Daten und Datenschutz im europäischen Wettbewerb

Vortrag auf der Landesdatenschutzkonferenz

am 15.10.2015

in Mainz

Sehr geehrter Herr Staatssekretär Hoch, vielen Dank für die freundlichen Worte,

sehr geehrte Damen und Herren Abgeordnete des rheinland-pfälzischen Landtags, die Sie sich trotz der aktuellen Haushaltsberatungen die Zeit nehmen,

sehr geehrte Vertreterinnen und Vertreter der Wirtschaft mit Herrn Präsidenten Dr. Braun von der Landesvereinigung der Unternehmerverbände Rheinland-Pfalz an der Spitze und begleitet von den zahlreich erschienenen betrieblichen Datenschutzbeauftragten,

sehr geehrte Vertreterinnen und Vertreter der Verbände und Gewerkschaften,

sehr geehrte Gäste.

Auch ich begrüße Sie sehr herzlich zur ersten rheinland-pfälzischen Landesdatenschutzkonferenz. Die an Sie gerichteten Willkommensworte des Chefs der Staatskanzlei erlauben es mir, direkt zu den Themen des heutigen Tages überzuleiten und diese sind nicht nur hochaktuell, sondern auch von großer gesellschaftlicher, rechtlicher und – dies soll in diesem Kreis besonders betont werden - wirtschaftlicher Bedeutung.

I. Einleitung

Die Digitalisierung durchdringt zunehmend alle Lebens-, Gesellschafts- und Arbeitsbereiche und beeinflusst die Art und Weise, wie wir leben, arbeiten, kommunizieren, uns informieren und beteiligen. Sie verändert Strukturen, Abläufe und Märkte. Digitale Agenden auf europäischer und Bundesebene legen Leitlinien fest um die politische, gesellschaftliche und wirtschaftliche Wettbewerbsfähigkeit zu erhalten. Die Studie „Zukunftspfade Digitales Deutschland 2020“ die der nach Artikel 91c des Grundgesetzes eingerichtete IT-Planungsrat unter Beteiligung von Rheinland-Pfalz erstellt hat, hat drei Grundthemen identifiziert, die gestaltet werden sollen:

- Digitale Infrastruktur,
- Digitale Souveränität,
- Digitale Sicherheit und Datenschutz.

Diese Themen bilden auch den Hintergrund der Diskussionen des heutigen Tages.

Wirtschaft und Gesellschaft stehen im Zuge der Digitalisierung vor ständig neuen Herausforderungen. Nach Lage der Dinge werden die Veränderungen in den kommenden Jahren noch grundlegender und weitreichender sein als bislang. Wie alle großen Entwicklungen birgt auch die Digitalisierung Chancen und Risiken und es kommt darauf an, die einen zu ergreifen und die anderen zu beherrschen. Datenschutz und IT-Sicherheit sind dabei wichtige Voraussetzungen um Vertrauen und Verlässlichkeit in einer digitalisierten Welt zu gewährleisten und sie können Rahmenbedingungen schaffen, um den Herausforderungen angemessen zu begegnen.

Entsprechende Konzepte können sinnvoll und nachhaltig nur im Dialog von Staat und Wirtschaft entwickelt werden. Die heutige Landesdatenschutzkonferenz - die erste ihrer Art in Rheinland-Pfalz – ist ein Forum, auf dem ein solcher Dialog stattfinden soll. Sie hat zwei Themenbereiche zum Gegenstand. Am Vormittag geht es um Reaktionen auf die Erkenntnis, dass die Verwundbarkeit digitaler Infrastrukturen weit über das bisher vermutete Maß hinaus reicht. In der Mittagspause besteht Gelegenheit, diese Verwundbarkeit im Rahmen eines live-hacking zu besichtigen. Ich bin sicher, dass spätestens dann die Brisanz des Themas restlos klar wird. Der Nachmittag ist den Auswirkungen der Novellierung des Datenschutzes durch die Europäische Datenschutzgrundverordnung gewidmet. Die Landesdatenschutzkonferenz greift diese Themen auf, führt beteiligte Akteure zusammen und will einen Beitrag dazu leisten, die rheinland-pfälzische Wirtschaft auf die aktuellen Entwicklungen vorzubereiten. Ich freue mich, dass es gelungen ist, hierzu namhafte Referentinnen und Referenten zu gewinnen.

