Der Bundesbeauftragte
für den Datenschutz und
die Informationsfreiheit

Vortrag

des Bundesbeauftragten für den Datenschutz und die Informationsfreiheit

Ulrich Kelber

„Datenschutz – Anforderungen und Kontrollmöglichkeiten“

Rotary Club Bonn-Siebengebirge

Bonn, 17.06.2019
Maritim Hotel Königswinter
19.00 Uhr bis 21.00 Uhr
Redezeit: 20 Minuten

Es gilt das gesprochene Wort

Sehr geehrter Herr Jacobi (Präsident),

Sehr geehrter Herr Dr. Ebert (Organisator),

I. Einleitende Worte

1. Bindung des BfDI an die Region Bonn

Ich freue mich sehr, als (fast) neuer Bundesdatenschutzbeauftragter hier in diesem schönen Rahmen ein paar Worte sagen zu dürfen.

Der Datenschutz und die zuständige Bundesbehörde des Beauftragten sind seit nunmehr über 40 Jahren eng mit Stadt und Region verbunden.

Der erste Bundesbeauftragte, Herr Prof. Bull, – damals noch ausschließlich für den Datenschutz zuständig – nahm seinen Sitz im Jahre 1978 hier in Bonn.

Ich bin froh, dass die Frage des Standorts meiner Behörde vom Parlament im Bundesdatenschutzgesetz geklärt wurde:

Der Standort des BfDI ist und bleibt Bonn.

Als früherer direkt gewählter Abgeordneter für die Region bin ich über diese Entscheidung besonders glücklich. (**an dieser Stelle evt. ein paar persönliche Anmerkungen zu Bonn als Bundesstadt).**

Seit dem 1. Januar 2016 ist meine Behörde eine unabhängige oberste Bundesbehörde.

Bis dahin war die Dienststelle beim Bundesministerium des Innern eingerichtet. Sie gehörte nicht zum nachgeordneten Geschäftsbereich des BMI. Dennoch konnte die verwaltungsorganisatorische Anbindung trotz ihrer Sonderstellung nicht zufriedenstellen. Immerhin bestand eine Dienstaufsicht des Bundesministeriums des Innern. Hinzu kam – für die Praxis wesentlich bedeutsamer – dass die Personalauswahl federführend vom BMI wahrgenommen wurde. Das hat sich mit der Unabhängigkeit komplett geändert und das ist auch gut so!

Seit dem 1. Januar 2016 untersteht der Bundesbeauftragte keiner Aufsicht mehr.

Ich bin jetzt seit dem 7. Januar 2019 im Amt und bei der Ausübung dieser Tätigkeit eines Amtes als Bundesbeauftragter für den Datenschutz und die **Informationsfreiheit völlig unabhängig.**

2. Bonn als IT-Hotspot

Bonn, das ist viel mehr als die jetzige Bundesstadt und der gesetzlich festgeschriebene Sitz des Bundesbeauftragten für den Datenschutz und die Informationsfreiheit.

Bonn ist IT-Hotspot in Deutschland.

Bonn hat große Unternehmen wie Telekom, Post, Postbank und Sicherheitsbehörden wie das BSI. Darüber hinaus gibt es eine rege Forschungslandschaft im IT-Grenzbereich, beispielsweise an der Uni Bonn und der Fraunhofer Gesellschaft. Dieser Schwerpunkt zeigt sich nicht zuletzt im Cyber Security Cluster Bonn. Das Ziel ist die Förderung und

Vernetzung von Wissenschaft, Forschung und Lehre in Wirtschaft und Behörden. Hier ist nicht zuletzt auch die Bundesregierung in der Pflicht, den IT-Standort Bonn mit Nachdruck zu fördern.

3. Rotary: Vernetzung vor der Zeit der sozialen Netzwerke

Was mich an Ihrer national und international tätigen Vereinigung beeindruckt, ist die Verbindung von Vernetzung der Mitglieder und einem ausgereiften ethischen Fundament für ihre Tätigkeit.

