzgesetzen in Europa eher zurückhaltend: So ersetzt das BDSG etwa die Meldepflichten bei den Aufsichtsbehörden sehr weitgehend durch die obligatorische Bestellung betrieblicher Datenschutzbeauftragter, was einerseits zur Entlastung der Unternehmen und andererseits zur Stärkung einer innerbetrieblichen Datenschutzkultur beigetragen hat.

Bei der Prüfung der datenschutzgerechten Ausgestaltung von Geschäftsmodellen wird sich für die Unternehmen natürlich immer wieder erweisen, dass das Datenschutzrecht nicht jede Geschäftsidee zulässt. So wären bspw. Big-Data-Anwendungen, die mit einer Zusammenführung personenbezogener Daten aus höchst unterschiedlichen Quellen und Kontexten und deren anschließender personenbezogener Auswertung verbunden sind, nur schwer in zulässiger Weise auszugestalten. Dies ist allerdings kein bürokratisches Hindernis, sondern zur Wahrung des Rechts auf informationelle Selbstbestimmung unabdingbar. Geschäftsmodelle müssen sich deshalb in den vorhandenen rechtlichen Rahmen grundsätzlich einpassen und nicht umgekehrt. In dem eben genannten Beispiel wäre z. B. zu prüfen, ob technische Lösungen zur Anonymisierung der Daten möglich sind.

Frage 2

Wie bewerten Sie vor diesem Hintergrund den sog. „risikobasierten Ansatz“ im Sinne der Differenzierung von Art und Umfang der datenschutzrechtlichen Pflichten nach potenzieller Grundrechtsbetroffenheit? Gibt es eine unterschiedliche Sensibilität der unterschiedlichen Datenarten bzw. gibt es risikofreie Daten? Inwieweit ist dieser Ansatz geeignet, das Recht auf informationelle Selbstbestimmung in der digitalen Welt sicherzustellen?

Bei dem Stichwort „risikobasierter Ansatz“ muss man sich sehr genau darüber verständigen, was damit gemeint ist. Ein risikobasierter Ansatz hat auch aus Sicht einer Datenschutzbehörde immer dort seinen Sinn, wo es darum geht, Risiken für den Einzelnen durch grundrechtssichernde Verpflichtungen zu flankieren. Konkret bedeutet das: Der Umfang der technischen und organisatorischen Pflichten, z. B. Maßnahmen zur Datensicherheit, Melde- und Konsultationspflichten oder die Durchführung von Vorabkontrollen bzw. in der Datenschutz-Grundverordnung vorgesehene Datenschutz-Folgenabschätzungen ist skalierbar und kann und darf sich an den für den Einzelnen bestehenden Risiken bestimmter Datenverarbeitungen orientieren.

Auch das aktuelle deutsche Datenschutzrecht weist zumindest im Zusammenhang mit der Interessenabwägung (§ 28 Abs. 1 Satz 1 Nr. 2 BDSG) gewisse risikobasierte Elemente auf. So muss die verantwortliche Stelle die Frage prüfen, ob das berechtigte Interesse an der Verarbeitung personenbezogener Daten die schutzwürdigen Interessen der Betroffenen überwiegt und welche Risiken für das Recht auf informationelle Selbstbestimmung durch die intendierte Datenverarbeitung entstehen können. Der risikobasierte Ansatz findet sich auch in der noch geltenden Europäischen Datenschutzrichtlinie sowie im Entwurf der Europäischen Datenschutzgrundverordnung (Art. 7 f der RL 95/46/EG, Art. 6(1)f Datenschutz-Grundverordnung).

Dieser risikobasierte Ansatz bezieht sich dabei nicht auf einzelne Datenarten, sondern auf konkrete Verarbeitungszusammenhänge, d. h. den Kontext der Datenverarbeitung, deren Zweck usw.

Einem Ansatz, der die unterschiedliche Sensibilität bestimmter Datenarten in Bezug nimmt und davon ausgeht, dass es auch risikofreie Daten gebe, kann keineswegs gefolgt werden. Ein solcher Ansatz muss scheitern, da es keine per se risikofreien Daten gibt. Dies hat bereits das BVerfG in seinem Volkszählungsurteil festgestellt, wonach es in Zeiten automatisierter Datenverarbeitung kein „belangloses Datum“ geben kann. Es kommt vielmehr immer auf den konkreten Verwendungszusammenhang an.