II. Daten als Wirtschaftsgut

Das ausgehende 20. Jahrhundert hat mit dem Siegeszug des Internet den Grundstein für die Digitalisierung unserer gesamten Lebenswelt gelegt. Neben den traditionellen drei Produktionsfaktoren, dem Boden samt seinen Rohstoffen, dem Kapital sowie der menschlichen Arbeitskraft sind technische und persönliche Daten zum vierten Produktionsfaktor in der Wirtschaft geworden. Und waren im 19. und 20. Jahrhundert noch die fossilen Rohstoffe wie Kohle und später das Erdöl der „Treibstoff" der Wirtschaft, so sind es heute persönliche und sachliche Informationen, deren wirtschaftliches Potenzial wir unter dem Schlagwort „Big Data" in seiner Reichweite gerade erst erkennen.

Gegen die wirtschaftliche Nutzung von Daten bestehen keine grundsätzlichen Einwände. Wer auf der Basis von Daten und Datensammlungen Geschäftsmodelle entwirft und betreibt, übt seine grundgesetzlich geschützten Eigentums- und Berufsfreiheit aus. Wie jedes wirtschaftliche Tätigwerden unterliegt auch die Verarbeitung von Daten allgemeinen Regeln, dies es zu beachten gilt. Das Internet ist kein rechtsfreier Raum, aber auch kein ökonomiefreier Tummelplatz von weltfremden Nerds. Im Gegenteil: Hier wird mindestens ebenso hart um die Verwirklichung von Geschäftsmodellen und um Marktanteile gekämpft wie in der analogen Welt.

Dabei ist zu berücksichtigen, dass die Verarbeitung von personenbezogenen Daten einen engen Bezug zu den Grundrechten hat. Eigentums- und Berufsfreiheit und das Recht auf informationelle Selbstbestimmung sind aber miteinander vereinbar. Jede und jeder Einzelne muss möglichst viel Einfluss auf den Umgang mit seinen Daten nehmen können. Denn die Daten sagen ja etwas über Personen aus, sind von diesen erhoben und unterliegen ihrer Selbstbestimmung.

Aufgabe der Datenschützer ist es, das Grundrecht aller natürlichen Personen, selbst über die Verwendung ihrer persönlichen Informationen zu entscheiden, zu schützen und die Betroffenen, seien es Kunden, Beschäftigten oder Geschäftspartner vor der Verletzung dieses Grundrechts zu bewahren. Im Zeitalter von Big Data stellen personenbezogene Daten aber auch ein besonderes, ein spezifisch „geschütztes Wirtschaftsgut" dar, bei dem die gegenläufigen Interessen immer wieder zu einem Ausgleich gebracht werden müssen.

Angesichts der unzähligen offenen oder verdeckten Datenverarbeitungsprozesse, die in jeder Sekunde ablaufen, ist es allerdings eine Illusion zu meinen, man hätte im Sinne eines „Meine Daten gehören mir" umfassende Herrschaftsmacht über Informationen, die einen selbst betreffen. Andererseits sollte der Datenschutz nicht voreilig abgeschrieben und die Bemühungen um effektive Vorkehrungen zur Sicherung der Privatsphäre eingestellt werden. Die These „Privacy is so eighties, just get over it (Privatsphäre ist eine Sache der 80iger Jahre, vergiss es)" verfängt nicht. Übrigens hat sich die die Urheberin dieser Sottise, Julia Schramm, inzwischen mit

den Worten „Alles unter 30 fällt unter Jugendsünde“ von dieser (post privacy-) Position abgewandt. Mag sein, dass man als Datenschützer gelegentlich die Arbeit eines Sisyphos verrichtet, aber die Herkulesaufgabe der Wahrung personenbezogener Daten in einer digitalisierten Welt bringt auch Erfolgserlebnisse.

