Rede von Frau Staatssekretärin im Bundesministerium der Justiz
und für Verbraucherschutz
Dr. Stefanie Hubig

auf dem Datenschutzkongress des rheinland-pfälzischen Innenministeriums
„Regelungsabsichten und Verfahrensstand des Gesetzgebungsverfahrens der Datenschutz-Grundverordnung“

am 15. Oktober 2015 in Mainz

Es gilt das gesprochene Wort!

Sehr geehrter Herr Staatssekretär,
sehr geehrter Herr Professor Kugelmann,
sehr geehrte Frau Hansen,
sehr geehrte Damen und Herren,

ich danke Ihnen für die Gelegenheit, heute zu Ihnen über ein Gesetzgebungsvorhaben sprechen zu dürfen, mit dem im Datenschutz gewissermaßen eine neue Zeitrechnung beginnt: die EU-Datenschutz-Grundverordnung.

Sie wird das Datenschutzrecht in Europa vor allem für Unternehmen und Verbraucherinnen und Verbraucher vereinheitlichen und weitgehend an die Stelle des geltenden Bundesdatenschutzgesetzes treten. Die Datenschutz-Grundverordnung wird also eine Art „Grundgesetz“ für den Umgang mit personenbezogenen Daten sein und damit auch Ihre tägliche Arbeit in den Unternehmen unmittelbar beeinflussen.

Ich möchte deshalb zunächst

- in einem ersten Teil über den Stand der Beratungen in Brüssel berichten,
- und sodann im zweiten Teil meiner Rede die wesentlichen Veränderungen vorstellen, insbesondere auch was Deutschland in den Beratungen erreicht hat,
- und ich will dabei auch offen sagen, wo wir uns noch mehr gewünscht haben, aber möglicherweise am Ende Kompromisse machen müssen.

I.

Zunächst zum aktuellen Stand der Verhandlungen:
Der Rat der Innen- und Justizminister hat im Juni dieses Jahres nach mehr als drei Jahren Verhandlungen seinen Standpunkt beschlossen. Aktuell befinden wir uns im Trilog. Es verhandeln also die Kommission, die jeweilige Ratspräsidentschaft – im Moment ist das Luxemburg – und die Berichterstatter des Europäischen Parlaments gemeinsam über den Verordnungsentwurf.

Das Europäische Parlament hatte seinen Standpunkt zur Verordnung bereits im März 2014 mit einer bemerkenswerten Mehrheit von 95 % festgelegt.

Die luxemburgische Präsidentschaft stimmt ihre Verhandlungsführung für den Trilog eng und kontinuierlich mit den Mitgliedstaaten ab. Allerdings sind die Trilogverhandlungen vertraulich. Daher bitte ich um Ihr Verständnis, wenn ich mich hier mit Details zurückhalte.
Aber: Die Verhandlungen im Trilog bewegen sich ganz weitgehend in dem Raum, den der Entwurf der Kommission und die Standpunkte von Rat und Europäischem Parlament

abstecken. Neue Vorschläge außerhalb dieses „Korridors“ haben kaum eine Chance, noch aufgegriffen zu werden. Wenn Sie sich also die vorliegenden Positionen der drei europäischen Institutionen ansehen, können Sie schon ganz gut abschätzen, wie das Ergebnis aussehen wird. Ich werde mich im Folgenden auch an diesen Ausgangspunkten für den Trilog orientieren.

Zu den Verhandlungen selbst kann ich Ihnen sagen: Es geht mit großen Schritten dem Ende zu. Der Wunsch, die Verordnung noch in diesem Jahr zu verabschieden, ist auf allen Seiten groß. Mein persönlicher Eindruck ist, dass dies gelingen kann. Es gibt noch ein paar Klippen zu umschiffen, auf die ich noch eingehen werde; aber auch das sollte uns gelingen. Und dann wird die Datenschutz-Grundverordnung im Frühjahr nächsten Jahres im Amtsblatt veröffentlicht werden. Dann bleibt uns allen voraussichtlich eine Übergangszeit von zwei Jahren, bis die Verordnung in den Mitgliedstaaten unmittelbar anwendbar sein wird.

