ZENTRUM FÜR EUROPÄISCHES WIRTSCHAFTSRECHT

Vorträge und Berichte

Nr. 224

herausgegeben von den Mitgliedern des Zentrums

Ulrich Kelber
Bundesbeauftragter für den Datenschutz
und die Informationsfreiheit

Datenschutz: Europäische Herausforderung – Nationale Umsetzung

Referate im Rahmen der Vortragsreihe
„Rechtsfragen der Europäischen Integration"
Bonn, den 12. Dezember 2019

INHALTSVERZEICHNIS

ausschließlich erhältlich beim Zentrum für Europäisches Wirtschaftsrecht
www.zew.uni-bonn.de
Druck: Rheinische Friedrich-Wilhelms-Universität Bonn

I. Technische Rahmenbedingungen des europäischen Datenschutzrechts

1. Skizzierung technologischer Herausforderungen

Die weltweite Datenmasse wächst wie ein Kuchenteig, der in der Weihnachtsbäckerei dank zu viel Hefe über den Rand der Schüssel quillt. Wie also umgehen mit Big Data, sozialen Netzwerken und insgesamt der üppig wuchernden staatlichen und privaten Datensammelwut? Schätzungsweise geht man davon aus, dass die weltweite Datenmenge von 2010 bis 2020 um das Vierzig- bis Fünfzigfache auf stattliche 40 Zettabyte anwächst. Ein Zettabyte ist eine 1 mit 21 Nullen.

In die analoge Welt übertragen würde das bedeuten, dass auf jeden Erdenbürger Informationen aus drei Millionen Büchern kommen. Selbst die als Bücherfresser bekannten fleißigen Juristen hätte da einiges zu lesen. Aus dieser Datenmasse – Big Data - soll nun nach dem Willen von Politik und Wirtschaft der wertvolle Schatz - Smart Data - gehoben werden.

Mit Ausnahme eines regional-monopolistischen Ölkonzerns sind datengetriebene Unternehmen wie Amazon, Facebook und Google die teuersten und gleichzeitig auch mächtigsten Unternehmen der Welt.

Daten sind das Geschäftsmodell des 21. Jahrhunderts!

Die Nutzerinnen und Nutzer zahlen ihre digitale Freundespflege, ihre Navigation, ihr bequemes Zahlen, ihre leicht zu organisierende Mobilität mit immer umfangreichen Datenprofilen über sie. Die werden dann mit Produktentwicklung und Produktplanung aufeinander abgestimmt, ohne dass die Nutzer das merken oder direkt zur Kasse gebeten werden.

In diesem Zusammenhang fällt mir immer die Fabel von den zwei Schweinen ein, die sich auf dem Bauernhof treffen und unterhalten. Sagt das eine Schwein: „ Uns geht es echt gut. Wir kriegen jeden Tag leckeres Essen gebracht, unser Stall wird regelmäßig ausgemistet und unsere Sulegrube lässt keine Wünsche offen.“ „Ja“ antwortet das andere Schwein, „es ist wirklich ein kleines Stück Paradies!“

Moral von Geschichte? Wenn etwas nichts kostet, ist die Chance groß, dass man selbst das Produkt ist!
Auch wenn sich das Datenschutzbewußtsein in der Bevölkerung insgesamt positiv entwickelt, ist diese Erkenntnis leider immer noch nicht flächendeckend verbreitet.
Ich sehe daher eine wesentliche Aufgabe des Datenschutzes darin, verbraucher- und datenschutzfreundliche Big Data -Anwendungen zu befördern. Mit diesen Produkten lässt sich Wachstum herstellen und zugleich die unbedingt erforderliche Akzeptanz sichern.

2. KI als Parameter für den Stand der Bürgerrechte

Ob es eine Balance zwischen Entwicklung der Technik und dem Schutz der Privatsphäre gibt - oder überhaupt geben kann - möchte ich anhand der Entwicklung der sog. *Künstlichen Intelligenz* mit Ihnen besprechen.
In den nächsten Jahren werden entscheidende Weichenstellungen für die KI getroffen. Und diese werden unsere Zukunft massiv und dauerhaft prägen. Das hat enorme Auswirkungen auf unsere Gesellschaftsordnung und damit natürlich auch auf unsere Rechtsordnung.