Darüber hinaus wird „risikobasierter Ansatz“ teilweise auch so verstanden, dass das grundsätzliche Regelungsmodell des Datenschutzrechts in Frage gestellt wird: Nach geltendem Recht ist die Erhebung, Verarbeitung und Nutzung personenbezogener Daten grundsätzlich unzulässig, sofern es hierfür nicht eine ausdrückliche Legitimation in Form einer Einwilligung oder einer Rechtsgrundlage gibt. Hier wird zum Teil gefordert, dieses Modell durch ein solches zu ersetzen, das die Erhebung, Verarbeitung und Nutzung personenbezogener Daten grundsätzlich erlaubt und nur bestimmte, besonders risikobehaftete Datenverarbeitungen verbietet.

Ein solches Modell ist abzulehnen. Jede Information über einen Einzelnen kann - je nach Kontext oder Verknüpfung - gleichzeitig eine triviale oder aber auch eine äußerst sensible Aussage treffen. Dies ist schwer vorhersehbar und macht schon deshalb eine standardisierte Abschätzung des Risikos schwierig. Der Gesetzgeber könnte immer nur solche Risiken regulieren, die er auch kennt. Dies wäre aber mit dem grundrechtlichen Schutz des Einzelnen nicht vereinbar.

Ein so verstandener risikobasierter Ansatz würde den Schutz der Betroffenen grundsätzlich schwächen: Nach dem geltenden Recht muss in der Gesetzgebung wie in der Gesetzesanwendung jeder neue Eingriff in das Recht auf informationelle Selbstbestimmung gerechtfertigt werden, sowohl politisch als auch ganz praktisch bei jeder Verarbeitung. Dies legt die Begründungslast auf die Seite derjenigen, die die Daten verarbeiten wollen. Dreht man dieses Prinzip um, müssten die Betroffenen rechtfertigen, warum bestimmte Datenverarbeitungen riskant sind. Dies würde ihre Position deutlich und unverhältnismäßig schwächen.

Deshalb sind die fundamentalen Prinzipien des Datenschutzes (Legitimierung der Datenverarbeitung durch den Verantwortlichen, Erforderlichkeit, Zweckbindung, Transparenz und Informiertheit des Betroffenen) einem risikobasierten Ansatz nicht zugänglich. Im gleichen Sinne hat sich auch die Art.-29-Gruppe in ihrem Statement zum risikobasierten Ansatz vom 30. Mai 2014 geäußert (WP 218, http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp218_en.pdf).

Frage 3

Welche regulatorischen Voraussetzungen müssen aus Ihrer Sicht gegeben sein, um datenbasierte Geschäftsmodelle (insbes. durch die Nutzung sog. „Big-Data"), aber auch Innovationen wie z. B. „Autonomes Fahren" insbesondere in Deutschland und Europa zu ermöglichen? Welche Rolle können in diesem Kontext die Konzepte einer Pseudonymisierung bzw. Anonymisierung zur Schutzerhöhung für Betroffene einnehmen? Welche anderen technischen Schutzkonzepte sind darüber hinaus denkbar?

Die regulatorischen Voraussetzungen sind im Datenschutzrecht vorhanden. Wie bereits zu Frage 1 bemerkt, ermöglichen das geltende und voraussichtlich auch das künftige Datenschutzrecht datenbasierte Geschäftsmodelle, auch durch Nutzung von Big Data. Dabei kommt vor allem dem Einsatz von Pseudonymisierung und Anonymisierung eine wichtige Rolle zu. So ist etwa die Zusammenführung und statistische Auswertung Nutzungsdaten aus der Inanspruchnahme verschiedener Internetdienste (z. B. durch den Betreiber einer Suchmaschine) rechtlich zulässig, wenn diese Daten unmittelbar nach Ende der Nutzung so anonymisiert werden, dass auch nach ihrer Zusammenführung keine personenbezogenen Profile mehr gebildet werden können. Gleichwohl kann auf dieser Datenbasis die Funktionalität einer Suchmaschine verbessert werden.

Auch bei dem genannten Beispiel der Entwicklung autonomer und zunehmend vernetzter Fahrfunktionen spielen Pseudonymisierung und Anonymisierung eine außerordentlich wichtige Rolle. Es zeigt sich, dass Datenschutz und digitale Innovation kein Gegensatzpaar sind. Im Rahmen meiner Mitarbeit beim „Runden Tisch Automatisiertes Fahren" des Bundesministeriums für Verkehr und digitale Infrastruktur habe ich festgestellt, dass sowohl die betroffene Industrie als auch die politischen Entscheidungsträger die datenschutzrechtlichen Aspekte bedenken und Interesse an Lösungen haben, die sowohl den Datenschutz als auch Erfordernisse der Datensicherheit berücksichtigen. Ich werde die Beteiligten weiter auf die datenschutzrechtlichen Grenzen und Möglichkeiten zu diesem Thema hinweisen. In den bisherigen Beratungen hat sich möglicher datenschutzrechtlicher Handlungsbedarf insbesondere in zwei Bereichen herauskristallisiert. In beiden Fällen geht es darum festzustellen, ob im konkreten Fall das Fahrzeug (autonom) oder ein Mensch als Fahrzeugführer gehandelt hat. Dies betrifft die datenschutzgerechte Gestaltung von Ereignis-(Unfall-)Datenschreibern und Systemen zur Fahreraktivitäts- bzw. Systemaktivitätserkennung, die für haftungs- und versicherungsrechtliche Fragen bedeutsam sind.

