ULD · Postfach 71 16 · 24171 Kiel

Deutscher Bundestag
Innenausschuss
Platz der Republik 1
11011 Berlin

Holstenstraße 98
24103 Kiel
Tel.: 0431 988-1200
Fax: 0431 988-1223

Ansprechpartner/in:
Herr Dr. Weichert
Durchwahl: 988-1200

Aktenzeichen:
LD -

Kiel, 17. März 2009

Stellungnahme zum Entwurf der Bundesregierung eines Gesetzes zur Regelung des Datenschutzaudits und zur Änderung datenschutzrechtlicher Vorschriften
Ihr Schreiben vom 24.02.2009

Sehr geehrte Damen und Herren Abgeordnete,

unten stehend gebe ich Ihnen die

Stellungnahme des Unabhängigen Landeszentrums für Datenschutz Schleswig-Holstein (ULD) zum

Gesetzentwurf der Bundesregierung zur Regelung des Datenschutzaudits und zur Änderung datenschutzrechtlicher Vorschriften (BT-Drs. 16/12011) sowie zu einigen damit in Verbindung stehenden Anträgen der Fraktionen FDP (BT-Drs. 1169) und Bündnis 90/Die Grünen (BT-Drs. 16/1499 u. 10216)

anlässlich der öffentlichen Anhörung des Innenausschusses des Deutschen Bundetages am 23.03.2009, 14.00 bis 18.00 Uhr, Paul-Löbe-Haus, Raum 4.900 zur Kenntnis.

I. Vorbemerkung

Das ULD begrüßt, dass anlässlich der Erfahrungen mit dem im Sommer 2008 allgemein bekannt gewordenen **illegalen Datenhandel** geplant wird, das Bundesdatenschutzgesetz (BDSG) zu überarbeiten und ein Datenschutzauditgesetz (DSAG) zu verabschieden.

Damit entspricht der Bundesgesetzgeber teilweise einem Beschluss des **Schleswig-Holsteinischen Landtags** vom 28.01.2009 (LT-Drs. 16/2421), in dem u.a. folgende Positionen festgelegt werden:

I. 1. „Die Übermittlung von personenbezogenen Daten an Dritte oder deren Nutzung zu Werbezwecken bedarf ausdrücklich der Einwilligung der Betroffenen."

I. 6 „Das Land Schleswig-Holstein tritt für ein Gesetz zur Einführung eines Datenschutzaudits auf Bundesebene ein, bei dem geregelt wird, dass von unabhängigen Stellen in einem unbürokratischen aber transparenten Verfahren informationstechnische Produkte und Einrichtungen auf ihre Datenschutzkonformität hin überprüft werden."

I. 6. „Die Bundesregierung möge sich in der Europäischen Union dafür einsetzen, dass der Schutz personenbezogener Daten auch im Waren- und Dienstleistungsverkehr im Bereich des europäischen Binnenmarktes durch entsprechende europarechtliche Regelungen gewährleistet wird."

Das ULD, das bei der datenschutzrechtlichen Ermittlung des illegalen Datenhandels beteiligt war und ist, hat sich von Anfang an dafür eingesetzt, dass die gesammelten tatsächlichen Erfahrungen zu einer gesetzgeberischen Reaktion führen.

https://www.datenschutzzentrum.de/bdsg-novellierung/
https://www.datenschutzzentrum.de/bdsauditg/

Mit den Vorschlägen wird **keine umfassende Aktualisierung und Modernisierung** des Datenschutzrechtes erreicht. Neben den geplanten Neuregelungen zur Bonitätskontrolle und zum Scoring (dazu https://www.datenschutzzentrum.de/presse/20080620-scoring.htm) bedarf es weiterer Änderungen im allgemeinen Datenschutzrecht (so auch Antrag Bündnis 90/Die Grünen, BT-Drs. 16/10216), die realistischerweise bis zum Ende der derzeit laufenden Legislaturperiode nicht umgesetzt werden können. Wegen der Komplexität und des Umfangs des bestehenden Modernisierungsbedarfs im allgemeinen Datenschutzrecht auf Bundesebene wird daher vom ULD empfohlen, die nötigen Änderungen in Themenbereiche aufzuteilen und im Rahmen eines kontinuierlichen öffentlichen Diskurses sowie in einer Folge von Gesetzgebungsverfahren zu verabschieden.

Im Folgenden wird vorrangig auf die Vorschläge des o.g. Gesetzentwurfes der Bundesregierung – unter Einbeziehung der o.g. Anträge – Stellung genommen.

II. Entwurf eines Gesetzes zur Regelung des Datenschutzaudits (Datenschutzauditgesetz – DSAG), Art. 1

II. 1. Allgemeine Bemerkungen

Das Vorhaben, ein Datenschutzauditgesetz auf den Weg zu bringen, ist angesichts des seit dem Jahr 2001 bestehenden Gesetzesauftrags des § 9a BDSG (Bundesdatenschutzgesetz) und des hohen und weiter **steigenden Bedarfs** an einem gesetzlich geregelten präventiven Instrument zur Bestätigung der Datenschutzkonformität von Produkten, Dienstleistungen und Verfahren sehr zu begrüßen.

Das ULD ist in Deutschland derzeit noch **die einzige öffentliche Stelle**, die umfassende Erfahrungen mit der Durchführung von Datenschutzaudits und der Erteilung von Datenschutz-Gütesiegeln hat. Nachdem hierfür in Schleswig-Holstein in den §§ 4 Abs. 2, 43 Abs. 2 Landes-

datenschutzgesetz (LDSG SH) die gesetzliche Grundlagen geschaffen worden sind, werden Verfahren sowie IT-Produkte erfolgreich vom ULD seit 8 Jahren auditiert bzw. zertifiziert (vgl. https://www.datenschutzzentrum.de/audit/ sowie https://www.datenschutzzentrum.de/guetesiegel/). Wegen der hohen Nachfrage und des nationalen wie internationalen Bedarfes hat das ULD im Rahmen eines von der Europäischen Union (EU) von Mitte 2007 bis März 2009 geförderten Projektes in Kooperation mit Partnern aus 8 europäischen Ländern das Datenschutzgütesiegel Schleswig-Holstein als Europäischen Gütesiegel (European Privacy Seal – EuroPriSe) mit europäischen Datenschutzstandards etabliert und bietet dies nunmehr gebührenpflichtig an (http://www.european-privacy-seal.eu).

Vor wie nach der Vorlage eines ersten Referentenentwurfes für ein DSAG, u.a. auch auf dem sog. Datenschutzgipfel am 4. September 2008, hat ULD die Verantwortlichen mehrfach darauf hingewiesen, dass die mit dem Entwurf verfolgte Konzeption eine Vielzahl von praktischen Probleme verursachen werde, die vermeidbar sind. Das ULD hat seine **Beratung angeboten**. Leider wurde weder dieses Beratungsangebot angenommen, noch die ausführlich begründete Kritik aufgegriffen und berücksichtigt. Die "Konsultierung zahlreicher Institutionen, die im Bereich der Akkreditierung und Zertifizierung im Datenschutzbereich tätig sind", die von der Bundesregierung als Begründung für die langjährige Verzögerung des 2001 mit § 9a BDSG gegebenen Versprechens eines Auditgesetzes vorgetragen wurde (BT-Drs. 15/4725, zit. in BT-Drs. 16/1169), erstreckte sich zu keinem Zeitpunkt auf das ULD. Ergebnis der unzureichenden Einbindung von Auditerfahrungen ist, dass der von der Bundesregierung beschlossene Regelungsvorschlag insgesamt nicht praktikabel ist.

Der DSAG-E basiert auf der Gesetzgebungskompetenz des Bundes für das Recht der Wirtschaft (Art. 72 Abs. 2, 74 Ans. 1 Nr. 11 GG). Im Interesse einer bundesweiten einheitlichen Regelung ist dies zu begrüßen. Die **Zuständigkeit** für die Erfüllung staatlicher Aufgaben liegt nach Art. 30 GG grundsätzlich bei den Ländern. Für die vorgesehenen Zuständigkeiten auf Bundesebene gibt es weitgehend keine sachliche Notwendigkeit und damit auch keine Rechtfertigung.

Adressat des DSAG sollen ausschließlich Stellen sein, die zueinander im Wettbewerb stehen, also v.a. nicht-öffentliche Stellen (§ 1 S. 1, 3 DSAG-E). Für öffentliche Stellen der Länder besteht auf Landesebene die Möglichkeit spezifischer Regelungen. Hiervon haben bisher die Länder Bremen und Schleswig-Holstein Gebrauch gemacht. **Öffentliche Stellen des Bundes** sollen gemäß dem Entwurf i.d.R. von Datenschutzaudits nicht profitieren können. Dies wird damit begründet, dass es für die erhöhte Akzeptanz der Bürgerinnen und Bürger bei der Inanspruchnahme einer E-Government-Anwendung "ausreichend" sei, "dass mit einem Datenschutzauditsiegel gekennzeichnete Datenschutzkonzepte und technische Einrichtungen eingesetzt werden können" (Begr. S. 8). Dies widerspricht den Erfahrungen von teilweise sehr umfassenden Datenschutzaudits in Kommunen und bei der Landesverwaltung in Schleswig-Holstein. Bei den bisher seit 2001 durchgeführten über 20 Verfahrensaudits nach § 43 Abs. 2 Landesdatenschutzgesetz Schleswig-Holstein (LDSG SH) war es möglich, auf äußerst effektive Weise teilweise gravierende Mängel insbesondere bei der Datensicherheit und beim Datenschutzmanagement zu beheben. Die öffentlichen Stellen in Schleswig-Holstein nehmen das Angebot im Rahmen der zur Verfügung stehenden Kapazitäten umfassend in Anspruch.

