Lutz Hasse und Eberhard Zehendner

Die Europäische Datenschutz-Grundverordnung in der Praxis

Am 21. April 2017 sprach Redaktionsmitglied Eberhard Zehendner mit dem Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI),[1] Lutz Hasse, über praktische Konsequenzen der Europäischen Datenschutz-Grundverordnung (DSGVO[2]). Die redaktionellen Anmerkungen wurden im Dezember 2017 bzw. Januar 2018 hinzugefügt.

Zehendner: *Die Europäische Datenschutz-Grundverordnung wurde durch Verkündung unmittelbar anwendbares Recht. Wann hat das stattgefunden?*

Hasse: Die Datenschutz-Grundverordnung wurde am 4. Mai 2016 verkündet[3] und ist dadurch am 25. Mai 2016 in Kraft getreten.[4] Von da ab gemessen haben wir zwei Jahre Zeit, uns darauf einzustellen; denn die Datenschutz-Grundverordnung wird erst Wirkung entfalten ab dem 25. Mai 2018.[5] Dann gilt sie unmittelbar und ersetzt damit auch das geltende Datenschutzrecht.

Welche gesetzlichen Grundlagen in Deutschland fallen damit weg?

Als Erstes das Bundesdatenschutzgesetz[6] – es wird allerdings schon an einem Nachfolgegesetz[7] gearbeitet. Die Landesdatenschutzgesetze stehen auf dem Spiel, man muss sehen, was davon übrig bleibt. Und es gibt spezialgesetzliche Normen, zum Beispiel im Sozialgesetzbuch, im Polizeirecht, in der Strafprozessordnung, die müssen sich auch an der Datenschutz-Grundverordnung ausrichten beziehungsweise an der neuen Datenschutzjustizrichtlinie[8] – das ist sozusagen die kleine Schwester der Datenschutz-Grundverordnung, die bindet die Strafverfolgungsbehörden und wird gerne übersehen.

Aufsichtsbehörden

Wenn das Bundesdatenschutzgesetz außer Kraft sein wird, wo ist dann genau bezeichnet, wer die Rolle der oder des Bundesdatenschutzbeauftragten übernimmt?

Daran wird gerade gearbeitet. Die Datenschutz-Grundverordnung enthält ja zum einen unbestimmte Rechtsbegriffe, sie enthält Beschränkungen des Grundrechts der informationellen Selbstbestimmung, und sie enthält sogenannte Öffnungsklauseln[9]. Wie viele sie enthält, ist ein bisschen strittig zwischen den Datenschutzbeauftragten und sonstigen Stellen, man sagt, so 50 bis 60.[10] Öffnungsklauseln bedeutet, dass der nationale Gesetzgeber eigene Regelungen treffen kann, die natürlich nicht gegen die Datenschutz-Grundverordnung verstoßen dürfen, aber die, so drückt sich die Datenschutz-Grundverordnung aus, spezifischere Regelungen treffen.[11]

Die Datenschutz-Grundverordnung spricht nun von Aufsichtsbehörden, definiert aber nicht genau, was das ist. Der Bundesgesetzgeber wird Regelungen treffen für die Bundesdatenschutzbeauftragte, die wie bisher Aufsichtsbehörde für alle Bundesbehörden sein wird.[12] Und ich nehme an, der Landesgesetzgeber macht dies auch für die Landesdatenschutzbeauftragten. Ich gehe davon aus, dass sich in der Struktur der Aufsichtsbehörden nicht viel ändern wird – wohl aber etwas im Aufgabenbereich. Da ist dann möglicherweise vorgesehen, dass die Bundesdatenschutzbeauftragte einen Kompetenzzuwachs erhalten könnte, beispielsweise bei der Aufsicht über die Finanzbehörden; die Landesfinanzbehörden unterliegen jetzt noch der Aufsicht der Landesdatenschutzbeauftragten, möglicherweise wandert die Kompetenz dort zur Bundesbeauftragten.[13]

Deutsches Gesetzgebungsverfahren

Es klang erst anders aus Berlin, zunächst hieß es, wir sind im Wahlkampfmodus,[14] wir machen da jetzt noch so ein Rumpf-BDSG, möglichst keine Widerstände, schnell durchwinken, und inhaltliche Arbeiten sind da nicht mehr möglich.[15] Was natürlich angesichts der Schwierigkeit der Materie ein bisschen seltsam ist. Also haben wir Datenschutzbeauftragten uns abgesprochen, haben unsere zuständigen Landesministerien munitioniert, und das hat auch gut geklappt: die haben einen sehr großen Teil – das hat mich echt überrascht – unseres Vorbringens in den Bundesrat getragen. Und dort hat sich Widerstand entwickelt: der Bundesrat hat rechtliche Gegenargumente gegen das geplante neue Bundesdatenschutzgesetz ins Feld geführt.[16] Und jetzt – offenbar auf Druck des Bundesrates – sollen wohl doch noch inhaltliche Änderungen stattfinden. Man wird sehen, wie viel von den Punkten, die der Bundesrat geltend gemacht hat, dann vom Bundestag aufgegriffen werden.[17]

Darüber hinaus gibt es die Gedankenhaltung bei den Datenschutzbeauftragten, dass, wenn dieses BDSG-Anpassungsgesetz Regelungen treffen sollte, die mit der Datenschutz-Grundverordnung nicht in Einklang stehen,[18] wir als Aufsichtsbehörden uns an die Datenschutz-Grundverordnung halten, denn der EuGH sieht den Anwendungsvorrang der Datenschutz-Grundverordnung. Natürlich kann es dort Grauzonen geben, strittige Bereiche. Aber wenn der nationale Gesetzgeber eine Regelung treffen würde, die klar gegen die Datenschutz-Grundverordnung verstößt, wenden wir die Datenschutz-Grundverordnung an – und nicht das nationale Recht. Da kann es innerhalb Deutschlands noch zu Konflikten kommen.

Mehr Kompetenzen (und mehr Arbeit) für Landesdatenschutzbeauftragte

Wird sich denn auf der Kompetenzebene für die Landesdatenschützer noch mehr verändern?

Die Datenschutz-Grundverordnung stellt ausdrücklich klar, dass wir völlig unabhängig sind.[19] Dieses Recht gilt jetzt unmittelbar, hat natürlich Durchschlagskraft, wirkt sich aus auf die rechtliche Anbindung der Datenschutzbeauftragten. Da tut sich in den Ländern Unterschiedliches; es gibt beispielsweise das Konstrukt der obersten Datenschutzbehörde, ähnlich einem Ministerium. Wir in Thüringen streben, auch aus Haushaltsgründen, wie bisher die Anbindung an den Landtag an: Die Landtagsverwaltung erbringt für uns Serviceleistungen, also Post, Fahrdienst, Repa-

raturen; das funktioniert ganz gut, und ich denke, dabei kann man es erst einmal belassen. Natürlich unter Abkopplung von jeglicher Aufsicht, auch etwaige rechtliche Einflüsse des Landtagspräsidenten müssen unterbunden werden.

Zusätzlich bekommen die Landesdatenschutzbeauftragten auch inhaltlich neue Aufgaben. Bisher waren wir im öffentlichen Bereich nur Kontrollbehörden: Wenn wir einen Verstoß bei einer Behörde festgestellt haben, zum Beispiel durch Tipp vom Bürger, vom Behördenmitarbeiter, oder auch durch eine anlassunabhängige Kontrolle, was wir ab und zu machen, dann haben wir beanstandet. Das war nicht viel mehr als ein erhobener Zeigefinger: Wir haben die Aufsichtsbehörde, für eine Kommune war das der Landkreis oder das Landesverwaltungsamt, über den Verstoß informiert und dann die Aufsichtsbehörde gebeten, diesen Verstoß abzustellen, also über Bande sozusagen. Das ändert sich jetzt durch die Datenschutz-Grundverordnung, wir werden Aufsichtsbehörden für Behörden, und das ist ein anderes, ein dichteres Verhältnis. Wir müssen dann dafür sorgen, dass alle Behörden Datenschutzrecht rechtskonform umsetzen. Und das bedeutet, wir können gegenüber Behörden Maßnahmen treffen, also Verwaltungsakte; können sagen, mach mal, lass mal, tu dies, tu das. Dagegen werden sich die Behörden möglicherweise wehren, dann kommt es zu Prozessen, allein in diesem Feld kommt einiges an Mehrarbeit auf uns zu.