Sofern für bestimmte Geschäftsmodelle die Anonymisierung und Pseudonymisierung nicht in Frage kommen, hält das Datenschutzrecht eine Reihe von Erlaubnistatbeständen bereit. Dabei spielt die Einwilligung auch weiterhin eine wichtige Rolle. So werden z. B. Geschäftsmodelle entwickelt, bei denen die Kreditwürdigkeit bei der Vergabe von Kleinkrediten aufgrund von Analysen des Facebook-Profils errechnet wird. Derartige Geschäftsmodelle wären auf der Basis einer wirksamen Einwilligung grundsätzlich möglich. An diesem Beispiel zeigt sich aber auch, dass nicht alles, was technisch möglich ist, auch rechtlich zulässig sein muss. Denn die Einwilligung stößt hier u. U. an Grenzen und eine Interessenabwägung geht – wegen der mit dem Scoring verbundenen sehr weitreichenden Eingriffe in das Persönlichkeitsrecht – zugunsten des Betroffenen aus. In solchen Fällen gebietet es die grundrechtlich gesicherte Gewährleistung des Persönlichkeitsrechts, dass Geschäftsmodelle unzulässig sein müssen.

Im Übrigen bedarf es in der Datenschutz-Grundverordnung einer Regelung zur Profilbildung, die klare rechtliche Rahmenbedingungen für die Verarbeitung personenbezogener Daten zur Bildung und Nutzung von Profilen schafft. Auch hier müssen Pseudonymisierung und Anonymisierung ebenso eine wichtige Rolle spielen wie die Gewährleistung eines Höchstmaßes an Autonomie für die Betroffenen.

Frage 4

Ist aus Ihrer Sicht der im derzeitigen deutschen und europäischen Datenschutzrecht festgelegte Einwilligungsvorbehalt (als „Opt-In-Lösung“) richtig und kann dieser angesichts der derzeitigen Herausforderungen der Digitalisierung das Recht auf informationelle Selbstbestimmung wirksam schützen? Falls nicht, wie müsste er aus Ihrer Sicht modifiziert oder weiterentwickelt werden, um der gerade bei Startups kontinuierliche bestehenden Perspektive einer Weiterentwicklung gerecht zu werden? Wäre eine Computeridentifikation – sofern in der Datenschutz-Grundverordnung geregelt - noch in Europa möglich? Würde dann ein Zustimmungsvorbehalt möglicherweise dazu führen, dass dies einigen US-Unternehmen möglich bleibt und damit deren Rolle im Wettbewerb gestärkt würde, insbesondere gegenüber dem deutschen Mittelstand und Startups?

Der Einwilligungsvorbehalt ist weiterhin richtig. Recht auf informationelle Selbstbestimmung bedeutet, dass jeder selbst darüber entscheiden können muss, wer was wann bei welcher Gelegenheit über ihn weiß. Einwilligung kann aber nur dort sinnvoll eingesetzt werden, wo ihre Voraussetzungen auch zweifelsfrei erfüllt werden können.

Es ist häufig zu beobachten, dass Geschäftsmodelle auf der Basis von Einwilligungen beruhen, deren Wirksamkeit mindestens zweifelhaft ist. So stehen vor allem die Freiwilligkeit der Einwilligung und deren Informiertheit häufig in Frage. In diesen Fällen bedarf es einer wirksameren Durchsetzung einer datenschutzgerechten Gestaltung. Zudem sollte das künftige europäische Recht die Anforderungen an die Wirksamkeit von Einwilligungen präzisieren, insbesondere im Hinblick auf die Freiwilligkeit bei besonderen Abhängigkeiten oder Monopolstellungen. Die Bundesregierung hatte hier konkrete Vorschläge unterbreitet, die durchaus positiv zu sehen sind. Unter anderem solle demnach eine Einwilligung unwirksam sein, wenn sie für den Betroffenen zu einer unzumutbaren Benachteiligung führt. Dies sei insbesondere dann der Fall, wenn die Einwilligung unklar oder unverständlich sei oder nicht freiwillig gegeben worden sei. Darüber hinaus soll die Unwirksamkeit einer Einwilligung immer dann vermutet werden, wenn sich der Betroffene zur verantwortlichen Stelle in einem Abhängigkeitsverhältnis befinde, sofern ihm die Datenverarbeitung nicht ausschließlich einen rechtlichen oder wirtschaftlichen Vorteil bringe. Die Vorschläge dürften allerdings keine Mehrheit im Rat finden.

