Erste Stellungnahme des ULD zum Referentenentwurf (Stand 07.09.2007) des Bundesministeriums des Innern (BMI) eines Bundesdatenschutzauditgesetzes (BDSAuditG)

vom 28.09.2007

Zum Vorschlag allgemein

Die Intention des Gesetzentwurfes ist sehr zu begrüßen. Die Umsetzung der Vorgabe des Bundesgesetzgebers aus dem Jahr 2001 in § 9a BDSG zur **Stärkung des Datenschutzes über Marktinstrumente** ist überfällig. Der in der Wirtschaft bestehende Bedarf nach datenschutzrechtlicher Zertifizierung kann mit den bisherigen rechtlichen Regelungen nicht ausreichend befriedigt werden.

Der Entwurf geht nicht substantiiert darauf ein, weshalb er dem **erfolgreichen Regelungsansatz des Landes Schleswig-Holstein** in § 4 Abs. 2 Landesdatenschutzgesetz (LDSG SH) nicht folgt, der eine öffentlich-rechtliche Zertifizierung auf der Basis von privaten Gutachten vorsieht (Datenschutz-Gütesiegel). Dieses Konzept hat sich in mehr als 5 Jahren in jeder Hinsicht bewährt und wurde von der Europäischen Kommission mit einem Europäischen Innovationspreis prämiert. In der Folge fördert die Europäische Kommission derzeit ein internationales Projektes, in dem das Datenschutz-Gütesiegel Schleswig-Holstein unter dem Begriff „European Privacy Seal" (EuroPriSe) in 8 Staaten der Europäischen Union eingeführt wird. Bedauerlicherweise sind diese internationalen Vorarbeiten in den bisherigen Referentenentwurf nicht eingeflossen, obwohl dem BMI diese Aktivitäten bekannt sind. Auf diese Weise entsteht die Gefahr eines nationalen Sonderweges.

Der Entwurf begründet sein Abweichen vom Datenschutzaudit in Schleswig-Holstein damit, dass eine „zweite Überprüfung durch die Datenschutzaufsichtsbehörde des Landes, in dem das Unternehmen, welches das Datenschutzaudit beantragt, seine Hauptniederlassung hat", entbehrlich werde und so ein „unbürokratisches Verfahren gewährleistet" sei. Wie zu den Einzelregelungen unten näher dargelegt ist, wird mit dem gewählten Vorgehen das Verfahren jedoch komplizierter, im Ergebnis aufwändiger und bürokratischer; die Grundlage für vielfältige Konflikte wird geschaffen. Der Entwurf verkennt die Notwendigkeit der Qualitätssicherung der Gutachten, um Gesetzeskonformität der Auditgegenstände und eine Vergleichbarkeit der Zertifizierung zu gewährleisten. Dem Grundanliegen des Entwurfes, ein möglichst einfaches, wirksames und **bürokratiearmes Verfahren** zu suchen, kann jedoch vollständig zugestimmt werden.

Der Entwurf ist als **Diskussionsgrundlage** sicherlich sinnvoll. Bevor der Entwurf in das Gesetzgebungsverfahren eingebracht wird, bedarf es aber der Klärung von Grundsatzfragen mit den von dem Entwurf betroffenen Stellen. Die Erfahrungen aus Schleswig-Holstein sowie die bisherigen nationalen und internationalen Aktivitäten müssen berücksichtigt werden. Die Vorlage des Gesetzentwurfes durch das BMI kann als Startschuss verstanden werden für die Erarbeitung eines national wie europaweit wirksamen Modells der Datenschutzzertifizierung.

Zu einzelnen Regelungen

§ 1 Datenschutzaudit

Absatz 1 beschreibt den Umfang der Prüfung und Bewertung durch ein Datenschutzaudit. Hierbei greift der Regelungsvorschlag die Formulierung des § 9 a BDSG auf, die „Datenschutzkonzept" und „technische Einrichtungen" als Objekte der Auditierung benennt. Die Erfahrungen in Schleswig-Holstein haben gezeigt, dass ein derart begrenzter Ansatz den Bedürfnissen der Praxis nicht gerecht wird: Von Marktrelevanz für den Datenschutz sind nicht nur Einrichtungen, sondern eine Vielzahl von **Verfahren und Produkten**, die nicht lediglich technisch beschrieben werden, sondern deren relevante Merkmale personeller, organisatorischer oder gar normativer Art sein können. Dies gilt beispielsweise für die Anbieter von Auftragsdatenverarbeitungsprozessen, deren vertragliche Bindung an einen Auftraggeber entscheidenden Einfluss auf die Vereinbarkeit mit dem Datenschutzrecht hat und daher Gegenstand eines Datenschutzaudits sein muss.