Gerade das Beispiel China zeigt, dass eine rein ökonomische Sichtweise viel zu kurz greifen.
China arbeitet mithilfe von umfassender Datenerhebung, Künstlicher Intelligenz und Social-Scoring an einem gigantischen Kontrollsystem aller Bürgerinnen und Bürger sowie von Unternehmen und Zivilgesellschaft.
Hierbei wird das Verhalten jedes einzelnen Bürgers sowohl im Netz als auch im realen Leben genau unter die Lupe genommen und ausgewertet. Wer sich im Sinne des Systems verhält, dem winken Prämien. Wer aber nicht dem Bild eines Musterbürgers entspricht, der muss mit Sanktionen rechnen.
Welche menschenrechtliche Dramatik mit dieser Entwicklung verbunden ist, zeigen aktuelle Berichte über die Uiguren, die mit diesem raffinierten

System technischer Überwachung gepaart mit der altbekannten Brutalität eines Polizeistaats unterdrückt werden.
Das ist eine Entwicklung, die wir alle sicher nicht wollen. Auch nicht in Teilbereichen. Weder vom Staat, noch von privaten Konzernen. Aber: Der Mix aus fernöstlicher staatlicher Überwachung und West-US-amerikanischer privater Ausspitzelung und umgekehrt träufelt sein Gift auch nach Europa.

Deswegen ist es falsch zu glauben, dass diese Gefahren – unter Bezugnahme auf unsere weitgehend gefestigte demokratische Grundordnung –nicht auf unsere Situation übertragbar sind.
Politik und Wirtschaft sehen in der KI zum einen immer noch vornehmlich die wirtschaftlichen Potentiale, die die Menge an nutzbaren, qualitativ hochwertigen Daten im Rahmen von KI-Anwendungen mit sich bringen**.** Zum anderen soll mit KI eine Optimierung von Prozessen in fast allen Lebensbereichen ermöglicht werden.
KI kann uns ganz sicher dabei helfen, einige der größten Herausforderungen unserer Zeit zu bewältigen.

- Ärztinnen und Ärzte können schnellere und genauere Diagnosen stellen und neue Therapien anwenden.
- Mit Hilfe Künstlicher Intelligenz können wir den Einsatz von Ressourcen optimieren.
- Mit der Anwendung Künstlicher Intelligenz lassen sich neue Werkstoffe entwickeln, Prozesse besser steuern und Menschen bei der Arbeit unterstützen.

Als einstmaliger KI-Forscher (wenn auch im bescheidenen Umfang) könnte ich stundenlang über die Chancen sprechen.
Ein anschauliches Beispiel stellt dar, dass mit Hilfe Künstlicher Intelligenz Ludwig van Beethovens unvollendete 10. Sinfonie nun doch noch vollendet wurde. Von der 10. Sinfonie, die der Komponist selbst nicht mehr vollenden konnte, sind nur einige handschriftliche Skizzen und Notizen erhalten.

Ein internationales Team aus Musikwissenschaftlern und Komponisten, arbeitete an dem Projekt. Sie haben einen Algorithmus so optimiert, dass er die vielen fehlenden Passagen Beethoven-gemäß ergänzt hat.
Initiiert wurde das Projekt von der Deutschen Telekom. Die Sinfonie soll demnach am 28. April vom Beethoven-Orchester in Bonn uraufgeführt werden. Für mich als Bonner ist das anlässlich des 250. Geburtstags natürlich eine gute Nachricht.
Ich habe bei der Beschreibung von Anwendungsfällen der KI den Bogen geschlagen vom Negativbeispiel China bis zur Vollendung einer Beethoven-Symphonie.

Der Kontrast beider Beispiele zeigt anschaulich, dass die KI weder gut noch böse ist. "Dem Anwenden muss das Erkennen vorausgehen." Dieser Satz des großen Physikers und Nobelpreisträgers Max Planck hat gerade auch beim Umgang mit Künstlicher Intelligenz nichts an seiner Aktualität verloren.
Soll KI den Menschen Nutzen bringen, müssen wir für jede der unterschiedlichen Anwendungen sicherstellen, dass

- die Persönlichkeitsrechte,
- das Recht auf informationelle Selbstbestimmung
- und die anderen Grundrechte

nicht unter die Räder kommen.