Sofern eine wirksame Einwilligung nicht zu erlangen ist, muss das Unternehmen versuchen, auf die anderen gesetzlichen Möglichkeiten (z. B. Erforderlichkeit zur Vertragserfüllung oder überwiegendes berechtigtes Interesse der verantwortlichen Stelle) zurückzugreifen, die eine

Verarbeitung personenbezogener Daten zu legitimieren vermögen. Liegen auch hierfür die Voraussetzungen nicht vor, ist eine Verarbeitung personenbezogener Daten nicht zulässig.

Einen Unterschied zwischen US- und europäischen Unternehmen wird es künftig nach der Datenschutz-Grundverordnung nicht mehr geben, sodass auch keine Wettbewerbsverzerrung besteht. Das Marktortprinzip wird grundsätzlich sicherstellen, dass der europäische Markt unter einheitlichen Bedingungen adressiert wird. Dies gilt auch für die Einwilligung.

Frage 5

Wie bewerten Sie die Innovations- und Wachstumschancen für kleine (wie Startups) und mittleren Unternehmen der digitalen Wirtschaft vor dem Hintergrund eines in Aussicht stehenden einheitlichen europäischen Rechtsrahmens für den Datenschutz durch die Datenschutzgrundverordnung? Welche Bedeutung messen Sie vor diesem Hintergrund – und vor dem Hintergrund der Wettbewerbsgleichheit - dem Marktortprinzip zu, nach dem alle Anbieter, die in Europa ihre Dienste anbieten, dem europäischen Datenschutzrecht unterliegen sollen?

Die Innovations- und Wachstumschancen für die Unternehmen der digitalen Wirtschaft werden im Vergleich zur geltenden Rechtslage zwar insofern tangiert, als sich die Rahmenbedingungen verändern werden. Ob die Datenschutz-Grundverordnung allerdings diese Chancen verbessern oder verschlechtern wird, ist schwer vorherzusagen. M. E. werden die Auswirkungen der Datenschutz-Grundverordnung für die europäische Digitalwirtschaft in diesem Punkt eher überschätzt.

Ob Geschäftsmodelle erfolgreich sind oder nicht, hängt in erster Linie von den üblichen Marktmechanismen ab. Angesichts des durchaus hohen Datenschutzbewusstseins in Europa wird die Akzeptanz von Geschäftsmodellen unter anderem auch davon abhängen, ob das Vertrauen in eine datenschutzgerechte und -freundliche Gestaltung dieser Geschäftsmodelle vorhanden ist. Innovation sollte und muss sich auch auf die Implementierung datenschutzfreundlicher Technologien beziehen.

Wie in der Antwort auf Frage 4 schon erwähnt, kommt dem Marktortprinzip eine herausragende Bedeutung zu. Auf diese Weise wird endlich klar geregelt, dass sich jedes Unternehmen, das Waren und Dienstleistungen auf dem europäischen Markt anbietet, an europäisches Datenschutzrecht halten muss und dies auch dann, wenn es innerhalb der EU über keine Niederlassung verfügt. Die bisher bestehende Wettbewerbsverzerrung durch das in anderen Weltregionen bestehende schwächere Datenschutzrecht wird dadurch für Europa weitgehend beseitigt.

Frage 6

Wie bewerten Sie Datensicherheit und ein europaweit einheitliches Datenschutz-Niveau als Standortfaktor und als Wettbewerbsmerkmal? Muss die EU-Reform ihrer Meinung nach durch gesetzgeberische Anpassungen auf nationaler Ebene flankiert werden? Wo sehen Sie konkrete Vorteile aus Sicht der Unternehmen, wenn es um Datenschutz als Standortfaktor und Wettbewerbsmerkmal geht?