Die Datenschutz-Grundverordnung wird das Datenschutzrecht in der EU weitgehend harmonisieren. Raum für nationale Regelungen wird es nur punktuell geben, nämlich dann, wenn die Datenschutz-Grundverordnung es ausdrücklich erlaubt. Öffnungsklauseln sind bisher etwa für den Beschäftigtendatenschutz vorgesehen sowie punktuell für den Umgang mit besonders sensiblen Daten, wie z. B. den Gesundheitsdaten. Von großer Bedeutung war es für die Bundesregierung, unser hohes Datenschutzniveau im öffentlichen Bereich zu erhalten, also für die Datenverarbeitung durch den Staat. Ein Grundpfeiler unseres hohen Datenschutzes in diesem Bereich sind unsere maßgeschneiderten bereichsspezifischen Regelungen. Denken Sie etwa an die Abgabenordung, das Sozialrecht oder die Datenschutzvorschriften in Schulgesetzen. Diese Regelungen werden weitgehend unverändert bleiben können. Die Datenschutz-Grundverordnung erlaubt es nämlich den Mitgliedstaaten, weiterhin spezielle Regeln für den öffentlichen Bereich zu schaffen, so dass uns hier voraussichtlich nichts an Datenschutz verloren gehen wird.

Die tiefgreifendsten Änderungen wird es in dem Bereich geben, der vor allem Sie betrifft: der Datenverarbeitung durch Private. Die bestehenden Regelungen des Bundesdatenschutzgesetzes für die Datenverarbeitung im nichtöffentlichen Bereich, vor allem die §§ 28 ff. BDSG, werden dann nahezu vollständig durch die Datenschutz-Grundverordnung abgelöst. Viele Spezialregelungen des deutschen Datenschutzrechts werden ersetzt, z. B. diejenigen zur geschäftsmäßigen Datenverarbeitung zu Zwecken der Markt- und Meinungsforschung oder zu Werbezwecken. Stattdessen gilt dann ab Frühjahr 2018 unmittelbar die Datenschutz-Grundverordnung.

II.

Meine Damen und Herren,

ich komme zum zweiten Teil, der Sie sicher am meisten interessiert:
Was wird die Datenschutz-Grundverordnung Neues bringen?

Lassen Sie mich zunächst eines klarstellen: Es wird sich nicht alles ändern.
Die Datenschutz-Grundverordnung behält die Prinzipien der Datenschutz-Richtlinie von 1995 bei, die auch unserem Datenschutzrecht zugrunde liegen. Aber sie entwickelt diese Prinzipien fort. Alles andere wäre mit der Bundesregierung auch nicht zu machen gewesen. Denn das geltende Datenschutzniveau war und ist für uns in den Verhandlungen immer die „rote Linie“ gewesen, hinter die wir nicht zurückgehen.

1.
Von mancher Seite hört man, das Datenschutzrecht und insbesondere das sog. „Verbot mit Erlaubnisvorbehalt“ sei überholt oder den neuen technischen Entwicklungen nicht gewachsen. Deshalb ist mir wichtig klarzustellen: die Grundsätze unseres bisherigen Datenschutzrechts standen in den Diskussionen auf europäischer Ebene niemals in Zweifel – auch nicht mit Blick auf das Internet, die Informatisierung unseres Alltags und Big Data. Das ist auch richtig so. Die Grundsätze unseres Datenschutzes leiten sich schließlich aus den Grundrechten unserer Verfassung und der Grundrechte-Charta ab. Mit den bewährten Grundprinzipien unseres Datenschutzrechts können wir auch die Herausforderungen dieser technischen Entwicklungen bewältigen.

