

Berlin, im März 2009
Stellungnahme Nr. 29/2009

abrufbar unter
www.anwaltverein.de

Stellungnahme des Deutschen Anwaltvereins

durch den Ausschuss Informationsrecht

zum

Entwurf eines Gesetzes zur Regelung des Datenschutzaudits und zur Änderung datenschutzrechtlicher Vorschriften (BR-Drs. 4/09, Stand: 02.01.2009)

Mitglieder des Informationsrechtsausschusses:

Rechtsanwalt Dr. Helmut Redeker, Bonn (Vorsitzender)

Rechtsanwalt Niko Härting, Berlin

Rechtsanwalt Prof. Dr. Rainer Hamm, Frankfurt am Main

Rechtsanwalt Prof. Dr. Jochen Schneider, München (Berichterstatter)

Rechtsanwalt Prof. Dr. Holger Zuck, Stuttgart

zuständiger DAV-Geschäftsführer:

Rechtsanwalt Jens Wagener

Verteiler:

- Bundesministerium des Innern
- Bundesministerium der Justiz

- Landesjustizverwaltungen

- Bundesrat
- Rechtsausschuss des Deutschen Bundestages
- SPD-Fraktion im Deutschen Bundestag
- CDU/CSU-Fraktion des Deutschen Bundestages, Arbeitsgruppe Recht
- Fraktionen BÜNDNIS 90/DIE GRÜNEN im Deutschen Bundestag
- FDP-Fraktion im Deutschen Bundestag
- Fraktion DIE LINKE im Deutschen Bundestag

- Vorstand und Geschäftsführung des Deutschen Anwaltvereins
- Vorsitzende der Gesetzgebungsausschüsse des Deutschen Anwaltvereins
- Vorsitzende des FORUMs Junge Anwaltschaft

- Deutscher Richterbund
- Bund Deutscher Verwaltungsrichter
- Deutscher Steuerberaterverband
- GRUR
- BITKOM
- DGRI
- Bundesverband der Freien Berufe

- Bundesrechtsanwaltskammer
- Bundesnotarkammer

- Redaktion NJW
- ver.di Bundesverwaltung, Fachbereich Bund und Länder, Richterinnen und Richter, Staatsanwältinnen und Staatsanwälte

Der Deutsche Anwaltverein (DAV) ist der freiwillige Zusammenschluss der deutschen Rechtsanwältinnen und Rechtsanwälte. Der DAV mit derzeit ca. 67.000 Mitgliedern vertritt die Interessen der deutschen Anwaltschaft auf nationaler, europäischer und internationaler Ebene.

1. § 9a BDSG regelt den **freiwilligen** Datenschutzaudit. Zur Verbesserung des Datenschutzes und der Datensicherheit können danach Anbieter von Datenverarbeitungssystemen und -programmen und Daten verarbeitende Stellen ihr Datenschutzkonzept sowie ihre technischen Einrichtungen durch unabhängige und zugelassene Gutachter prüfen und bewerten lassen und das Ergebnis der Prüfung veröffentlichen. Nach Satz 2 werden Anforderungen an die Prüfung und Bewertung sowie das Verfahren durch besonderes Gesetz geregelt. Dem soll der Entwurf des Gesetzes zur Regelung des Datenschutzaudits und zur Änderung datenschutzrechtlicher Vorschriften, Bundesratsdrucksache 4/09 vom 02.01.2009 die überfällige Grundlage geben.

Dem entspricht der Entwurf nicht, da er nicht Gutachter und deren Verfahren regelt.

2. Selbstverständlich ist es zu begrüßen, dass eine Ausfüllung der Möglichkeiten des Datenschutzaudits, insbesondere die Anforderungen daran, wie sie in § 9a Satz 1 BDSG vorgesehen sind, nun durch das Vorhaben erfüllt würden. Auch die Stärkung des Audit-Gedankens im Sinne einer verstärkten Selbstkontrolle, aber auch einer Publikation bzw. Werbung mit dem „Zertifikat“ Datenschutz ist zu begrüßen, weil es den Gedanken an die Recht- und Ordnungsmäßigkeit der Datenverarbeitung („Compliance“) fördert.

Ob aber der vorliegende Gesetzesentwurf dem tatsächlich dienen kann, ist aus verschiedenen Gründen zweifelhaft.

3. Zweifel ergeben sich bereits aus der Ausführlichkeit der Regeln. Die Entscheidung, sich einem Datenschutzaudit zu unterziehen, ist freiwillig. Selbstverständlich bedarf es der Standards bzw. der Kontrollierbarkeit dessen, anhand dessen sich jemand auditieren lässt und dies dann auch noch publiziert. Wenn aber die Regelung dazu insgesamt 20 Paragraphen enthält und neben der Organisation der *Kontrollstellen* die Zuständigkeit des *Bundesbeauftragten* eröffnet wird, materiellrechtlich wirkende Richtlinien zur Verbesserung des Datenschutzes und der Datensicherheit als Maßgaben für die Erlangung des Datenschutzauditsiegels zu schaffen (§ 1 Satz 2 Nr. 2 Entwurf), stellt sich sowohl die Frage nach dem bürokratischen Aufwand als auch den Chancen der Erlangung für kleinere und mittlere Betriebe und schließlich die nach der „Gutachter“-Qualität.
4. Ein erheblicher Teil der Regelung betrifft die **Kontrollstelle** und deren Zulassung (§§ 3 und 4 (einschließlich der Entziehung der Zulassung)). § 5 regelt die Anforderungen an das Personal der Kontrollstelle, § 6 deren Pflichten. Diese Kontrollstelle wird wiederum von der zuständigen Behörde des Landes überwacht (§ 7 Abs. 1 i.V.m. der Zuständigkeit nach § 1 Abs. 1). § 8 wiederum regelt die Überwachung. Neben Kontrollstelle und zuständiger Behörde des Landes und dem Bundesbeauftragten gibt es dann den Datenschutzauditausschuss beim Bundesbeauftragten, der die oben erwähnten Richtlinien erlässt.
5. Die Regelungen sind typisch für Verwaltungsverfahren, erhöhen den bürokratischen Aufwand um sowohl Instanzen als auch Verfahren. Nach § 9a Satz 2 BDSG wären die Anforderungen an die Prüfung und Bewertung, das Verfahren sowie die Auswahl und