Ich habe gelesen, dass bereits seit 1943 Rotary International einige Fragen als Leitlinien im täglichen Leben verwendet.

"Bei allem, was wir denken, sagen oder tun, sollten wir uns fragen:
1. Ist es wahr?
2. Ist es fair für alle Beteiligten?
3. Wird es Freundschaft und guten Willen fördern?
4. Wird es dem Wohl aller Beteiligten dienen?"

Als gelernter Informatiker, langjähriger Abgeordneter des Deutschen Bundestages und jetzt als Bundesdatenschutzbeauftragter frage ich mich, was aus diesen Grundsätze für die ubiquitäre Datenverarbeitung unserer heutigen Zeit, angefangen bei Künstlicher Intelligenz über Big Data bis hin zu den **Sozialen** Netzwerken abgeleitet werden kann oder sollte..

1. Entspricht es der Wahrheit, was in den sozialen Netzwerken Tag für Tag ungeprüft und ungefiltert verbreitet wird und wenn nein, was tun wir dagegen?

2. Was hat es mit Fairness zu tun, Menschen mit Fakes, manipulierten Bildern und glatten Lügen öffentlich in Misskredit zu bringen, bloßzustellen und ihnen nicht einmal die Chance zu lassen, sich dagegen zu wehren?

3. Schaffe ich über „Freunde“ bei Facebook wirklich die belastbaren und auch stabilen persönlichen Bindungen, auf die ich angewiesen bin, wenn ich einmal wirklich in Not bin und Zuwendung brauche?

4. Dient die Macht von Menschen über Menschen mit automatisierter Profilbildung und der Zerlegung der Persönlichkeit mit Hilfe von Algorithmen wirklich dem allgemeinen Wohl, ober doch nur den Partikular- und Wirtschaftsinteressen einiger weniger.

Wir erleben gerade in China, was der Staat mit den modernen Methoden des Profiling mit seinen Bürgerinnen und Bürgern anstellt, wenn er sie nach politischer Willfährigkeit durchsortiert. **Vor 30 Jahren setzte die Partei- und Staatsführung Panzer gegen demonstrierende Studenten ein – heute durchleuchtet sie ihr ganzes Volk. Die Methoden sind andere, der antidemokratische Geist einer autoritären Obrigkeit ist der gleiche.**

II. Neue Rechtsgrundlage für den Datenschutz in der EU

1. Neues europäisches Datenschutzrecht als Chance

Anders als in China steht der Datenschutz in Deutschland und in der EU auf einem festen Fundament. Nach Artikel 8 Absatz 1 der Charta der Grundrechte der Europäischen Union sowie Artikel 16 Absatz 1 des Vertrags über die Arbeitsweise der Europäischen Union hat jede Person das Recht auf Schutz der sie betreffenden personenbezogenen Daten.

Das europäische Datenschutzrecht macht erfreulicherweise deutlicher denn je, dass Datenschutz ein Grund- und Freiheitsrecht ist und das Persönlichkeitsrecht des Menschen im Mittelpunkt steht.

2. Folgende Vorgaben setzt die Grundverordnung um

Die Grundverordnung ist die **datenschutzrechtliche Zeitenwende.** Sie ist von dem Anspruch geleitet, die Menschen vor einer Verletzung ihrer Privatsphäre zu schützen.

Ihr zentrales Element ist der Schutz der informationellen Selbstbestimmung auf der Grundlage EU-weit einheitlich geltender Regelungen. Ein Schutz der stets wichtig ist, ganz gleich ob in der realen oder in der digitalen Welt, die ohnehin zunehmend miteinander verschmelzen.

Datenschutz darf allerdings nicht in Elfenbeintürmen der Wissenschaft und den Besprechungszimmern von Politik und Konzernspitzen austrocknen. Er muss vielmehr für den Alltag sowohl der Verantwortlichen wie der Betroffenen praktikable Lösungen bieten.