Diese Aufgabe kann keiner allein erfüllen, sie trifft alle, die mit Datenverarbeitung befasst sind. Wer Daten als Wirtschaftsgut nutzen möchte, tut gut daran, dies rücksichtsvoll und mit Bedacht zu tun und die gegenläufigen Interessen der Betroffenen von vornherein mit einzubeziehen. Um diese schwierige Aufgabe gut zu erfüllen, stehen den Unternehmen Fachleute zur Seite, die für die komplexe Aufgabe dieses Interessenausgleichs besonders geschult sind.

An erster Stelle möchte ich hier die betrieblichen Datenschutzbeauftragten nennen, die nach dem deutschen Verständnis des Datenschutzes eine gar nicht zu überschätzende Bedeutung haben. Sie sind diejenigen, die nicht nur die Positionen und Forderungen des Datenschutzes kennen, sondern auch die wirtschaftlichen Gegebenheiten und Bedürfnisse des Unternehmens – ihres Unternehmens. Sie sind die Sachverständigen vor Ort und sie begleiten und gestalten die beschriebene komplexe Aufgabe des Interessenausgleichs innerhalb des Betriebes. Sie begleiten die digitalen Geschäftsprozesse und gestalten jeden Tag die Vereinbarkeit von Ökonomie und Datenschutz. Eine zunehmende Rolle spielen externe Datenschutzsachverständige, die etwa über die Auditierung und Zertifizierung des Datenschutzniveaus im Unternehmen einen wichtigen Beitrag leisten können, um das betriebliche Datenschutzniveau zu prüfen, wo erforderlich zu verbessern und nach außen hin belastbar zu dokumentieren. Ich freue mich sehr, dass meine Kollegin Marit Hansen aus Schleswig-Holstein gleich im Anschluss einen Vortrag zu den Vorteilen von Datenschutz- und Sicherheitsaudits halten wird.

III. Datenschutz und Datensicherheit

1. Wirkungen des Datenschutzes im Wettbewerb

Gerade weil es sich beim Wirtschaftsgut „persönliches Datum“ um ein besonders geschütztes Gut handelt, wäre es ein folgenschweres Missverständnis, den Datenschutz als Wettbewerbshindernis zu betrachten. Richtig verstandener und vernünftig umgesetzter Datenschutz ist vielmehr eine Voraussetzung dafür, dass ein fairer Wettbewerb um die besten Geschäftsmodelle überhaupt funktionieren kann. Und das meine ich nicht nur im engen juristischen Sinne, wonach meine Behörde als Datenschutzaufsicht unzulässige Datenverarbeitungen jederzeit unterbinden und sogar sanktionieren kann, also den Wettbewerb mit unrechtmäßigen Geschäftsmodellen verhindern kann. Datenschutz kann einen Wettbewerbsvorteil bringen. Denn im lokalen wie globalen Wettbewerb sind Glaubwürdigkeit und Vertrauen in die Rechtschaffenheit und Verlässlichkeit von Unternehmen und ihren Angeboten entscheidende Faktoren.

Ich muss an dieser Stelle gar keine Beispiele dafür benennen, dass traditionsreiche und hochangesehene Unternehmen innerhalb kürzester Zeit ihre Reputation und ihr Standing verspielen können, wenn sie staatliche Regeln verletzen. Dies gilt im Bereich des Umweltschutzes genauso wie im Bereich des Datenschutzes. Denn dabei geht es nicht nur um „formale“ Verstöße gegen die Pflichten, welche die Gesetze jedem einzelnen Wirtschaftstreibenden auferlegen. Sondern es geht um die Verletzung gewichtiger und grundsätzlich gleichberechtigter Interessen wie demjenigen an der Erhaltung unserer natürlichen Lebensgrundlagen oder eben dem Respekt vor der Selbstbestimmung hinsichtlich unserer persönlichen Daten.

Glaubwürdigkeit und Vertrauen sind daher die Münze, in der der Datenschutz die Investitionen zurückzahlt, die zuvor in ihn getätigt wurden. Der Fall des bekannten deutschen Autounternehmens etwa hat überdeutlich gezeigt, dass Verlässlichkeit und Vertrauenswürdigkeit der eingesetzten Software von grundlegender Bedeutung sein können. Wer seinen betrieblichen Datenschutzbeauftragten nicht nur gut aus- und fortbildet, sondern ihm auch genügend Zeit zur Verfügung stellt, um seine verantwortungsvolle Aufgabe qualifiziert wahrnehmen zu können, leistet einen vernünftigen Beitrag zur Sicherung des guten Rufs seines Unternehmens und sichert das Vertrauen von Kunden und Geschäftspartnern. Und nach innen sind die befriedenden und motivierenden Wirkungen eines funktionierenden Arbeitnehmerdatenschutzes nicht zu verkennen.