Außerdem ist in der Datenschutz-Grundverordnung eine Beratungsfunktion der Aufsichtsbehörden gegenüber Unternehmen festgehalten.[20] Die Unternehmen werden vor große neue Aufgaben gestellt, hatten ja streckenweise schon Probleme mit dem alten Datenschutzrecht – und mit dem neuen Datenschutzrecht haben sie möglicherweise noch mehr Probleme, weil das nicht so konkret ist. Es ist eine zusätzliche Aufgabe für uns, dass wir Unternehmen bereits im Vorfeld der Wirksamkeit der Datenschutz-Grundverordnung beraten müssen und auch wollen. Um die Unternehmen einigermaßen darauf vorzubereiten, was auf sie zukommt, versuchen wir jetzt schon Information mit Hilfe von Newslettern und Infoblättern[21] zu streuen. Fragen wie: Brauche ich immer noch einen Datenschutzbeauftragen, oder brauche ich jetzt erst recht einen? Welche großen Veränderungen gegenüber der alten Rechtslage bestehen, welche Veränderungen bestehen nicht? Was ist komplett neu?

Wir Datenschutzbeauftragten haben allerdings derzeit – mit oder ohne Bundesdatenschutzgesetz – selbst gewisse Probleme mit der Datenschutz-Grundverordnung, weil sie eine etwas andere Rechtssprache spricht als das deutsche Recht, weil sie etwas anders strukturiert ist. Beispielsweise steht in Artikel 23 sinngemäß, dass Daten verarbeitet werden dürfen, sofern der „Wesensgehalt" des Grundrechts der informationellen Selbstbestimmung nicht angetastet wird. „Wesensgehalt" ist ein Begriff aus dem Grundgesetz, bezeichnet einen bestimmten Kernbereich, dazu gibt es Rechtsprechung vom Bundesverfassungsgericht. Wenn dieser Rechtsbegriff aber in der Europäischen Datenschutz-Grundverordnung steht, taucht sofort die Frage auf, ist damit das deutsche Rechtsverständnis gemeint, und falls nicht, was ist damit gemeint? Das wissen wir nicht! Das steht nirgendwo! Und das sind Probleme, die wir allein schon mit dem Text haben.

Das ist jetzt wie ein Neuanfang: neues Recht, keine Rechtsprechung, auf die wir zurückgreifen können, Kommentierung entwickelt sich erst – Kommentare greifen ja üblicherweise Rechtsprechung zu einer bestimmten Norm auf, um die Norm zu erläutern. Wir sind froh, dass einige Kommentare jetzt sozusagen im Niemandsland versuchen, Akzente zu setzen, aber es steht eben noch nicht viel drin. Ganz wichtig sind die Erwägungsgründe in der Datenschutz-Grundverordnung, mehr noch als Gesetzesbegründungen im nationalen Recht. Die Erwägungsgründe erläutern, was der Verordnungsgeber eigentlich wollte. Manchmal steht dort mehr als in den eigentlichen Vorschriften selbst, daran hat sich dann die Exekutive, und damit auch wir, auszurichten.[22]

Auf europäischer Ebene wird sich natürlich Rechtsprechung entwickeln, aber es kann Jahrzehnte dauern, ehe wir bei dem Durchdringungsgrad angekommen sind, den wir jetzt nach alter Rechtslage erreicht haben. Wir Datenschutzbeauftragte müssen jetzt also Tausende von Datenschutzproblemen – die bereits geklärt waren, durch den Gesetzgeber, durch Rechtsprechung, auch ein bisschen durch uns – wieder aufgreifen und messen an dem neuen Recht. Da kommt man unter Umständen zu anderen Ergebnissen. Und wir tingeln jetzt gerade durch die Lande, treffen uns hier und treffen uns da, es gibt die Datenschutzkonferenz, es gibt Arbeitskreise, Unterarbeitskreise, das bindet sehr viel Personal.

Besteht denn eine Chance, dass im Gegenzug die Datenschützer besser ausgestattet werden?

Darauf hoffe ich noch, speziell in Thüringen steht ja im Koalitionsvertrag, dass Datenschützer auch vor dem Hintergrund der Datenschutzreform besser ausgestattet werden. Die Haushaltsverhandlungen laufen noch, dazu möchte ich jetzt nicht viel sagen, ich bin ganz guter Hoffnung.[23]

Beschränkung des Grundrechts der informationellen Selbstbestimmung

Sie haben vorhin von Einschränkungsmöglichkeiten gesprochen, könnten sie das noch konkretisieren?

Ich gebe Ihnen ein Beispiel für eine Einschränkungsmöglichkeit. Eine ganz neuralgische Vorschrift betrifft die Zweckbindung, das ist für Datenschützer immer ganz wichtig. Daten werden, sagen wir von einem Unternehmen, für einen Zweck A erhoben. Dürfen diese Daten weiterverarbeitet werden? Also übermittelt, gespeichert und so weiter, benutzt, oder auch tatsächlich weiterverarbeitet, also mit anderen Daten kombiniert, neue Daten daraus generiert werden, zu einem Zweck B. Das ist nach altem Datenschutzrecht so gut wie nicht möglich. Aber das neue Datenschutzrecht, die Datenschutz-Grundverordnung, sagt dazu leider nicht so erheiternde Dinge: In Artikel 6 Absatz 4 erfährt dieses Prinzip der Zweckbindung, also dass zum Zweck A erhobene Daten auch nur zum Zweck A weiterverarbeitet werden dürfen, entscheidende Eingrenzung. Dieser Absatz 4 nennt unter anderem „das Vorhandensein geeigneter Garantien, wozu Verschlüsselung oder Pseudonymisierung gehören kann". Also, auf den ersten Blick, das wird nicht näher erläutert, wenn ein Unternehmen verschlüsselt oder pseudonymisiert, dürfen die Daten zu einem anderen Zweck verarbeitet und auch übermittelt werden an ein anderes Unternehmen, das die Daten möglicherweise wieder entschlüsselt, entpseudonymisiert; damit wäre die Zweckbindung umgangen. Diese Vorschrift ist erst spät reingekommen und aus

Sicht der Datenschützer ganz seltsam. Das könnte ein Einfallstor sein für Datenverarbeitung unter jeglichem Gesichtspunkt.

Schon ganz weit vorne, in Artikel 1 – Gegenstand und Ziele – Absatz 3 steht: „Der freie Verkehr personenbezogener Daten in der Union darf aus Gründen des Schutzes natürlicher Personen bei der Verarbeitung personenbezogener Daten weder eingeschränkt noch verboten werden." Geht das in die gleiche Richtung? Datenschutz wäre künftig geringer einzuschätzen als beispielsweise die Auffassung von Daten als wertvollem nationalen Gut?

Das ist eine wichtige Frage! In Erwägungsgrund 4 heißt es: „Das Recht auf Schutz der personenbezogenen Daten ist kein uneingeschränktes Recht; es muss im Hinblick auf seine gesellschaftliche Funktion gesehen und unter Wahrung des Verhältnismäßigkeitsprinzips gegen andere Grundrechte abgewogen werden." In Artikel 23 ist dann aufgelistet, in welchem Umfang das Grundrecht der informationellen Selbstbestimmung eingeschränkt werden kann, und zwar entweder durch weitere Vorschriften der EU oder durch Vorschriften der Mitgliedstaaten. Es gibt hier einen ganzen Katalog von a) bis j), unter welchen Voraussetzungen Einschränkungen stattfinden könnten.

Aus meiner Sicht ist der Buchstabe e) sehr wichtig. Da gibt es zunächst ein paar Bedingungen in Absatz 1 Satz 1: muss von einer demokratischen Gesellschaft gemacht und das Angemessenheitsprinzip gewahrt sein, und so weiter. Und dann steht da aber, eine Einschränkung kann erfolgen zum „Schutz sonstiger wichtiger Ziele des allgemeinen öffentlichen Interesses der Union oder eines Mitgliedstaats," – jetzt kommt's – „insbesondere eines wichtigen wirtschaftlichen oder finanziellen Interesses". Da klingt möglicherweise an, was Sie in Bezug auf Artikel 1 Absatz 3 angesprochen haben: Dass der freie Warenverkehr, also „das neue Öl" – oder wie die Politiker dazu sagen: „neue Gold", es heißt ja auch „Data Mining", und inzwischen spricht man auch von „Data Brokering", also Daten werden aktiv gehandelt – dass diese wirtschaftlichen, finanziellen Interessen eben dazu in der Lage sind, das Grundrecht einzuschränken. Also der Datenhandel etc. darf nicht verboten werden, das Grundrecht kann zurückgefahren werden. Es muss zwar die Verhältnismäßigkeit, die Angemessenheit gewahrt sein. Aber dieser Satz, den ich einmal gehört habe, „die Würde des Menschen ist unantastbar, nicht aber ein Geschäftsmodell" – sprich: Geschäftsmodelle sind antastbar – wird hierdurch in der Tat offenbar relativiert. Wirtschaft ist da, und dieses Grundrecht muss dazu in eine Konkordanz, wie wir Juristen sagen, gebracht werden, es muss abgewogen werden. Dass das Grundrecht absoluten Vorrang hat, ist nach diesem Text schwer vorstellbar.