Mir sind diese Überlegungen zur technischen Entwicklung besonders wichtig. Datenschutz ist eben kein „Innovationshemmer", der technologischen und wirtschaftlichen Fortschritt ausbremst und Investoren abschreckt.
Vielmehr plädiere ich für ein vertieftes Verständnis essentiell notwendiger Schutzmechanismen für die Persönlichkeitsrechte. Datenschutz ist Grundrechtsschutz. Ohne diese Maßnahmen wird eine verantwortungsbewusste und gesellschaftlich sinnvolle technologische Weiterentwicklung kaum möglich. Die besondere Verbindung von

wirtschaftlicher Entwicklung, wissenschaftlicher Innovation und gleichzeitiger Wahrung von Persönlichkeitsrechten, kann richtig in die Wege geleitet schon auf kürzere Sicht den entscheidenden Unterschied zu rein datengetriebenen und politisch missbrauchsgefährdeten Geschäftsmodellen ausmachen. Künftige KI-basierte Anwendungen werden ständig neue Herausforderungen mit sich bringen und damit auch entsprechende Regulierungen erfordern.

Dabei müssen wir uns ständig fragen, welche Chancen und Risiken bei der Nutzung von KI-Systemen für uns Menschen bestehen und wie wir die Chancen bestmöglich nutzen und den Risiken adäquat begegnen. Im Bereich der Künstlichen Intelligenz muss es uns gelingen, eigene europäische Lösungen aktiv zu fördern. Voraussetzung hierfür ist eine Technologie der man vertraut.

Als Datenschützer will ich für eine zukunftsorientierte, transparente und faire Technikgestaltung arbeiten, der die Menschen vertrauen können.

3. Schutz der Privatsphäre: Schlüsselbegriff des Europäischen Datenschutzrechts

Das Beispiel der KI hat uns gezeigt: Ob eine Informationstechnik Fluch oder Segen ist, hängt von der Qualität ihrer faktischen und rechtsstaatlichen Gestaltung ab.

Was steht zwischen Dr. Jekyll und Mr. Hyde?

Unter anderem und vor allem auch: Der Datenschutz!

II. Datenschutz als Menschenrecht

In der EU ist der Datenschutz als Bestandteil der Menschenwürde und als unveräußerliches Grundrecht anerkannt. Das Recht auf Privatsphäre und auf ein Privatleben ist:

- in der Allgemeinen Erklärung der Menschenrechte (Artikel 12),
- der Europäischen Menschenrechtskonvention (Artikel 8),

- und der Europäischen Charta der Grundrechte (Artikel 7) verankert.

Privatsphäre und Datenschutz sind auch in den EU-Verträgen verankert**.**

Die Charta enthält ein ausdrückliches Recht auf den Schutz personenbezogener Daten (Artikel 8).

Mit dem Inkrafttreten des Vertrags von Lissabon im Jahr 2009 erhielt die Charta der Grundrechte dieselbe Rechtsverbindlichkeit wie die Verfassungsverträge der EU. Sie ist damit für die EU-Organe und Einrichtungen und die Mitgliedstaaten bindend.

III. Das neue europäische Datenschutzrecht

Seit Jahrzehnten gibt die EU im Datenschutzrecht hohe Standards vor.

Der epochale Sprung von der von der technischen Entwicklung überholten Richtlinie aus dem technologisch so fernen 1995 zu einer europaweit unmittelbar rechtsverbindlichen Datenschutz-Grundverordnung erfolgte dann in 2016.

Mit der DSGVO verabschiedete die EU nach jahrelangem Ringen diesen neuen Rechtsrahmen und die Datenschutzrichtlinie für Polizei und Strafjustiz.

Die DSGVO gilt nach einer Übergangsfrist von zwei Jahren seit dem 25. Mai 2018 in der EU uneingeschränkt.

Sie ist die weltweit die umfassendste und fortschrittlichste Regelung des Datenschutzes. Sie ist auf die aktuellen Herausforderungen des digitalen Zeitalters und einer global vernetzten Wirtschaft zugeschnitten.

Sie gilt auch für Organisationen und Unternehmen ohne Sitz in der EU, wenn sie Waren und Dienstleistungen für Einzelpersonen in der EU anbieten oder deren Verhalten beobachten.

Sie schafft neue Rechte für Einzelpersonen im digitalen Umfeld und mehrere neue und detailliert festgelegte Kooperationsverpflichtungen.