2. Datensicherheit

Meine Damen und Herren, Daten leben gefährlich. Das gilt insbesondere, wenn sie auf Reisen gehen. Und Daten reisen viel, schnell und weit. Die Risiken für das Schiff der Daten sind vielfältig. Auf dem Grund des Meeres lauern unersättliche Datenkraken, die zum Beispiel facebook oder google heißen. Die Piraten des 21. Jahrhunderts sind Geheimdienste wie die NSA, die sich auf das Abfangen von Daten spezialisieren, oder aber rein kommerziell ausgerichtete Piraten, die Wirtschaftsspionage betreiben. Die Hoffnung, das Schiff der Daten könnte, wenn es denn alle Gefährdungen auf der Reise überstanden hat, in einen sicheren Hafen einlaufen, hat sich seit der Entscheidung des Europäischen Gerichtshofes zur völligen Unsicherheit des safe harbor zerschlagen. Die Übermittlung von Daten ist also ebenso unsicher wie für die Wirtschaft oftmals unverzichtbar.

Das Jahr 2011 ist als das „Jahr der Hacker“ in die Geschichte eingegangen, weil in diesem Jahr so oft wie nie zuvor erfolgreiche Angriffe auf Anwendungen und IT-Strukturen von Unternehmen und Behörden stattgefunden haben. Und die Reihe der Nachrichten, die uns vor Augen führen, dass in der digitalen Welt Sicherheit nicht nur relativ, sondern ein nur schwer und mühsam erreichbares Ziel ist, hört seitdem nicht auf. Unabhängig von der Frage geheimdienstlicher Zugriffe sind Meldungen über spektakuläre Hackerangriffe Routine geworden. Der Angriff auf den Deutschen Bundestag ist nur die Spitze des Eisbergs.

Aus Angst vor Reputationsverlust wagt kaum ein Unternehmen öffentlich über Sicherheitsprobleme zu sprechen. Eine Untersuchung des Branchenverbandes BITKOM hat ergeben, dass nahezu jedes dritte Unternehmen in Deutschland in den vergangenen zwei Jahren Angriffe auf seine IT-Systeme verzeichnet hat. Nach Auskunft der betroffenen Unternehmen ist dies in 58 Prozent der Fälle vor Ort erfolgt, 30 Prozent der Unternehmen berichten über Angriffe über das Internet.

Ganz gleich, welche Motivation im Einzelfall hinter Angriffen steckt: das angegriffene Unternehmen erleidet regelmäßig einen Schaden, der letztlich erhebliche materielle Auswirkungen hat. Auch ein bloßer Imageschaden kann existenzielle Auswirkungen haben.

Derartige Attacken bedrohen aber nicht nur große Unternehmen. Der Mittelstand kann nicht sicher sein, unter dem Radar krimineller Angreifer zu bleiben. Obwohl Sicherheitsfragen als wichtig wahrgenommen werden, zögern nach einer Untersuchung der Initiative „Deutschland sicher im Netz“ die mittelständischen Unternehmen bei der praktischen Umsetzung. Das Sicherheitsbewusstsein hält mit dem Digitalisierungszuwachs nicht Schritt. Mangelnde Kenntnisse, Defizite in der Organisation und Überforderung spielen dabei eine wesentliche Rolle.

Die Vorkehrungen im Bereich des Datenschutzes und des IT-Sicherheitsmanagements weisen nach dem Sicherheitsmonitor für den Mittelstand im Vergleich zu 2011 die geringsten Zuwächse auf. Immer noch gibt ein Drittel der Unternehmen an, keinerlei organisatorische Maßnahmen festgelegt zu haben. In nahezu jedem vierten Unternehmen können weiterhin alle Mitarbeiter auf sämtliche Daten zugreifen.