Das könnte für Ihre Arbeit als Landesdatenschützer auch heißen, dass sie im Vorfeld selbst eine Abwägung treffen müssen, ob sie irgendwo eingreifen?

Das machen wir jetzt auch schon, denn nach bisherigem Datenschutzrecht ist immer wesentlich – das zieht sich wie ein roter Faden durch Bundes- und Landesdatenschutzgesetz – ob die Datenverarbeitung erforderlich ist, für Geschäftszwecke, für behördliche Aufgaben. Wenn wir da mit Unternehmen und Behörden diskutieren, prallen jetzt schon verschiedene Welten aufeinander. Und wenn wir uns nicht überzeugen lassen und Maßnahmen anordnen, jetzt nur gegenüber Unternehmen, künftig auch gegenüber Behörden, dann kommt es zwangsläufig zu Rechtsstreitigkeiten. Die Gerichte werden künftig mehr und mehr in die Pflicht genommen werden, solche Dinge justiziell zu entscheiden. Vielleicht sollte ich Kontakt mit den Verwaltungsgerichten aufnehmen, um die darauf vorzubereiten, was da auf sie zurollt.

Rechtsweg für Betroffene

Was hat sich verändert, falls Betroffene den Rechtsweg beschreiten wollen?

Manche Dinge klingen in der Tat gut. Beispiel Datenportabilität: Wenn man von einem sozialen Netzwerk zu einem anderen wechseln möchte, soll man die eigenen Daten mitnehmen können, so dass sie dann nicht mehr beim alten Netzwerk liegen, sondern beim neuen. Frage: Wie können wir das kontrollieren, wenn die Server nicht in Europa stehen, sondern in den USA? Da haben wir keine Möglichkeiten. Die Kontrollbefugnisse, um dieses geschriebene Recht durchzusetzen, hinken hinterher.

Recht auf Vergessenwerden, um ein anderes Beispiel zu nennen, klingt auch gut. Darunter stellt der Bürger sich vielleicht vor, man drückt irgendeinen Knopf, und die Daten sind aus dem Netz verschwunden. Dem ist natürlich nicht so, weil zwischenzeitlich irgendwer irgendwo die Daten heruntergeladen haben könnte, und das herauszufinden ist unmöglich.

Das Marktortprinzip gemäß Artikel 3 Absatz 2, also dass europäisches Recht gilt, wenn beispielsweise ein amerikanischer Datenverarbeiter hier etwas anbietet, könnte man auch als Fortschritt auffassen.[24] Wenn man sich aber die Erwägungsgründe dazu durchliest und auch die Kommentierung, dann ist das so formuliert, dass große Player Schlupflöcher finden können, um

Lutz Hasse

Dr. jur. **Lutz Hasse** legte die Juristischen Staatsexamina in Niedersachsen ab. Es folgten Assistenzen an der Universität Osnabrück und ab 1992 an der Friedrich-Schiller-Universität Jena. Die Promotion erfolgte während der „Jenenser Phase" an der Universität Osnabrück. Anschließend erfolgte der Wechsel zur Thüringer Verwaltungsfachhochschule – Fachbereich Polizei; dort wurde er Leiter der Rechtsausbildung. Nach Tätigkeiten als Referatsleiter im Thüringer Innenministerium, beim Thüringer Landesbeauftragten für den Datenschutz und im Thüringer Sozialministerium wurde er 2012 vom Thüringer Landtag zum Landesbeauftragten für den Datenschutz und die Informationsfreiheit gewählt.

diese Vorschriften zu umgehen. Man wird sehen, wie diese Vorschrift durch Aufsichtsbehörden und Gerichte ausgelegt wird.

Auch der Aspekt der Beweislastumkehr ist formal verstärkt worden. Privacy by default and by design ist in Artikel 25 DSGVO festgelegt und stellt eine Verbesserung gegenüber dem bisherigen Datenschutzrecht dar.

In der Rechtspraxis werfen diese hehren Begriffe und hehren Grundsätze ganz schöne Probleme auf. Insgesamt kann ich weiterhin vertreten, das habe ich vorausgesagt und das ist auch eingetreten, dass gemessen am bisherigen deutschen Datenschutzstandard ein erheblicher Rückschritt stattfindet.

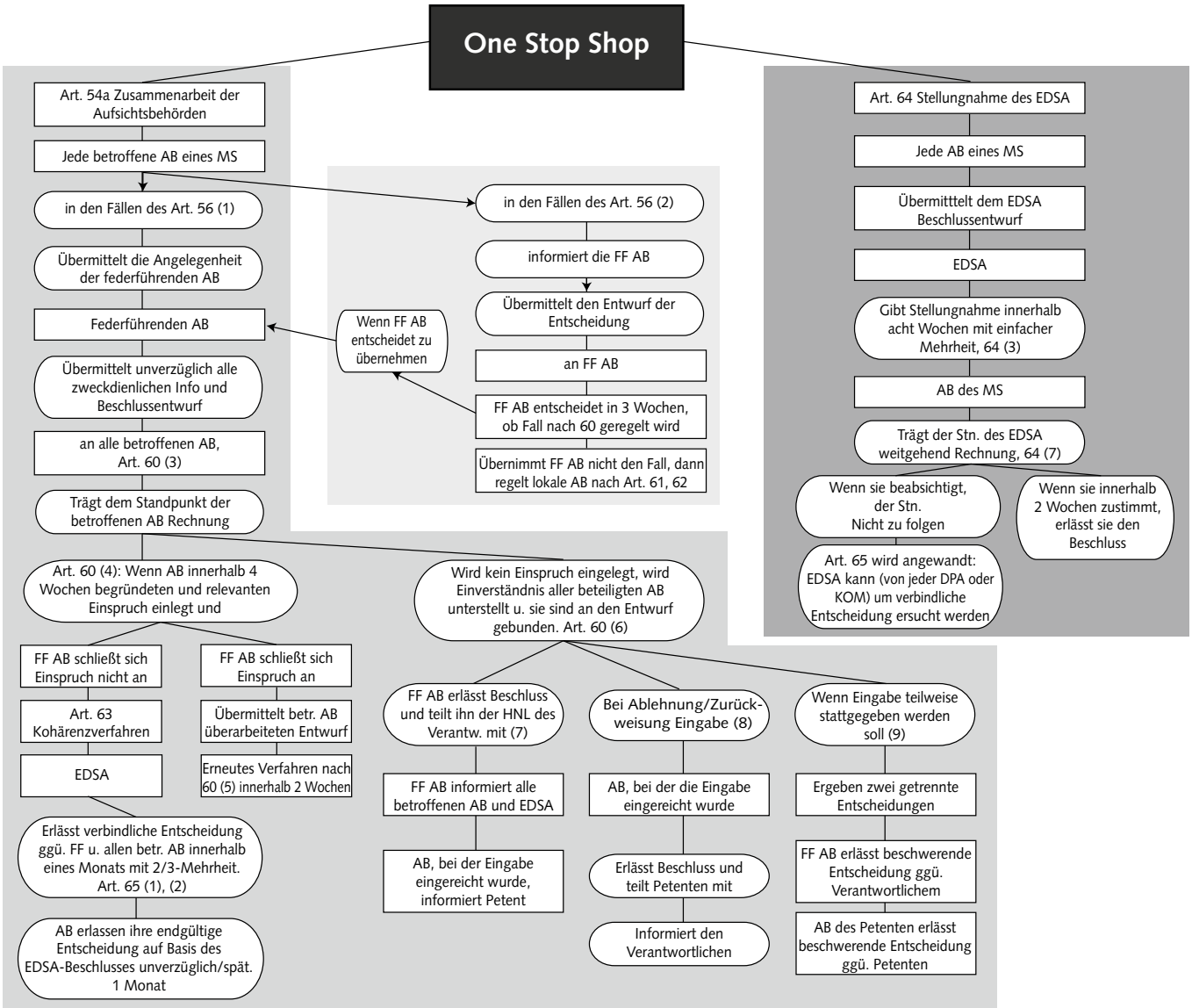
Das ist interessant, denn Jan Philipp Albrecht[25] hat meines Wissens die Meinung vertreten, es gäbe nur Fortschritte.