Unklar ist, warum der Gesetzentwurf das Zertifikat nicht auch den Herstellern von **Soft- und Hardwareprodukten** anbietet. Mangels Regelungskompetenz kann der Bund nicht in und für Landesbehörden durchgeführte Auditverfahren betreffen.

Der **Ausschluss der Sicherheitsprüfung** informationstechnischer Systeme und Komponenten in Absatz 3 konterkariert die datenschutzrechtlichen Anforderungen, die der Entwurf in Absatz 1 an eine Datenschutzauditierung stellt. Materiell handelt es sich – wie Absatz 1 zutreffend formuliert – um eine Prüfung und Bewertung „mit den Vorschriften des Datenschutzes". Diese umfassen das materielle und das prozedurale Datenschutzrecht einschließlich der Vorschriften zur Datensicherheit durch technisch-organisatorische Maßnahmen (§ 9 BDSG). Eine Datenschutzauditierung ohne Prüfung der technisch-organisatorischen

Sicherheitsmaßnahmen bleibt aussage- und damit sinnlos und ignoriert eine grundlegende Anforderung des Datenschutzrechts (Art. 17 Europäische Datenschutzrichtlinie/EU-DSRL – Sicherheit der Verarbeitung).

Eine Datenschutzzertifizierung kann sich auf eine zuvor erfolgte **Sicherheitszertifizierung** durch das Bundesamt für Sicherheit in der Informationstechnik (BSI) nach § 4 BSI-Gesetz stützen. Die Erfahrungen des ULD aus über 40 Gütesiegelverfahren zeigen, dass eine qualitativ gute sicherheitstechnische Konzeptionierung eines Produktes in der Regel eine solide **Grundlage für eine Datenschutzzertifizierung** darstellt. Dabei ist allerdings zu berücksichtigen, dass sich Zielgruppe und Zielrichtung des BSI-Sicherheitszertifikats von einem Datenschutz-Gütesiegel unterscheiden können. Das Datenschutzzertifikat adressiert eine Aussage zum Datenschutz gegenüber den Betroffenen, deren Daten mit dem Produkt oder Verfahren verarbeitet werden. Das Sicherheitszertifikat hat eine weitaus geringere Verbraucherrelevanz und wird häufig im Rahmen eines internen Riskmanagements oder zur Qualitätssicherung zwischen Unternehmen verwendet. Die Erfahrungen aus Schleswig-Holstein zeigen, dass Erkenntnisse aus der BSI-Zertifizierung für eine Datenschutzzertifizierung berücksichtigt werden können und sollten. Fehlt allerdings eine solche BSI-Zertifizierung, dann erweitert sich der Prüfungsumfang der Datenschutz-Zertifizierung notwendig um die Erfüllung der gesetzlich vorgeschriebenen Sicherheitsanforderungen nach § 9 BDSG (bzw. Art. 17 EU-DSRL).

§ 2 Sachverständige

Die **Akkreditierung** der Sachverständigen **durch die Aufsichtsbehörde** gem. Absatz 1 ist eine mögliche Form der Zulassung als Gutachter. Im Interesse einer erhöhten Wirtschaftsnähe könnte die Akkreditierung auch von einzelnen regionalen Industrie- und Handelskammern oder anderen vergleichbaren Organisationen wahrgenommen werden. Es ist kein rechtlicher oder sonstiger Grund erkennbar, warum die Tätigkeit der Sachverständigen örtlich gebunden sein muss. Die Erfahrungen aus Schleswig-Holstein zeigen, dass eine räumliche Nähe von Sachverständigen und Anbietern mitnichten eine Voraussetzung für ein erfolgreiches Durchlaufen des Verfahrens ist. In Schleswig-Holstein sind Gutachter aus dem gesamten Bundesgebiet akkreditiert, ohne dass dies in der Praxis zu Problemen geführt hätte. Eine Ortsbindung erzeugt vielmehr zusätzliche Bürokratie, da ein Sachverständiger, der für einen Auftraggeber mit Sitz in einem anderen Bundesland tätig sein will, sich zusätzlich in diesen Bundesländern bestellen lassen muss (vgl. Begründung zu § 2 Abs. 1), also eine Mehrfachbestellung benötigt. Da die Maßstäbe einer Bestellung bundeseinheitlich sein sollten, ist eine Mehrfachbestellung reiner Formalismus. Zu prüfen bleibt, ob eine Mehrfachbestellung nicht gegen die Berufsanerkennungsrichtlinie 2005/36/EG verstößt.