Er muss auch im Alltag ankommen:

- bei den Bürgerinnen und Bürgern
- in der Wirtschaft
- in den Verwaltungen
- sowie bei Vereinen und anderen Organisationen

Drei Fragen müssen wir dabei stellen:

- Hat die DSGVO die Erwartungen gefüllt?
- Wer kontrolliert die Umsetzung des neuen Rechts in der Praxis?
- Welchen künftigen Anforderungen muss der Datenschutz mit der DSGVO als Grundnorm erfüllten?

3. Hat die DSGVO die Erwartungen erfüllt?

Die DSGVO wurde nach einer zweijährigen Übergangszeit am 25. Mai des vergangenen Jahres wirksam. Die Verordnung der EU ist unmittelbar geltendes Recht in allen EU-Mitgliedsstaaten. Ebenfalls zum 25. Mai 2018 trat auch das neue Bundesdatenschutzgesetz in Kraft.

Dieses neue Bundesdatenschutzgesetz hat trotz Namensgleichheit mit dem alten Gesetz einen gänzlich anderen rechtlichen Charakter.

Es regelt nur noch die Bereiche, die von der EU-Grundverordnung offen gelassen wurden.

Die vorher gültige Europäische Datenschutz-Richtlinie aus dem Jahre 1995 setzte zwar einen ersten europarechtlichen Rahmen für den Datenschutz. Da es sich seinerzeit – anders als bei der DSGVO – um eine Richtlinie handelte, musste sie von den Mitgliedstaaten jeweils in ihr nationales Recht umgesetzt werden. Der von der Richtlinie vorgegebene Rahmen wurde aber von den einzeln en Mitgliedsstaaten sehr unterschiedlich ausgefüllt. Das hat sich nun grundlegend geändert.

Maßgeblich ist immer die Grundverordnung. Sie ist das Mutterschiff des deutschen und europäischen Datenschutzes. Die übrigen Schlauchboote folgen dann im Geleitzug. Ich warne an dieser Stelle mit Nachdruck vor jeder national gefärbten Romantik.

Datenschutz beswchränkt auf das eigene Land: das funktioniert längst nicht mehr.

Öffentlichkeit, Regierungen und Parlamenten müssen immer daran erinnert werden, dass erst auf der Grundlage der **europäischen** DSGVO die Betroffenen:

- mehr Kontrolle
- und Transparenz bei der Datenverarbeitung erlangt haben,

und wie wichtig dies gerade im digitalen Zeitalter ist.

Die DSGVO gibt den Menschen erheblich mehr Rechte als bisher:

- Datenportabilität
- Vergessenwerden,
- erweiterte Widerspruchsrechte,
- erweiterte Informationspflichten der Unternehmen
- oder erweiterte Auskunftsansprüche

sind hierfür besonders prägnante Beispiele.

Über die Einhaltung der neuen Regelungen in Deutschland wachen die Datenschutz-Aufsichtsbehörden des Bundes und der Länder.

Ein weiterer nicht zu unterschätzender Vorteil der DSGVO entsteht für Bürgerinnen und Bürger sowie für Unternehmen, die in mehreren Mitgliedstaaten der EU tätig sind, durch den so genannten One-Stop-Shop. Nach diesem Prinzip haben sie es bei den Aufsichtsbehörden jeweils nur noch mit einem Ansprechpartner zu tun. Ein zugegeben ziemlich komplexer und noch nicht zufriedenstellend funktionierender Kooperationsmechanismus sorgt dann im Hintergrund dafür, dass sich die involvierten Aufsichtsbehörden in der EU abstimmen und zu einheitlichen und verbindlichen Entscheidungen kommen.

Der Fall einer grenzüberschreitenden Verarbeitung ist übrigens auch bei einem Mittelständler durchaus schnell erreicht: Hierfür genügt es schon, dass ein Unternehmen sowohl auf dem deutschen als auch auf dem österreichischen Markt tätig ist.