IV. Holpriger Start in eine bessere Datenschutzzukunft

Wenn ich über den Start der DSGVO und ihre Erfolge spreche, muss ich aber auch ansprechen, wie holprig und schwierig diese Anfangsphase war.

Das Internet war voll mit gezielt verbreiteter Verängstigung, aber auch glatten Fehlinformationen. Eine Abmahnwelle wurde heraufbeschworen – ein Tsunami an Kostenbescheiden und Bußgeldern gegen kleine Unternehmen und Vereine zog am dunklen Horizont herauf.

Heute wissen wir: Diese Besorgnisse und Ängste waren unbegründet oder zumindest deutlich überzogen.
Manche Unsicherheiten konnten durch die Aufklärungsarbeit der Aufsichtsbehörden gerade gerückt werden.

Angesichts von noch immer bestehenden Befürchtungen und Vorurteilen möchte ich auch daran erinnern:

Erst auf der Grundlage der DSGVO haben die Betroffenen
mehr Kontrolle und Transparenz bei der Datenverarbeitung erlangt,
und das ist gerade im digitalen Zeitalter von großer Bedeutung.

V. Systematik des Datenschutzrechts und Vorrang der DSGVO

1. Vorfahrt der DSGVO

Die DSGVO geht als europäische Verordnung unmittelbar jedem mitgliedstaatlichen Recht mit gleicher Zielrichtung vor.
Die nationalen Gesetzgeber dürfen keine von der DSGVO widersprechenden Vorschriften erlassen, es gibt aber auch Regelungsoptionen.

Zu den zwingend zu regelnden Vorschriften gehören auch die über meinen eigenen Status (§§ 8 bis 16 BDSG) als Bundesdatenschutzbeauftragter sowie die Regelungen über die Zusammenarbeit der Aufsichtsbehörden in Bund und Ländern.
Einen weiten Regelungsspielraum gem. Art. 6 Abs. 2 und 3 DSGVO haben die Mitgliedstaaten vor allem bei der Verarbeitung personenbezogener Daten im öffentlichen Bereich. Hier ist es den Mitgliedstaaten möglich, die Rechtsgrundlagen für die Verarbeitung zu konkretisieren.
Die Folge dieses Spielraums ist, dass das bereichsspezifische materielle Datenschutzrecht der Mitgliedsstaaten in seiner Substanz im Wesentlichen erhalten bleiben kann.
Und glauben Sie mir: Entgegen des meistens geäußerten Selbstverständnisses als Datenschutz-Paradies hat Deutschland hier keineswegs die datenschutzfreundlichsten Regeln.

2. Neue Rolle des BDSG

Die neue Systematik des Datenschutzrechts weist dem alt-ehrwürdigen Bundesdatenschutzgesetz eine gänzlich neue – untergeordnete – Rolle zu.
Das BDSG - neu - zugleich mit der DSGVO am 25. Mai 2018 in Kraft getreten - ist damit in doppelter Hinsicht nachrangiges Recht:

- Im Verhältnis zur DSGVO gelten seine Regelungen nur dann, soweit die DSGVO nicht unmittelbar gilt (§ 1 Abs. 5 BDSG).

- Wie bisher gilt das BDSG auch dann nicht, wenn der Bund andere Rechtsvorschriften über den Datenschutz bereithält. Diese bereichsspezifischen Datenschutzvorschriften gehen den Vorschriften des BDSG vor.

Böse Zungen sprechen daher beim neuen Bundesdatenschutzgesetz – aus meiner Sicht zu despektierlich – von einer Resterampe.
Auf jeden Fall ist seine Bedeutung gegenüber dem alten BDSG deutlich herabgestuft.

3. Wichtigste inhaltliche Neuregelungen für die Bürgerinnen und Bürger

Lassen sich mich ein paar Stichworte für die Neuregelungen nennen, die m.E. aus Sicht der Bürgerinnen und Bürger wichtig sind.
Der Überblick ist nur skizzenhaft und bei weitem nicht vollständig. Er soll vielmehr nur verdeutlichen, wie umfassend das neue Recht die Stellung der Betroffenen stärkt:

- **Zulässigkeit der Datenverarbeitung nach der DSGVO**

Die zentrale Vorschrift für die Zulässigkeit der Verarbeitung personenbezogener Daten findet sich in Art. 6 DSGVO. Sie enthält sechs verschiedene Tatbestände, bei deren Vorliegen eine Verarbeitung personenbezogener Daten **erlaubt** ist.