Nehmen wir Big Data als Beispiel. Vernetzte Maschinen in der Industrie 4.0 steigern die Produktivität. SmartCars, SmartPhones, SmartHomes und SmartTVs werden das Leben der Verbraucherinnen und Verbraucher sicherer und angenehmer machen. Solche neuen technischen Möglichkeiten führen aber nicht dazu, dass wir von unseren Prinzipien abweichen müssten. Im Gegenteil: Wo große Datenmengen, Vernetzung und Automatisierung das Recht auf informationelle Selbstbestimmung besonders verletzlich machen, muss das Recht nachziehen, um faire Rahmenbedingungen zu erhalten. Auch deswegen müssen sich die Anbieter immer fragen: Brauchen wir alle diese Informationen wirklich? In den meisten Fällen wird es ausreichen, auf pseudonymisierte oder anonymisierte Daten zurückzugreifen. Wie bei einer Statistik kommt es dem Datenanalytiker ja nicht auf die einzelne Person an. Im Gegenteil: Wer aus den Suchanfragen im Internet zu Medikamenten und Symptomen den Verlauf einer Grippewelle prognostizieren möchte, den interessiert nicht, wer was sucht, sondern nur wie viele und wo. Niemand will zum gläsernen Bürger, Autofahrer, Patienten oder Arbeitnehmer werden. Es ist deshalb bedauerlich, dass sich die Mehrheit der Mitgliedstaaten im Rat nur auf Regelungen zur Verwendung von Profilen, nicht aber auch schon auf Regelungen zur Profilbildung verständigen konnte.

Hier hätten wir uns aus Sicht des Daten- und Verbraucherschutzes mehr gewünscht. Der Rats-Standpunkt wie schon der Entwurf der Kommission führt nun nur das Verbot automatisierter Einzelfallentscheidungen fort, das wir auch aus § 6a BDSG kennen. Das Europäische Parlament will hier allerdings weitergehende Regelungen. Ob sich also im Trilog noch etwas ändern wird, werden wir abwarten müssen.

2.
Auch eine andere Errungenschaft des deutschen Datenschutzes haben wir gesichert: die betrieblichen Datenschutzbeauftragten. Betriebliche Datenschutzbeauftragte sind nah dran an den Problemen des Unternehmens, kennen die Abläufe und können in den Unternehmen Anwälte für den Datenschutz sein. Wir haben im Rat erreicht, dass die Mitgliedstaaten betriebliche Datenschutzbeauftragte weiterhin verpflichtend vorsehen können.

Für die deutsche Wirtschaft wird sich also nichts ändern. Wir möchten die Institution des betrieblichen Datenschutzbeauftragten aber gerne auf ganz Europa ausweiten, schon um Wettbewerbsnachteile für die deutsche Wirtschaft zu vermeiden. Leider sehen viele Mitgliedstaaten darin eine überflüssige bürokratische Last. Sie wollen stattdessen die Unternehmen verpflichten, sich bei einer für die Betroffenen besonders risikoreichen Datenverarbeitung mit den Datenschutzaufsichtsbehörden abzustimmen. Wir haben dagegen die Erfahrung gemacht, dass gerade die Datenschutzbeauftragten viel Abstimmungsaufwand abnehmen. Das Parlament und die Kommission sind hier unsere Mitstreiter. Warten wir also den Fortgang des Trilogs ab. Hier bewegt sich hoffentlich noch etwas, auch wenn die Position der Mehrheit der Mitgliedstaaten uns nicht allzu großen Mut macht.

3.
Einwilligung und Zweckbindung bleiben weiterhin die Grundlagen der Selbstbestimmung über die persönlichen Daten. Aber auch hier kann und soll einiges verbessert werden.
Die Einwilligung wird oft kritisiert, es heißt: „Die seitenlangen Einwilligungserklärungen liest doch eh keiner...“ Das ist nicht ganz von der Hand zu weisen. Aber der Grundsatz, dass persönliche Daten nur mit der Einwilligung des Betroffenen genutzt werden dürfen, bleibt richtig. Nicht ohne Grund sprechen wir von informationeller Selbstbestimmung. Aber wir müssen verhindern, dass Einwilligungen zur bloßen Fiktion verkommen. Statt auf das Institut der Einwilligung zu verzichten, müssen wir die Selbstbestimmung des Einzelnen stärken. Das ist die Herausforderung für den Datenschutz heute!