Der Film „Im Rausch der Daten", in dessen Zentrum insbesondere Albrecht steht – wir haben den Film auch für das Thüringer Schulportal beschafft[26] – stellt dar, unter welch schwierigen Bedingungen diese Datenschutz-Grundverordnung zustande gekommen ist, und mit welchem erheblichen Druck – ich glaube, 4000 Änderungsanträge sind eingegangen, insbesondere aus der Wirtschaftslobby – die Abgeordneten zu kämpfen hatten, um diese einseitigen Interessen wenigstens ein bisschen zu kanalisieren.

Wenn gesagt wird, die Datenschutz-Grundverordnung sei ein Erfolg: Ja, im Vergleich zum bisher geltenden EU-Standard, denn da gab es grottige Datenschutzstandards in bestimmten Staaten, das ist jetzt nach oben geliftet. Aus deutscher Sicht meiner Meinung nach aber eine Absenkung.

One-Stop-Shop

In Zusammenhang mit der Datenschutz-Grundverordnung ist manchmal vom sogenannten One-Stop-Shop die Rede. Inwiefern betrifft das die Bürger?



Schema des One-Stop-Shop-Verfahrens im Rahmen der Europäischen Datenschutz-Grundverordnung. Diese komplexen Abläufe werden vollständig von den Datenschutzbehörden durchgeführt. Betroffener bzw. Verantwortlicher merken davon nichts und kommunizieren jeweils nur mit einem einzigen Ansprechpartner.

Quelle: Textinhalte aus einem Vortrag von Sven Hermerschmidt, BfDI, am 7.9.2016

Ein deutscher Bürger beispielsweise, der sich in Spanien aufhält und dort einen Datenschutzverstoß feststellt, kann sich u. a. an die für ihn zuständige deutsche Aufsichtsbehörde wenden. Die muss dann für ihn – mit dem zuständigen spanischen Datenschutzbeauftragten, da gibt es bestimmte Verfahren – klären, wie dieser Datenschutzverstoß zu behandeln ist. Das erleichtert es natürlich für den Bürger: Er gibt das Problem praktisch ab, hat nur eine Anlaufstelle,[27] die ihm bekannte Datenschutzaufsichtsbehörde, die das dann für ihn regelt. Im Hintergrund kann dabei unter Umständen eine Riesenmaschinerie in Gang gesetzt werden. Die Angelegenheit landet evtl. sogar im Europäischen Datenschutzausschuss[28], ein ganz neues Gremium, das dann letztendlich darüber befindet, wie mit diesem Datenschutzverstoß umzugehen ist.

In diesem Zusammenhang finde ich Artikel 3 Absatz 2 interessant: „Diese Verordnung findet Anwendung auf die Verarbeitung personenbezogener Daten von betroffenen Personen, die sich in der Union befinden …" Dies gilt doch sogar, so wie es hier steht, wenn man nicht die Staatsbürgerschaft eines der Unionsstaaten hat oder nicht einmal ein Niederlassungsrecht, bezieht sich auf alle Personen, die sich gerade im Geltungsgebiet aufhalten? Auch ein Tourist aus Japan wäre durch diese Klausel geschützt?

Die Datenschutz-Grundverordnung regelt tatsächlich den Datenschutz für alle Menschen, die sich in der EU aufhalten.[29] Wir haben das bisher auch schon im Bundesdatenschutzgesetz Paragraph 1 Absatz 1: „Zweck dieses Gesetzes ist es, den Einzelnen davor zu schützen …" Das Grundrecht wurzelt ja in der Würde, und die Würde kann nicht abhängig sein von der Staatsangehörigkeit. Also nicht der Bürger, der Europäer, der Deutsche wird geschützt, wie manchmal in anderen Gesetzen, sondern jeder Einzelne.

Bei europäischen Bürgern ist also immer die Behörde aus dem Nationalstaat zuständig, dem sie angehören? Und für alle anderen gibt es weitere Regelungen der Zuständigkeit?

Nein, jede betroffene Person kann insbesondere auch im Mitgliedstaat ihres Aufenthaltsorts, ihres Arbeitsplatzes oder des Orts des mutmaßlichen Verstoßes Beschwerde einlegen.[30]

Harmonisierung des Datenschutzrechts?

Ist der Aspekt der Vereinheitlichung, der ja auch Ziel der Verordnung war, in gewisser Weise vorangekommen?

Die Datenschutz-Grundverordnung ist ein Rechtskompromiss, der den relativ niedrigen Standard des europäischen Datenschutzrechts heben sollte. Aufgrund der schon erwähnten Öffnungsklauseln und Beschränkungen bietet sich im Moment ein Bild, dass jeder europäische Staat eigene Regelungen treffen kann. Wird das gemacht, und alles deutet darauf hin, dann ist die Absicht gescheitert, zu einem einheitlichen Standard zu kommen, wie hoch oder niedrig der immer sein mag. Dann wird sich unterschiedliches Datenschutzrecht in Europa entwickeln, denn die Öffnungsklauseln befinden sich an wesentlichen Stellen.

Wie sieht es mit einer Harmonisierung zwischen dem Bund und den einzelnen Bundesländern aus?

Die Öffnungsklauseln müssen jetzt nach und nach ausgefüllt werden. Das Bundesdatenschutzgesetz-Anpassungsgesetz hat prinzipiell zwar diese Funktion, füllt aber noch nicht alle Öffnungsklauseln aus. Und solange der nationale Gesetzgeber in Deutschland diese Öffnungsklauseln nicht befüllt hat, ist für uns Datenschutzbeauftragte das Datenschutzrecht noch nicht komplett. Möglicherweise wird das Landesrecht hier auch noch Lücken ausfüllen müssen. Es ist ausgesprochenes Ziel, dass wir die Datenschutz-Grundverordnung (möglichst) einheitlich umsetzen, damit nicht auch noch im Bundesgebiet 16 – plus Bundesbeauftragte 17 – verschiedene Meinungen zu etwas undurchsichtigen Rechtslagen entstehen. Deshalb treffen wir Datenschutzbeauftragte und unsere Mitarbeiter uns häufig, in der Datenschutzkonferenz, in Groups und Subgroups, die auch schon auf europäischer Ebene arbeiten.

Sind die Landesdatenschützer denn in den europäischen Dialog direkt einbezogen?

Ja, da haben wir Vertreter, das ist die Bundesbeauftragte und, das wechselt, ein Landesvertreter. Und die bringen die deutsche Meinung – wenn Sie so wollen – die mit uns restlichen Datenschutzbeauftragten abgestimmt ist, dort ein. Deutschland hatte immer ein hohes Datenschutzniveau und war sozusagen Vorturner im Datenschutzrecht, aber jetzt verlagert sich das auf die europäische Ebene. Also wie bestimmte Rechtsbegriffe in der Datenschutz-Grundverordnung auszulegen sind, wie was aufzufassen ist.

Verschenkte Chancen

Wie beabsichtigt der Bundesgesetzgeber die Öffnungsklauseln in der DSGVO zu nutzen?

Wir Datenschützer haben uns intensiv mit dem BDSG-Anpassungsgesetz-Entwurf, der vom Bundesinnenministerium entworfen wurde, beschäftigt und sind zu zahlreichen Kritikpunkten gekommen. Auch, aber nicht nur, deshalb, weil diese Ausfüllung der Lücken nach unserer Auffassung nicht mit der Datenschutz-Grundverordnung harmoniert. Wir hatten gehofft, der Bundesgesetzgeber würde diese Öffnungsklauseln nutzen, um sozusagen den Standard der Datenschutz-Grundverordnung, was möglich wäre, zu heben, wieder in Richtung alter Standard in Deutschland. Diese Hoffnung können wir aber komplett aufgeben: Der Bundesgesetzgeber, insbesondere das Innenministerium, hat die Möglichkeit genutzt, um den Standard noch weiter zu senken, zum Teil sogar unter das, was rechtlich im Rahmen der Datenschutz-Grundverordnung eigentlich möglich ist. Rein gesetzestechnisch geht das aber, weil es diese Öffnungsklauseln gibt. Und Deutschland hat auch eine gewisse Vorreiterfunktion; es wird die Meinung vertreten, wenn diese Öffnungsklauseln nun so durch nationales deutsches Recht ausgefüllt werden, werden sich möglicherweise andere Staaten daran orientieren.

