DVD Deutsche Vereinigung für Datenschutz e. V.

Stellungnahme zum Gesetzentwurf der Bundesregierung

Entwurf eines Gesetzes zur Regelung des Datenschutzaudits und zur Änderung datenschutzrechtlicher Vorschriften, BT-Drs. 16/12011

1. Allgemeine Bewertung

Die vorgelegten Regelungen eines Datenschutzauditgesetzes sind aus verschiedenen Gründen ungeeignet, das gesteckte Ziel zu erreichen:

- Aufgrund offensichtlich mangelhafter inhaltlicher Auseinandersetzung ist der Auditgegenstand vollkommen unzureichend konzeptioniert.

- Das Verfahren sieht auch für die Inhalte der Richtlinien lediglich die üblichen gesetzlich geforderten Vorgaben vor. Im Ergebnis wird daher lediglich Gesetzestreue, nicht aber ein besonders hohes Datenschutzniveau zertifiziert.

- Das beschriebene, noch nicht einmal einstufige Kontrollverfahren (der Antragsteller soll das Siegel bereits führen, bevor überhaupt auch nur eine einzige Begutachtung stattgefunden hat) kann Datenschutz-Qualität weder fördern noch verlässlich erkennen.

- Die Vermischung kommerzieller Dienstleistung (Kontrollstellen müssen vom Antragsteller bezahlt werden) mit hoheitlichen Aufgaben als Kontrollstelle führt zwingend zu Interessenskonflikten, gefährdet die unparteiische Begutachtung und widerspricht jeglichen international üblichen Zertifizierungsstandards.

- Der vorgesehene bürokratische Aufwand steht in krassem Missverhältnis zu der dünnen und wenig durchdachten Inhalten.

- Das Siegel ist daher ungeeignet, Verbraucherinnen und Verbrauchern verlässliche Entscheidungskriterien zu vermitteln.

- Die alle Fachdiskussionen und praktischen Erfahrungen ignorierende Umsetzung beschädigt das Instrument „Gütesiegel“ mehr als dass sie ihm nutzt. Es würde der Sache eher dienen, auf dieses Gesetz vollständig zu verzichten.

Die vorgelegten Regelungen zur Stärkung betrieblicher Datenschutzbeauftragter sind grundsätzlich zu begrüßen. Sie sind allerdings nicht ausreichend und sollten um Kapazitätsvorgaben ergänzt werden.

Die vorgelegten Regelungen zur Neuordnung des Umgangs mit personenbezogenen Daten zu Zwecken der Werbung, des Adresshandels und der Markt- und Meinungsforschung sind – möglicherweise aufgrund von Lobbytätigkeit der betroffenen Branchen – im Ergebnis so unübersichtlich, dass die Einhaltung kaum erwartet werden kann. Obwohl der Paradigmenwechsel zu einwilligungsabhängiger Datenverwendung zu begrüßen ist, erzeugen die vielfältigen und unübersichtlichen Ausnahmetatbestände einen unakzeptablen Zulässigkeitswirrwarr.

Der vorgelegte Entwurf verwendet außerdem eine Vielzahl von Begriffen aus Informationstechnologie, Zertifizierungsnomenklatur und Datenschutzpraxis in unüblicher, widersprüchlicher oder undefinierter Weise. Dieser handwerkliche und inhaltliche Mangel ist für ein Gesetz unakzeptabel. Auf die diesbezügliche Kritik des Bundesrates wird ausdrücklich verwiesen.

Zu Regelungen des Auditgesetzes

2. Auditgegenstand

Auditierbar sollen laut Gesetzentwurf Datenschutzkonzept oder informationstechnische Einrichtungen sein. Damit ist der mögliche Gegenstand eines Audits jedoch nicht annähernd ausreichend definiert. Was die Schlagworte „Datenschutzkonzept“ und „informationstechnische Einrichtungen“ inhaltlich bedeuten sollen und ob ein Audit alternativ oder gemeinsam beide Gegenstände prüfen soll bleibt unklar.

Eine wesentliche Anforderung an die fachliche Solidität eines Auditgesetzes besteht in der eindeutigen Definition der Prüfgegenstände, so dass die in der Praxis auftretenden Fälle zweifelsfrei und sinnvoll als auditierbar oder nicht auditierbar einzuordnen sind.