Obwohl 97 % der Unternehmen E-Mail als Mittel zur Kommunikation mit Geschäftspartnern und Kunden einsetzen, verzichtet die Hälfte dabei auf jegliche Absicherung und offenbart damit ein Paradoxon: Trotz Kenntnis der Risiken und Sensibilität im Umgang mit vertraulichen oder personenbezogenen Daten bleiben praktische Sicherheitsmaßnahmen häufig aus. E-Mail ist hier nur ein Beispiel. Im zunehmend bedeutsamen Bereich des Cloud Computing ist die Auseinandersetzung mit Sicherheits- und Vertraulichkeitsaspekten ebenfalls nur wenig ausgeprägt. 70 % der Unternehmen, die sich in der Cloud befinden oder mit ihr arbeiten, kennen die bestehenden Sicherheitsanforderungen und rechtlichen Rahmenbedingungen nur teilweise oder gar nicht. Nur in einem Drittel der Unternehmen existiert ein von der Geschäftsleitung getragenes IT-Sicherheitskonzept.

Nach Angaben des Branchenverbandes BITKOM sehen 57 % der Unternehmen Angriffe auf IT-Systeme, etwa von Hackern, Kriminellen oder ausländischen Geheimdiensten als reale Gefahr an, weniger als die Hälfte hat jedoch einen Notfallplan für IT-Sicherheitsvorfälle. Lediglich 24 % der mittelständischen Unternehmen verfügen über eine Sicherheitsstrategie, um sich gegen Angriffe zu schützen. Eine mögliche Erklärung könnte darin liegen, dass kleinere Unternehmen

nicht über das nötige Problembewusstsein verfügen, aber auch, dass sie mit der Technik überfordert sind und Risiken verdrängen oder schlicht die Kosten scheuen.

Die Einbindung von Produzenten, Lieferanten, Geschäftspartnern, Dienstleistern, Konzernunternehmen oder Kunden in Konstruktions- oder Produktionssysteme muss daher mit Sicherheits- und Datenschutzkonzepten abgesichert werden, um Risiken angemessen begegnen zu können und Datenabflüsse zu vermeiden. Der Schutz der IT-Infrastruktur und der Kommunikation müssen als unternehmenskritische Faktoren gesehen werden, deren mangelnde Berücksichtigung Risiken für den Bestand eines Unternehmens oder seine Position im Markt bergen. Neben der Sensibilisierung und Aufklärung der Unternehmensleitungen und Beschäftigten braucht es Sicherheits- und Datenschutzkonzepte. Diese zeigen aber nur dann Wirkung, wenn Datenschutz und IT-Sicherheit als wesentliche Unternehmensziele von der Unternehmensleitung vorgegeben werden. So haben die Telekom und die Deutsche Bahn seinerzeit nach Ihren Datenschutzskandalen Vorstandsressorts für Datenschutz und Compliance geschaffen. Für den Mittelstand bieten sich spezifische Lösungen an, um Datenschutz und IT-Sicherheit auch zu leben.

Vor dem Hintergrund globalisierter Märkte und sich verändernder weltpolitischer Konstellationen hat die Bedeutung von Wirtschaftsspionage on den letzten Jahren stetig zugenommen. Mit einer fortschreitenden Digitalisierung der Wirtschaft rücken zunehmend Angriffe auf IT-Strukturen durch staatliche Stellen, Wettbewerber oder Kriminelle in den Fokus. Informationen über Wettbewerber und Märkte, Technologien, Kunden und aktuelles Know-how zur Produktentwicklung und Produktionstechnik wecken vielfältige Begehrlichkeiten. Medienberichte gehen davon aus, dass auch westliche Staaten derartige Wirtschaftsspionage betreiben. Valide Belege für eine systematische Wirtschaftsspionage westlicher Dienste liegen bisher nicht vor, Vorfälle in der Vergangenheit und geleakte Unterlagen deuten darauf hin, dass überall in der Welt und auch in Deutschland Informationen erhoben werden, die ökonomische Vorteile bringen.