Zulassung der Gutachter durch das Gesetz zu regeln, nicht das Verwaltungsverfahren. Die Frage ist also völlig ausgeklammert, die zentral wäre, wie nämlich in der Kombination von Datenschutz und IT, in der Kombination also von Rechtmäßigkeit der Datenverarbeitung und Sicherheit, eine Prüfung stattzufinden hat, welche Bewertungskriterien dabei, abgeleitet aus der Datenschutzgesetzgebung (und zwar nicht zukünftiger, sondern der jeweils bestehenden), vorzunehmen ist. Weiter wäre das Verfahren hinsichtlich der Begutachtung zu regeln. Dem entspricht keine einzige Vorschrift des Gesetzes. Dass der Datenschutzauditausschuss sich eine Geschäftsordnung gibt und diese der Genehmigung durch das Bundesministerium des Inneren bedarf, ist mit der Intention Steigerung der Selbstverantwortung und der Unabhängigkeit der Gutachter schwer zu vereinbaren.

6. Während die Zusammensetzung der Mitglieder des Datenschutzauditausschusses nach Herkunft geregelt ist, gibt es keine konkreten Angaben, welche Qualifikationen im einzelnen die Gutachter haben müssen und wie sie diese nachweisen. "Gründliche Fachkenntnisse" und "mindestens dreijährige fachliche Erfahrung auf dem Gebiet des Datenschutzes" sind keine Qualifikationen für einen Gutachter. Dies wären vielleicht Voraussetzungen dafür, jemanden zum Datenschutzbeauftragten insgesamt zu bestellen, aber nicht für diese Aufgabe des Datenschutzaudits, also den Datenschutzbeauftragten seinerseits indirekt zu prüfen. Das Thema „**Gutachter**“ ist verfehlt.
7. Zu den Voraussetzungen, unter denen das *Siegel* zu erlangen ist, gehört die Einhaltung der Richtlinien nach § 11. Diese Richtlinien sind nicht abschließend inhaltlich geregelt, sondern nur beispielhaft. So hat sich Datenschutzaudit auch zur Voraussetzung zu nehmen, dem Ziel der Datenvermeidung und Datensparsamkeit zu dienen, auch der organisatorischen Stärkung des Beauftragten für den Datenschutz. Dies sind keine auditfähigen, objektivierbaren Prüfungsgegenstände. § 3a Satz 1 BDSG fordert eine Ausrichtung an einem Ziel. Dies ist nicht justiziabel. D. h., es ist unter qualitativen Zwecken schon praktisch nicht überprüfbar. Unter quantitativ, objektivierbaren ist dies erst recht nicht möglich. Nach § 3a Satz 2 BDSG ist insbesondere von den Möglichkeiten der Anonymisierung und Pseudonymisierung Gebrauch zu machen. Dies zielt in eine bestimmte Richtung, die als beispielhafte, aber auch als maßgebliche Anforderung durch ein Auditgesetz eher zu konkretisieren, denn auszuweiten wäre. § 11 BDSG bezieht sich lediglich auf diese Regelung, ohne irgendeine Konkretisierung vorzunehmen.
8. Am Rande sei noch erwähnt, dass der **Interessenskonflikt**, der beim Bundesbeauftragten für den Datenschutz und Informationsfreiheit bereits in der Ausstattung des Amtes angelegt ist, noch intensiviert wird. Unter Gesichtspunkten der Wahrung der Autonomie und der wirtschaftlichen Entfaltungsmöglichkeiten des Unternehmens ist eine Sicherheitspolitik erforderlich, die den Bestand des Unternehmens sichert, selbstverständlich unter Wahrung des Datenschutzes. Aufgabe des Bundesbeauftragten für den Datenschutz ist zugleich die Wahrung der Informationsfreiheit, die erhebliche Eingriffe in die betriebliche Autonomie ermöglicht.

So kann ein Unternehmen zwar einerseits dem Datenschutz genügen, andererseits aber gezwungen sein, im Rahmen der Informationsfreiheit bestimmte Informationen zu liefern. Wenn es sich hierbei nicht um gewerbliche Schutzrechte handelt, entsteht ein abzuwägender Konflikt zum Datenschutz. Dies wäre vielleicht noch durch den Datenschutzbeauftragten als solches hinzunehmen. Durch das Hinzukommen eines Dritt-Interesses, nämlich das Interesses des Unternehmens an der Sicherheit, ist hier ein Interessenkonflikt vorprogrammiert. Die Zuständigkeit des Bundesbeauftragten für den Datenschutz ist demnach verfehlt.