Wo wird denn nun wirklich etwas besser im deutschen Datenschutzrecht?

Hinsichtlich dieses BDSG-Anpassungsgesetzes kann ich da nichts erkennen. In der Datenschutz-Grundverordnung an sich wäre es, außer schon Genanntem, dass bei Verstößen durch Unternehmen die Bußgeldgrenzen exorbitant angehoben worden sind, von 300.000 auf 20 Millionen Euro oder bis zu 4 % des gesamten vom Unternehmen weltweit erzielten Jahresumsatzes des vorangegangenen Geschäftsjahrs, je nachdem, welcher der Beträge höher ist.[31] Der datenschutzrechtliche Druck auf Unternehmen wird höher. Das sind Werkzeuge, die uns an die Hand gegeben werden; die aber dann, wenn sie signifikant sind, vor Gerichten landen werden, insbesondere Verwaltungsgerichten, und dann muss sich eine Rechtsprechung nach und nach herausbilden.

Datenschutz im Konflikt mit Informationsfreiheit?

Als TLfDI sind Sie Landesbeauftragter sowohl für Datenschutz als auch für Informationsfreiheit. Ist diese Bündelung von Aufgaben in irgendeiner Hinsicht durch die zukünftige Rechtslage gefährdet?[32] Wenn ich es richtig verstehe, trifft ja die Datenschutz-Grundverordnung zur Informationsfreiheit keine Aussage.

Wir haben das geprüft, sind auch auf einzelne Punkte gestoßen, aber die waren nicht so wichtig. Da wird sich nicht viel ändern, wir können also weiter am Transparenzgesetz[33] arbeiten.

Verständlichkeit des neuen Datenschutzrechts

Verstehen Bürger beziehungsweise Unternehmen eigentlich, was die Datenschutz-Grundverordnung – und alles damit Zusammenhängende – für sie konkret bedeutet?

Es ist für Unternehmer auch neu, merke ich immer wieder, dass sie mit den Daten nicht tun und lassen können, was sie wollen, sondern eine Rechtsgrundlage brauchen wie eine Behörde. Wir haben in der Vergangenheit versucht, das bisherige deutsche Datenschutzrecht anhand des Paragraphen 28 Bundesdatenschutzgesetz verständlich darzustellen, der sozusagen die Grundnorm für Unternehmen war. Ich habe diesen Paragraphen beim ersten Durchlesen auch nicht verstanden, und ich mache das ja nun schon ein bisschen länger! Diesen einen Paragraphen, speziell für Unternehmer, haben wir versucht zu übersetzen, und daraus ist eine ganze Broschüre geworden. Die gut aufgenommen wurde; wir bekamen super Rückmeldungen.

Aber wir haben sozusagen vom – verständlicheren – Bundesdatenschutzgesetz nur eine einzige Norm in eine Sprache übersetzt, die verständlich ist. Das müssten wir eigentlich mit allen Normen des Bundesdatenschutzgesetzes machen. Dann müssten wir zum Landesdatenschutzgesetz übergehen. Und wenn man es ernst nimmt, müsste man eigentlich alle Gesetze für den Bürger übersetzen, weil die draußen nicht mehr verstanden werden.

Und jetzt kommt das europäische Datenschutzrecht mit neuen Rechtsbegriffen, mit Konstruktionen, die dem deutschen Recht eher fremd sind. Die unmittelbar geltende DSGVO und das ergänzende Bundes- und Landesdatenschutzrecht müssen künftig nebeneinandergelegt und zusammen gelesen werden – das macht es wirklich nicht einfacher. Da müssen wir Begriffe und Zusammenhänge auslegen, müssen sehen, wie sich das neue nationale Recht dazu verhält, und das müssen wir dann auch noch vermitteln. Also das ist eine Heidenaufgabe.

Ist denn das eine originäre Aufgabe für die Datenschutzbehörden? Oder sollte das nicht einfach eine Ebene höher angesetzt sein, zentral angegangen werden, dass man sagt, Gesetzgebung muss verständlich sein, das kann nicht in jedem einzelnen Ressort separat geleistet werden.

Ja, die Idee ist nicht neu, aber nach meinem Eindruck ist das bisher so nicht umgesetzt worden. Da können sie die Bürger fragen; die kennen die Gesetze nicht, und wenn Sie denen eine Norm vorlesen, verstehen sie sie nicht. Das kann eigentlich nicht Sinn von Recht und Gesetz sein. Ich sehe es als meine Aufgabe an, bei der Übersetzung von Gesetzen zu helfen, die Bürger, Unternehmen und Behörden anwenden müssen. Sonst wäre ich ja sozusagen nur repressiv unterwegs, immer mit der Bußgeldkeule, und das wäre doch wenig hilfreich.

Aufklärungsarbeit

Nein, mein Ansatz ist eigentlich anders. Ich möchte Bürger, Behörden, Unternehmen darauf vorbereiten, was auf sie zukommt, wie die Rechtslage aussieht, das möglichst verständlich darstellen. Und wenn sie sich dann nicht daran halten, dann habe ich es auch ein bisschen leichter zu sagen, eigentlich hättet ihr es wissen müssen.

Deshalb versuche ich auch, in diese Prozesse reinzukommen. Ich gebe Ihnen mal ein Beispiel: Ich bin ja Vorsitzender des Arbeitskreises „Datenschutz und Bildung“ der Datenschutzkonferenz. Da sind wir recht aktiv, und derzeit steht auf dem Programm der Verlage das Aus der Schulbücher und das Forcieren digitalen Lehrens und Lernens. Da entwickeln sich Lehr- und Lernplattformen von allen großen Spielern, die im Schulbuchmarkt unterwegs sind. Und ich stehe da in Kooperation mit der Kultusministerkonferenz, aber auch in Kooperation mit diesen Playern.

Da gibt es Organisationen, in denen ich Fuß gefasst habe, die wollen eben auch datenschutzrechtlich andere Meinungen hören. Denn immerhin wäre es theoretisch ja möglich, dass irgendein Datenschutzbeauftragter käme und würde eine regionale Lehr- und Lernplattform stilllegen, weil sie nicht datenschutzkonform – selbst nach dieser Datenschutz-Grundverordnung – arbeiten würde. Allein aus Kostengründen möchten sich da die großen Spieler absichern, das ist ja auch verständlich. Und das sehe ich als Chance, dort datenschutzrechtliche Inhalte zu transportieren, um zu datenschutzkonformen Lösungen zu gelangen.

Das ist nur ein Feld, doch jeder Datenschutzbeauftragte ist Vorsitzender eines Arbeitskreises[34] – andere sind z. B. „Sicherheit“ oder „Europa“ – und versucht dort etwas Ähnliches. Aber das Geschäft wird schwieriger – was könnte man für ein Bild nehmen, ich komme ja von der Küste – etwa dass man trotz Windes, der landab weht, versucht, mit einem Segelboot das Land zu erreichen, indem man gegen den Wind kreuzt. Ja, das wird aber immer schwieriger, je stärker der Wind weht.

Fazit

Hatten Sie sich mehr erhofft von diesem europäischen Gesetz?

Ja. Ich hatte mir von der Datenschutz-Grundverordnung erhofft, dass sie nicht so viele Öffnungsklauseln und Einschränkungsmöglichkeiten enthält. Und dann noch die inzwischen zerstörte Hoffnung, dass der Bundesgesetzgeber die Öffnungsklauseln national nutzt, um das Datenschutzniveau zu heben. Der politische Zug, und damit auch der rechtliche Zug, fährt aber in die entgegengesetzte Richtung: Data Mining, Data Brokering, Öl der Zukunft, Gewinnerzielung.

Ja, das bleibt ein spannendes Thema. Haben Sie vielen Dank für das ausführliche Gespräch.