Absatz 2 regelt nicht, nach welchen **Kriterien eine Bestellung** der Sachverständigen erfolgt (bspw. Fachkunde) und unter welchen Voraussetzungen eine solche Bestellung entzogen werden kann. Eine solche Regelung muss als Beschränkung der Berufsausübungsfreiheit der Gesetzgeber selber treffen. Er kann sie nicht an den Verordnungsgeber delegieren.

Die in Absatz 2 vorgesehene Beschränkung der Durchführung eines Audits auf örtlich akkreditierte Sachverständige ist sachlich nicht nachzuvollziehen und verfassungsrechtlich eine unzulässige Beschränkung der Berufsausübung der Sachverständigen. Es liegt im öffentlichen Interesse, dass die Antragsteller eine freie Auswahl zwischen den bestellten Sachverständigen haben, um sich auch den oder die auf ihr Produkt spezialisierten und qualifizierten Sachverständigen auswählen zu können. Es ist kein rechtlicher oder sonstiger Grund erkennbar, weshalb für deutsche Antragsteller eine **Ortsbindung** gelten soll. Dies gilt insbesondere für die Zertifizierung von Produkten, die nicht nur in dem jeweiligen Bundesland, sondern u.U. weltweit vertrieben werden. Die Ortsbindung liefe im Übrigen leer, wenn ein Antragsteller durch die (evtl. nur vorübergehende) Gründung einer Niederlassung im Bundesland seiner Wahl oder im europäischen Ausland die formellen Voraussetzungen zur Antragstellung bei einem Sachverständigen seiner Wahl schafft.

§ 3 Zertifikat, Datenschutzauditsiegel

Nach Absatz 1 erteilt das Zertifikat der Sachverständige. Dabei ist unklar, ob er privatrechtlich oder hoheitlich als Beliehener handelt. Ein grundlegender Mangel des Gesetzentwurfes ist, dass eine **Qualitätssicherung des Zertifikates** nicht vorgesehen ist. Damit besteht das Risiko, dass - wie bei ähnlichen Verfahren in anderen Staaten - Gefälligkeitszertifikate ohne inhaltlichen Wert und ohne öffentliche Anerkennung erteilt werden. Die Erfahrung aus Schleswig-Holstein ist, dass eingereichte Gutachten häufig erst nach mehreren vom ULD geforderten Nachbesserungen den datenschutzrechtlichen Anforderungen genügen. Dies mag einerseits mit (noch) ungenügenden Erfahrungen der Gutachter begründet sein. Der Hauptgrund liegt aber darin, dass sowohl die Gutachter als auch die Sachverständigen ein übereinstimmendes ökonomisches Interesse daran haben, mit möglichst wenig Aufwand bzw. möglichst geringen Kosten zu einer Zertifizierung zu kommen. Dieses Problem lässt sich nur dadurch, aber auch schon allein dadurch beheben, dass eine öffentliche, also unabhängige, fachlich anerkannte und öffentlicher Kritik zugängliche Stelle die Qualitätssicherung und damit letztendlich die Vergabe der Zertifikate vornimmt.

Eine weiterer Grund für die Überprüfung der Plausibilität eines Gutachtens ist, dass die Zertifizierung ähnlicher Systeme und Verfahren gegenüber den Betroffenen, deren Daten verarbeitet werden, ebenso wie gegenüber den Wettbewerbern vergleichbar sein muss. Eine solche **Vergleichbarkeit** kann aber nur erreicht werden, wenn die Gutachten der Sachverständigen von einer Zertifizierungsstelle systematischen Plausibilitätskontrollen unterzogen werden. Eine vergleichbare Situation besteht im Europäischen Kontext: Im Rahmen von EuroPriSe ist eine Koordination der nationalen Zertifizierungsstellen vorgesehen.

Der Bund verfolgt für die Vergabe von **IT-Sicherheitszertifizierungen durch das BSI** denselben Weg, den Schleswig-Holstein beim Datenschutz-Gütesiegel beschritten hat. Zertifizierungen von Produkten (nach Common Criteria) oder von Sicherheitskonzepten (IT-Grundschutz / ISO 27001) durch das BSI setzen eine Begutachtung von beim BSI akkreditierten und lizenzierten Prüflaboren und IT-Sicherheitsauditoren voraus. Die Letztentscheidung liegt in der Hand des BSI und ergeht im Verwaltungsverfahren.