- **Informationspflichten**

Nach der DSGVO muss der Verantwortliche geeignete Maßnahmen ergreifen, um der betroffenen Person alle Informationen nach den Artikeln 13 und 14 zu übermitteln. Beispielsweise können hier der Zweck und die Rechtsgrundlage der Datenverarbeitung, Informationen über die Speicherdauer oder die Kontaktinformationen der für die Verarbeitung Verantwortlichen und der Datenschutzbeauftragten genannt werden.

- **Auskunftsrecht**

Art. 15 DSGVO sieht ein Auskunftsrecht für betroffene Personen vor. Ihr ist danach auf Antrag Auskunft zu geben über:

  - die Verarbeitungszwecke
  - die Kategorien personenbezogener Daten, die verarbeitet werden
  - die Empfänger oder Kategorien von Empfängern
    die Dauer der Speicherung; falls nicht möglich die Kriterien für die Festlegung dieser Dauer

- das Bestehen der Rechte betroffener Personen auf Berichtigung, Löschung, Einschränkung der Verarbeitung, auf Widerspruch aufgrund der besonderen Situation einer betroffenen Person
- das Recht auf Beschwerde bei der Aufsichtsbehörde

- **Recht auf Berichtigung**

Nach Art. 16 DSGVO hat die betroffene Person das Recht, von dem Verantwortlichen unverzüglich die Berichtigung sie betreffender unrichtiger personenbezogener Daten oder - unter Berücksichtigung der Zwecke der Verarbeitung - die Vervollständigung unvollständiger personenbezogener Daten zu verlangen. Gegenstand des Berichtigungsrechts sind grundsätzlich Informationen, die objektiv nicht mit der Realität übereinstimmen, z. B. ein falscher Name oder ein falsches Geburtsdatum.

Die Berichtigung unrichtiger personenbezogener Daten muss unverzüglich, das heißt ohne schuldhaftes Zögern, erfolgen.

- **Recht auf Löschung**

Nach Art. 17 Abs. 1 DSGVO hat die betroffene Person unter den in der Vorschrift genannten Voraussetzungen das Recht, von dem Verantwortlichen zu verlangen, dass sie betreffende personenbezogene Daten unverzüglich gelöscht werden.
Löschen bedeutet, dass die personenbezogenen Daten unkenntlich gemacht werden müssen.
Grundsätzlich muss die Löschung auf allen Datenträgern erfolgen.

Neu ist in der DSGVO das „Recht auf Vergessenwerden" nach Art. 17 Abs. 2 DSGVO, auch wenn dies vorher durch Rechtsprechung bereits in Teilbereichen eingeführt war.

Hiernach müssen Verantwortliche bei einem berechtigten Löschverlangen bestmöglich dafür Sorge tragen, dass sie in vertretbaren Rahmen weitere Stellen über die Löschverpflichtung informieren.
So sollen auch Links auf die Daten oder Kopien oder Repliken bei der Löschung berücksichtigt werden. Dies ist insbesondere von Bedeutung bei Suchmaschinenbetreibern, die die Betreiber weiterer Webseiten, auf die sie verlinken, über Ihren Löschwillen informieren müssen.
Aber auch hier gilt: kein Recht ohne Ausnahme.
Das macht des dem Publikum oft schwer – eröffnet Juristinnen und Juristen aber auch ein breites Betätigungsfeld.

- **Automatisierte Einzelfallentscheidung**

Die alte Regelung im früheren § 6a BDSG zu automatisierten Einzelentscheidungen wird durch die DSGVO erweitert.
Nach Art. 22 DSGVO hat die betroffene Person das Recht, nicht einer ausschließlich auf einer automatisierten Verarbeitung - einschließlich Profiling - beruhenden Entscheidung unterworfen zu werden, die ihr gegenüber rechtliche Wirkung entfaltet oder sie in ähnlicher Weise beeinträchtigt.
Das Recht besteht allerdings nicht,

- wenn eine ausdrückliche Einwilligung der betroffenen Person vorliegt
- oder die Entscheidung für den Abschluss oder die Erfüllung eines Vertrags zwischen der betroffenen Person und dem Verantwortlichen erforderlich ist,
- oder wenn sie nach Rechtsvorschriften der Union oder eines Mitgliedstaates zulässig ist und diese Rechtsvorschriften angemessene Maßnahmen zur Wahrung der Betroffenenrechte enthalten.