Ein europaweit einheitliches Datenschutzniveau ist höchst wünschenswert. Die derzeit – trotz der bereits als vollharmonisierend angesehenen geltenden Datenschutz-Richtlinie 95/46/EG – bestehende Zersplitterung in 28 verschiedene Datenschutzgesetze ist eher wettbewerbshemmend und ist auch mit Blick auf das Datenschutzniveau nicht förderlich, denn es besteht ein Risiko eines *„Race to the bottom".* Das Anbieten von Waren und Dienstleistungen auf dem europäischen Markt wird durch die Harmonisierung deutlich einfacher und transparenter, wobei gleichzeitig das Datenschutzniveau gehalten oder sogar verbessert werden kann.

Sofern die Datenschutz-Grundverordnung als unmittelbar in den EU-Mitgliedstaaten geltendes Recht überhaupt noch Spielräume lässt, werden Anpassungen des nationalen Rechts notwendig sein. Im Bereich der für die Wirtschaft geltenden Regelungen wird dies voraussichtlich aber kaum der Fall sein. Insbesondere werden die §§ 28 ff. BDSG ersatzlos wegfallen.

Spielräume für den nationalen Gesetzgeber werden vor allem im öffentlichen Bereich bestehen, aber auch beispielsweise bei der Frage, ob und unter welchen Voraussetzungen betriebliche Datenschutzbeauftragte zu bestellen sind, beim Beschäftigtendatenschutz oder im Zusammenhang mit dem Ausgleich zwischen Meinungs- und Informationsfreiheit und Datenschutz.

Die Vorteile für die Unternehmen liegen auf der Hand: Sie erhalten ein höheres Maß an Rechtssicherheit durch einheitliche Regeln und durch Mechanismen zu deren einheitlicher und kohärenter Umsetzung (Stichwort: One-Stop-Shop). Zudem besteht die Erwartung, dass die Akzeptanz europäischer Angebote steigt, wenn das Vertrauen in einen guten Datenschutz gegeben ist. Letztlich muss aber auch hervorgehoben werden, dass über den Erfolg der europäischen Digitalwirtschaft nicht in erster Linie das Datenschutzrecht, sondern der Markt entscheidet.

Besonders vor dem Hintergrund der hier zur Diskussion stehenden wirtschaftlichen Aspekte möchte ich darauf hinweisen, dass zu einem gedeihlichen Umfeld für die Internet-Ökonomie

auch das Vertrauen der Bürgerinnen und Bürger auf einen glaubwürdig transparenten Umgang der Marktteilnehmer mit deren Daten und natürlich eine effiziente Cyber-Sicherheit gehört. Cyber-Sicherheit steht dabei für nichts anderes als die Integrität, Vertrauenswürdigkeit und Verfügbarkeit der digitalen Infrastrukturen. Sie ist deshalb augenscheinlich auch ein besonderes Anliegen der Bundesregierung, die etwa mit dem IT-Sicherheitsgesetz dazu beitragen möchte, die Cyber-Sicherheit zu stärken. Der Begriff Cyber-Sicherheit nimmt nicht zufällig auch eine prominente Rolle in der Digitalen Agenda der Bundesregierung ein, mit welcher sie sich die Gestaltung der fortschreitenden Digitalisierung der Gesellschaft zu einem Handlungsfeld gemacht hat.

Frage 7

Gibt es aus Ihrer Sicht - ergänzende Instrumente (beispielsweise im Bereich der Werbung; Auditierung, Gütesiegel etc.), die das Recht auf informationelle Selbstbestimmung zusätzlich wirksam schützen können? Wenn ja, wie müssten diese ausgestaltet sein? Welche Rahmenvorgaben bedarf es, um wirklich aussagefähige und wirksame Audits oder Gütesiegel zu bekommen?

Audits und Gütesiegel, aber auch Codes of Conduct (CoC) sind wichtige und notwendige ergänzende Instrumente zur Verbesserung des Datenschutzes. Sie sind zudem ein Wettbewerbsfaktor.

Die Datenschutz-Grundverordnung sieht einen rechtlichen Rahmen für CoC und Zertifizierung (Audits und Gütesiegel) vor. Bei der Zertifizierung hat sich der Rat für ein Modell entschieden, bei dem Zertifizierungsstellen die Zertifizierung vornehmen. Diese sollen durch die Datenschutzbehörden oder durch Nationale Akkreditierungsstellen nach VO 765/2008 akkreditiert werden. Die Kriterien für die Zertifizierung und die Verleihung von Gütesiegeln werden durch die Datenschutzbehörde bzw. den Europäischen Datenschutzausschuss festgelegt.

Die Datenschutz-Grundverordnung wird voraussichtlich auch Anreize für die Zertifizierung enthalten. Hierzu gehört etwa der Nachweis der Einhaltung des technischen und organisatorischen Datenschutzes bei der Auftragsdatenverarbeitung oder der Nachweis angemessener Schutzmaßnahmen bei der Drittstaatenübermittlung. Beide Nachweise können beispielsweise auch mithilfe einer Zertifizierung geführt werden.