Es haben sich auch schon öffentliche Stellen des Bundes an das ULD mit der Bitte gewandt, ein gebührenpflichtiges Audit durchzuführen. Ein derartiges rechtsförmliches Audit war dem ULD wegen der Rechtslage nicht möglich. Es ist kein Grund ersichtlich, weshalb den öffentlichen Stellen des Bundes diese Chance vorenthalten werden soll.

Gegenstand des Datenschutzaudits sollen Datenschutzkonzepte sowie technische Einrichtungen sein. Deren Umfang soll durch das beantragende Unternehmen festgelegt werden. Anders als in Schleswig-Holstein geht der BDSAG-E nicht auf die Unterschiede der **Zertifizierung von Produkten und Dienstleistungen** einerseits (Datenschutzgütesiegel nach § 4 Abs. 2 LDSG SH) und der **Auditierung von Stellen, Organisationseinheiten oder Verfahren** ein. Diese vom DSAG-E nicht nachvollzogene Differenzierung ist nicht zwingend. Das im DSAG-E vorgeschlagene Verfahren ist aber nicht ansatzweise für die Zertifizierung von Produkten geeignet. Dies zeigt sich schon an § 1 S. 2 DSAG-E, wo z.B. die Anforderung der Nr. 3 (Beachtung der Normen zum betrieblichen Datenschutzbeauftragten) für die Qualität von IT-Produkten regelmäßig überhaupt keine Relevanz hat, so wichtig und sinnvoll es auch ist, dass sowohl bei der Entwicklung von Produkten wie auch bei deren Einsatz eine Einbeziehung des betrieblichen Datenschutzbeauftragten erfolgt. Bei Produkten kommt es darauf an, dass sich deren Nutzer zum Zeitpunkt der Entscheidung der Anschaffung darauf weitgehend verlassen können muss, dass diese gesetzeskonform eingesetzt werden können. Während bei umfassenden, in der Regel schon im Betrieb befindlichen Verfahren eine Nachbesserung bei auftretenden Mängeln nachträglich möglich ist, ist dies bei Produkten oft nicht oder nur sehr schwer machbar. In der verlässlichen hoheitlichen Bestätigung der Rechtskonformität sehen Produktanbieter den wesentlichen Wettbewerbsvorteil der vom ULD mit einem Gütesiegel ausgezeichneten Produkte. Diese Chance wird relativiert bzw. vertan, wenn nicht eine vertrauenswürdige, unabhängige öffentliche Stelle die Datenschutzkonformität vorab feststellt. Vertrauen wird nicht durch das Siegel selbst geschaffen, sondern ausschließlich durch die Vertrauenswürdigkeit der das Siegel verleihenden Einrichtung und des Auditverfahrens. Gegenüber dem schleswig-holsteinischen Gütesiegel entfällt bei dem nach dem DSAG-E gewählten Verfahren zudem der Wettbewerbsvorteil, dass bei öffentlichen Beschaffungen zertifizierte Produkte vorrangig zu berücksichtigen sind (§ 4 Abs. 2 LDSG SH).

Bei Produkten ist es grundsätzlich sinnvoll und wünschenswert, eine Zertifizierung auch vornehmen zu können, wenn die Produkte nicht von Stellen in Deutschland hergestellt bzw. vermarktet werden. Eine Vielzahl von **ausländischen IT-Produkten und Dienstleistungen** wird angesichts der Globalisierung der Informationstechnik auf dem deutschen Markt angeboten. Es ist nicht ersichtlich, weshalb diese IT-Produkte und Dienstleistungen von den Vorteilen einer Auditierung nicht profitieren können sollen. So hat z.B. das Unternehmen Microsoft aus Redmond/USA zur Verbesserung seiner Wettbewerbschancen auf dem europäischen Markt schon zwei seiner Produkte in Schleswig-Holstein zertifizieren lassen. Es ist zudem fraglich, ob die Beschränkung auf deutsche Anbieter (§ 1 S. 1) mit europäischem Recht vereinbar ist.

Der DSAG-E sieht vor, dass eine Auditierung nur dann erfolgen soll, wenn über die gesetzlichen Anforderungen hinaus Verbesserungen für den Datenschutz implementiert sind (Begr. S. 10). Dies ist ein zweifellos ehrgeiziges Anliegen. Dieses Ziel wird aber nicht erreicht, wenn selbst **bei festgestellten Datenschutzverstößen** von mittlerer Bedeutung das Siegel beibehalten werden kann (§ 7 Abs. 2 S. 1).

Der Entwurf legt selbst nicht fest, welches Maß der **Übererfüllung der rechtlichen Anforderungen** notwendig ist. Gerade bei Produkten wäre es für den Datenschutz schon ein großer Gewinn, wenn deren rechtmäßige Einsatzmöglichkeit bestätigt würde. Die Entwurfsautoren gehen fälschlich davon aus, dass die Einhaltung der Datenschutzgesetze die Regel wäre. Dies liegt nicht am bösen Willen oder gar an der kriminellen Absicht der Anwender. Es gibt viele Produkte, die teilweise eine Marktabdeckung von mehr als 50% in einem bestimmten Segment in Deutschland haben, die auf Grund der technischen Gegebenheiten nicht rechtskonform eingesetzt werden können (z.B. wegen fehlender oder mangelhafter Protokollierung, mangels der Möglichkeit einer Einzeldatenlöschung, wegen fehlender Einwilligungswahlmöglichkeit für den Betroffenen, auf Grund der Einbeziehung von Übermittlungen ins Drittausland). Wegen oft fehlender eigener hinreichender technischer und rechtlicher Kompetenz kommt es dem Erwerber eines IT-Produktes v.a. darauf an, sich zu vergewissern, dass er mit dessen regulärem Einsatz "auf der sicheren Seite" ist. Auch ein sich auf Gesetzeskonformität beschränkendes Datenschutzauditsiegel würde nicht Gefahr laufen, die darüber hinausgehenden Kontrollen von Datenschutzaufsichtsbehörden zu entwerten oder gar einen faktischen Zwang zur Auditierung auszulösen. Die dies behauptende Passage der Begründung (S. 10) zeigt, dass die Autoren des DSAG-E die Besonderheit der Datenschutzzertifizierung nicht vollständig erfasst haben: Während bei der Zertifizierung "auf dem Gebiet des ökologischen Landbaus", die als Vorbild herangezogen wurde (Begr. S. 11), die Einhaltung von klaren rechtlichen Anforderungen (Grenzwerte, überschaubare Produktpalette und einfache Abläufe) von den Aufsichtsbehörden relativ einfach festgestellt werden kann, hängt die Datenschutzkonformität des Einsatzes eines IT-Produktes nicht nur von diesem selbst ab, sondern von den gegebenen technischen und organisatorischen Rahmenbedingungen, von den Schnittstellen zu angeschlossenen Verfahren und v.a. von der konkreten Nutzung durch die Anwender, d.h. von Organisationen und ihren Beschäftigten. Mit einem Audit kann und soll die Voraussetzung dafür geschaffen werden, dass ein rechtskonformer Einsatz möglich und erleichtert wird. Die tatsächliche Beachtung der Datenschutzgesetze, deren Kontrolle den Aufsichtsbehörden obliegt, ist ein weit über die Zertifizierung hinausgehendes Feld.

Der Grundansatz des DSAG-E, der abweicht von allen in diesem Bereich üblichen staatlich geregelten Zertifizierungen, besteht darin, die Auditierung durch private Stellen (sog. Kontrollstellen) vornehmen zu lassen. Dem gegenüber sieht z.B. die Zertifizierung des Bundesamtes für die Sicherheit in der Informationstechnik (BSI) oder des ULD eine **Qualitätssicherung** der von privaten Gutachtern durchgeführten Audits vor. Diese Qualitätssicherung ist dringend notwendig, um Billig- und Gefälligkeitszertifikate auszuschließen. Anders als etwa im Bereich des Umweltschutzes oder des biologischen Landbaus (Begr. S. 11 f., 14) sind die datenschutzrechtlichen und -technischen Anforderungen hoch komplex, von Produkt und Verfahren zu Produkt und Verfahren unterschiedlich und in einer dauernden Fortentwicklung. Die Erfahrungen des ULD zeigen, dass selbst engagierten und qualifizierten privaten Gutachtern aktuelle Anforderungen oft nicht bekannt und bewusst waren bzw. sind. Diese Anforderungen lassen sich auch nicht durch ein schwerfälliges Verfahren in einem Datenschutzauditausschuss (§ 13 DSAG-E) festlegen, sondern ergeben sich oft aus technologischen Neuentwicklungen und der aktuellen Forschung. Im Dialog zwischen Gutachtern und Zertifizierungsstelle war es in Schleswig-Holstein bisher möglich, einen Konsens über die rechtlich geforderte Qualität des Produktes, der Dokumentation und des Gutachtens herzustellen. Hierbei hat es sich als vor-

teilhaft erwiesen, dass auf die Kontroll- und Beratungserfahrung einer Aufsichtsbehörde nach § 38 BDSG zurückgegriffen werden konnte, die im Diskussionszusammenhang mit den anderen Aufsichtsbehörden (sog. Düsseldorfer Kreis) bzw. Datenschutzbeauftragten (Konferenz der Datenschutzbeauftragten des Bundes und der Länder) steht. Die Qualitätssicherung liegt nicht nur im Interesse der Produktanbieter und der Produktkäufer, sondern auch der Gutachter, die vor Abgabe des endgültigen Gutachtens oft auf einen Dialog mit der Zertifizierungsstelle angewiesen sind, um Fehlbeurteilungen zu vermeiden.