Dies gilt auch für Rheinland-Pfalz. Die rheinland-pfälzische Wirtschaft weist eine ähnliche Struktur auf, wie die Wirtschaft in Deutschland insgesamt: Der Anteil des produzierenden Gewerbes an der Bruttowertschöpfung beträgt rund 31 %, der des Dienstleistungsbereichs ca. 68 %. Chemie, Fahrzeugbau und Maschinenbau – Felder in denen technologische Kompetenz und Know-How von essentieller Bedeutung sind, sind dabei die wichtigsten Industriebereiche. Mit einer Exportquote von über 50 Prozent im verarbeitenden Gewerbe weckt gerade Rheinland-Pfalz hier Begehrlichkeiten.

Im Kern geht es um die Vertrauenswürdigkeit, Verlässlichkeit und Sicherheit der unternehmerischen Prozesse und der eingesetzten Informationstechnik. Wichtige Bausteine zur Sicherung eines hohen Datenschutz- und Sicherheitsniveaus sind hierbei Auditierung und Zertifizierung. Es geht um die Prüfung der vorhandenen Strukturen und Prozesse anhand vorgegebener Kriterien und um die dokumentierte Bestätigung darüber, diese erfüllt zu haben. Im Grunde handelt es sich um bewährte

Mechanismen, die für Unternehmen nicht neu sind. Vergleichbare Instrumente gibt es schon länger im Bereich des Qualitäts- und Energiemanagements oder der Umweltverträglichkeit. Sinnvoll ist dies aber auch für das IT-Sicherheitsmanagement eines Unternehmens. Daher greift auch das im Juni dieses Jahres verabschiedete IT-Sicherheitsgesetz solche Mechanismen auf. Sie schaffen Transparenz, Vertrauen und Sicherheit. Innerhalb des Unternehmens und gegenüber Kunden und Geschäftspartnern. Und auch - diesen Hinweis werden Sie mir erlauben – gegenüber Aufsichtsbehörden.

IV. EU Datenschutzreform

Meine Damen und Herren, grundstürzende Umwälzungen des Datenschutzes kommen aus Europa – und zwar überwiegend hin zum Besseren.

Wie sehr Europa den Datenschutz beeinflusst bzw. wie eng Datenschutzfragen mit wirtschaftlichen Fragen verknüpft sind, zeigt sich einmal mehr am aktuellen Urteil des Europäischen Gerichtshofs zur Frage der Übermittlung von Daten in die USA. Mit seinem Urteil hat der EuGH die Übermittlung von Daten in die USA unter das Regime der Grundrechte gestellt und klare Maßstäbe benannt, anhand derer die Datenschutzaufsichtsbehörden Datentransfers in die USA prüfen können. Der EuGH hält Regelungen über einen generellen Zugriff von Sicherheitsbehörden auf personenbezogene Daten für mit dem Grundrecht auf Privatheit nicht vereinbar und sieht darin den Wesensgehalt des Grundrechts verletzt. Auch wenn er dies nicht auf die USA bezieht, ist doch aufgrund einer Reihe von anderen Gründen die Entscheidung aus dem Jahr 2000, die eine generelle Zulässigkeit der Datenübermittlung bei gleichzeitig mangelnder Kontrolle ermöglicht, ungültig.

Die Entscheidung hat sehr konkrete Folgen für die Unternehmen in Deutschland insgesamt und auch in Rheinland-Pfalz. Formal hat der EuGH zwar nur ein Urteil zu Facebook getroffen, die Entscheidungsgründe treffen jedoch eine Vielzahl von Unternehmen, die Daten in die USA übermitteln. Jeder Betrieb, der Dienstleister wie etwa Cloud-Anbieter aus den USA nutzt, der einen Mutter- oder Tochterkonzern mit Sitz in den USA hat oder dort Leistungen anbietet, muss prüfen, ob diese Datentransfers auch zukünftig zulässig sind. Denn ein Großteil der Unternehmen hat sich dabei auf die Safe-Harbor Entscheidung der EU-Kommission verlassen und steht jetzt vor der schwierigen Frage, ob und wie er weiterhin mit Partnerbetrieben in den USA zusammenarbeiten kann. Gravierende Umstellungen bei den Unternehmen könnten dabei nicht ausgeschlossen werden.