Das Modell des Europäischen Rates entspricht grundsätzlich auch meinen Vorstellungen. Es entlastet die Aufsichtsbehörden, ohne deren Kompetenzen zu beschneiden und trägt dennoch zu einer Verbesserung des Datenschutzes bei.

Das Modell des Europäischen Parlaments ähnelt dem des Europäischen Rates, allerdings mit einem entscheidenden Unterschied: Die Begutachtung wird auch hier von akkreditierten Zertifizierungsstellen durchgeführt, die endgültige Entscheidung und Verleihung des Gütesiegels aber durch die Datenschutzbehörden vorgenommen.

Unabhängig davon, wofür man sich entscheidet, entsteht dadurch auch ein europaweiter Markt für die Zertifizierungsstellen.

Frage 8

Welche Instrumente und Möglichkeiten sehen Sie, um die Daten-Souveränität der Nutzer beispielsweise durch privacy by design und privacy by default, durch nutzerkompatible Formen der AGBs und spezifische Opt-Out-Möglichkeiten, Interoperabilität von Daten zwischen Diensten, der Ermöglichung von entsprechenden Datenschutzeinstellungen (jenseits der grundsätzlichen Einwilligung in AGB) oder Transparenz-Verpflichtungen zu erhöhen und so auch die Akzeptanz neuer Geschäftsmodellen zu stärken?

Alle genannten Aspekte sind positiv zu bewerten. Die Instrumente sind in der Datenschutz-Grundverordnung überwiegend auch angelegt oder werden diskutiert:

- Privacy by Design/Default sowie der Grundsatz der Datenvermeidung und Datensparsamkeit finden sich in Art. 5 und 23 Datenschutz-Grundverordnung.
- Spezifische Opt-Out-Möglichkeiten enthalten etwa das Widerspruchsrecht nach Art. 19 und ggf. zusätzlich die Vorschrift zum Profiling (Art. 20).
- Die Interoperabilität von Daten wird durch das Prinzip der Datenportabilität (Art. 18 Datenschutz-Grundverordnung) adressiert. Einzelheiten dazu werden zzt. noch verhandelt.
- Die Erhöhung von Transparenzverpflichtungen ist Gegenstand des Kapitels III, über das zzt. im Rat verhandelt wird.
- Die Anforderungen an die Wirksamkeit von Einwilligungen müssen gestärkt werden (Stichwort Koppelungs- und Diskriminierungsverbote), hierzu s. o. zu Frage 4.

Frage 9

Ist das Prinzip der Datensparsamkeit aus Ihrer Sicht noch zeitgemäß? Welche anderen Instrumente sind denkbar, die das Recht auf informationelle Selbstbestimmung und die Entwicklung von Innovationen und neuer und innovativer Geschäftsmodelle in Einklang bringen?

Das Prinzip der Datensparsamkeit ist zeitgemäß und aktueller denn je. Es schafft den nötigen Anreiz, dass sich Unternehmen bei der Entwicklung von Innovationen und neuen Geschäftsmodellen immer daran orientieren müssen, so wenig wie möglich personenbezogene Daten zu verarbeiten, um die Eingriffe in das Recht auf informationelle Selbstbestimmung möglichst gering zu halten. Das bedeutet im Zeitalter allgegenwärtiger Datenverarbeitung und Big Data vor allem, dass technische Lösungen für eine möglichst frühzeitige Beseitigung des Personenbezugs gefunden werden, sofern die Entstehung personenbezogener Daten nicht vermieden werden kann.

Andere Instrumente finden sich in ausreichender Zahl und Qualität im geltenden wie auch im künftigen Datenschutzrecht. Es ist eine der zentralen Funktionen des Datenschutzrechts, das Recht auf informationelle Selbstbestimmung mit den berechtigten oder rechtlichen Interessen von Unternehmen in einen angemessenen Ausgleich zu bringen. Vorschriften wie etwa die Interessenabwägung (§ 28 Abs. 1 Satz 1 Nr. 2 BDSG, Art. 6(1)(f) DSGVO) beleuchten geradezu exemplarisch diesen Ausgleich. Ein Bedarf für gänzlich neue Instrumente wird daher nicht gesehen.