Eine mangelnde Qualitätssicherung bei der Zertifizierung ist absehbar **Quelle vielfältiger Konflikte**, die letztendlich rechtlich – und damit mit hohen Kosten und hohem Verwaltungsaufwand – ausgefochten werden dürften. Eine Vielzahl von Konfliktpartnern können gegenüber dem Antragsteller ins Spiel kommen: Sachverständige, Konkurrenten, Aufsichtsbehörden, die Betroffenen als Verbraucherinnen bzw. Verbraucher, die Abnehmer eines Produktes bzw. Nutzer einer Einrichtung. Denkbar sind weitere Konfliktkonstellationen zwischen den Beteiligten ohne Einbezug des Antragstellers. Derartige Konflikte und Streitverfahren reduzieren den Aussagewert der Zertifizierungen erheblich. Dieses Risiko kann entscheidend dadurch minimiert werden, dass die Zertifizierung in der Hand einer hoheitlichen und unabhängigen Stelle liegt, die durch ihre sachliche und wirtschaftliche Neutralität und ihre rechtliche Bindung die Akzeptanz aller Beteiligten findet.

Wie die Erfahrungen in Schleswig-Holstein zeigen, haben die Antragsteller ein wirtschaftliches Interesse an einer Zertifizierung durch eine unabhängige und öffentlich anerkannte Stelle. Nur eine solche Stelle rechtfertigt den Aufwand in die Zertifizierung, weil sie über die Mechanismen der Qualitätssicherung und der Vergleichbarkeit eine relevante Aussage gegenüber den Betroffenen trifft. Die dadurch zusätzlich entstehenden Kosten und der dadurch ausgelöste zusätzliche Aufwand sind im Verhältnis zu der auf diese Weise erreichten fachlichen Qualität der Aussage eines solchen Zertifikates gering. Zudem machen die Kosten der Zertifizierungsstelle regelmäßig nur einen geringen Anteil der Gesamtkosten einer Begutachtung aus. Die Verfahren beim ULD können nach Vorlage aussagekräftiger Unterlagen regelmäßig innerhalb weniger Wochen abgeschlossen werden. Sowohl die Gutachter als auch die Produktanbieter sind dankbar für die durch die Rückmeldung des ULD ausgelösten Qualitätsverbesserungen, die bisher bei praktisch jedem der zertifizierten Produkte im Rahmen der Plausibilitätsprüfungen durch die Zertifizierungsstelle des ULD erreicht wurden. Die in der Entwurfsbegründung aufgestellte Behauptung, eine zweistufige Prüfung würde die **Verfahrensdauer** erheblich verlängern und die **Kosten** des Audits wesentlich erhöhen (zu § 9) ist nicht begründet und steht in diametralem Widerspruch zu den in Schleswig-Holstein gesammelten Erfahrungen.

Die Regelung des Absatzes 4 deutet darauf hin, dass die **Zertifikatserteilung als Verwaltungsakt** anzusehen ist. Zumindest ist von der Bestandskraft einer Ablehnung die Rede. Die Begründung spricht von einem „ablehnenden Bescheid“. Unklar ist, ob gegen die Ablehnung das Widerspruchsverfahren eröffnet ist (§§ 68 ff. VwGO) und wer in diesem Fall die Widerspruchsbehörde sein wird. Gegner im verwaltungsrechtlichen Anfechtungsverfahren wird in jedem Fall der Sachverständige sein, der regelmäßig keine administrativen, geschweige denn verwaltungsgerichtliche Erfahrungen hat. Daher wird er – schon allein um gerichtliche Auseinandersetzungen mit seinem Auftraggeber zu vermeiden – sehr zurückhaltend mit der Forderung von Nachbesserungen sein. Dieses Problem besteht bei einer fachlich qualifizierten Stelle der staatlichen Verwaltung nicht.

Unklar ist, ob sich die Bestandskraft der Zertifizierung auf den jeweiligen Gutachter beschränkt. Beabsichtigt ist dies – so die Begründung – nicht. Ist dies aber nicht der Fall, dann entsteht ein großer – bisher nicht geregelter – bürokratischer **Abstimmungsaufwand**, um zu verhindern, dass der Antragsteller im Fall einer Ablehnung bei einem anderen Sachverständigen eine Zertifizierung beantragen wird. Das Ziel Doppelprüfungen auszuschließen, um die Suche nach dem „großzügigsten“ Sachverständigen zu verhindern (so die Begründung), lässt sich mit dieser Regelung nicht erreichen. Der Antragsteller muss den von ihm definierten Zertifizierungsgegenstand nur geringfügig ändern, um ein neues Antragsverfahren zu begründen. Die Entwurfsbegründung ist an dieser Stelle nicht nachvollziehbar, da sie keine Hinweise zur praktischen Umsetzung der Regelung enthält.