Diese Regelung ist nach meiner Überzeugung unbefriedigend.
Erst in den letzten Tagen wurden auch aus dem Bereich der Bundesregierung Stimmen lauter, beispielsweise die Profilbildung für Kinder

und Jugendliche zu verbieten. Diese Überlegungen begrüße ich sehr; aber auch der Schutz der sonstigen Verbraucherinnen und Verbraucher muss noch deutlich weiter verbessert werden.
Für die Praxis wäre es sehr wichtig, die Rechte der Verbraucherinnen und Verbraucher an diese Stelle zu stärken.
Was gegenwärtig bei der Scorebildung in der Praxis geschieht, ist in hohem Maße intransparent und kann nicht länger hingenommen werden.
Ich werde mich daher im Rahmen der laufenden Evaluierung der DSGVO für eine Verbesserung der Verbraucherrechte einsetzen.

4. Unabhängigkeit der Aufsichtsbehörden

Ein Kernelement des europäischen Datenschutzrechts ist die Unabhängigkeit der Aufsichtsbehörden.

Schon vor dem Inkrafttreten der DSGVO war in der EU gesetzlich festgelegt, dass Datenschutz- oder Aufsichtsbehörden unabhängig sein müssen.

Einschlägig sind hier die Artikel 16 Absatz 2 des Vertrags über die Arbeitsweise der Europäischen Union (AEUV) und Artikel 8 Absatz 3 der Charta der Grundrechte der EU.

Der Europäische Gerichtshof verlangte schon lange vor der DSGVO, dass die Kontrolle durch eine unabhängige Behörde ein unabdingbarer Bestandteil des Rechts auf Datenschutz ist, Er hat die Kriterien für deren Unabhängigkeit festgelegt.

Dem ist der Europäische Gesetzgeber gefolgt.

Die DSGVO hebt die Bedeutung der Unabhängigkeit hervor und erweitert sie noch gegenüber der früheren Richtlinie aus dem Jahre 1995.

Die Aufsichtsbehörde muss völlig unabhängig handeln, also unabhängig von jedem direkten oder indirekten Einfluss von außen entscheiden können.

Kapitel VI der DSGVO sieht detaillierte Regeln für die Funktionsweise unabhängiger Aufsichtsbehörden vor:

- **Untersuchungs- und Abhilfebefugnisse**

Die DSGVO bietet den Aufsichtsbehörden umfassende Untersuchungs- und Abhilfebefugnisse, um die datenschutzrechtlichen Vorgaben gegebenenfalls durchsetzen zu können. Viele Unternehmen fürchten dabei insbesondere die drohenden Geldbußen.

- **Warnungen**

Aufsichtsbehörden können etwa gegenüber Verantwortlichen und Auftragsverarbeitern Warnungen aussprechen, sofern Datenverarbeitungen beabsichtigt werden, die voraussichtlich einen Verstoß gegen datenschutzrechtliche Bestimmungen darstellen.

- **Anweisungen**

Die Aufsichtsbehörden können den Verantwortlichen und Auftragsverarbeitern im Rahmen eines förmlichen Verwaltungsverfahrens auch anweisen, datenschutzrechtswidrige Datenverarbeitungen einzustellen, oder Pflichten gegenüber Betroffenen nachzukommen.

- **Anordnung der Aussetzung der Übermittlung**

Auch die Aussetzung einer Datenübermittlung kann von den Aufsichtsbehörden angeordnet werden, wenn sich der Empfänger in einem Drittland befindet oder es sich um eine internationale Organisation handelt. Dabei kann die Behörde auch weitere Beschränkungen und Verbote der Datenverarbeitung oder aber auch Berichtigungen oder Löschungen bestimmter Daten sowie eine Einschränkung der jeweiligen Datenverarbeitung anordnen.