4. Holpriger Start der DSGVO: Viel Lärm und Missverständnisse

Ich habe bei aller Freude über das neue Datenschutzrecht aber auch Verständnis dafür, dass eine so grundlegende Reform Unsicherheiten, ja auch Ängste, auslöst. Das kennen Sie sicher aus Ihrem beruflichen Alltag. Wird ein neues Computerprogramm im Betrieb eingeführt oder sogar die gesamte Datenverarbeitung neu strukturiert, herrscht am Anfang immer etwas Chaos.

Wenn dann – nach und nach – alle Beteiligten mit den Neuerungen vertraut sind, wächst langsam die allgemeine Einsicht in die Notwendigkeit, sich von den alten Schätzchen zu trennen und sich für Neues zu öffnen.

Der schwierige Start der DSGVO lag aber nicht nur an dieser bei jeder großen Reform üblichen Unsicherheit. Er war auch verursacht durch Übermaß an gezielt verbreiteter Beunruhigung.

Der Berufsverband der Datenschutzbeauftragten brachte das mit der Formulierung auf den Punkt **„Heiß gekochte Berater helfen nicht“.**

So wurden im Vorfeld eine Abmahnwelle und die massenweise Verhängung von Bußgeldern auch gegen kleine und mittlere Unternehmen sowie Vereine und Verbände befürchtet. Diese Besorgnisse haben sich als unbegründet herausgestellt.

Als ich im Mai den 27. Datenschutzbericht meiner Behörde dem Präsidenten des Deutschen Bundestages überreichen durfte, konnte ich ge-

rade einmal über 5 Beschwerden über solche Abmahnungen berichten, die bis dahin in meiner Behörde eingegangen sind.

5. DSGVO: ein internationales Muster „made in Europe“

An der DSGVO **orientieren sich mittlerweile auch andere Staaten, die nicht der EU angehören.**

Die Entwicklungen in Japan, aber auch das hohe Interesse weiterer Staaten in Lateinamerika und Asien belegen dies eindrucksvoll.

Erfreulich ist besonders die Entwicklung des Datenschutzes im Bundesstaat Kalifornien. Kalifornien ist der Sitz zahlreicher Technologiekonzerne und hat daher eine wichtige Pilotfunktion.

Dort wurde als **Reaktion auf den Facebook-Skandal nach dem Vorbild der DSGVO der "California Consumer Privacy Act" verabschiedet.** Unternehmen müssen dann ab dem 1. Januar 2020 offenlegen, welche Kunden- und Nutzerdaten sie speichern. Die Nutzer wiederum erhalten das Recht, die Verwendung ihrer persönlichen Daten zu kommerziellen Zwecken zu unterbinden.

In den USA steht Kalifornien nicht allein. Im US-Kongress liegen Pläne vor, den Datenschutz auch auf Bundesebene zu verbessern.

Sogar der Chef von Facebook, Mark Zuckerberg, musste gegenüber dem US-Kongress und dem Europäischen Parlament die DSGVO als Vorbild loben. Wie echt das ist, steht auf einem anderen Blatt. Aber dem

alten datenschutzrechtlichen Flickenteppich in Europa hätte er mit Sicherheit nicht seine Referenz erwiesen.

6. Kartellbehörden unterstützen den Datenschutz

Der Datenschutz steht in seiner Auseinandersetzung mit den Internetkonzernen nicht allein.

Zuversichtlich stimmt mich die Arbeit der Kartellbehörden. Das gilt für die nationale Ebene ebenso wir für die EU und so wie es aussieht auch für die Kartellbehörden in den USA.

Das Bundeskartellamt hat **Facebook** im Februar dieses Jahres klare Beschränkungen für die Verarbeitung von Nutzerdaten auferlegt. Wird die Entscheidung bestandskräftig, muss Facebook eine Art innere Entflechtung seiner Datenbestände vornehmen.