Die Datenschutzreform der EU wird den Datenschutz in Europa vereinheitlichen und grundlegend neu gestalten. Dies wird allerdings erhebliche Anforderungen an uns alle stellen, an den Gesetzgeber und die Verwaltung, an die Datenschutzbehörden, aber auch an jedes einzelne Wirtschaftsunternehmen. Ein wesentlicher Schwerpunkt der Tätigkeit der Aufsichtsbehörden wird damit auch nach Inkrafttreten der

Grundverordnung die Beratung der Wirtschaftsunternehmen sowie der Bürgerinnen und Bürger sein.

Eine einheitliche Regelung des Datenschutzes in der Europäischen Union schafft eine einheitliche und verlässliche Grundlage für grenzüberschreitende wirtschaftliche Tätigkeit. Dies ist eines der wesentlichen Ziele der Reform. Gleichzeitig wird die Europäische Datenschutzgrundverordnung eine Reform des Datenschutzes insgesamt mit sich bringen. Vieles, worauf sich die Datenschützer in Deutschland bisher verständigt haben, wird auf den Prüfstand gestellt werden. Dies gilt auch für Ausstattung und Ausrichtung der Datenschutzbehörden. Änderungen und Neuregelungen sind unausweichlich. Der Datenschutz wird europäischer, einheitlicher und gleichzeitig schlagkräftiger werden.

Bei den Verhandlungen in Brüssel konnte sich Deutschland nicht mit all seinen Vorstellungen durchsetzen, das kann in einer Union von 28 Mitgliedstaaten auch nicht anders sein. So wird es etwa einen verpflichtend zu bestellenden betrieblichen Datenschutzbeauftragten europaweit wohl nicht geben. Auch wenn vieles dafür spricht, dass wir jedenfalls in Deutschland mit dem Erfolgsmodell „betrieblicher Datenschutzbeauftragter“ weiterarbeiten können, so werden doch einige Rahmenbedingungen geändert werden. Wo bislang der innerbetriebliche Datenschutzbeauftragte Risiken abgeschätzt, interne Prüfungen vorgenommen und Vorschläge unterbreitet hat, wird dies zukünftig in die Verantwortung der Datenschutzaufsichtsbehörde fallen. Ich bin zuversichtlich, dass im Jahre 2018, also beim voraussichtlichen Inkrafttreten der Datenschutzgrundverordnung, meine Behörde so ausgestattet sein wird, dass wir diesen neuen und essentiellen Herausforderungen auch gewachsen sein werden.

Gleichzeitig werden sich auf europäischer Grundlage die Sanktionsmöglichkeiten bei Datenschutzverstößen wesentlich erweitern. Dies hat Auswirkungen auf den Wettbewerb, da alle in der Europäischen Union ansässigen Unternehmen die gleichen Mindestanforderungen erfüllen müssen. So kann das europäische Datenschutzrecht den fairen Wettbewerb unterstützen.

V. Schluss

Meine Damen und Herren,

zum Schluss bleibt festzuhalten: Die Herausforderungen sind vielfältig und das Themenspektrum ist weit. Die Landesdatenschutzkonferenz greift eine Reihe der aktuellen und relevanten Themen auf und will einen Beitrag dazu leisten, die rheinland-pfälzische Wirtschaft verlässlich und innovativ auf aktuelle Entwicklungen vorzubereiten. Darin liegt ein Schritt auf einem Weg zur Behauptung in der digitalen Wirtschaftswelt, den meine Behörde und ich gemeinsam mit Ihnen gehen wollen.

Die Gewährleistung von Transparenz und Vertrauen von Bürgern und Unternehmen ist eine der wesentlichen Leitlinien meiner Arbeit als Landesdatenschutzbeauftragter. Wenn es zum Schutz der Freiheit erforderlich sein sollte, Maßnahmen zu ergreifen, werde ich es an Entschlossenheit nicht fehlen lassen. Im europäischen Kontext erfordert die Sicherung der Freiheitssphäre dabei zuallererst Kooperation. Und eine konstruktive Zusammenarbeit von Behörden und Unternehmen ist auch die Grundlage dafür, dass unterschiedliche Interessen in Ausgleich gebracht werden können und der Datenschutz im Wettbewerb eine gute und ausgewogene Rolle spielt.

Ich bedanke mich für Ihre Aufmerksamkeit!