- **Empfindliche Bußgelder drohen**

Für die meisten Verantwortlichen und die Öffentlichkeit steht die Frage im Mittelpunkt, wie teuer ein Verstoß gegen die Vorschriften des Datenschutzes wird.
Da hat sich mit der DSGVO viel getan. Geldbußen von bis zu 10.000.000 € oder 20.000.000 € bzw. 2 % oder 4 % des gesamten weltweit erzielten Jahresumsatzes des vorangegangenen Geschäftsjahres sind nicht von Pappe.
Bei der Bemessung von Bußgeldern wird grundsätzlich der Gesamtumsatz der Unternehmensgruppe (Mutter- und Tochtergesellschaften) zu Grunde gelegt.
Darüber hinaus richtet sich die maximale Obergrenze für Bußgelder nach dem jeweils höheren der genannten Beträge.
Für die Bemessung der Geldbußen ist entscheidend, dass diese insbesondere wirksam und verhältnismäßig, aber auch abschreckend ist.
Wie Sie vielleicht mitbekommen haben, haben wir vor wenigen Tagen unsere erste große Geldbuße in Höhe von 9,5 Millionen Euro gegen einen Telekommunikationsanbieter ausgesprochen. Das klingt viel, lag vorliegend aber – unter anderem aufgrund der Einsichtigkeit und guten Kooperation des Unternehmens im Verfahren – im unteren Bereich des möglichen Rahmens. Die Obergrenze hätte hier bei über 73 Millionen Euro gelegen. Sie sehen also, dass wir sehr gründlich dem Gebot des angemessenen Verwaltungshandelns Tribut zollen.
Überhaupt ist es nicht unser Ziel möglichst viele und möglichst hohe Geldbußen zu verhängen. Wir vereinnahmen diese übrigens auch nicht. Eigentlich wollen wir erreichen, dass die von uns beaufsichtigten Stellen durchweg so datenschutzkonform verhalten, dass Geldbußen überhaupt nicht notwendig werden.

Mitwirkungspflicht und weitere Konsequenzen

Sowohl die Verantwortlichen als auch die Auftragsverarbeiter können Mitwirkungspflichten treffen. So können sie angewiesen werden, bestimmte Informationen bereitzustellen.

Die Aufsichtsbehörden sind in der Lage, ihre Anordnungen auch mit Zwangsmitteln, beispielsweise eines Zwangsgeldes, durchzusetzen. Bestehen Zweifel an der Rechtmäßigkeit einer Anordnung, kann eine verwaltungsgerichtliche Klärung herbeigeführt werden.
Wichtig: Bessere Informationen über Risiken
Im Rahmen ihrer Öffentlichkeitsarbeit sollen die Aufsichtsbehörden künftig nach Artikel 57 Abs. 1 lit. b EU-DSGVO z.B. über Risiken der Datenverarbeitung informieren. Ein weites Feld, bei dem wir noch viel zu leisten haben.

5. Europäischer Datenschutzausschuss

Der Europäische Datenschutzausschuss (EDSA) ist eine unabhängige europäische Einrichtung mit eigenem Rechtsstatus. Er befördert die einheitliche Anwendung der Datenschutzvorschriften in der gesamten Europäischen Union. Der EDSA koordiniert die Zusammenarbeit zwischen den EU-Datenschutzbehörden und sorgt dafür, dass die europäischen Datenschutzaufsichtsbehörden mit einer Stimme sprechen.

Es wäre äußerst misslich, wenn die Kontrollpraxis in den EU-Mitgliedsstaaten mal so und mal anders gehandhabt würde.

Der EDSA besteht aus Vertretern der nationalen Datenschutzbehörden und dem Europäischen Datenschutzbeauftragten (EDSB).

Dieses Gremium hat also die wichtige Aufgabe das europäische Datenschutzrecht rechtlich auszulegen und in der Praxis durchzusetzen. Das führt mitunter zu weiteren Herausforderungen, da die hierfür erforderlichen Prozesse in der rechtlichen Theorie zwar durchaus gut klingen, in der Praxis allerdings nicht immer ganz einfach durchzusetzen sind.

Nicht zuletzt aufgrund der in den europäischen Staaten teilweise grundverschiedenen Mentalitäten und des nationalen Verwaltungsrechts

sowie der Rechtskultur. Allerdings lohnt sich die Mühe, denn im Ergebnis werden wir uns nur gemeinsam als ein starkes Europa die internationalen Standards setzen können.