Nach den – nunmehr verworfenen – Geschäftsbedingungen von Facebook müssen die Nutzerinnen und Nutzer des sozialen Netzwerks hinnehmen, dass Facebook auch außerhalb der Facebook-Seite Daten über den Nutzer im Internet oder auf Smartphone-Apps sammelt und dem Facebook-Nutzerkonto zuordnet. So können sämtliche auf Facebook selbst und seinen konzerneigenen Diensten wie WhatsApp und Instagram sowie den auf Drittwebseiten gesammelten Daten mit dem Facebook-Nutzerkonto zusammengeführt werden.

Das Bundeskartellamt will dieser Praxis nunmehr ein Ende bereiten. Die zum Facebook-Konzern gehörenden Dienste dürfen zwar weiterhin die Daten sammeln. Die Zuordnung dieser Daten zum Nutzerkonto bei Facebook ist aber künftig nur noch mit – freiwilliger! – Einwilligung des Nut-

zers möglich. Wenn diese Einwilligung nicht erteilt wird, müssen die Daten bei den anderen Diensten verbleiben und dürfen nicht kombiniert mit den Facebook-Daten verarbeitet werden.

Zudem ist die Sammlung und Zuordnung von Daten von Drittwebseiten zum Facebook-Nutzerkonto ist nur noch dann zulässig, wenn der Nutzer freiwillig in die Zuordnung zum Facebook-Nutzerkonto einwilligt.

Die Bedeutung des Kartellrechts bei der Kontrolle der Internetkonzerne zeigt auch die **Entscheidung der Europäischen Kommission im Fall Google.**

Der Konzern muss ein Rekord-Bußgeld von 2,42 Milliarden Euro bezahlen. Die EU-Wettbewerbskommissarin wirft dem Unternehmen einen Missbrauch seiner Marktmacht vor, weil er eigene Anzeigen in den Suchergebnissen gegenüber denen der Konkurrenz bevorzugt.

Es handelt es sich hier um das mit Abstand höchste Strafgeld, das je in Europa gegen ein Unternehmen verhängt worden ist.

Wettbewerbskommissarin Margrethe Vestager räumte dem US-Konzern lediglich 90 Tage Zeit ein, seine Verfahrensweise zu ändern. Andernfalls drohte sie dem Google-Mutterkonzern Alphabet weitere Strafen von bis zu fünf Prozent eines Tagesumsatzes an.

III. Wer kontrolliert?

Die neue Rolle der Datenschutz- Aufsichtsbehörden

Eine zentrale Verantwortung für die Umsetzung der Grundverordnung haben die Datenschutz-Aufsichtsbehörden. In Deutschland spiegeln sie anders als in anderen EU-Ländern den föderalen Staatsaufbau wieder. So gibt es neben dem Bundesbeauftragten noch 17 weitere Kontrollbehörden. Bei 16 von ihnen liegt der überwiegende Teil der Kontrolle von Wirtschaftsunternehmen.

Mein Haus ist neben der Aufsicht über die gesamte Bundesverwaltung seit der Liberalisierung des Post- und Telekommunikationsmarktes 1995 auch zuständig für sämtliche Post- und Telekommunikationsunternehmen, soweit diese zur Erbringung ihrer Dienste personenbezogene Daten verarbeiten.

Die Aufsichtsbehörden sind so etwas wie die oberen und unteren Extremitäten: Arme und Beine des neuen europäischen Datenschutzrechts.

Sie sind die Ansprechpartner für Datenverarbeiter und Verbraucher. Sie werden aber auch hin und wieder die Rolle der **Zuchtmeister** zu spielen haben.

Das europäische Recht sorgt dafür, dass den Aufsichtsbehörden dafür auch die passenden Instrumente zur Verfügung stehen.

IV. Perspektiven der DSGVO – auch als Standortvorteil für die Wirtschaft

1. Neue Pflichten und Chancen Daten verarbeitender Stellen

Ich gehe davon aus, dass einige Anwesende aus dieser Runde mit der Grundverordnung in ihrem beruflichen oder privaten Umfeld zu tun haben. Sicher, es gibt bestimmte Verpflichtungen, die auch mal eher gedämpfteFreudeauslösen können.