Frage 10

Was sind aus Ihrer Sicht denkbare Ansätze, wie das (nationale und europäische) Datenschutzrecht weiterentwickelt werden kann, um im Kern mit der heutigen Entwicklung mithalten zu können und wie bewerten Sie vor diesem Hintergrund mögliche Vorschläge, nach denen sich die Weiterentwicklung des Datenschutzrechtes an einem materiellen Immaterialgüterrecht und dem Recht der Verfügung über Daten und deren Nutzung orientieren sollte, um einerseits auch den Marktwert personenbezogener Daten zu unterstreichen und den Rechtsträger mit Ausschließlichkeitsrechten auszustatten? Sollten und wenn ja wie, der Wert personenbezogener Daten in die kartell- wettbewerbs- und fusionsrechtliche Bewertung von Unternehmen einfließen?

Der bisherige Ansatz des Datenschutzrechts (Anknüpfung an dem personenbezogenen Datum des Einzelnen) hat sich grundsätzlich bewährt und ist auch innovations- und entwicklungsoffen. Deshalb folgt die Datenschutz-Grundverordnung auch dem der Europäischen Datenschutzrichtlinie (RL 95/46/EG) zugrunde liegenden Ansatz.

Gleichwohl bedarf es einer fortwährenden wissenschaftlichen, juristischen und gesellschaftlichen Debatte, wie das Datenschutzrecht weiterentwickelt werden kann. Im Mittelpunkt müssen dabei in jedem Falle immer die Grundrechte des Einzelnen und die Gewährleistung seiner Autonomie stehen.

Die Einbeziehung des Wertes personenbezogener Daten in die kartell-, wettbewerbs- und fusionsrechtliche Bewertung von Unternehmen ist ein bedenkenswerter Ansatz, um deutlich zu machen, dass Daten einen wirtschaftlich enormen Wert haben und dass etwa eine monopolhafte Datenmacht – abgesehen von den wettbewerbsrechtlichen Bedenken – auch zu einer Beherrschung und Monopolisierung von Meinungsbildung und Informationszugang und letztlich zu einer Verhaltenssteuerung führt. Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder hat in einer Entschließung vom Oktober 2014 auch auf diese Problematik aufmerksam gemacht und eine bessere Zusammenarbeit der Kartell- und Datenschutzbehörden angemahnt (www.bfdi.bund.de/SharedDocs/Publikationen/Entschliessungssammlung/DSBundLaender/88DSK_Marktmacht.pdf?__blob=publicationFile&v=3).

Die Datenschutzkonferenz hat darauf hingewiesen, dass das in der Datenschutz-Grundverordnung vorgesehene Prinzip der Datenportabilität ein wichtiges Instrument ist, um die sowohl die Souveränität des einzelnen Nutzers zu stärken als auch die auf der Samm-

lung personenbezogener Daten beruhende Machtposition einzelner Unternehmen zu begrenzen.

Darüber hinaus könnte daran gedacht werden, Instrumente zur Vielfaltsicherung vorzusehen, wie es sie bspw. im Medienbereich mit der Konzentrationskontrolle durch die KEK nach dem RStV gibt. Denkbar wäre es etwa, die Änderung von Beteiligungsverhältnissen oder sonstigen Einflüssen bei Unternehmen mit einer bedeutenden Datenmacht bei den Datenschutzaufsichtsbehörden zu melden und diese mit entsprechenden kartellrechtsähnlichen Instrumenten auszustatten. Dies wäre allerdings rechtliches Neuland.

Frage 11

Wie beurteilen Sie den Zielkonflikt sicherheitspolitischer Interessen und einem effektiven Grundrechtschutz, bspw. bei Fragen des Schutzes von Grundrechten durch die Sicherung der Privatsphäre einerseits (beispielsweise durch Verschlüsselung und Anonymisierung) und dem Interesse von Geheimdiensten, die Integrität digitaler Infrastrukturen und Datenschutz bspw. durch Zero-Day-Exploits zu untergraben andererseits?

Den beschriebenen Zielkonflikt sehe ich natürlich. Aber es ist eine wichtige Aufgabe des Rechtsstaates, Grenzen zu setzen. Datenschutz ist ein wichtiges Grundrecht und Teil des Rechtsstaats. Daher setzt natürlich auch der Datenschutz Grenzen. Diese Grenzen sind aber nicht absolut. Der Gesetzgeber und im Einzelfall die die mit der Gefahrenabwehr betrauten Behörden müssen gleichwohl jeweils gute Gründe liefern, weshalb es gerechtfertigt ist, im Einzelfall in Grundrechte einzugreifen. Nach den Vorgaben des BVerfG müssen die Grundrechte gegeneinander abgewogen werden.