Ein zentraler Aspekt der Qualitätssicherung besteht darin, dass alle interessierten Personen und Stellen die Berechtigung des Zertifikats überprüfen können. Dies gilt insbesondere für den Datenschutz und die Datensicherheit, die beide wegen ihrer dauernden Weiterentwicklung und Komplexität, auch durch Wechselwirkungen mit anderen Funktionalitäten, weder von Gutachtern noch von Aufsichtsbehörden abschließend beurteilt werden können. Daher kommt der **Transparenz gegenüber der Öffentlichkeit** eine zentrale Bedeutung für die Qualität und Vertrauenswürdigkeit des Zertifikats zu (so auch Anträge FDP, BT-Drs. 16/1169, Bündnis 90/Die Grünen, BT-Drs. 1499). Transparenz beginnt mit einer präzisen Beschreibung des Auditierungsgegenstands, um keine falschen Vorstellungen vom Umfang der Zertifizierung entstehen zu lassen. Beschrieben werden müssen alle wesentlichen Eigenschaften, Abläufe, Schnittstellen, Einsatzbedingungen und Sicherheitsvorkehrungen. Nur wenn das Audit auch qualifiziert öffentlich in Frage gestellt werden kann, findet es die nötige allgemeine Akzeptanz. Dies setzt nicht voraus, dass die zum Einsatz kommenden Algorithmen, Quellcodes oder Betriebs- und Geschäftsgeheimnisse offengelegt werden müssten. Wohl aber ist es nötig, die wesentlichen Funktionsweisen plausibel und nachvollziehbar darzustellen. Dies begründet bei Betroffenen und Anwendern das notwendige Vertrauen, bei kritischer Öffentlichkeit und Aufsichtsbehörden den Ansatz zur Überprüfung, und bei Gutachtern und Anbietern das nötige Feedback auf Auftreten von Angriffsmöglichkeiten. Bei den in Schleswig-Holstein durchgeführten Auditierungen wird die Transparenz dadurch hergestellt, dass die Kurzgutachten im Internet allgemein bereitgestellt bzw. veröffentlicht werden. Eine entsprechende Transparenz ist im DSAG-E überhaupt nicht angelegt. Die Veröffentlichung soll sich auf "das angezeigte Datenschutzkonzept sowie die technische Einrichtung" beschränken (§ 9 Abs. 1 S. 3 Nr. 3 u. S. 4). Eine Dokumentation der Erkenntnisse der Kontrolle durch die Kontrollstelle erfolgt nicht, sondern lediglich die nicht näher überprüfbare Erklärung der Kontrollstelle, bei welchen Stellen Kontrollen durchgeführt wurden (§ 6 Abs. 2).

Es drängt sich der Eindruck auf, dass der DSAG-E nicht darauf abzielt, eine vertrauenswürdige präventive Datenschutzüberprüfung durchzuführen, sondern darauf, die staatliche **Aufsicht durch eine nachträgliche private Kontrolle zu ersetzen**. Mit dem Gesetz würde die Verantwortlichkeit für die Rechtmäßigkeit der Datenverarbeitung von der kontrollierten Stelle zu einem Teil auf die Kontrollstelle übertragen, aber auch die Verantwortlichkeit für die Datenschutzkontrolle durch die Aufsichtsbehörde würde teilweise auf die Kontrollstelle übertragen. Die Kontrollstelle käme ihren daraus sich ergebenden Pflichten dadurch förmlich nach, dass sie gegenüber den Aufsichtsbehörden bestätigt und sich verpflichtet, Kontrollen nach § 3 durchzuführen. Qualifiziertere Feststellungen werden grds. von der Kontrollstelle nicht abverlangt (§ 6 Abs. 2). Das Konzept würde dazu führen, dass bei der Feststellung von Verstößen die Verantwortung jeweils auf eine andere Stelle abgeschoben werden kann. Tatsächliche Anreize zu einer ernsthaften Kontrolle werden nicht gegeben und würden erst dann entstehen,

wenn Verstöße öffentlich bekannt würden. Damit würde keine Verbesserung des Datenschutzes, sondern eine Verschlechterung gegenüber dem aktuellen Zustand erreicht.

Die faktische Entbindung von staatlicher Kontrolle durch das DSAG ist wohl nicht mit Art. 28 Abs. 3 S. 1 3. Sp. der **Europäischen Datenschutzrichtlinie** (EU-DSRL) vereinbar, wonach "jede Kontrollstelle" über "wirksame Einwirkungsbefugnisse" verfügen muss. Die Festlegung von rechtsinterpretierenden Richtlinien durch den Datenschutzauditausschuss unter der Rechtsaufsicht des Bundesministeriums des Innern (BMI) verletzt zudem tendenziell die von Art. 28 Abs. 1 S. 2 EU-DSRL geforderte Unabhängigkeit von Kontrollstellen (auch der Länder).

Das Problem der mangelnden Qualitätssicherung versucht der DSAG-E durch ein **kompliziertes nachträgliches Kontrollverfahren** zu kompensieren. Damit wird aber die Idee des Datenschutzaudits als präventives Instrument ad absurdum geführt, weil dessen Validität von der Repression, also der aufsichtsbehördlichen Kontrolle und der Sanktionierung von Verstößen abhängig gemacht wird. Angesichts der teilweise sehr schlechten personellen und sonstigen Ausstattung der Aufsichtsbehörden ist faktisch nicht ansatzweise die notwendige nachträgliche Qualitätssicherung gewährleistet. Dem versucht der DSAG-E offensichtlich dadurch Rechnung zu tragen, dass er die Möglichkeit einräumt, private Stellen mit den Aufsichtsaufgaben zu beleihen (§ 16 Abs. 1 S. 2, Abs. 2 Nr. 2). Da aber auch diese Tätigkeit beaufsichtigt werden muss, diese jedoch noch weniger transparent ist als die staatliche Aufsichtstätigkeit, entsteht weder ein Effekt der Entlastung von Behörden noch der einer verbesserten Kontrolle. Vielmehr werden alle Beteiligten über die Wertigkeit des konkreten Zertifikats bis zu dem Zeitpunkt im Ungewissen gehalten, zu dem über eine aufwändige Prozedur das Zertifikat wegen übermäßiger Datenschutzverstöße aufgehoben wird.

Das konzeptionelle Defizit des vom DSAG-E vorgesehenen Audits besteht darin, dass die Zertifizierung nicht durch eine **unabhängige Stelle** erfolgt. Zwar kann durch das Zulassungsverfahren eine hinreichende Qualifizierung, finanzielle Unabhängigkeit und Zuverlässigkeit sichergestellt werden (§ 4 DSAG-E). Dies ändert aber nichts an dem Umstand, dass sowohl die Kontrollstelle als auch die nicht-öffentliche Stelle ein gemeinsames Interesse haben, möglichst ohne großen Aufwand und Kosten ein Zertifikat zu führen. Um die Parteilichkeit der Auditierung zu verhindern, muss - zumindest bei der Zertifizierung von Produkten - eine ökonomisch nicht interessierte Stelle schon im Auditverfahren einbezogen werden.

Während der Entwurf eines DSAG von September 2007 offensichtlich noch davon ausging (Referententwurf des BMI vom 07.09.2007; dazu Stellungnahme des ULD vom 28.09.2007: https://www.datenschutzzentrum.de/bdsauditg/20070928-stellungnahme.html), dass die Zertifizierung ein von Beliehenen erlassener Verwaltungsakt ist, geht der aktuelle DSAG-E davon aus, dass es sich bei der Auditierung nicht um ein Verwaltungsverfahren, sondern um ein rein **privatrechtliches Geschäft** handelt (§ 3 S. 1).

Die Formulierung des Gesetzentwurfes ist **unstrukturiert und zusammengestückelt**. So werden z.B. die materiellen Anforderungen an ein Audit in § 1 S. 2 aufgeführt; in § 9 Abs. 1 wird dann jedoch geregelt, dass eine ausdrückliche Feststellung dieser Anforderungen gar nicht nötig ist. Der Entwurf verwendet eine eigene Terminologie, die sich weder aus bisherigen Gesetzen noch aus dem allgemeinen Sprachgebrauch erschließt. So wird z.B. durch den

DSAG-E der Begriff "Kontrollstelle" verwendet, der von der EU-DRSL in Art. 28 anderweitig für die Datenschutzaufsichtsbehörden genutzt wird. Dies führt dazu, dass der Inhalt des Gesetzes nur von Experten, die sich intenisiv mit dem Gesetz beschäftigen, erfasst werden kann, und dass dieser von anderen zwangsläufig falsch verstanden wird.

Für Betroffene dürfte das Gesetz regelmäßig zu kompliziert und unverständlich sein. Schon aus diesem Grund ist der DSAG-E nicht geeignet, bei **Betroffenen** Vertrauen in die Qualität der Audits zu fördern. Den Betroffenen wird in dem Entwurf keine aktive Rolle zugewiesen. Sie haben nicht einmal die Möglichkeit, sich über die Qualitätsmerkmale der auditierten Stelle bzw. des Auditgegenstands zu informieren und dies auf ihren Realitätsgehalt hin zu überprüfen.

Die Durchführung des Datenschutzaudits soll freiwillig sein (Begr. S. 8). Dies würde es notwendig machen, dass **positive Marktanreize** für eine solche Durchführung geschaffen würden. Davon kann beim DSAG-E aber keine Rede sein. Vielmehr entstehen neben den Kosten- und Gebührenpflichten für das Unternehmen weitgehende zusätzliche Unterrichtungspflichten (§ 8) sowie zusätzliche Sanktionsandrohungen (§§ 17, 18).

Die **Freiwilligkeit** gerät auch dadurch in Gefahr, dass ein Datenschutzaudit für bestimmte Anwendungen zur Pflicht gemacht wird. Einen solchen Regelungsvorschlag machte das Bundeskabinett in seinem Gesetz zur Regelung von Bürgerportalen. Gegen gesetzliche Marktanreize ist nichts einzuwenden. So sieht z.B. § 4 Abs. 2 LDSG SH vor, dass zertifizierte Produkte in der öffentlichen Verwaltung vorrangig einzusetzen sind. Wird jedoch die fehlende Zertifizierung zu einem gesetzlichen Hindernis für den Zugang zu bestimmten Märkten, so müssen an die Qualität der Zertifizierung höchste Anforderungen gestellt werden. Diesen Anforderungen wird der vorliegende DSAG-E nicht gerecht.