Neben der Einhaltung der Grundsätze für die Verarbeitung personenbezogener und der Gewährleistung der Betroffenenrechte enthält Kapitel IV der Datenschutz-Grundverordnung einige zentrale Vorschriften für die Pflichten der Daten verarbeitenden Stellen. Die gelten für Behörden und Betriebe gleichermaßen.

Die neuen Regelungen ergeben sich unmittelbar aus der Datenschutz-Grundverordnung.

Ich kann jedoch sogleich auch Entwarnung geben: Diese Pflichten ähneln an vielen Stellen der bisherigen Rechtslage in Deutschland. Sie erfordern allerdings gerade für den Übergang einige Anpassungen, die ich auch ansprechen möchte:

Grundgedanke dieser Pflichten des Verantwortlichen ist folgende Überlegung:

Je wahrscheinlicher das von der Datenverarbeitung ausgehende Risiko ist oder je schwerer es wiegt, desto umfangreicher und höher sind die Pflichten des Verantwortlichen.

Dieser Ansatz nimmt gerade auf die **Belange kleinerer und mittlerer Unternehmen** Rücksicht, die keine risikobehafteten Daten verarbeiten. So sind von der Pflicht zur Führung eines Verarbeitungsverzeichnisses Unternehmen mit weniger als 250 Mitarbeitern befreit, sofern deren Datenverarbeitung kein Risiko für die Rechte und Freiheiten der betroffenen Personen birgt.

Kommt es zu einer Verletzung des Schutzes personenbezogener Daten, entfällt die **Meldepflicht gegenüber der Aufsichtsbehörde**, wenn die Verletzung voraussichtlich nicht zu einem Risiko für die Rechte und Freiheiten der Betroffenen führt. Die Pflicht zur Benachrichtigung der betroffenen Personen über einen Vorfall besteht nur dann, wenn die Verletzung voraussichtlich ein hohes Risiko für die betroffenen Personen zur Folge hat.

Eine **Datenschutz-Folgenabschätzung** ist auch nur dann durchzuführen, wenn die Verarbeitung aufgrund der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung voraussichtlich ein hohes Risiko für die Rechte und Freiheiten natürlicher Personen zur Folge hat. Dann ist sie jedoch ein sehr gut geeignetes methodisches Instrument, um die Belange des Datenschutzes bei der Verarbeitung personenbezogener Daten konkret umzusetzen. Denn sie zwingt Unternehmen und Behörden dazu, sich die Risiken bewusst zu machen und sich zur Minimierung dieser Risiken die geeigneten Maßnahmen zu überlegen. Gelingt diese Ri-

sikobegrenzung dennoch nicht, besteht eine Pflicht zur vorherigen Konsultation der zuständigen Datenschutzaufsichtsbehörde.

Daneben sieht die DSGVO auch noch einige technische und organisatorische Maßnahmen vor. Die einschlägigen Artikel 24, 25 und 32 wollen die Einhaltung der Datenschutz-Grundverordnung sicherzustellen. Das erfordert auch entsprechende Nachweise zur Erfüllung der Rechenschaftspflicht.

Gerade für die Gewährleistung des Datenschutzes durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen (Artikel 25) sowie der Datensicherheit (Artikel 32) spielen technische und organisatorische Maßnahmen – wie die Pseudonymisierung und Verschlüsselung sowie Maßnahmen zur Gewährleistung der Schutzziele der IT-Sicherheit (z. B. Vertraulichkeit, Integrität, Verfügbarkeit) – eine wichtige Rolle.

An dieser Stelle sollte ein entscheidender Vorteil auch für die europäische Digitalwirtschaft liegen: IT-Verfahren und- Produkte „made in Europe“ sollten diejenigen sein, die eine vertrauenswürdige – am Grundsatz des Datenschutzes und der Datensicherheit orientierte – Digitalisierung ermöglichen. Hier wünsche ich mir auch deutlich mehr Unterstützung auf europäischer, aber auch nationaler Ebene, um die Entwicklung solcher Produkte nachhaltig zu fördern.