Wir kennen das Problem ja schon lange aus dem Verbraucherschutz und den seitenlangen Geschäftsbedingungen vieler Verträge. Gegen komplizierte oder überraschende Klauseln schützt hier das AGB-Recht. Es sorgt dafür, dass der Verbraucher sich darauf verlassen kann, dass ihm nur faire Vertragsbedingungen vorgelegt werden und nichts

„untergeschoben“ wird. Dieses Grundkonzept aus dem Vertragsrecht sollten wir in das Datenschutzrecht übertragen – und es sieht im Moment auch ganz gut aus, dass uns dies gelingt!

Nach dem Willen von Rat und Parlament müssen vorformulierte Einwilligungserklärungen künftig verständlich und in klarer Sprache formuliert sein. Der Inhalt darf nicht zu sehr von dem abweichen, was Verbraucherinnen und Verbraucher in der konkreten Situation erwarten. Wenn wir davon noch die Kommission überzeugen können, setzen wir einen Standard, den wir so in Europa noch nicht hatten. Wir konnten den Rat sogar überzeugen, noch einen Schritt weiter zu gehen: In zwei Konstellationen soll künftig die Vermutung gelten, dass eine Einwilligung nicht freiwillig erteilt worden ist:

Erster Fall: Wenn die Einwilligung Voraussetzung für einen Vertragsabschluss ist, dann gilt sie als nicht erteilt, wenn – erstens – die Datenverarbeitung, in die wir einwilligen, für die Vertragsabwicklung gar nicht gebraucht wird, und – zweitens – wenn es uns zudem nicht zumutbar ist auf einen anderen Anbieter auszuweichen. Dieses Problem stellt sich zum Beispiel bei einer Änderung der AGB von Facebook. Wenn ich nicht in die Datenverarbeitung einwilligen will, kann ich theoretisch in ein anderes soziales Netzwerk wechseln. Aber kann ich das tatsächlich, wenn all meine Freunde oder Kontakte weiterhin bei Facebook sind? Selbstbestimmt, aber einsam? Das ist nicht wirklich eine Alternative.

Ähnlich ist es, wenn mich Hardware an Software eines Herstellers „fesselt“, wie z.B. bei Apple, Smartphones oder vielen vernetzten Geräten. In diesen Fällen soll künftig vermutet werden, dass die Einwilligung nicht freiwillig erteilt wurde. Im Ergebnis handelt es sich demnach um ein begrenztes Koppelungsverbot im Falle einer marktbeherrschenden Stellung. Für die Werbung gilt das bereits nach § 28 Absatz 3b BDSG. Das Europäische Parlament will übrigens noch weiter gehen und schlägt sogar ein allgemeines Koppelungsverbot vor.

Die zweite Konstellation, in der künftig die Vermutung für eine unfreiwillige Einwilligung gilt betrifft die sogenannten Globaleinwilligungen. Ein Unternehmen wie zum Beispiel Google wird dann nicht mehr so leicht behaupten können, jeder habe freiwillig die 22seitigen Datenschutzbestimmungen gelesen und in sie eingewilligt. Tatsächlich gibt es Berechnungen, dass wir 67 ganze Arbeitstage bräuchten, um alle Bestimmungen, in die wir im Jahr so einwilligen, tatsächlich von A bis Z zu lesen. Das zeigt die faktische Unmöglichkeit dessen, was uns abverlangt wird. Unabhängig davon, ob wir wirklich alles gelesen haben, stehen wir Nutzer hier ohnehin nur vor der Alternative „Alles oder nichts“. „Take it or leave it“! Darauf, ob wir wirklich mit jedem Punkt einverstanden sind, kommt es gar nicht an. Denn wir können einzelnen Punkten der Erklärung gar nicht widersprechen.

In Zukunft ist dieses „Alles oder nichts“-Prinzip dann nicht mehr zulässig, wenn es dem Anbieter zumutbar ist, die Einwilligung zu zerlegen. Dann kann man künftig in manche Ich stelle mir dies ähnlich vor, wie beim Smartphone. Dort kann ich auch genau festlegen, welche App auf meine Kontakte oder Standortdaten zugreifen soll. Solche Ansätze wollen wir fördern. Eine solche „differenzierte“ Einwilligung wäre ein deutlicher Zugewinn an Entscheidungsfreiheit für die Verbraucherinnen und Verbraucher. Die Einwilligung soll also wieder das werden, was sie auch sein soll: ein Instrument zur Sicherung der persönlichen Datensouveränität. Das war einer der Punkte, die der Bundesregierung in den Verhandlungen besonders wichtig gewesen sind.