II. 2. Zu den spezifischen Regelungen

Zu § 1 - Datenschutzaudit

Die Beschreibung des **Auditierungsgegenstands** (Target of Evaluation - ToE) als "Datenschutzkonzept oder eine angebotene informationstechnische Einrichtung" nach Satz 1 ist zu eng. Die Datenschutzkonformität von Produkten und Verfahren kann oft nur über die Beschreibung der Datenflüsse, der Organisation und/oder von internen Normen hergestellt werden, was mit der verwendeten Terminologie begrifflich nicht erfasst wird. Daher wird empfohlen, entweder umfassend von "Produkten und Verfahren" zu sprechen oder präziser von "Produkten, Dienstleistungen, Datenverarbeitungskonzepten und Verfahren".

Die Beschränkung auf **nicht-öffentliche Stellen** i.S.d. § 2 Abs. 4 BDSG ist - wie oben dargestellt - zu eng. Erfasst werden sollten auch öffentliche Stellen des Bundes sowie ausländische Stellen. Dies lässt dadurch kurz und knapp beschreiben, dass keinerlei Einschränkung bzgl. der Anwendung erfolgt außer den nicht erfassten "öffentlichen Stellen eines Landes".

Zur zusätzlichen Anforderung in "Richtlinien zur **Verbesserung des Datenschutzes** und der Datensicherheit" siehe oben (II. 1.) sowie die Ausführungen zu § 11.

Die in S. 2 Nr. 3 vorgesehene Beschränkung der Organisationskontrolle auf den "Beauftragten für den Datenschutz" ist zu eng. Bei einem Verfahrensaudit muss zur organisatorischen Gewährleistung des Datenschutzes ein den betrieblichen Datenschutzbeauftragten einbeziehendes, aber sich nicht hierauf beschränkendes funktionierendes, umfassendes **Datenschutzmanagement** etabliert sein (vgl. Nr. 7 der Anwendungsbestimmungen des ULD zur Durchführung eines Datenschutzbehördenaudits nach § 43 Abs. 2 LDSG SH).

Nach S. 1 Nr. 4 ist die Datenschutzkonformität **nach § 3 zu kontrollieren**. Dieses Verfahren ist in manchen Bereichen zweifellos sinnvoll, in vielen Fällen aber auch unnötig aufwändig. Für den Bereich des Produktaudits ist dieses Vorgehen oft nicht praxisgerecht, da die Notwendigkeit einer Überprüfung sich nur ergibt, wenn Änderungen am Produkt erfolgen, oder wenn sich das Umfeld wandelt, z.B. durch Gesetzesänderungen oder Fortentwicklungen der Technik. Vorzuziehen ist, so wie dies in Schleswig-Holstein praktiziert wird, die Auditierung z.B. auf zwei oder drei Jahre zu befristen und nach der bestimmten Frist eine Reauditierung insofern vorzunehmen, als rechtliche, organisatorische oder technische Veränderungen erfolgt sind. Ergeben sich wesentliche Änderungen zu einem früheren Zeitpunkt, sollte die verantwortliche Stelle verpflichtet werden, dies anzuzeigen, so dass geprüft werden kann, ob eine Nachkontrolle erforderlich ist.

Zu § 2 - Zuständigkeit

Nach Abs. 1 werden die jeweils zuständigen **Datenschutzaufsichtsbehörden** der Länder nach § 38 BDSG bzw. im Bereich der Post und der Telekommunikation der Bundesbeauftragte (BfDI) für Auditierungsfragen für zuständig erklärt. Den Landesbehörden werden damit Aufgaben auferlegt, die mit dem derzeit vorhandenen Personal nicht ansatzweise erledigt werden können, wenn die Aufgaben ernsthaft wahrgenommen werden sollen. Eine Aufstockung des Personals ist in vielen Bundesländern derzeit leider wenig realistisch. Sinnvoller wäre es, die präventiv, nicht repressiv auszugestaltenden Zertifizierungsaufgaben eigenständigen Stellen zu übertragen, die sich über Gebühren selbst finanzieren.

In Abs. 2 wird die Zuständigkeit für die **Zulassung der Kontrollstellen** und die Entziehung der Zulassung dem BfDI übertragen. Nach Art. 30 GG liegt die Verwaltungszuständigkeit bei den Ländern. Es gibt keinen Grund, diese Aufgaben dem Bund zu übertragen. Die einheitliche Präsentation der Zulassungen kann auch durch eine gemeinsame Stelle der Länder erfolgen.

Zu § 3 - Kontrollen

Gemäß dieser Regelung haben die zugelassenen Kontrollstellen die Auditierung durchzuführen. Nach S. 3 sollen sich Art und Häufigkeit der Kontrollen "nach dem Risiko des Auftretens von Unregelmäßigkeiten und Verstößen in Bezug auf die Erfüllung der Anforderungen dieses Gesetzes und der auf Grund dieses Gesetzes erlassenen Rechtsverordnungen" richten, wobei Kontrollen zunächst einmal jährlich, später 18monatig erfolgen sollen. Diese Regelung gibt nicht ansatzweise die Gewähr, dass eine umfassende Überprüfung der Rechtmäßigkeit der Datenverarbeitung stattfindet, da Rhythmus und Prüftiefe der **nicht überprüfbaren Entscheidung der Kontrollstelle** überlassen wird. Im schlechtesten Fall erfolgt die erste Überprüfung 1 Jahr nach der ersten Anzeige gemäß § 9 Abs. 1 S. 1 (s.u.).

Zu § 4 - Zulassung der Kontrollstellen und Entziehung der Zulassung

Die allgemeinen Anforderungen an Kontrollstellen werden in einer Verordnung nach § 16 Abs. 3 Nr. 2 präzisiert. Dem **BfDI** kommt die Aufgabe zu, die Zulassung zu entziehen. Da jedoch die Kenntniserlangung von Unzulänglichkeiten i.d.R. durch die jeweiligen **Aufsichtsbehörden** erfolgen, wird ein aufwändiges bürokratisches Verfahren etabliert, bei dem letztlich die Feststellung von Rechtsverstößen bei den zertifizierten Stellen zu einem Entzug der Zulassung gegenüber der Kontrollstelle führt bzw. führen kann. Nur die Nichterfüllung der Verpflichtungen des Gesetzes "in schwerwiegender Weise" soll nach Abs. 4 Nr. 2 zur Entziehung der Zulassung führen. Eine derart unbestimmte Regelung gewährt nicht hinreichend die Qualität der Tätigkeit der Kontrollstellen sowie der von ihnen durchzuführenden Kontrollen.

Zu § 5 - Anforderungen an Kontrollstellen

Die Norm konkretisiert die in § 4 Abs. 1 Nr. 1 genannten Anforderungen an Kontrollstellen. Dabei taucht in Abs. 3 die Differenzierung zwischen rechtlicher und technischer Eignung auf, die in einer Kontrollstelle beide vorhanden sein müssen.

Zu § 6 - Pflichten der Kontrollstellen

Abs. 1 S. 1 verpflichtet Kontrollstellen auf Verlangen zum Abschluss eines Auditvertrages "gegen angemessene Vergütung". Über diesen **Kontrahierungszwang** kann nicht gewährleistet werden, dass von Seiten der Kontrollstellen eine seriöse Auditierung erfolgt. Nach Abs. 1 S. 2 Nr. 2 entfällt der Kontrahierungszwang, wenn "das Durchführen der Kontrollen durch eine andere Kontrollstelle sichergestellt ist". Es wird aber nicht gewährleistet, dass tatsächlich genügend qualifizierte Kontrollstellen bereit stehen. Dies kann zur Folge habe, dass Kontrollstellen zu Kontrollen gezwungen sind, die sie nicht durchführen wollen. Dies hätte keine positiven Auswirkungen auf die Qualität der Kontrolle. Wenn die Kontrollstellen nicht freiwillig die Auditierung durchführen, wird i.d.R. eine qualifizierte Kontrolle nicht stattfinden. Die Entbindung vom Kontrahierungszwang soll beim BfDI oder bei der Aufsichtsbehörde in einem bürokratischen Verfahren erfolgen. Dieses Verfahren hat keinerlei datenschutzrechtlichen Mehrwert.

Der Kontrahierungszwang soll nach Abs. 1 S. 1 nur bestehen, wenn eine „angemessene Vergütung“ erfolgt. Die **Angemessenheit einer Vergütung** lässt sich nur beurteilen, wenn die dafür zu erbringende Leistung hinreichend präzise benannt würde. Dies ist aber nicht möglich. Als Mindestleistung würde eine formale, oberflächliche 12- bzw. 18monatige Kontrolle ausreichen (§ 3 S. 4, 5). Damit würde aber kein Mehrwert für den Datenschutz erreicht. Je tiefer gehend und qualifizierter eine Prüfung durchgeführt wird, umso höher wäre eine angemessene Vergütung. Angesichts der Komplexität der regelmäßig vorzunehmenden Prüfungen, lässt sich vorab oft eine Beurteilung der Angemessenheit des Kontrollaufwands nicht vornehmen.

Die Kontrollstelle wird in Abs. 2 zu einem **jährlichen Bericht** gegenüber den Aufsichtsbehörden verpflichtet, an den keine inhaltlichen Anforderungen gestellt werden. So ist auch über diesen Bericht nicht gewährleistet, dass qualifizierte Auditierungen durchgeführt werden.

Nach Abs. 3 S. 1 erteilen die Kontrollstellen einander die für die "ordnungsgemäße Durchführung dieses Gesetzes notwendigen **Auskünfte**". Ob diese Übermittlung obligatorisch oder freiwillig sein soll, ergibt sich aus der Regelung nicht. Da die Kontrollstellen zueinander im Wettbewerb stehen, kann nicht davon ausgegangen werden, dass die notwendige Kommunikation tatsächlich stattfindet. Unklar ist auch, welche Auskünfte als erforderlich angesehen werden. Konflikte zwischen den Kontrollstellen sind vorprogrammiert.