§ 4 Datenschutzauditregister

Ein Auditregister ist eine wichtige Komponente der Auditverfahren, um gegenüber den von einer Datenverarbeitung Betroffenen sowie den Wettbewerbern eine **größtmögliche Transparenz und Publizität** zu gewährleisten. Die Entwurfsregelung ist aber unzureichend, weil sie nicht vorsieht, dass die Eigenschaften, die Zwecke, die Anwendungsbereiche, die besonderen datenschutzrechtlichen Vorzüge und Probleme in dem Register beschrieben werden sollen. Das wichtigste Kriterium der Transparenz der Begutachtung ist die Beschreibung des Produktes, über die eine dauernde Weiterentwicklung der Produktstandards erreicht wird und über die die Betroffenen, deren Daten verarbeitet werden, sowie mögliche Wettbewerber die Berechtigung eines

Zertifikats überprüfen können. Die Beschreibung erfolgt daher in dem schleswig-holsteinischen Verfahren in Form eines aussagekräftigen Kurzgutachtens, in dem alle für das Zertifizierungsverfahren relevante Angaben mitgeteilt werden sollen.

Da der Bund für die Ausführung von Bundesgesetzen regelmäßig über **keine Verwaltungskompetenz** verfügt, kann ein solches Register nicht bei oder von einer Einrichtung der Bundesverwaltung geführt werden. Die Verwaltungskompetenz liegt nach Art. 83 ff. GG bei den Ländern.

§ 5 Rücknahme und Widerruf

Da bei der Zertifizierung keine ausreichende Qualitätssicherung vorgesehen ist, wird diese sich nur über die Rücknahme bzw. den Widerruf der Zertifizierung realisieren lassen. Dies hat zur Folge, dass auf die Aufsichtsbehörden ein **großer zusätzlicher Arbeitsaufwand** zukommt. Diese müssen, ebenso wie bei der Kontrolle nach § 38 BDSG, repressiv und können bzw. dürfen nicht präventiv und fördernd tätig werden. Den Schaden haben auch die Betroffenen, deren Daten unzulässig verarbeitet worden sind. Das Rücknahme- bzw. Widerrufsverfahren wird zudem dadurch kompliziert, dass es durch eine andere Stelle durchgeführt werden muss als die Stelle, die das Zertifikat erteilt hat. Die Folge ist ein zusätzlicher bürokratischer Prüf- und Beteiligungsaufwand.

§ 8 Rechtsverordnungen

Die Regelung soll das, was gesetzlich ungeregelt geblieben ist, normativ sichern. Hierbei werden aber die **wichtigsten Regelungsbereiche** nicht erwähnt: die Voraussetzungen für die Bestellung der Sachverständigen und die inhaltlichen Anforderungen des Datenschutzes und der Datensicherheit an die Eigenschaften des Verfahrens oder Produktes (Kriterienkatalog).

Die Kriterien für die Zertifizierung sind einem dauernden rechtlichen und technischen Wandel ausgesetzt. In Schleswig-Holstein wurde im Rahmen des e-Region Projektes ein **Kriterienkatalog** für Gütesiegelverfahren entwickelt, der seit 2003 erfolgreich angewendet wird. Die Zertifizierungskriterien bedürfen für ihre Konkretisierung einer hohen Sachkompetenz. Diese besteht jedoch – mangels Praxiserfahrung – nicht beim Bundesinnenministerium des Innern (BMI), welches für den Erlass der Rechtsverordnungen zuständig sein soll. Der Effekt der Regelung wäre daher ein aufwändiger und bürokratischer Kommunikationsprozess zwischen Sachverständigen, Aufsichtsbehörden und BMI. Dieser Aufwand lässt sich dadurch minimieren, dass die nähere Ausgestaltung des Verfahrens durch die Zertifizierungsbehörde erfolgt, die schon im Rahmen des Zertifizierungsverfahrens im engen Austausch mit den Sachverständigen steht. Ein derartiges Vorgehen hat Schleswig-Holstein gewählt.