4.
Zur Datensouveränität gehört auch das in der Datenschutz-Grundverordnung erstmals vorgesehene Recht auf Datenportabilität. Es ermöglicht vor allem den Nutzern von E-Mail-Diensten und von sozialen Netzwerken mit ihrem kompletten Account zu einem Konkurrenten zu wechseln. Auch dies ist ein Freiheitsgewinn für die Nutzerinnen und Nutzer. Und es stärkt den Wettbewerb, wie jüngst die Monopolkommission hervorgehoben hat.

5.
Ein weiterer bewährter Grundsatz des Datenschutzrechts ist die Zweckbindung. Ihm liegt der Gedanke zu Grunde, dass es für den Betroffenen erkennbar bleiben muss, für welche Zwecke seine Daten verwendet werden. Der Datenverwendung für andere Zwecke als die, für die sie beim Betroffenen erhoben wurden, werden damit Grenzen gesetzt. Der Entwurf der Kommission weicht hier von der Systematik der Datenschutz-Richtlinie von 1995 leicht ab. Das hat bei den Beratungen im Rat und wohl auch im Parlament für einige Diskussionen gesorgt. Im Rat haben wir die Beratungen zu diesem Komplex letztlich „eingefroren“, um den Beginn des Trilogs nicht zu verzögern. Die Verhandlungen zu diesem wichtigen Punkt sind seither noch nicht abgeschlossen.

Auch bei der Zweckbindung ist der Erhalt des Datenschutzniveaus des geltenden Rechts unsere „rote Linie“. Dabei kommt es weniger darauf an, ob die einzelnen Regelungen deckungsgleich mit denen der Richtlinie von 1995 sind. Entscheidend ist, dass das Datenschutzniveau in der Gesamtschau nicht unterschritten wird. Um das zu beurteilen, muss man alle einschlägigen Regelungen in den Blick nehmen, zum Beispiel auch die gegenüber dem geltenden Recht erweiterten Informationspflichten.

Kritisch sehen wir in diesem Zusammenhang die geplante Privilegierung der Datenverarbeitung zu Zwecken der Forschung und Statistik. Grundsätzlich stellt man sich das wenig problematisch vor, denn die Datenverarbeitung dient ja einem guten Zweck. Die Privilegierung, wie sie derzeit im Ratsentwurf enthalten ist, geht dennoch zu weit. Das will ich an einem Beispiel deutlich machen: Stellen Sie sich vor, Sie gehen zu einer Ihrer

regelmäßigen Vorsorgeuntersuchungen zu Ihrem Hausarzt und dieser entnimmt Ihnen eine Blutprobe. Würde die derzeit im Ratstext vorgesehene Regelung übernommen, könnten künftig Ihre Labor-Ergebnisse von dem Labor für beliebige Forschungsprojekte genutzt oder an Forschungseinrichtungen weitergegeben werden. Und zwar nicht nur ohne Ihre Einwilligung, sondern sogar mit Ihren Personalien. Für die Weitergabe der Daten würde es ausreichen, dass diese für Forschung und Statistik „erforderlich“ ist. Die Rechte und Interessen des Patienten werden nicht berücksichtigt. Bei allem Verständnis für die Bedeutung der Forschung – eine solche Privilegierung geht zu weit. An diesem Punkt muss aus unserer Sicht im Trilog noch nachgebessert werden.

6.
Eine der wichtigsten Neuerungen der Datenschutz-Grundverordnung ist das Marktortprinzip. Damit sich datenschutzfreundliche Angebote auf dem europäischen Markt entwickeln können, braucht Europa mehr Gestaltungsmacht gegenüber den Global Playern, und dafür brauchen wir das Marktortprinzip.