Stellt die Kontrollstelle Datenschutzverstöße fest, so wird sie nach Abs. 3 S. 2, 3 verpflichtet, die zuständige Aufsichtsbehörden und Kontrollstellen zu unterrichten. Um derartige **Unterrichtungen** nicht vornehmen zu müssen, die negative Folgen für die kontrollierte Stelle hätten, wird sich Kontrollstelle veranlasst sehen, so oberflächlich wie möglich zu prüfen. Erfolgt jedoch eine Mitteilung an die Aufsichtsbehörde, so wird das Gegenteil der Entbürokratisierung erreicht, nämlich dass sich mit dem Verstoß sowohl die Kontrollstelle als auch die Aufsichtsbehörde befassen und diese sich insofern koordinieren müssen (vgl. § 7 Abs. 1).

Zu § 7 - Pflichten der zuständigen Behörde

Nach Abs. 1 **überwacht** die Aufsichtsbehörde die **Tätigkeit der Kontrollstelle**. Damit tritt an die Stelle der direkten Kontrolle der Daten verarbeitenden Stelle die Kontrolle der durch die Kontrollstelle durchgeführten Kontrollen. Hierdurch wird - anstelle einer Entlastung der Aufsichtsbehörde - eine zusätzliche Belastung bewirkt. Nach Feststellung eines Datenschutzverstoßes muss nämlich zusätzlich festgestellt werden, wem dieser Verstoß zuzurechnen ist - der unzureichend kontrollierenden Kontrollstelle oder der verantwortlichen Stelle? Im ersteren Fall muss die Aufsichtsbehörde nach Abs. 1 S. 3 die Tatsachen sammeln, die eine Entziehung oder Beschränkung einer Zulassung begründen. Dem schließt sich ein bürokratisches Verfahren der Unterrichtung der für die Entziehung der Zulassung zuständigen Aufsichtsbehörden (v.a. BfDI) an.

Nach Abs. 2 kann die Aufsichtsbehörde die **Entziehung des Datenschutzauditsiegels** anordnen. Gemäß dieser Regelung darf dies aber nur erfolgen, wenn zuvor die Kontrollstelle nach § 6 Abs. 3 S. 2 eine Unterrichtung über einen Datenschutzverstoß vorgenommen hat. Keine Aussage enthält der Entwurf, wenn der Verstoß auf andere Weise der Aufsichtsbehörde bekannt wird. Weitere Voraussetzung ist, dass dieser Entzug "in einem angemessenen Verhältnis" steht. Danach soll das Zertifikat also auch bei Feststellung von Rechtsverstößen beibehalten werden. Dies führt letztlich dazu, dass die Glaubwürdigkeit des Siegels diskreditiert werden kann, zumal es für die Frage, wie die Angemessenheit des Entzugs bewertet werden soll, keinerlei Anhaltspunkte gibt. Bei einem schwerwiegenden Verstoß bzw. einem mit Langzeitwirkung soll eine Auditierung für einen bestimmten Zeitraum untersagt werden können. Dies Regelung ist so gefasst, dass nach Ablauf dieses Zeitraums das Auditsiegel geführt werden kann, ohne dass der Fehler behoben wurde und ohne dass die Behebung kontrolliert worden wäre.

Zu § 8 - Überwachung

Die Regelung begründet eine umfassende **Auskunftspflicht** sowie Duldungspflichten von den nicht-öffentlichen Stellen und von Kontrollstellen gegenüber den Aufsichtsbehörden. Die Ver-

letzung dieser Vorschrift wäre als Ordnungswidrigkeit zu ahnden (§ 17 Nr. 5). Auch die weiteren Überwachungsbefugnisse der Aufsichtsbehörde sind dem § 38 BDSG nachempfunden.

Nach Abs. 5 sollen die Kontrollbefugnisse der Aufsichtsbehörden **entsprechend für die Kontrollstellen** gelten. Eine Missachtung dieser Pflicht zur Mitwirkung an der Kontrolle ist jedoch nicht bußgeldbewehrt. Der Regelung ist auch nicht zu entnehmen, welchen Charakter die Auskunfts- und Duldungspflichten gegenüber den Kontrollstellen haben sollen und wie deren Einhaltung durchgesetzt werden kann.

Zu § 9 - Datenschutzauditsiegel, Verzeichnisse

Nach Abs. 1 soll ein Siegel geführt werden können, wenn die Voraussetzungen des § 1 S. 2 erfüllt sind. Voraussetzung ist also nicht, dass dies von der Kontrollstelle positiv festgestellt wird. Es genügt, dass eine Kontrollstelle per Kontrahierungszwang zur Kontrolle verpflichtet wurde. Damit genügt es für die Führung des Siegels, dass man sich zu einer Auditierung verpflichtet, ohne dass tatsächlich ein Audit durchgeführt sein müsste. Nach Abs. 2 besteht keine Nachweispflicht, dass die Anforderungen erfüllt sind. Eine Anzeige gegenüber dem BfDI soll vielmehr genügen. Dieser soll daraufhin die Stelle in ein von ihm zu führendes **Audit-Verzeichnis** aufnehmen, das jedoch nur eine Bezeichnung des Auditierungsgegenstandes enthalten soll, nicht eine Beschreibung und Bewertung.

Außerdem soll der BfDI nach Abs. 2 ein **Verzeichnis der Kontrollstellen** führen.

Zu § 10 - Gebühren und Auslagen

Nach Abs. 1 kann der BfDI Gebühren und Auslagen erheben; nach Abs. 2 gilt dies auch für die Aufsichtsbehörden.

Zu § 11 - Datenschutzauditausschuss

Ein Datenschutzauditausschuss soll die **Anforderungen an das Audit** festlegen, die über das bestehende Datenschutzrecht hinausgehen können. Gemäß dem Wortlaut darf er keine Gesetzesinterpretation vornehmen, sondern lediglich über das Gesetz hinausgehende Anforderungen formulieren. Um dies aber zu können, bedarf es zunächst einer verbindlichen Feststellung der gesetzlichen Pflichten der verarbeitenden Stellen. Eine derartige bundesweite Feststellung würde tendenziell die in Art. 28 Abs. 1 S. 2 EU-DSRL geforderte Unabhängigkeit beeinträchtigen. Als Beispiele für die Übererfüllung gesetzlicher Regeln werden in Abs. 1 S. 2 genannt: Transparenz, Datensparsamkeit und Stärkung der Stellen des betrieblichen Datenschutzbeauftragten. Dabei wird verkannt, dass die zentralen Fragen einer Auditierung in Bereich der Auslegung des materiellen Rechts und der technisch-organisatorischen Maßnahmen liegen. Hierbei sind wegen der vielen unterschiedlichen möglichen Anwendungsfälle und wegen der sich dauernd weiter entwickelnden Technik die Anforderungen nicht einheitlich festzulegen. Es lassen sich allenfalls für bestimmte Anwendungen (z.B. Videoüberwachung, Online-Shops, Archivierungssysteme, Auswertungsverfahren medizinischer Daten) Schutzprofile entwickeln, denen aber wegen der jeweils weiterhin möglichen Fallgestaltungen nur beispielhafter Empfehlungscharakter zukommen kann, nicht aber förmliche Verbindlichkeit. Es ist

nicht ansatzweise praktisch vorstellbar, in welcher Form der Datenschutzausschuss seiner Aufgabe zur Festlegung von Richtlinien nachkommen soll.

Zu § 12 - Mitglieder des Datenschutzauditausschusses

Die Regelung bestimmt die **Zusammensetzung**, also welche Vertreter von Interessengruppen bzw. Institutionen an dem Ausschuss beteiligt werden soll: 2 Verwaltung Bund, 2 Bundesamt für Sicherheit in der Informationstechnik, 2 BfDI, 2 Verwaltung Länder, 4 Landes-Aufsichtsbehörden, 6 Wirtschaft. Nicht erklärlich ist, weshalb völlig Fachfremde an dem Ausschuss beteiligt werden (Verwaltung Bund, Länder), nicht aber Vertreter der Betroffenen (Verbraucherverbände, Arbeitnehmervertreter). Die Darstellung in der Begründung, dass Vertreter der Verwaltung des Bundes und der Länder "in verschiedener Weise für fachspezifische Vorschriften des Datenschutzes zuständig" seien (S. 19), ist nicht nachvollziehbar. Nach Abs. 1 S. 2 soll die Tätigkeit der Ausschussmitglieder nicht nur weisungsfrei, sondern auch ehrenamtlich, d.h. grundsätzlich unentgeltlich sein. Angesichts der geforderten hohen Qualifikation und des mit der Tätigkeit verbundenen Aufwands - wenn diese wirkungsvoll sein soll - ist es befremdlich, dass hierfür keine Bezahlung erfolgen soll. Dies führt wohl dazu, dass die entsendenden Einrichtungen vorrangig Interessenvertreter benennen, die dann aber nicht in der intendierten Unabhängigkeit agieren können. An der Unabhängigkeit der Ausschusstätigkeit entstehen auch insofern Zweifel, als nach Abs. 3 - wohl im Einvernehmen mit dem BfDI, den obersten Landesbehörden, den Aufsichtsbehörden und den Wirtschaftsverbänden - die Berufung durch das Bundesministerium des Innern erfolgen soll. Das aufwändige Bestellungsverfahren ist ein bürokratischer Vorgang, der keinerlei positive Effekte für den Datenschutz entfaltet.

Zu § 13 - Geschäftsordnung, Vorsitz und Beschlussfassung des Datenschutzauditausschusses

Die Geschäftsordnung des Ausschusses bedarf nach Abs. 1 der Genehmigung durch das Bundesministerium des Innern (BMI). Der Ausschuss beschließt nach Abs. 3 Nr. 1 über die "Richtlinien zur Verbesserung des Datenschutzes und der Datensicherheit" nach § 11 Abs. 1 S. 2 mit der Mehrheit von zwei Dritteln. Dies hätte zur Folge, dass die Richtlinien geprägt wären von **Kompromissen**.