2. Neue Vorschriften helfen der Wirtschaft

Ich habe eben einige Pflichten für die Datenverarbeiter angesprochen. Ich räume ein, dass die nicht nur Freude hervorrufen, aber die Harmonisierung des europäischen Datenschutzrechts bietet enorme Chancen insbesondere für grenzüberschreitend tätige Unternehmen. Sie sollten

sich von der hohe Abstraktion der Datenschutz-Grundverordnung nicht ins Bockshorn jagen lassen.

Ich bin davon überzeugt, dass die Vorteile der Grundverordnung bereits mittelfristig die gewisse Mehrarbeit am Anfang deutlich überwiegen wird. Die Wirtschaft wird nach Überwindung der ersten Startschwierigkeiten auf den nationalen und internationalen Märkten von fairen Wettbewerbsbedingungen für datenschutzfreundliche Produkte und Dienstleistungen profitieren, da bin ich mir sicher.

Mittlerweile erkennen viele Unternehmen, dass einheitliche Regeln für ganz Europa ihre Position im Wettbewerb stärken. Nicht nur kleine und mittlere Unternehmen sind an das neue Recht gebunden, sondern gerade auch die internationalen Großkonzerne wie **Amazon, Google, Microsoft u.a.** Diese größeren weltweit agierenden **und zugleich teuersten** Unternehmen der Welt haben die zweijährige Übergangszeit vom Inkrafttreten der DSGVO bis zu ihrem „Scharfstellen“ am 25. Mai 2018 intensiv genutzt, um sich entsprechend vorzubereiten.

Die DSGVO gilt in vielen Fällen auch für Datenverarbeitungen, die anderswo stattfinden, beispielsweise in der Schweiz oder den USA. Sie stellt nicht mehr allein auf eine Niederlassung in der EU und auch nicht auf den Ort ab, an dem technisch die Datenverarbeitung erfolgt.

Den Ausschlag ergibt entweder die Niederlassung des Verantwortlichen oder Auftragsverarbeiters in der EU – oder der Aufenthaltsort des Betroffenen in der EU. Denn auch wenn Unternehmen überhaupt keine Niederlassung in der EU haben und „lediglich“ ihre Waren und Dienstleistungen an betroffene Personen in der EU anbieten, müssen sie die

DSGVO beachten. Gleiches gilt, wenn solche Unternehmen mittels Datenverarbeitung das Verhalten von Personen in der EU beobachten, beispielsweise durch Tracking-Mechanismen im Internet.

Auf diese Weise müssen sich drittstaatliche Unternehmen also unter Umständen an höhere Anforderungen halten, als es ihre nationalen Gesetze möglicherweise vorsehen.

Das Ziel des europäischen Gesetzgebers, den Anwendungsbereich der DSGVO möglichst breit zu gestalten, ist damit erfolgreich umgesetzt.

Der Vollständigkeit halber weise ich außerdem darauf hin, dass die DSGVO – ebenso wie das vorherige Recht – auch dadurch weit über die EU hinauswirkt, dass eine Übermittlung personenbezogener Daten in Länder außerhalb der EU bzw. des EWR weiterhin nur dann erlaubt ist, wenn beim Empfänger ein angemessenes Datenschutzniveau besteht. Dieses kann auch nach der DSGVO auf verschiedenen Wegen hergestellt werden.

3. Verhaltensregeln und Zertifizierungen als Wettbewerbsvorteile

Die DSGVO bieten Mechanismen, mit deren Hilfe die Wirtschaft in die Lage versetzt wird, auch durch eigene Initiative zur Konkretisierung der Datenschutz-Grundverordnung beizutragen. Die Instrumente der Verhaltensregeln, so genannte **Codes of Conduct**, und der **Datenschutz-Zertifizierung** werden durch die Datenschutz-Grundverordnung gestärkt. Sie sind wirkungsvolle Instrumente zur Schaffung von mehr Rechtssi-

cherheit. Sie können dazu beitragen, Datenschutz-Konformität nachzuweisen und auf diese Weise Vertrauen zu schaffen, bei allen Beteiligten.