Anmerkungen der Redaktion

1 *Homepage des TLfDI: https://www.tlfdi.de*

2 *Für die Europäische Datenschutz-Grundverordnung werden u. a. die Abkürzungen DS-GVO, DSGVO oder EU-DSGVO benutzt. Die Verordnung selbst weist keine Abkürzung aus. In diesem Beitrag wird die vom Europäischen Datenschutzbeauftragten (EDSB) benutzte Form DSGVO verwendet, vgl. dessen Entwicklungsgeschichte der Datenschutz-Grundverordnung, https://edps.europa.eu/data-protection/data-protection/legislation/history-general-data-protection-regulation_de.*

3 *Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung). ABl. L 119/1 vom 4.5.2016.*

4 *Regelung in Art. 99 Abs. 1 DSGVO. Überraschenderweise scheint keine Einigkeit über das genaue Datum des Inkrafttretens zu bestehen. Während meist der 25. Mai 2016 genannt wird – vgl. Jahresbericht der Bundesregierung 2015/16, Stand 16.1.2017, Tätigkeitsbericht 2015-2016 der Bundesbeauftragten für den Datenschutz und die Informationsfreiheit (BfDI), Entschließung „EU-Datenschutz-Grundverordnung erfordert zusätzliche Ressourcen für Datenschutzbehörden" der Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder (Datenschutzkonferenz – DSK) vom 25.5.2016 – geht der EDSB in seiner Entwicklungsgeschichte vom 24. Mai 2016 aus, vgl. auch seine Pressemeldung „Datenschutz für die digitale Generation: Der Countdown für die Datenschutz-Grundverordnung läuft" vom 24.5.2016, ebenso der Innenausschuss des Bundestags, https://www.bundestag.de/dokumente/textarchiv/2017/kw13-pa-innen-datenschutz/499054, Roßnagel in seinem Gutachten „Datenschutzaufsicht nach der EU-Datenschutz-Grundverordnung", die stellvertretende TLfDI Pöllmann in ihrem Vortrag „Datenschutz im Krankenhaus" am 12.4.2017, https://tlfdi.de/mam/tlfdi/datenschutz/safeharbor/votrag_im_krankenhaus.pdf, sowie Paal/Pauly, Datenschutz-Grundverordnung, 1. Aufl. 2017, Rn. 1 zu Art. 99 DSGVO; gestützt wird Letzteres durch die Formulierung „Datum des Wirksamwerdens: 24/05/2016; Inkrafttreten Datum der Veröffentlichung +20 Siehe Art. 99" in http://eur-lex.europa.eu/legal-content/DE/ALL/?uri=CELEX%3A32016R0679.*

5 *Explizite Regelung in Art. 99 Abs. 2 DSGVO*

6 *Bundesdatenschutzgesetz v. 20.12.1990, neugefasst durch Bek. v. 14.1.2003, zuletzt geändert durch Art. 10 Abs. 2 G v. 31.10.2017 I 3618; aufgeh. durch Art. 8 Abs. 1 Satz 2 G v. 30.6.2017 I 2097 mWv 25.5.2018.*

7 *Mittlerweile beschlossen: Bundesdatenschutzgesetz v. 30.6.2017, verkündet als Art. 1 G v. 30.6.2017, Gesetz zur Anpassung des Datenschutzrechts an die Verordnung (EU) 2016/679 und zur Umsetzung der Richtlinie (EU) 2016/680 (Datenschutz-Anpassungs- und -Umsetzungsgesetz EU – DSAnpUG-EU), BGBl. 2017 I, 2097. Inkrafttreten gem. Art. 8 Abs. 1 dieses Gesetzes am 25.5.2018.*

8 *Richtlinie (EU) 2016/680 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die zuständigen Behörden zum Zwecke der Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten oder der Strafvollstreckung sowie zum freien Datenverkehr und zur Aufhebung des Rahmenbeschlusses 2008/977/JI des Rates. ABl. L 119/89 vom 4.5.2016.*

9 *Bereits über die Bedeutung des Begriffs gibt es Kontroversen. Der Kabinettschef von EU-Kommissionspräsident Juncker, Selmayr, an der Entstehung der DSGVO maßgeblich beteiligt, lehnt die Verwendung des Begriffs „Öffnungsklausel" in Bezug auf die DSGVO strikt ab – wie die EU-Kommission insgesamt, vgl. Hülsmann, Regelungsräume der nationalen Gesetzgeber in der Datenschutz-Grundverordnung, https://dsgvo.expert/regel, wo sich auch eine ausführliche sachliche Darlegung findet. Selmayr benutzt stattdessen die Begriffe „Spezifizierungsklausel" bzw. „Spezifizierungsbefugnisse", vgl. z. B. die Rezension von Tinnefeld zu Ehmann/Selmayr, Datenschutz-Grundverordnung, in ZD-Aktuell 2017, 04265, https://rsw.beck.de/cms/?toc=ZD.60&docid=395066, oder Artikel und Bericht zum Hamburger Rechtsgespräch „Die Datenschutz-Grundverordnung kommt: Welche Änderungen ergeben sich im geltenden Recht?" am 9.5.2017, Universität Hamburg, https://www.wiso.uni-hamburg.de/fachbereich-sozoek/professuren/koerner/fiwa/rechtgespraeche/ds-gvo.html. Laut Flyer zur Veranstaltung und o. g. Bericht waren die Veranstalter aber ganz anderer Meinung, und im Sprachgebrauch hat sich der Begriff „Öffnungsklauseln" ohnehin bereits weitestgehend durchgesetzt, vgl. z. B. den Gesetzentwurf der Bundesregierung zum DSAnpUG-EU, BT-Drs. 18/11325 v. 24.2.2017, der intensiv mit dem Begriff „Öffnungsklauseln" operiert; die Bundesrats-Drucksache 110/1/17 (neu) v. 1.3.2017, in der an mehreren Stellen ausdrücklich von Öffnungsklauseln gesprochen wird; den o. g. Tätigkeitsbericht der BfDI, die von weitgehenden Öffnungsklauseln im gesamten öffentlichen Bereich spricht, und das BfDI-Info 6 „Datenschutz-Grundverordnung", 5. Auflage, September 2017, wo auf eine Vielzahl von Öffnungsklauseln hingewiesen wird; die Entschließung „Stärkung des Datenschutzes in Europa – nationale Spielräume nutzen" der 91. DSK vom 7.4.2016, die sich auf „Öffnungs- und Konkretisierungsklauseln" in der DSGVO bezieht; den Vortrag „Spielräume der EU-Datenschutz-Grundverordnung und weitere Regelungsbedarfe" des TLfDI auf der 2. Digitalisierungskonferenz EU-DSGVO, 25.8.2016, https://www.tlfdi.de/mam/tlfdi/datenschutz/safeharbor/vortrag_zur_2._digitalisierungskonferenz.pdf, der das methodische System der Öffnungsklauseln sowohl systematisch als auch an Beispielen erklärt; den Fachartikel von Benecke/Wagner, Öffnungsklauseln in der Datenschutz-Grundverordnung und das deutsche BDSG – Grenzen und Gestaltungsspielräume für ein nationales Datenschutzrecht, DVBl 2016, 600; die Rechtsgutachten von Kühling/Martini u. a., Die Datenschutz-Grundverordnung und das nationale Recht, Juni 2016, angefertigt für das Bundesministerium des Innern, sowie Roßnagel, Datenschutzaufsicht nach der EU-Datenschutz-Grundverordnung, März 2017, ursprünglich angefertigt für die Datenschutzbehörden der Länder und dann an den von der Bundesregierung beschlossenen Entwurf eines neuen Bundesdatenschutzgesetzes angepasst; den Überblicksvortrag „Die 69 Öffnungsklauseln der DS-GVO" von Feiler (Co-Autor des ersten österreichischen Kommentars zur Datenschutz-Grundverordnung), http://www.lukasfeiler.com/presentations/Feiler_Die_69_Oeffnungsklauseln_der%20DS-GVO.pdf; sowie die einschlägigen Kommentare von Franzen/Gallner/Oetker, Gola, Kühling/Buchner, Paal/Pauly, Sydow, Wolff/Brink.*

10 *Konkrete zahlenmäßige Nennungen in Quellen der Anmerkung 9: etwa 30 (Univ. Hamburg), ca. 48 (TLfDI), 50 (Kühling/Martini u. a.), 69 (Feiler),*

70 (Roßnagel), ca. 70 (Bundesregierung). Unterschiede in der Zählung gehen zumindest teilweise auf sog. unechte Öffnungsklauseln zurück, vgl. z. B. o. g. Vortrag des TLfDI oder das Gutachten von Kühling/Martini u. a.