Schon jetzt gilt: Wer eine Niederlassung in Europa hat, muss europäische Standards im Datenschutz beachten. Die Datenschutz-Grundverordnung geht darüber hinaus. Sie wird für alle Unternehmen gelten, die Waren und Dienstleistungen auf dem europäischen Markt anbieten oder das Verhalten von Verbraucherinnen und Verbrauchern in der EU beobachten. Ein New Yorker Online-Versandhändler kann sich dann nicht mehr darauf zurückziehen, dass er mit Europa nicht in Berührung kommt: Europäischer Datenschutz gilt künftig auch für ihn, und zwar auch dann, wenn seine Firma allein in den USA eine Niederlassung hat, wenn er die Waren ausschließlich von dort verschickt und er seine Website ausschließlich auf einem amerikanischen Server hostet. Entscheidend ist, dass sich sein Angebot auch an EU-Bürger richtet. Wer hier am Markt aktiv ist, der muss sich auch an europäisches Recht halten. Gleiches Recht für alle, die ihre Waren und Dienstleistungen auf demselben Markt anbieten. Das ist ein wichtiger Fortschritt. Mit dem Marktortprinzip werden wir Datenschutzoasen austrocknen. Und das ist nicht nur für die Verbraucherinnen und Verbraucher gut, sondern auch für die europäische Wirtschaft. Denn es schafft gleiche Wettbewerbsbedingungen, ein „level playing field“, zwischen Unternehmen aus der EU und ihren außereuropäischen Konkurrenten.

Das Marktortprinzip ist auch Ausdruck eines stärkeren europäischen Selbstbewusstseins: In Europa gelten Europas Regeln. Und die informationelle Selbstbestimmung ist ein Wert von grundlegender Bedeutung für unser Zusammenleben und soll es auch bleiben! Das ist nicht nur im Wirtschaftsleben wichtig, sondern auch dort, wo es um den Datentransfer in Drittstaaten geht, zum Beispiel an Unternehmen in die USA, die massenhaft Daten an die dortige Nachrichtendienste und Sicherheitsbehörden heraus geben müssen.

Der Europäische Gerichtshof hat hier in der letzten Woche ein starkes Signal für die Grundrechte gesetzt, indem er die Safe Harbor-Entscheidung der EU-Kommission für ungültig erklärt hat. Für die Mitgliedstaaten und insbesondere für die Europäische Kommission ist das Urteil ein Auftrag: Wir müssen dafür kämpfen, dass europäische Daten auch nach einer Übermittlung in ein Land außerhalb der EU ausreichend geschützt sind. Aber klar ist auch: Wir brauchen einen praktikablen Mechanismus für den Datenaustausch von einer Seite des Atlantiks auf die andere. Die Verhandlungen mit den USA über eine verbesserte Grundlage für die Datenübermittlung müssen daher weitergehen. Die USA müssen aber akzeptieren: Wir Europäer entscheiden, unter welchen Bedingungen eine Übermittlung in die USA zulässig ist. Die Bundesregierung hat den Safe Harbor-Mechanismus schon seit Längerem kritisch gesehen. Wir haben daher die Kommission immer in ihren Verhandlungen mit den USA unterstützt und sind gespannt, wie es hier nun weitergeht.

Seit den Enthüllungen von Edward Snowden fordern zudem nicht nur wir, dass Übermittlungen an ausländische Gerichte und Behörden in Zukunft erst in Europa genehmigt werden müssen. Das stellt Facebook und Co. sicherlich vor ein Dilemma. Sie müssen sowohl das europäische Datenschutzrecht beachten als auch die Herausgabepflicht in den USA. Auch da wird die Marktmacht wirken. 500 Millionen europäische Kunden werden ein Argument sein, über das auch Facebook nicht einfach hinwegsehen kann. Und wenn wir dieses Dilemma rechtlich absichern, wäre das auch ein starkes politisches Signal über den Atlantik. Dieses Signal wünschen wir uns, und wir haben dabei das Europäische Parlament an unserer Seite.