Die in der unterschiedlichen Fachliteratur verwendeten Definitionen des Begriffs „Datenschutzkonzept“ zeigen deutlich, dass kein begrifflicher Konsens besteht, auf den ein Gesetz berechtigterweise zurückgreifen könnte.

Die Unterscheidung zwischen „verantwortlichen Stellen“ und „Anbietern von Datenverarbeitungsanlagen und –programmen“ ist in der Praxis unbrauchbar, da es sich nicht um disjunkte Mengen handelt. Die in der Begründung gewählte Unterscheidung zwischen Datenverarbeitungsanlagen und Datenverarbeitungsprogrammen ist in Bezug auf mögliche Auditgegenstände weder fachlich korrekt noch wird auf sie im Weiteren zurückgegriffen. Letztlich wäre nach dieser Pseudo-Definition zwar ein Kabel datenschutzauditierbar (!) nicht aber ein Online-Shop, der auf Standard-Software aufbaut (denn es handelt sich beim Shop-Betreiber nicht um den Anbieter des Programms). Gerade solche Anwendungen sind aber für Verbraucher in Zeiten zunehmender Internet-Geschäfte interessant. Außerdem reicht die Beurteilung des Datenschutzkonzepts allein nicht aus, um den tatsächlichen Datenschutzstandard zu beurteilen. Auf eine Prüfung der Umsetzung, mindestens in geeignet ausgewählten Stichproben, kann seriöserweise nicht verzichtet werden.

Die Einschränkung auf Datenschutzkonzept und informationstechnische Einrichtungen erscheint daher insgesamt deutlich zu kurz gesprungen.

Will man verantwortlichen Stellen die Möglichkeit aussagekräftiger Audits bieten, kommt man um die sachgerechte Definition der Prüfobjekte nicht herum. Dabei muss der fachlich durchdachten Abgrenzung des Prüfgegenstands besondere Aufmerksamkeit gewidmet werden: Wenn nicht das Unternehmen/die Organisation als Ganzes auditiert werden sollen, muss das Prüfobjekt so deutlich für sich stehen, dass keine Gefahr eines pars pro toto-Effekts besteht: dass nämlich das Unternehmen einen kleinen, marginalen Teilbereich prüfen und zertifizieren lässt, anschließend aber in der Öffentlichkeit als insgesamt datenschutzzertifiziert wahrgenommen wird.

3. Datenschutzniveau

Ist bereits die alleinige Einhaltung datenschutzrechtlicher Vorgaben zertifizierungsfähig oder muss ein besonders hohes Datenschutzniveau nachgewiesen werden? Zur Beantwortung dieser Frage wären zwei logische Wege denkbar:

Ist der Gesetzgeber der Meinung, dass eine Mehrzahl der Unternehmen gegen Datenschutzvorschriften verstoßen, müsste eine Zertifizierung verpflichtend eingeführt werden um die Einhaltung der Gesetze zu befördern. In diesem Fall würde lediglich die Gesetzeskonformität bestätigt, was aber keinen Wettbewerbsvorteil brächte.

Geht der Gesetzgeber jedoch grundsätzlich von gesetzestreuer Umsetzung der Datenschutzvorgaben aus, kann ein Zertifikat auf freiwilliger Basis erfolgen. Es bringt jedoch nur dann einen Wettbewerbsvorteil, wenn die gesetzlich vorgeschriebenen Standards deutlich überschritten werden.

Formal wird im vorgelegten Entwurf der Eindruck erweckt, dass in den durch den Auditausschuss erarbeiteten Richtlinien Vorgaben für einen hohen Datenschutzstandard gemacht werden sollen. Die dünnen inhaltlichen Vorgaben führen jedoch lediglich Aspekte auf, die ohnehin Gegenstand gesetzlicher Datenschutzvorgaben sind (§9-Maßnahmen, Einhaltung von Transparenz, Datenvermeidung und Datensparsamkeit).

Im Ergebnis wird daher lediglich Gesetzeskonformität verlangt um ein Zertifikat zu erteilen. Ein Zertifikat dafür, dass jemand keinen Gesetzesverstoß begeht(!) birgt jedoch die falsche Botschaft und ist für Verbraucher wertlos.