11 *Dies wird in den Erwägungsgründen 10 und 19 der DSGVO erläutert: Die Mitgliedstaaten sollten in bestimmten Kontexten die Möglichkeit haben, nationale Bestimmungen, mit denen die Anwendung der Vorschriften der DSGVO genauer festgelegt wird, beizubehalten oder einzuführen. Dass solche, die Öffnungsklauseln ausfüllende, Regelungen „natürlich nicht gegen die Datenschutz-Grundverordnung verstoßen dürfen", war zweifellos auch der Wille der EU-Kommission: Die DSGVO setze, so Selmayr in Hamburg, dezidiert den rechtlichen Rahmen, nationales Recht könne lediglich spezifizieren. Der Spielraum für die öffentliche Verwaltung, meint dazu die BfDI im o. g. Tätigkeitsbericht, erlaube keine grundsätzlichen Abweichungen vom Datenschutzniveau der DSGVO. Jedoch weckte die Bezeichnung „Grundverordnung" – statt wie von Art. 288 Abs. 2 AEUV vorgesehen „Verordnung" – (unbegründete) Begehrlichkeiten hinsichtlich daraus folgender mitgliedstaatlicher Rechtsetzungsbefugnisse, wie Benecke/Wagner feinsinnig feststellen. Siehe Anmerkung 18 für Beispiele mutmaßlicher Verstöße im DSAnpUG-EU.*

12 *Regelungen §§ 8–16 BDSG-neu, in Einklang mit Art. 54 DSGVO; bisher §§ 22–26 BDSG. Es handelt sich weiterhin um eine oberste Bundesbehörde, die Amtsbezeichnung „Die oder der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit" wird beibehalten.*

13 *Eine solche Kompetenzverschiebung hat der Bundestag am 1.6.2017 dann auch tatsächlich in erster Lesung beschlossen; allerdings nicht, wie zu erwarten gewesen wäre, über die Neufassung des BDSG, sondern durch Änderung der Abgabenordnung, und dies wiederum verdeckt im Schlepptau einer Neufassung des Bundesversorgungsgesetzes. Der Bundesrat hat dem am 7.7.2017 zwar zugestimmt, dies aber mit einer umfangreichen Rüge der Vorgehensweise des Bundestags verbunden, die unbedingt lesenswert ist, BR-Drs. 450/17(B). Der gesamte Vorgang hat insbesondere auch bei den Landesdatenschützerinnen und -schützern für sehr viel Verärgerung gesorgt, vgl. z. B. Schulzki-Haddouti, Datenschutz-Aufsicht Länderfinanzbehörden: Kontrollkompetenz geht an den Bund, IITR, 8.6.2017, https://www.datenschutzbeauftragter-online.de/datenschutz-aufsicht-laenderfinanzbehoerden-kontrollkompetenz-bund/10780/. Beschlossenes Gesetz siehe BGBl. 2017 I, 2541.*

14 *Die formelle Anpassungsfrist bis zum 25. Mai 2018 trügt: Wegen des Diskontinuitätsgrundsatzes, vgl. z. B. Deutscher Bundestag, Parlamentsbegriffe, Diskontinuität, stand für Gesetzesvorhaben auf Bundesebene praktisch nur der Zeitraum bis zum Ende der Legislaturperiode, also bis September 2017, zur Verfügung. Frühzeitig wurde darauf hingewiesen, dass der Bundestagswahlkampf zu einer weiteren Verkürzung der nutzbaren Spanne führen könnte, vgl. z. B. Kühling/Martini, EuZW 2016, 449 f. oder Benecke/Wagner, 608.*

15 *In welch fragwürdigem Stil die Bundesregierung Anpassungen des Bundesrechts an die DSGVO vollzieht, erschließt sich exemplarisch aus der Pressemitteilung der Landesbeauftragten für den Datenschutz und für das Recht auf Akteneinsicht Brandenburg v. 2.6.2017, Verschlechterungen beim Datenschutz in Nacht-und-Nebel-Aktion vom Deutschen Bundestag verabschiedet, http://www.lda.brandenburg.de/cms/detail.php/bb1.c.517569.de; vgl. diesbezüglich auch Anmerkung 13.*

16 *Vgl. den Gesetzentwurf der Bundesregierung, BT-Drs. 18/11325 v. 24.2.2017, und die darauf bezogenen Empfehlungen der Bundesrats-Ausschüsse, BR-Drs. 110/1/17 (neu) v. 1.3.2017.*

17 *Der Bundestag hat dann allerdings am 27.4.2017 seinen o. g. Gesetzentwurf fast ohne Änderungen verabschiedet, vgl. Hülsmann, DSAnpUG-EU mit BDSG-neu am 27.04.2017 vom Bundestag verabschiedet, https://dsgvo.expert/dsanpug-eu-mit-bdsg-neu-am-27-04-2017-vom-bundestag-verabschiedet/, m. w. N., und damit insbesondere die meisten der Bedenken des Bundesrats ignoriert.*

18 *Diese Gefahr besteht in der Tat noch: Zwar hat der Bundesrat dem DSAnpUG zugestimmt, doch wurden etliche seiner diesbezüglichen Einwände auch in der verabschiedeten Fassung des Gesetzes nicht berücksichtigt, vgl. z. B. Hülsmann, Synopse Bundesdatenschutzgesetz (neu, BDSG-RegE) und Beschlussempfehlung des Innenausschusses des Bundestages, https://dsgvo.expert/BDSG-n-Syn, und die entsprechenden Textstellen in der Bundesrats-Drucksache 110/1/17 (neu) v. 1.3.2017: Ziffer 53, „… Auch bestehen Zweifel, ob diese Ausnahmeregelung überhaupt mit den Anforderungen der Öffnungsklausel in Artikel 23 der Verordnung (EU) 2016/679 vereinbar ist. … Eine derart weite Auslegung der Öffnungsklausel zugunsten privater Datenverarbeiter läuft dem erkennbaren Ziel der Verordnung (EU) 2016/679 zuwider, für Verbraucherinnen und Verbraucher ein EU-weit einheitliches Schutzniveau bei der unternehmerischen Nutzung ihrer Daten zu gewährleisten. …"; Ziffer 70, „… Das entspricht aber weder den Interessen der Betroffenen, noch scheint eine entsprechende Regelung von einer Öffnungsklausel der Verordnung (EU) 2016/679 gedeckt zu sein. …"; Ziffer 72, „… Eine Ermächtigung des nationalen Gesetzgebers zu einer so weitreichenden Einschränkung des Löschungsanspruchs der betroffenen Person findet sich in Artikel 23 Absatz 1 der Verordnung (EU) 2016/679 nicht. …"; Ziffer 73, „… Die Einschränkung des Löschungsrechts gemäß Artikel 17 DSGVO für Fälle, in denen wegen der besonderen Art der Speicherung die Löschung nicht oder nur mit unverhältnismäßig hohem Aufwand möglich ist, ist europarechtlich unzulässig. …"*

19 *Art. 52 Abs. 1 und 2 DSGVO. Vgl. auch § 10 Abs. 1 BDSG-neu.*

20 *Art. 57 Abs. 1 Buchst. l i. V.m. Art. 36 Abs. 2 DSGVO.*

21 *Siehe z. B. die Pressemitteilung „Die EU-DSGVO – Erste Schritte" des TLfDI vom 19.7.2017, https://www.tlfdi.de/mam/tlfdi/presse/170719_pm_.pdf, und die bisher erarbeiteten 11 Kurzpapiere der DSK unter https://www.tlfdi.de/tlfdi/gesetze/europaeische-dsgvo/.*

22 *Vgl. Benecke/Wagner, DVBl 2016, 607: „Erwägungsgründe sind Bestandteil des jeweiligen Rechtsakts und insbesondere im Rahmen der teleologischen Auslegung bei Ermittlung von Sinn und Zweck des jeweiligen Rechtsakts heranzuziehen. Da auch über die Erwägungsgründe als Bestandteil des Gesamtrechtsakts im Europäischen Parlament abgestimmt wird, nehmen sie ebenfalls an der besonderen Legitimität des Rechtsakts teil, die etwa über die Legitimität deutscher Gesetzesbegründungen hinausgeht. Teils wird ihnen sogar verbindliche Wirkung beigemessen."*

23 *Die DSK hat in ihrer Entschließung „EU-Datenschutz-Grundverordnung erfordert zusätzliche Ressourcen für Datenschutzbehörden" vom 25.5.2016 deutlich gemacht, welche neuen bzw. erweiterten Aufgaben durch die Anwendung der DSGVO auf sie zukommen, und unter Verweis auf Art. 52 Abs. 4 DSGVO erweiterte personelle und finanzielle Ressourcen für die Datenschutzbehörden in Deutschland gefordert.*

24 *Vgl. DSK-Kurzpapier Nr. 7 „Marktortprinzip: Regelungen für außereuropäische Unternehmen"*