Zu § 15 - Rechtsaufsicht

Nach Abs. 1 und 2 soll der Ausschuss der Aufsicht des BMI unterliegen, das gegenüber dem Ausschuss weitgehende direktive Kompetenzen erhält. Nach Abs. 3 S. 1 müssen Richtlinienbeschlüsse durch die Aufsichtsbehörde, also das BMI, genehmigt werden. Nach Abs. 4 hat das BMI sogar das Recht, den Datenschutzauditausschuss aufzulösen. Angesichts eines derart **rigiden und bürokratischen Verfahrens** bestehen Zweifel, ob der Ausschuss die ihm auferlegten Aufgaben wirksam und unabhängig erfüllen kann. Die technischen und rechtlichen Herausforderungen verlangen Flexibilität und schnelle Reaktionsfähigkeit. Es könnte sich der Zustand einstellen, dass die Tätigkeit des Ausschusses eher innovationshindernd als -fördernd ist.

Zu § 16 - Verordnungsermächtigungen

Abs. 1 S. 1 Nr. 2 und Abs. 2 sehen vor, dass zugelassene Kontrollstellen von den Ländern bzw. vom BMI mit den Aufgaben der staatlichen Aufsicht beliehen werden können. Die Notwendigkeit einer solchen **Beleihung** ist nicht erkennbar. Die Übertragung der Kontrolle von Privaten, die Aufgaben der staatlichen Aufsicht wahrnehmen sollen, auf weitere Private, die zugleich mit den Kontrollierten in Konkurrenz stehen, wäre ein Sichentziehen aus der Verantwortung durch den Staat. Die Beleihung soll v.a. durch das BMI erfolgen, was wohl mit Art. 28 Abs. 1 S. 2 EU-DSRL nicht vereinbar ist, da eine Aufgabe des europarechtlich unabhängigen BfDI (bzw. der Landesbehörde) auf ein privates Unternehmen übertragen würde, das (wohl?) der Rechtsaufsicht des BMI unterläge.

Nach Abs. 3 erhält das BMI die Ermächtigung zum Erlass einer Rechtsvorordnung, in der alle Einzelheiten "über die Voraussetzungen und das Verfahren der Zulassung ... sowie ... der Entziehung der Zulassung" von Kontrollstellen sowie die "Mindestkontrollanforderungen und im Rahmen des **Kontrollverfahrens** vorgesehene Vorkehrungen festzulegen" sind. Es bestehen Zweifel, dass mit einer derart rigiden Regulierung durch das BMI, das selbst über keinerlei praktische Kontrollerfahrung verfügt, hinreichende Voraussetzungen für die freiwillige Nutzung des Auditinstruments geschaffen werden können.

Zu § 17 - Bußgeldvorschrift

Für die Verletzung von formellen Pflichten soll eine Geldbuße bis zu 300.000 Euro verhängt werden können. Diese Bußgeldhöhe steht im Widerspruch zu dem parallelen geplanten § 43 Abs. 3 BDSG, wonach die maximale **Bußgeldhöhe** bei formellen Verstößen gegen das BDSG mit 50.000 Euro vorgesehen ist. Dies hätte zur Folge, dass bei Teilnahme an dem freiwilligen Audit das Bußgeldrisiko versechsfacht würde, was der Bereitschaft zur Teilnahme für Unternehmen nicht förderlich wäre.

Zu § 18 - Strafvorschrift

Der **Abschreckungseffekt** von einer Auditierung würde durch die Strafandrohung bei absichtsvoller unbefugter Verwendung des Datenschutzauditsiegels noch weiter erhöht. Eine strafrechtliche Sanktionierung bei formellen Verstößen war und ist im BDSG bisher nicht vorgesehen.

III. Änderung des Bundesdatenschutzgesetzes (BDSG), Art. 2

III. 1. Allgemeine Bemerkungen

Ein großes **Problem des sog. Listenprivilegs** liegt in der mangelnden Transparenz für Verbraucherinnen und Verbraucher. Nach einem Verkauf der Daten ist für diese letztlich nicht mehr nachvollziehbar bzw. nur unter erheblichen Aufwand an Zeit und Porto feststellbar, welche Firmen Zugriff auf ihre Daten haben und an wen diese weitervermittelt wurden. In der Aufsichtspraxis zeigt sich, dass die Verbraucher kaum eine Chance haben, die Verkaufskette vernünftig nachzuvollziehen und zu kontrollieren, um sich gegen Bewerbungen und damit ver-

bundene Belästigungen und Eingriffe zu schützen.

Wird der Datenverkauf von einer Einwilligungserklärung des Betroffenen abhängig gemacht, muss der Betroffene konkret darüber informiert werden, wer seine Daten bekommt (**klare Benennung der Empfänger**). Der Betroffene hat einen konkreten Ansprechpartner, nämlich die Daten erhebende Stelle. Diese kann ihre Hände nicht mehr unter Verweis auf das sog. Listenprivileg in Unschuld waschen, sondern zeichnet dafür verantwortlich, dass die Zustimmung des Verbrauchers zur Weitergabe vorliegt. Sollten die Daten an anderer Stelle auftauchen, kann das Unternehmen zur Verantwortung gezogen werden. Eine klare Unterscheidung zwischen zulässigem und unzulässigem Verkauf wird möglich und auch für die Betroffenen nachvollziehbar.

In der Praxis bleibt es nicht beim Verkauf und bei der Vermietung des beschränkten Datensatzes nach dem Listenprivileg. Adresshändler werben mit Listen von Adressen, die nach sehr differenzierten Merkmalen, z.B. nach Wohnumfeld, Onlineaktivitäten und Interessengebieten, selektiert sind. Im Beispielsfall handelt es sich um drei Gruppenmerkmale i.S.d. § 28 Abs. 3 Nr. 3 BDSG, über welche die Listen miteinander verschnitten sind. Durch diese Verschneidungen bzw. Datenanreicherungen entstehen immer **detailliertere Profile** über die Verbraucher, deren Erstellung mit dem Listenprivileg im rechtlichen Sinne nicht gerechtfertigt werden kann.

Ergänzend verweisen wir auf die Ausführungen des ULD in der Stellungnahme zum BDSG-Entwurf (Stand 22.10.08) (https://www.datenschutzzentrum.de/bdsg-novellierung/20081029-Stellungnahme-bdsg-e.pdf) sowie auf die Ausführungen in der Stellungnahme zum Permission Marketing (https://www.datenschutzzentrum.de/wirtschaft/20081125-permission-marketing.html) sowie in der Stellungnahme zum Änderungsbedarf im BDSG (https://www.datenschutzzentrum.de/bdsg-novellierung/20080924-uld-aenderungsbedarf-bdsg.pdf).

III. 2. Zu den spezifischen Regelungen

Zu § 4f Absatz 3 Sätze 5, 6, 7 - Betrieblicher Datenschutzbeauftragter

Die Regelung eines **Kündigungsschutzes** für den betrieblichen Datenschutzbeauftragten ist zu begrüßen. Das Wort „Abberufung“ in Satz 6 der neuen Regelung kann allerdings Verwirrung stiften. Nach § 38 Abs. 5 S. 3 BDSG ist die Abberufung eines Beauftragten der zuständigen Aufsichtsbehörde für den Fall vorbehalten, dass der Beauftragte nicht die erforderliche Fachkunde und Zuverlässigkeit besitzt. Für die Beendigung der Bestellung durch die Daten verarbeitende Stelle selbst kennt das Gesetz den Begriff „Widerruf“ (§ 4f Abs. 3 S. 4).

Der Entwurfswortlaut kann zu dem Missverständnis führen, dass nur in Fällen der Abberufung durch die Aufsichtsbehörde der nachträgliche Kündigungsschutz eingreifen soll. Laut Gesetzesbegründung soll sich die Kündigungsschutzfrist auf ein Jahr nach „**Beendigung des Amtes des Beauftragten**“ erstrecken, d.h. es sollen alle möglichen Fälle der Beendigung erfasst sein. Die Bestellung kann z.B. befristet ausgesprochen sein und nach Fristablauf auslaufen. Es kann eine einvernehmliche Beendigung erfolgen bzw. der Beauftragte kann einseitig sein

Amt niederlegen. Gerade in diesen Fällen sollte der nachträgliche Kündigungsschutz zum Tragen kommen, so dass sich insofern eine Konkretisierung des Wortlautes empfiehlt.

Die in Abs. 3 S. 7 vorgenommene weitere **Konkretisierung der Unterstützungspflicht** ist positiv zu bewerten. Systematisch passt sie aber besser in § 4f Abs. 2 oder Abs. 5 BDSG.

Zur Anpassung der Überschrift des § 28 BDSG

Nicht ersichtlich ist, warum die Überschrift des § 28 BDSG an „die Überschrift des § 29“ (Entwurfsbegründung S. 26) angepasst, d.h. dahingehend geändert wird, dass die Verarbeitung und Nutzung in der Überschrift nicht mehr erwähnt wird. Die Tatbestände des § 28 BDSG ermöglichen auch nach einer Änderung durch den Gesetzesentwurf eine Verarbeitung und Übermittlung von Daten zu eigenen Geschäftszwecken. Diese Verwendungsbefugnisse sollten auch durch eine Nennung in der Überschrift zum Ausdruck kommen.