Die Aufsichtsbehörden spielen auch hier eine wichtige Rolle. Sie sind in die Ausarbeitung von Verhaltensregeln und der Zertifizierungskriterien eng einzubinden. Die Aufsichtsbehörden genehmigen Verhaltensregeln und sind in die Akkreditierung von Zertifizierungsstellen eng eingebunden.

Über das Instrument der Verhaltensregeln können Verbände und andere Vereinigungen die Anwendung der notwendigerweise sehr abstrakt gehaltenen DSGVO für spezielle Verarbeitungsbereiche oder Branchen präzisieren und so auch auf die speziellen Bedürfnisse kleinerer und mittlerer Unternehmen Rücksicht nehmen.

Diese Verhaltensregeln werden von der zuständigen nationalen Aufsichtsbehörde – bei grenzüberschreitenden Verhaltensregeln unter Einbeziehung des Europäischen Datenschutzausschusses – genehmigt und veröffentlicht. Keine Sorge: der Europäische Datenschutzausschuss ist keine ferne abgehobene Einrichtung – schließlich habe ich dort einen festen Sitz.

Und wenn sich der Bundesrat irgendwann einmal auf einen Ländervertreter verständig, sind wir sogar zu Zweit.

4. Vorbehalte ernst nehmen / Evaluierung nutzen

Ich verschließe mich nicht manchen Einwänden und Beschwerden gegenüber bestimmten Schwächen der DSGVO. Der europäische Gesetz-

geber war an dieser Stelle vorausschauend genug, einen **Evaluierungsprozess** als Grundlage für ihre Weiterentwicklung in der Verordnung festzuschreiben.

Ich habe – auch öffentlich – darauf aufmerksam gemacht, dass es Punkte gibt, wo beispielsweise der bürokratische Aufwand keinen datenschutzrechtlichen Mehrwert bringt. Es ergibt keinen Sinn, Regelungen zu verteidigen, die nur Arbeit machen und dem Datenschutz nicht von Nutzen sind.

Als Aufsichtsbehörden sind wir in diesem Prozess dabei doppelt gefordert. Zum einem müssen wir auch weiterhin aktiv helfen und Ängste nehmen. Wir arbeiten weiter mit Hochdruck an Hilfestellungen und bemühen uns engagiert um eine pragmatische Rechtsauslegung.

Zum anderen sehe ich es auch als Aufgabe der Aufsichtsbehörden an, zwischen dem europäischen und dem nationalen Gesetzgeber zu vermitteln und an bestimmten Stellen auch Reformbedarf anzuzeigen.

Im Rahmen der in der DSGVO vorgesehenen Evaluierung werden wir konkrete Vorschläge für eine Optimierung des geltenden Rechts vorlegen. Dies gilt gerade für die umfangreichen Nebenpflichten, die ein Verantwortlicher hat, ganz gleich welche Größe er hat. Wo der Aufwand zum Selbstzweck wird, sind Korrekturen angebracht.

Ich denke hier z. B. an

- die Erfüllung der Informationspflichten

- den Umfang der Verpflichtung, ein Verzeichnis der Verarbeitungstätigkeiten zu führen
- und die Voraussetzungen für eine Meldung von Datenschutzverstößen an eine Aufsichtsbehörde

V. Schlussbemerkung:

Ich hoffe, dass ich Ihnen einen kleinen Überblick über die neue Rechtslage des Datenschutzes geben konnte.

Mir ist es wichtig, die vielen Vorteile und Fortschritte herauszustellen. Ich bin aber auch offen für Kritik und Reformvorschläge – immer nach dem Motto:

Das Bessere ist stets Feind des Guten.

Ich danke Ihnen für Ihre Aufmerksamkeit und ich freue mich auf Ihre Diskussionsbeiträge und Anregungen.