25 *Jan Philipp Albrecht war Verhandlungsführer des Europäischen Parlaments für die Datenschutz-Grundverordnung. Hinsichtlich seiner Einschätzung der DSGVO vgl. z. B. die Zusammenfassung seines Vortrags am 25.11.2016 auf der FIfF-Konferenz in Berlin, FIfF-Kommunikation 1/2016, 26–28, der Vortrag selbst ist unter https://media.ccc.de/v/fiffkon16-4005-weitergehende_erkenntnisse_aus_den_verhandlungen_zur_eu_datenschutzgrundverordnung verfügbar, seine Ausführungen auf dem Hamburger Rechtsgespräch „Die Datenschutz-Grundverordnung kommt: Welche Änderungen ergeben sich im geltenden Recht?" am 9.5.2017, Universität Hamburg, https://www.uni-hamburg.de/newsroom/im-fokus/20170516-Datenschutz-Grundverordnung-jan-philipp-albrecht.html, und das Interview der Bundeszentrale für politische Bildung mit ihm, veröffentlicht am 10.11.2017, http://www.bpb.de/gesellschaft/medien/democracy/254242/interview-*

mit-jan-philipp-albrecht. Ähnlich positiv wie Albrecht äußert sich auch der Europäische Datenschutzbeauftragte Giovanni Buttarelli in seiner Entwicklungsgeschichte der Datenschutz-Grundverordnung: „Durch die DSGVO werden eine Vielzahl der bestehenden Rechte des Einzelnen gestärkt und neue Rechte geschaffen. Hierzu zählt auch das Recht auf Löschung (Recht auf Vergessenwerden): Sie können verlangen, dass ein Unternehmen Ihre personenbezogenen Daten löscht, wenn Ihre Daten beispielsweise für die Zwecke, für die sie erhoben wurden, nicht mehr notwendig sind oder Sie Ihre Einwilligung widerrufen haben."

26 *Hinweise dazu auf der Seite „Schule" des TLfDI, https://www.tlfdi.de/tlfdi/datenschutz/schule/index.aspx.*

27 *Daher die Bezeichnung „One-Stop-Shop", ein Begriff aus der englischen Fassung der DSGVO. In der deutschen Fassung wird stattdessen die Bezeichnung „Verfahren der Zusammenarbeit und Kohärenz" verwendet.*

28 *Art. 68 ff. DSGVO*

29 *Vgl. Erwägungsgrund 2 der DSGVO*

30 *Art. 77 Abs. 1 DSGVO*

31 *Art. 83 Abs. 5 bzw. 6 DSGVO; ähnlich auch Art. 83 Abs. 4 DSGVO*

32 *Siehe dazu beispielsweise das internationale Symposium „Datenschutz und Informationsfreiheit – Widerspruch oder Ergänzung?" am 28.9.2017 in Potsdam, http://www.lda.brandenburg.de/media_fast/4055/Programm_Symposium_2017_170927.pdf.*

33 *Das geltende Thüringer Informationsfreiheitsgesetz soll laut Koalitionsvertrag der Regierungsparteien zu einem echten Transparenzgesetz nach dem Vorbild Hamburgs unter Einbeziehung der Erfahrungen auch anderer Bundesländer fortentwickelt werden. Ein Vorschlag des TLfDI findet sich unter https://www.tlfdi.de/mam/tlfdi/info/vorschlag_des_tlfdi_f__r_ein_th__ringer_transparenzgesetz.pdf.*

34 *Vgl. Übersicht über die Arbeitsgremien der Datenschutzkonferenz, Anlage 1 zur Geschäftsordnung der DSK, http://www.lda.brandenburg.de/media_fast/4055/GO_Anlage_DSK_Gremien.pdf.*

Martin Rost

Bob, es ist Bob!

Seit bestimmt zwanzig Jahren zählt es unter FIfFlern zum selbstgewiss-aufklärerischen Gestus, Nicht-Technikern mehr Interesse an der notorischen Unsicherheit von IT und dem ungenügenden Datenschutz abzuverlangen. Allerdings rechtfertigen viele Artikel in der FIfF-Kommunikation diesen selbstgewissen Gestus nicht, weil es den Autoren vielfach an analytisch bedeutenden Kenntnissen zum Datenschutz – im Unterschied beispielsweise zu Themen der IT-Sicherheit – mangelt. Was genau meint denn „Datenschutz"?

Die vielfach festzustellende Inkompetenz in Bezug auf Datenschutz ist insbesondere deshalb ein ernsthaftes Problem, weil das FIfF als „kritischer Berufsverband der Informatiker" (Wikipedia) im deutschsprachigen Raum in meinen Augen die politische Avantgarde unter den Informatiker.innen repräsentiert. Zwar werden in vielen Artikeln verlässlich Grundrechtsverstöße aufgelistet und beleuchtet, aber ein zweifellos notwendiges Skandalisieren allein ersetzt keine ernsthafte theoretische Befassung – wobei eine ernsthafte Beschäftigung sich wiederum auch nicht darin erschöpft, über eine detaillierte Orientierung im komplizierten Datenschutzrecht zu verfügen. Es drängt sich mir seit l
dass ein, allerdings die gesamte Da
Empörungsaktivismus den Mang
oder theoretischen Diskussionen
möchte nachfolgend ebenfalls einmal diesen selbstgewiss-lauten
rischen Gestus simulieren, den Spieß umdrehen und Ihnen mehr ernsthaftes Interesse für Datenschutz abverlangen.

erschienen in der FIfF-Kommunikation, herausgegeben von FIfF e.V. - ISSN 0938-3476 www.fiff.de

Ich bitte Sie, dass Sie sich vor dem Weiterlesen selbst zwei Fragen beantworten:

1. Welcher zentrale Konflikt soll durch „Datenschutzrecht" geregelt werden?

2. Was unterscheidet Schutzmaßnahmen des Datenschutzes von denen der IT-Sicherheit? Notieren Sie sich doch bitte Ihre Antworten, vielleicht mit nur wenigen groben Stichworten. Dann können Sie sich selber davon überzeugen, wie schlüssig Ihr Wissen zum Datenschutz ist.

These 1: Datenschutz nimmt nicht den Schutz von Privatheit zum Ausgangspunkt der Bestimmung, ebenso wenig wie den Schutz von Freiheit, Autonomie und Selbstbestimmung einer Person. Auch nicht der Schutz der Rechte von Betroffenen und noch viel weniger

irgendwelche Vorstellungen von Privacy, die mal so oder mal so und mal auch ganz anders oder gar nicht ausfallen können, bilden den Ursprung des Datenschutzes. Und auch die Differenz „öffentlich/privat" erzeugt nicht den wesentlichen Datenschutzkonflikt. Datenschutz nimmt vielmehr die Risiken erzeugende Machtasymmetrie zwischen Organisationen und Personen zum Ausgangspunkt. Das Datenschutzrecht und die technischen und organisatorischen Datenschutzaktivitäten sind bereits Formen des Unterbedingungstellens (Konditionierung) dieses strukturellen Machtkonflikts in modernen Gesellschaften. Welche Rolle dabei Recht und Technik
dige Konditionierung der Machta-
achfolgend erläutern.

mächtigen Organisationen als Ri-
sikogeber – hier denke man paradigmatisch als erstes natürlich an den Staat, aber nicht nur. Auf der anderen Seite befinden sich die von Organisationen abhängigen Personen, denen durch die Organisationen die Rolle als Risikonehmer aufgebürdet wird. Risiko meint hier: Organisationen erzeugen durch die von ihnen betriebenen personenbezogenen Verfahren Risiken, die es ohne diese Verfahren für die Personen nicht gäbe. Dieser Konflikt ist der Ursprung der regulativen Idee des Datenschutzrechts. In den 70er-Jahren hatten Datenschützer.innen vornehmlich den Staat vor Augen, heute sind es vor allem die global agierenden Unternehmen, die von keinem Leviathan gebremst werden. Von Technik ist hier noch überhaupt keine Rede. War Ihnen dieser kristallklare Gedanke der Konditionierung von Machtasymmetrie zwischen Organisationen und Personen als Gegenstand des Datenschutzrechts als Antwort in den Sinn geschossen oder haben Sie ihn vielleicht sogar notiert? Nein? Sehen Sie! Ja? Dann heiße ich Sie willkommen in Level 2, das sogleich folgt.

Was heißt jetzt „Konditionierung der Machtasymmetrie"? Das verfasste Rechtsstaatsversprechen, das im Datenschutzrecht