Besonders vor dem Hintergrund der hier zur Diskussion stehenden wirtschaftlichen Aspekte möchte ich darauf hinweisen, dass zu einem gedeihlichen Umfeld für die Internet-Ökonomie auch das Vertrauen der Bürgerinnen und Bürger auf einen glaubwürdig transparenten Umgang der Marktteilnehmer mit deren Daten und natürlich eine effiziente Cyber-Sicherheit gehört. Zu einem glaubwürdigen Datenschutz gehören auch die Anonymisierung und Pseudonymisierung von Daten, wo immer diese möglich ist. Insbesondere für statistische Auswertungen ist der Personenbezug entbehrlich. Auch Big Data ist mit anonymisierten oder zumindest pseudonymisierten Daten möglich. Einer der geladenen Fachexperten (Stephan Noller) hat diesen Beweis mit dem von ihm optimierten Verfahren zur Auswertung des Nutzerverhaltens auf Basis anonymisierter Nutzerdaten erbracht.

Die Cyber-Sicherheit bildet eine Voraussetzung für das Vertrauen von Nutzern in die digitale Infrastruktur. Die Integrität digitaler Infrastrukturen zu untergraben, würde auch die Cyber-Sicherheit untergraben. Zur Cyber-Sicherheit gehört unabdingbar, dass einmal erkannte Sicherheitslücken und Schwachstellen in der digitalen Infrastruktur schnellstmöglich behoben werden, um Nutzer, zu denen Behörden, Unternehmen sowie Bürgerinnen und Bürger gleichermaßen gehören, nicht unnötigen Risiken auszusetzen. Mit dem Aufkauf von Sicherheitslücken für einen anderen Zweck, als dem der schnellen Schließung dieser Lücken, würde man mit der einen Hand einreißen, was man mit der anderen Hand aufgebaut hat. Nicht nur, das Betroffene weiterhin Risiken ausgesetzt wären, weil Sicherheitslücken nicht geschlossen werden, es wäre womöglich für Experten auch attraktiver ihre einmal erlangte

Kenntnis von Sicherheitslücken an Behörden weiter zu verkaufen, anstatt wie bisher üblich die Öffentlichkeit zu warnen und Hersteller fehlerhafter Produkte zu informieren.

Die Bedeutung von Verschlüsselung für die Cyber-Sicherheit kann gar nicht überschätzt werden. Verschlüsselung ist offensichtlich die erste Maßnahme, die Anbieter weltweit einsetzen, um ihre Transportwege in der digitalen Infrastruktur abzusichern. Sie bildet einen wesentlichen Bestandteil der Initiative "E-Mail made in Deutschland", die einige deutsche Anbieter von E-Mail-Diensten ins Leben gerufen haben. Ende-zu-Ende-Verschlüsselung ist nicht zuletzt das ultimative Mittel, das Grundrecht auf informationelle Selbstbestimmung durchzusetzen. Meine Kollegen haben dazu in der DSK schon 2013 im Jahr 1 der Snowden-Enthüllungen einen Entschluss gefasst, der auch heute nicht an seiner Gültigkeit eingebüßt hat. Diese Entschließung enthält im Titel eine Aufforderung "Sichere elektronische Kommunikation gewährleisten - Ende-zu-Ende-Verschlüsselung einsetzen und weiterentwickeln" (www.bfdi.bund.de/SharedDocs/Publikationen/Entschliessungssammlung/DSBundLaender/86_DSKSiichereElektronischeKommunikationGewaehrleisten.pdf?__blob=publicationFile&v=1). Diese Aufforderung hat die Bundesregierung dankenswerterweise aufgegriffen. In der Digitalen Agenda wird nicht zufällig an mehreren Stellen betont, dass man Deutschland zum Verschlüsselungsstandort Nr. 1 in der Welt machen wolle.

Frage 12

Welche konkreten Innovationshemmnisse sehen Sie für deutsche IT Startups und welche Beispiele können Sie dafür nennen? Für wie zentral halten Sie eine Fokussierung der Politik auf die finanziellen Mittel von IT Startups? Welche anderen Aufgaben- und Problemfelder halten Sie für ebenfalls wichtig? Haben Sie konkrete Vorschläge für eine Hilfestellung für IT Startups, die sich nicht mit der Frage der Finanzierung beschäftigen?

Diese Frage richtet sich ersichtlich an die anderen Sachverständigen und nicht in erster Linie an mich. Datenschutzrechtliche Rahmenbedingungen sind m. E. kein Innovationshindernis, wie bereits mehrfach bei verschiedenen obigen Antworten dargelegt. Inwieweit andere Innovationshemmnisse bestehen, kann hier nicht beurteilt werden und muss von mir auch nicht beantwortet werden.

Andrea Voßhoff