7.
Meine Damen und Herren,
ich komme zu einem weiteren wesentlichen Punkt der Datenschutz-Grundverordnung. Jedes Recht ist nur so gut wie seine Durchsetzung. Die Verordnung stellt die Rechtsdurchsetzung auf drei Säulen:

- Erstens: eine einheitliche Aufsicht,
- Zweitens: gleiche Regeln in ganz Europa, die auch einheitlich ausgelegt werden, und
- Drittens: gleiche und vor allem effektive Sanktionen für alle.

Die Aufsicht war bislang auf zu viele Akteure verteilt. Derzeit überwachen in den Mitgliedstaaten lokale Datenschutzbehörden die Einhaltung des Rechts. Jeder kann sich an seine örtliche Aufsichtsbehörde wenden. Das sorgt für Bürgernähe – auch wenn die heimatliche Datenschutzbehörde unter Umständen dann das Datenschutzrecht des Herkunftslands des Verarbeiters anwenden muss.

Die Kehrseite sieht so aus: Ein Unternehmen mit Niederlassungen in mehreren Mitgliedstaaten wurde bisher in jedem Land gesondert beaufsichtigt. Und manches Unternehmen wählt seinen Sitz in einem Mitgliedstaat, in dem es weniger „lästige“ Aufsichtsbehörden erwartet. Damit soll nun Schluss sein. Ob ein europaweit tätiger Konzern die Regeln einhält oder nicht, wird in Zukunft nur noch eine einzige Behörde prüfen – nämlich die am Sitz der Hauptniederlassung. Das ist das Konzept der „einheitlichen Anlaufstelle“ – des sogenannten One-Stop-Shop. Die lokale Datenschutzaufsichtsbehörde bleibt nur für rein lokale Sachverhalte zuständig, etwa die Videoüberwachung in einem Laden. Die Aufsicht über die europaweite Kundendatei liegt hingegen bei der einheitlichen Anlaufstelle am Hauptsitz des Unternehmens.

Für die Bürgerinnen und Bürger ändert sich trotzdem nichts. Die Verhandlungen im Rat zu diesem Punkt waren außergewöhnlich intensiv und schwierig. Kein Wunder, denn Zuständigkeitsfragen sind Machtfragen. Aber wir haben eine Lösung gefunden, die Bürgernähe weiter gewährleistet und von der wir jetzt hoffentlich auch das Parlament und Kommission überzeugen können. Ein Mainzer, der sich etwa gegen neue Datenschutzbestimmungen bei Facebook wehren will, muss auch in Zukunft nicht nach Irland schreiben, an den europäischen Hauptsitz von Facebook. Er kann seine Beschwerde weiter an die Behörde vor Ort richten. Erst der Rheinlandpfälzische Landesbeauftragte für den Datenschutz ist dann verpflichtet, die Kollegen in Dublin einzuschalten. Ich halte das für eine gute Lösung. Die Ansprechpartner bleiben vor Ort, und trotzdem werden die Entscheidungen übergreifend getroffen.

Zugleich steht dieser Ansatz für den zweiten Aspekt der europaweiten Rechtsdurchsetzung – die einheitliche Auslegung und Anwendung des europäischen Datenschutzrechts.
In Gefahr gerät sie, wenn die Datenschützer vor Ort und die am Sitz des Unternehmens unterschiedliche Rechtsauffassungen vertreten. In solchen Fällen soll in Zukunft der Europäische Datenschutzausschuss entscheiden, in dem alle Datenschutzbeauftragten aus den verschiedenen EU-Staaten vertreten sind. Mit einer Zweidrittel-Mehrheit kann der Ausschuss verbindliche Entscheidungen bei Meinungsverschiedenheiten zwischen den nationalen Aufsichtsbehörden treffen und damit für Klarheit sorgen. Die Zweidrittel-Mehrheit stellt dabei auch sicher, dass die gefundene Auslegung ausreichend breite Akzeptanz hat. Wer für Deutschland im Europäischen Datenschutzausschuss sitzen wird, ist übrigens noch eine spannende Frage.