VI. DSGVO als internationales Erfolgsmodell

Die DSGVO gibt den Bürgerinnen und Bürger mehr Rechte in die Hand, als dies früher der Fall war.

Sie installiert ein Kontrollregime, das nicht nur mit erhobenem Zeigefinger „Du Du Du" sagen, sondern auch zufassen kann.

Die DSGVO gilt für die Mitgliedstaaten wie auch für die Europäische Union selbst. Und sie setzt durch das Marktortprinzip auch „Weltrecht".

Erfreulich ist für mich, dass unser neues Datenschutzrecht damit weltweit Maßstäbe gesetzt hat.

Weltweit gibt es immer mehr Rechtsvorschriften zum Datenschutz (in Ländern außerhalb der EU manchmal als „data privacy" bezeichnet).

Über 100 Länder in aller Welt haben inzwischen Datenschutzgesetze eingeführt, weniger als die Hälfte dieser Länder (28 EU-Mitgliedstaaten und andere) befindet sich in Europa. Und viele der neuen Gesetze beziehen sich explizit auf die DSGVO als Vorbild. Insofern kann man hier wirklich von einem Goldstandard sprechen.

Die Mehrzahl der Datenschutzgesetze wurde also außerhalb von Europa verabschiedet, wobei an der öffentlichen Wahrnehmung vorbei gerade in den afrikanischen Ländern die schnellste Entwicklung zu verzeichnen ist.

Wichtig ist auch die Entwicklung in den USA. Kalifornien und New York haben eigene Datenschutzgesetze erlassen und auch auf nationaler Ebene wird ein entsprechender Rechtsakt diskutiert. Gerade weil immer noch ein Großteil der datenbasierenden Technologien von Unternehmen aus den USA

angeboten werden, ist das aus datenschutzrechtlicher Sicht ein äußerst erfreulicher Prozess.

Umso wichtiger, dass wir DSGVO in Europa auch in allen Details durchsetzen.

VII. Exkurs: Anwendungsbereich der JI-Richtlinie

Meine positive Darstellung der Datenschutz-Grundverordnung darf indes nicht unterschlagen, dass sie sich gerade in den Kernbereichen exekutiver Eigenverantwortung der Nationalstaaten schamhaft bedeckt halten muss.

1. DSGVO: im staatlichen Kernbereich gilt sie nicht

Anders als bei der Grundverordnung sieht Rechtslage beim Anwendungsbereich **der JI-Richtlinie 2016/680** aus.
Unter diesen fallen alle öffentlichen Stellen des Bundes, die für die Verhütung, Ermittlung, Aufdeckung, Verfolgung oder Ahndung und Verhütung von Straftaten oder Ordnungswidrigkeiten personenbezogene Daten verarbeiten.
Gleiches gilt für die Vollstreckung von Strafen oder anderer strafrechtlicher Maßnahmen zuständigen Stellen.
Erfasst sind hier beispielsweise das BKA, die Bundespolizei, der Generalbundesanwalt, das Zollkriminalamt oder die Tätigkeit anderer öffentlicher Stellen als Verwaltungsbehörde im Sinne des Ordnungswidrigkeitenrechts.
Da die Richtlinie - anders als die DSGVO - nicht unmittelbar geltendes Recht ist, muss sie erst in nationales Recht umgesetzt werden.
Dies ist bislang immer noch nicht vollständig erfolgt. Zwar finden sich Umsetzungen in den Teilen 1 und 3 des BDSG oder auch im neuen BKA-Gesetz.

Im bereichsspezifischen Datenschutzrecht fehlt allerdings an vielen Stellen noch die nationale Implementierung, z.B. im Bundespolizeigesetz. Ganz praktisch: Europarechtswidrig fehlt mir als Aufsichtsbehörde gegenüber der Bundespolizei die Durchsetzungsmöglichkeit.

2. Öffentliche Stellen außerhalb des EU-Rechts

Für die öffentlichen Stellen, die überhaupt nicht unter das Unionsrecht fallen, auch nicht die JI-Richtlinie, gilt nach wie vor ausschließlich nationales Datenschutzrecht.

Die Nachrichtendienste des Bundes, auch im Bereich Verteidigung, oder besondere Verfassungsorgane wie der parlamentarische Bereich des Deutschen Bundestages bleiben europarechtsfreie Zonen.