Zu § 28 Absatz 3 n.F. - Werbung u. Markt- und Meinungsforschung

Insbes. zu § 28 Abs. 3 S. 1 und S. 2

Die Regelung im § 28 Abs. 3 BDSG ist insgesamt zu begrüßen. Es wird eine einheitliche Regelung zur Verarbeitung von Daten zu Werbezwecken geschaffen, die eine **Spezialregelung zu § 28 Abs. 1 BDSG** darstellt. Die Rechtslage in Bezug auf die Datenverarbeitung zu Werbezwecken wird dadurch wesentlich vereinfacht. Die Verarbeitung setzt nicht mehr eine durch die verantwortliche Stelle durchzuführende Interessenabwägung voraus. Dabei ist von zentraler Bedeutung, dass § 28 Abs. 3 S. 1 BDSG-E eindeutig die grundsätzliche Regel für die Datenverarbeitung zu Werbezwecken festlegt, nämlich dass die Verarbeitung und Nutzung personenbezogener Daten für Zwecke des Adresshandels, der Werbung oder der Markt- oder Meinungsforschung von der Einwilligung des Betroffenen abhängig gemacht wird.

Systematisch stellt sich die Frage, warum die **Zwecke des Adresshandels** in Satz des § 28 Abs. 3 BDSG-E behandelt werden. § 28 BDSG erfasst nur solche Fällen, in denen Daten zu eigenen Geschäftszwecken verwendet werden. Der Adresshandel ist typischerweise ein Fall der Datenverarbeitung zum Zwecke der Übermittlung, d.h. eine Datenverwendung, die im Übrigen von § 29 BDSG geregelt wird. Selbst wenn eine Daten verarbeitende Stelle die Daten für eigene Geschäftszwecke erhebt und diese dann zweckändernd für Zwecke des Adresshandels weiterverarbeitet, entspricht dies einer Verwendung nach § 29 BDSG. Ein- und dieselbe Stelle kann sowohl eine Datenverarbeitung nach § 28 als auch nach § 29 BDSG durchführen. Die Neuregelung für die Datenverarbeitung zum Zwecke des Adresshandels passt daher besser zu § 29 BDSG.

Bei allen erfreulichen Neuerungen – die Bundesregierung hat sich nicht durchringen können, zur Wahrung bzw. Herstellung der Selbstbestimmung der Betroffenen auf das Listenprivileg völlig zu verzichten und damit ein echtes „Permission Marketing“ vorzuschlagen. Es sind mehrere **Ausnahmen vom Permission Marketing** vorgesehen. Gemäß der Einschränkung nach Abs. 3 S. 2 Nr. 1 BDSG dürfen Listendaten zur Werbung für eigene Angebote verwendet werden. § 28 Abs. 3 S. 1 Nr. 1 BDSG-E lässt dabei sowohl die Nutzung als auch die Verarbei-

tung, d.h. auch die Übermittlung, der Daten zu. Unklar ist, welche Vorgänge in der Praxis damit erfasst werden sollen. Wenn ein Unternehmen Daten im sog. Lettershop-Verfahren an einen externen Dienstleister herausgibt, also die Etikettierung sowie die Versendung der Werbebriefe vornimmt, geschieht dies typischerweise in Form einer Auftragsdatenverarbeitung nach § 11 BDSG. In diesem Fall ist der Tatbestand der Übermittlung nicht gegeben; vielmehr handelt es sich um eine Nutzung der Daten, da das Handeln des Auftragnehmers rechtlich dem Auftraggeber zugeordnet wird. Eine Übermittlung setzt voraus, dass die Daten an einen Dritten, d.h. an eine i.S.d. BDSG eigenverantwortlich handelnde Stelle, herausgegeben werden.

Gemäß § 28 Absatz 3 Satz 6 wird der Empfänger der Daten zwar verpflichtet, diese nur für den Zweck zu nutzen, zu dem ihm die Daten übermittelt wurden. Anders als bei der Weitergabe im Wege der Auftragsdatenverarbeitung verlassen die Daten bei der Übermittlung den Herrschafts- und Kontrollbereich und rechtlich gesehen den Verantwortungsbereich der erhebenden Stelle. Werden die Daten **nach einer Übermittlung zweckentfremdet** und missbräuchlich durch den Empfänger verwendet, kann sich der Betroffene nicht an seinen Vertragspartner halten, sondern muss versuchen, seine Daten bei dem Dritten „einzusammeln". Auch wenn diese Daten gesetzlich nur zweckgebunden verarbeitet werden dürfen, erweitert sich durch die Freigabe der Daten zur Übermittlung der Kreis derjenigen, die mit den Daten eigenverantwortlich arbeiten dürfen, so dass sich die Gefahr des Missbrauchs erhöht.

Aus der Entwurfsbegründung (S. 29) wird nicht deutlich, ob die Regelung des § 28 Abs. 3 S. 6 BDSG-E eine Spezialregelung zu § 28 Abs. 5 BDSG sein soll. In der Entwurfsbegründung heißt es, dass der Satz 6 eine „im Bundesdatenschutzgesetz übliche Zweckbindung" enthält, „wie sie sich unter anderem in Absatz 5 Satz 1 für Dritte befindet". Auch die Zweckbindung des § 28 Abs. 3 S. 6 BDSG-E enthält eine Regelung für „Dritte", da die Daten ja übermittelt werden. Nach der Definition der Übermittlung in § 3 Abs. 4 Nr. 3 BDSG erfolgt diese Datenweitergabe an Dritte. Handelt es sich nicht um eine vorrangige Regelung, so ergibt sich über den § 28 Abs. 5 S. 2 BDSG eine erweiterte Nutzungsmöglichkeit der Listendaten für den Empfänger nach § 28 Abs. 2 Nr. 1 BDSG-E i.V.m. § 28 Abs. 1 S. 1 Nr. 2 BDSG oder § 28 Abs. 2 Nr. 2 BDSG-E (z.B. zur Wahrung berechtigter Interessen Dritter). Der Empfänger könnte danach die Daten unter der Voraussetzung des § 28 Abs. 3 S. 2 Nr. 2 und Nr. 3 BDSG-E **auch für Werbezwecke nutzen** und gem. § 28 Absatz 3 Satz 3 BDSG-E Daten hinzuspeichern. Dies entspräche nicht der Intention des Entwurfs, der die Datenverarbeitung zu Werbezwecken grundsätzlich von der Einwilligung des Betroffenen abhängig machen möchte.

Die Privilegierung der Werbung für Spendenunternehmen liegt nach den Praxiserfahrungen der Datenschutzaufsichtsbehörden nicht im Interesse des Schutzes informationeller Selbstbestimmung. Danach erfolgt durch gemeinnützige Vereine und sonstige Einrichtungen regelmäßig kein sorgsamerer Umgang mit den Daten der Betroffenen. Eine Privilegierung beim Verfolgen gemeinnütziger, mildtätiger oder kirchlicher Zwecke mag mit der Ziel der finanziellen Förderung zu begründen sein. Die Belästigungswirkungen und die persönlichkeitsrechtliche Beeinträchtigungen können aber bei gemeinnützigen, mildtätigen und kirchlichen Zwecken denen rein kommerzieller Zielsetzung entsprechen.

Insbes. zu § 28 Abs. 3 S. 3 und S. 4

Der Anwendungsbereich des § 28 Abs. 3 S. 3 BDSG-E bleibt auch nach der Lektüre der Entwurfsbegründung unverständlich. Die Begründung erklärt, dass der verantwortlichen Stelle die Möglichkeit eröffnet werden soll, rechtmäßig erhobene Daten dem eigenen **Datenbestand hinzuzuspeichern**, um diesen für Zwecke der Eigenwerbung zu selektieren und die Kunden gezielter ansprechen zu können. Die Selektion eines Kundendatenbestandes ist zunächst eine Nutzung oder Veränderung von Daten; erst danach erfolgt eine Datenspeicherung. Weder die Nutzung noch die Veränderung sind nach § 28 Abs. 3 S. 3 BDSG-E jedoch erlaubt.

Eine Nutzungsbefugnis der hinzu gespeicherten Daten ergibt sich dann aus § 28 Abs. 3 S. 4 BDSG-E. Die Entwurfsbegründung bezieht die Regelung ausschließlich auf Fälle der sog. Beipackwerbung, d.h. dass der Kunde per Post angesprochen wird. Allerdings wäre es nach dem Wortlaut des § 28 Abs. 3 S. 3-4 BDSG-E ebenso vorstellbar, dass die Telefonnummer des Betroffenen gem. § 28 Abs. 3 S. 3 BDSG-E, die zuvor entweder beim Betroffenen selbst oder aus allgemein zugänglichen Quellen erhoben wurde, dem Werbedatensatz des Kunden zugespeichert und dann im Rahmen von § 28 Abs. 3 S. 4 BDSG-E zu sog. Cross-Selling-Maßnahmen im Unternehmensverbund genutzt wird. Eine solche Vorgehensweise hat der Bundesgerichtshof (BGH-Rechtsprechung – Telefonwerbung I-IV) bisher für einwilligungsbedürftig angesehen. Die Formulierung des Gesetzes müsste deutlich machen, dass die Werbeansprache – wenn überhaupt – **nur per Post** erfolgen darf. Zu diesem Ergebnis kann man derzeit nur durch Auslegung unter Heranziehung des § 28 Abs. 3 S. 4 BDSG-E „zusammen … mit der Durchführung eines rechtsgeschäftlichen oder rechtsgeschäftsähnlichen Schuldverhältnisses“ sowie des § 28 Absatz 3 Satz 5 BDSG-E kommen.

Zu § 28 Abs. 3a - Anforderung an Einwilligung

Die **Klarstellung der Gestaltungsform** einer wirksamen Einwilligung in § 28 Abs. 3a BDSG-E ist zu begrüßen. Sie trägt dazu bei, dass es für die wirksame Einwilligung auf eine selbstbestimmte bewusste Erklärung und nicht – wie in der Praxis häufig zu finden – auf die bestmögliche Überrumpelung des unaufmerksamen oder unentschiedenen Verbrauchers ankommt. Nicht eindeutig ist, ob die Klarstellungen nach § 28 Abs. 3a BDSG-E nur für die Werbeeinwilligung nach § 28 Abs. 3 S. 1 BDSG-E gelten sollen. Die ausdrückliche Nennung in § 28 Abs. 3 S. 1 BDSG-E sowie die Ausführungen in der Entwurfsbegründung deuten in diese Richtung. Es wäre wünschenswert, dass die Anforderungen von Absatz 3a BDSG-E für alle Einwilligungserklärungen gelten.