Die dritte Komponente, mit der die Datenschutz-Grundverordnung eine effektive Rechtsdurchsetzung sicherstellen will, sind einheitliche und vor allem effektivere Sanktionen. Für Deutschland wird das eine drastische Anhebung der möglichen Bußgelder bedeuten. Statt maximal 300.000 Euro, dem Höchstsatz im Bundesdatenschutzgesetz, soll sich das Bußgeld am weltweiten Jahresumsatz bemessen. Die Kommission schlägt 2 % des

Jahresumsatzes als Obergrenze vor, das Europäische Parlament sogar bis zu 5 %; da muss man sich noch einigen.

Natürlich werden diese Sanktionen Unternehmen empfindlich treffen.
Das sollen sie aber auch. Sonst profitieren die „schwarzen Schafe“ – und die Wettbewerber, die sich an die Regeln halten, haben das Nachsehen. In dynamischen Märkten wie in der IT-Industrie können sie damit einen uneinholbaren Vorsprung gewinnen. Wir müssen daher den Aufsichtsbehörden ein scharfes Schwert in die Hand geben, damit sich Datenschutzverstöße nicht lohnen. Eine effektive Rechtsdurchsetzung stärkt damit auch den Wettbewerb.

III.

Meine Damen und Herren,
ich habe Ihnen nun eine ganze Reihe von Vorteilen der künftigen Verordnung geschildert. Zum Abschluss möchte ich Ihnen auch unsere Enttäuschungen nicht vorenthalten.

Wenn Sie mit 27 anderen Mitgliedstaaten verhandeln, sind Kompromisse unvermeidlich, und manchmal kommen sie in einer großen Gruppe auch langsamer voran, als es ihnen lieb ist. Wir hätten uns an einigen Stellen etwas mehr Mut zu zukunftsweisenden Ansätzen des Datenschutzes gewünscht. Hier nur zwei Beispiele dafür:

Das erste betrifft die Prinzipien des Datenschutzes durch Technik („privacy by design“) und der datenschutzfreundlichen Voreinstellungen („privacy by default“). Die Technik soll helfen und sicherstellen, dass das Gesetz eingehalten wird; eigentlich eine Selbstverständlichkeit. Es ist ein Fortschritt, dass diese Prinzipien das erste Mal auf europäischer Ebene gesetzlich festgeschrieben werden. Auf mehr digitale Selbstbestimmung des Betroffenen zielen die Regelungen aber leider nicht.

Wir wären hier gerne noch etwas ambitionierter gewesen. So sollten aus unserer Sicht, zum Beispiel auch die Hersteller von Hard- und Software in die Pflicht genommen werden, datenschutzrechtliche Prinzipien bereits bei der Entwicklung zu berücksichtigen. Das wäre ein zukunftsweisender Ansatz, gerade wenn Alltagsgegenstände immer weiter vernetzt werden – Autos, Fernseher, Kühlschränke usw.

Auf wenig Resonanz in Brüssel ist auch unser Vorschlag zu mehr Pseudonymisierung und Anonymisierung gestoßen. Wir wollten das gar nicht vorschreiben, sondern nur Anreize schaffen, damit mehr Daten als Schutzmaßnahme zugunsten des Betroffenen pseudonymisiert werden. Möglicherweise ist dieses Konzept in anderen Mitgliedstaaten noch nicht so bekannt wie in Deutschland. Aber immerhin sind entsprechende Ansätze in den

Texten von Rat und EP enthalten, so dass dazu voraussichtlich auch etwas in der Verordnung stehen wird.

Meine Damen und Herren,
wenn das Europäische Parlament und der Rat die Datenschutz-Grundverordnung in wenigen Wochen beschließen, wird dies ein großer Erfolg für den Datenschutz sein. Es wird aber auch ein großer Erfolg für Europa sein. Die Materie ist sehr komplex; die Ausgangspositionen der Mitgliedstaaten waren sehr unterschiedlich. Trotzdem werden wir zu einem guten Kompromiss gelangen, daran habe ich wenig Zweifel. Auch wenn es manchmal etwas länger dauert: Europa funktioniert!

Vielen Dank für Ihre Aufmerksamkeit!