4. Kontrollverfahren

Die zur Durchführung der Zertifizierung vorgesehenen Strukturen und Prozesse sind durch übertriebene Bürokratie einerseits und Verletzung grundlegender, international anerkannter Zertifizierungsgepflogenheiten andererseits gekennzeichnet.

Die Möglichkeit zur Führung eines Siegels bevor überhaupt irgendeine Kontrolle des zu zertifizierenden Gegenstands stattgefunden hat, öffnet irreführendem Siegelgebrauch Tür und Tor.

Die fehlende Trennung zwischen begutachtender und zertifizierender Stelle bringt zwingend eine Reihe von Interessenkonflikten mit sich. Die begutachtende Stelle wird vom Auftraggeber bezahlt und ist daher wirtschaftlich nicht unabhängig, wie dies für eine zertifizierende Stelle eigentlich unerlässlich ist. Sie müsste sich nach diesem Gesetzentwurf vielmehr im Falle unzureichenden Datenschutzniveaus gegen den eigenen Auftraggeber wenden, also das Siegel verweigern aber trotzdem eine Rechnung schreiben. Dass hier im Zweifel lieber alle Augen zugedrückt werden, liegt auf der Hand. Die begutachtende Stelle ist außerdem grundsätzlich verpflichtet, jeden Antragsteller zu begutachten, der dies wünscht, unabhängig davon, für wie ausgereift und erfolgversprechend sie dieses Ansinnen hält. Steigt die Zahl der Anträge, muss die begutachtende Stelle aufgrund ihrer regelmäßigen Kontrollpflichten auch für bereits erteilte Siegel die vorhandenen Kapazitäten aufteilen. Es ist nicht davon auszugehen, dass die Kontrollstelle ihre Ressourcen großzügig aufstocken kann. Es ist zu befürchten, dass schon alleine aus Kapazitätsgründen die einzelne

Zertifizierung oder Rezertifizierung einen bestimmten Aufwand nicht überschreiten darf, so dass komplexe Auditgegenstände eher oberflächlich geprüft werden.

Es ist unerklärlich, warum kein Ansatz gewählt wurde, der die Begutachtung durch akkreditierte Sachverständige und die Siegelerteilung durch eine unabhängige Stelle vorsieht, wie dies z.B. in ISO-Verfahren üblich ist. Vor allem die internationale Anerkennung eines Zertifikats ist durch das gewählte Verfahren verunmöglicht.

5. Prüfungsinhalte und Ablauf

Substantiierte Beschreibungen der Prüfungsinhalte fehlen im Gesetzentwurf vollständig. Statt dessen wird diese Aufgabe einem Datenschutzauditausschuss übertragen. Dessen Zusammensetzung lässt jedoch nicht hoffen, dass er die nicht triviale Aufgabe der Festlegung von Prüfungsinhalten für so unterschiedliche Auditgegenstände wie Datenschutzkonzepte und informationstechnische Systeme befriedigend lösen kann.

Es drängt sich der Verdacht auf, dass die Verfasser des vorliegenden Entwurfs mangels ausreichender Kenntnisse den grundlegendsten Teil des Vorhabens delegiert haben um sich dieser unangenehmen Aufgabe zu entledigen. Warum statt dessen ausgerechnet diejenige öffentliche Aufsichtsstelle federführend sein soll, nämlich der Bundesbeauftragte für den Datenschutz, die am wenigsten mit privatrechtlichen Unternehmen und deren Datenschutzorganisation befasst ist, ist unerklärlich. Dies insbesondere deswegen, weil hierdurch eine Parallelkonstruktion zu den eigentlich zuständigen Aufsichtsbehörden aufgebaut wird, die diese schwächt und gleichzeitig die ohnehin zu schwachen Ressourcen durch einen bürokratischen Popanz bindet.

Karin Schuler, stv. Vorsitzende der Deutschen Vereinigung für Datenschutz e.V.
Bonner Talweg 33-35
53113 Bonn
Tel. 0228/24 20 733, Fax. 0228/24 20 734, schuler@datenschutzverein.de