Zu § 28 Abs. 3a und 3b - Koppelungsverbot

Die Regelung des Koppelungsverbotes in § 28 Abs. 3b BDSG ist missglückt; sie wird in der Praxis genau den gegenteiligen Effekt des Angestrebten erzielen. Gemäß der Gesetzesbegründung soll Abs. 3b die Position des Betroffenen stärken. Durch den Ausnahmecharakter des Koppelungsverbotes wird aber letztlich der Schutz des Betroffenen aus § 4a BDSG beschränkt. Gemäß der Gesetzesbegründung wird eine umfassendere Normierung des Koppelungsverbots durch die Vertragsgestaltungsfreiheit verhindert. Die datenschutzrechtliche Einwilligung ist eine einseitige Erklärung und kein Vertragsgegenstand. Es geht mit dem Koppelungsverbot gerade darum, die Autonomie des Betroffenen zur Abgabe von Einwilligungen vor

der einseitigen Festlegung durch den ökonomisch Stärkeren zu schützen. Gem. § 4 Abs. 1 BDSG ist die Verarbeitung personenbezogener Daten nur dann erlaubt, wenn der Betroffene entweder einwilligt, oder wenn das Gesetz (z.B. in § 28 Abs. 1 Nr. 1 BDSB: Vertragsverhältnis) einen Rechtfertigungstatbestand vorsieht. Der Gesetzgeber sieht die Einwilligung als einen vom Vertragsverhältnis vollkommen unabhängigen eigenständigen Rechtfertigungstatbestand an. Der Gesetzgeber hat mit § 4 Abs. 1 BDSG und § 28 Abs. 1 Nr. 1 zum Ausdruck gebracht, dass die im Rahmen eines Vertragsverhältnisses als „Nebenprodukt" stattfindende Datenverarbeitung nicht automatisch **Bestandteil des Vertragsgegenstands** werden soll. Das Unternehmen soll die im Rahmen der Vertragsabwicklung erhaltenen Daten nicht einfach zum Verfügungsgegenstand machen dürfen. Vielmehr dürfen Daten nur für die Erfüllung des Vertrages Verwendung finden; nur soweit kann auch die Vertragsautonomie nur gehen. Eine Einbeziehung in einen Vertrag kann nur dadurch erfolgen, dass personenbezogene Daten selbst zum Vertragsgegenstand gemacht werden und als „Ware" gegen eine Gegenleistung ausgetauscht werden. Dieser Grundsatz wird unterlaufen, wenn durch Absatz 3b zum Ausdruck bringt, dass auch die Einwilligungserklärung des Betroffenen der Vertragsgestaltungsfreiheit und damit der Festlegung durch den ökonomisch stärkeren Vertragspartner unterworfen wird.

Zur Streichung des § 28 Absatz 3 Satz 2 a.F. – besonders geschützte Daten

Der § 28 Abs. 3 S. 2 a.F. wird in der Regelung des BDSG-E ersatzlos gestrichen. Darin wird klargestellt, dass ein überwiegendes Schutzinteresse des Betroffenen besteht bei Daten zu Strafverfahren und Ordnungswidrigkeiten sowie zu Arbeitsverhältnissen. Laut Entwurfsbegründung sei dieser „infolge der Neuregelung in Absatz 3 entbehrlich geworden". Dies ist nicht der Fall. Die Streichung des Absatzes 3 Satz 2 stellt eine Schlechterstellung des Betroffenen dar. Auch nach den neuen Regelungen zur Datenverarbeitung zu Werbezwecken dürfen **Listendaten übermittelt** werden. Es erschließt sich nicht, warum in diesen Fällen die Einschränkungen des § 28 Abs. 3 S. 2 a.F. keine Geltung mehr erlangen sollen.

Zu § 28 Absatz 4 - Widerspruchsrecht

Die zusätzliche Informationspflicht über das Widerspruchsrecht zum Zeitpunkt des Vertragsschluss ist zu begrüßen. Unklar ist, warum die **Pflicht zur Sperrung** der Daten nach Widerspruch des Betroffenen nach wie vor nur den Dritten treffen soll, dem die Daten übermittelt wurden. Es wäre sinnvoll, auch die erhebende Stelle ausdrücklich zu verpflichten, die Daten für Werbezwecke zu sperren.

Äußerst fragwürdig ist die Ergänzung in § 28 Abs. 4 S. 4 BDSG-E. Nach allgemeiner Ansicht unterlag der Widerspruch bisher keinen **Formvorgaben**; d.h. solche durften auch nicht durch die Daten verarbeitende Stelle festgelegt werden. Warum dies für die verantwortliche Stelle nun ermöglicht werden soll, ist nicht ersichtlich.

Zu § 29 - Verarbeitung zum Zweck der Übermittlung

Der Gesetzesentwurf sieht vor, dass der Verweis des § 29 Abs. 1 S. 2 auf den § 28 Abs. 1 S. 2 ersetzt werden soll durch den Verweis auf § 28 Abs. 1 S. 1 sowie § 28 Abs. 3-3b BDSG-E. Diese Neureglung ist nicht nachvollziehbar. Die Entwurfsbegründung bezeichnet sie als „notwendige **redaktionelle Änderungen und Folgeänderungen**“, obwohl es sich hier um eine inhaltliche Neuregelung handelt. Weitere Erläuterungen enthält die Entwurfsbegründung nicht. Der § 28 Abs. 1 S. 2 BDSG a.F. ist durch den Gesetzesentwurf nicht betroffen, d.h. die Regelung ist weder geändert noch gestrichen worden. Nach § 28 Abs. 1 S. 2 BDSG wird die verantwortliche Stelle verpflichtet, die Zwecke der Verarbeitung bei der Erhebung konkret festzulegen. Dass diese Vorgabe für die Datenverarbeitung nach § 29 BDSG nun keine Bedeutung mehr haben soll, ist weder verständlich noch vertretbar. Dabei kann es sich nur um ein redaktionelles Versehen handeln.

Darüber hinaus ist unverständlich, warum in § 29 Abs. 1 S. 2 auf alle Regelungen des **§ 28 Abs. 3-3b verwiesen** wird. Für die Datenverarbeitung nach § 29 BDSG ist ausschließlich die Regelung des § 28 Abs. 3 S. 1 und des § 28 Abs. 3a BDSG-E sowie, wenn überhaupt, noch die Regelung des § 28 Abs. 3 S. 2 Nr. 2 und Nr. 3 einschlägig. Die Entwurfsbegründung erklärt, dass „die Änderungen in § 28 Absatz 3 bis 3b auch für die geschäftsmäßige Erhebung, Speicherung oder Veränderung personenbezogener Daten zum Zweck der Übermittlung gelten“. Das macht allerdings vor dem Hintergrund keinen Sinn, dass die Werbenutzung des § 28 Abs. 3 S. 2 Nr. 1 BDSG-E gerade daran anknüpft, dass die Daten zu "eigenen Geschäftszwecken" verarbeitet werden und beim Betroffenen selbst nach § 28 Abs. 1 S. 1 Nr. 1 BDSG erhoben sein müssen. Dies ist typischerweise bei einer geschäftsmäßigen Datenverarbeitung zum Zwecke der Übermittlung, etwa bei einem Adresshändler, nicht der Fall. Die Stellen, die nach § 29 BDSG Daten verarbeiten, unterhalten regelmäßig kein Vertragsverhältnis zum Betroffenen und werben auch nicht für „eigene Angebote“. Sollte dies doch der Fall sein, richtet sich die Datenverarbeitung ohnehin nach § 28 BDSG. Dafür bedarf es keines Verweises.

Zudem ist auch ein **Verweis auf § 28 Abs. 3 S. 2 Nr. 2-3** BDSG-E fraglich. Diese Vorgaben machen die Datenverarbeitung und -übermittlung davon abhängig, dass sie zum Zwecke der Werbung "erforderlich" sind. Erforderlich kann eine Datenverwendung aber immer nur in Bezug auf ein konkretes mit der Datenverarbeitung zu erreichendes Ziel sein. Der § 29 BDSG sieht traditionell keine Erforderlichkeit vor, da das Geschäftsziel hier die Übermittlung an einen Dritten ist, d.h. es werden weiter keine eigenen Geschäftszwecke verfolgt. Ob die Datenübermittlung zum Zwecke der Werbung durch den Dritten erforderlich ist, vermag das übermittelnde Unternehmen kaum zu überprüfen. Gleiches gilt für den neu eingeführten Verweis in § 29 Abs. 2 S. 2 BDSG-E.

Zu § 42a - Breach Notification

Die Regelung eine **Informationspflicht bei unrechtmäßiger Kenntniserlangung von Daten** ist vom Grundsatz her zu begrüßen. Allerdings lassen sich zwei Hauptproblempunkte identifizieren: Zum einen knüpft die Regelung an die konkrete Kenntnisnahme durch einen Dritten an, da auf die „Übermittlung“ bzw. die in sonstiger Weise erfolgte unrechtmäßige Kenntniserlangung durch Dritte abgestellt wird. Die Unterrichtungspflicht setzt damit erst ein, wenn der nichtöffentlichen Stelle bekanntgeworden ist, dass ein Dritter auf die Daten zugegriffen hat und nicht schon zu einem Zeitpunkt, zu dem der Zugriff möglich gewesen wäre. Darüber hin-

aus wird in § 42a BDSG-E die nichtöffentliche Stelle erwähnt. In der Entwurfsbegründung ist allerdings von der „verantwortlichen Stelle“ die Rede. Unklar ist danach, ob und in welcher Form die Unterrichtungspflicht auch den Auftragsdatenverarbeiter trifft.

Mit freundlichen Grüßen

Dr. Thilo Weichert
(Leiter des Unabhängigen Landeszentrums für Datenschutz Schleswig-Holstein – ULD)