DVD Deutsche Vereinigung für Datenschutz e. V.

Stellungnahme zum Bundesdatenschutzauditgesetz vom 7. September 2007

Auch wenn es sechs Jahre gedauert hat: Die Umsetzung der Vorgaben des § 9a BDSG ist grundsätzlich zu begrüßen. Allerdings lässt die fachliche Ausführung in erschreckendem Maße zu wünschen übrig, wie im Folgenden ausgeführt wird.

1. Gegenstand des Audits

Auditierbar sollen laut Gesetzentwurf „Datenschutzkonzept sowie technische Einrichtungen" sein. Damit ist der mögliche Gegenstand eines Audits jedoch nicht annähernd ausreichend definiert. Was die Schlagworte „Datenschutzkonzept" und „technische Einrichtungen" tatsächlich inhaltlich bedeuten sollen und ob ein Audit alternativ oder gemeinsam beide Gegenstände prüfen soll bleibt unklar. Eine wesentliche Anforderung an die fachliche Solidität besteht jedoch in der eindeutigen Definition der Prüfgegenstände, so dass die in der Praxis auftretenden Fälle zweifelsfrei 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 Einschränkung auf Datenschutzkonzept und technische Einrichtungen erscheint außerdem insgesamt deutlich zu kurz gesprungen. Unter dieser Definition lassen sich beispielsweise weder Webportale noch Online-Shops auditieren. 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.

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.

In der Frage des erforderlichen Datenschutzniveaus, das zu einer Zertifizierung berechtigt, 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.

Es ist daher fragwürdig, dass der vorliegende Entwurf vorsieht, das freiwillige Zertifikat bereits für bloße Gesetzeseinhaltung zu erteilen. Das würde bedeuten, dass man ein Zertifikat dafür erteilt, dass jemand keinen Gesetzesverstoß begeht(!). Unabhängig von der falschen Botschaft ist ein Wert für Verbraucher so nicht zu erzielen.

Der Verzicht auf die Bewertung der Sicherheit der zu prüfenden Komponenten stellt einen direkten Widerspruch zu den Bestimmungen des BDSG dar, in dem die Umsetzung geeigneter technischer und organisatorischer Sicherheitsmaßnahmen eine wesentliche Anforderung darstellt. Man fragt sich, welchen Inhalts die Prüfungen der zu prüfenden technischen Einrichtungen sein sollen, wenn dies keine Sicherheitsüberprüfung sein soll. Auch inhaltlich ist die Trennung von Datenschutz- und Datensicherheitsmaßnahmen unmöglich und kontraproduktiv. Wirksamer Datenschutz ist ohne die sichere Gestaltung der beteiligten Systeme nicht möglich. Ein derart auditiertes Objekt könnte niemals seriöserweise als datenschutzgerecht bezeichnet werden. Der Verweis auf die durch das BSI mögliche Zertifizierung, der Datenschutz und Datensicherheit als divergente Schutzziele konstatiert, kündet von absoluter Praxisferne. Will man die Leistungen und Kenntnisse des BSI in Bezug auf Sicherheitszertifizierungen angemessen würdigen, würde man dies am besten dadurch erreichen, dass man seine ISO 27001-Zertifizierungen als ausreichenden Nachweis von Datensicherheitsmaßnahmen in Datenschutzaudits anerkennt. Nicht jedoch, indem man auf den Nachweis von Datensicherheitsmaßnahmen vollständig verzichtet.

2. Sachverständige

Es erscheint übertrieben bürokratisch, die föderale Struktur zur Bestellung von Sachverständigen zu nutzen. Bereits heute ist eine stark unterschiedliche Praxis durch die Landesbeauftragten und die Aufsichtsbehörden der Länder erkennbar. Eine einheitliche Handhabung der Zulassungsvoraussetzungen ist so kaum zu erzielen; unterschiedliche Anforderungen und Kenntnisse der Sachverständigen wären die Folge. Will der Sachverständige bundesweit tätig werden, muss er sich durch 16 Akkreditierungsverfahren quälen. Sowohl für Sachverständige wie auch für Antragsteller besteht die Gefahr eines Audittourismus in Länder, in denen die Anforderungen an Sachverständige als besonders gering gelten.

Stattdessen sollte die Akkreditierung von Sachverständigen einer einzelnen, unabhängigen Stelle übertragen werden, die eine einheitliche Handhabung sicherstellen kann. Mindestens ist jedoch eine gegenseitige Anerkennung der Akkreditierungen innerhalb der Länder sicherzustellen. Dies würde auch verhindern, dass Unternehmen mit ihrem Antrag in Bundesländer ausweichen, die als besonders „einfach“ gelten. Besonders für große Unternehmen mit Niederlassungen in verschiedenen Bundesländern wäre dies der vorgeschlagenen Regelung nach nämlich problemlos möglich. Unternehmen, denen diese Möglichkeit nicht zur Verfügung steht, sind außerdem zusätzlich gegenüber ausländischen Antragstellern benachteiligt, die sich den Sachverständigen frei im Bundesgebiet aussuchen können.

Es ist auch abzulehnen, dass allein den Sachverständigen die Vollmacht übertragen wird, engültig über die Vergabe eines Zertifikats zu entscheiden. Eine wirksame Kontrolle ist weder vorgesehen noch könnte sie in der beabsichtigten föderalen Struktur einheitlich realisiert werden.

Statt dessen sollte einem zweistufigen Verfahren der Vorzug gegeben werden, das sich an üblichen internationalen Zertifizierungsnormen orientiert und eine unabhängige Zertifikatsvergabe garantieren kann.

3. Begriffe und Prüfverfahren

Die Verwendung der Begriffe folgt nicht allgemein üblichen Zertifizierungsverfahren, was allerdings, auch im Sinne der Einhaltung internationaler Normen, wünschenswert wäre. Gerade die konstatierte Übereinstimmung mit europäischem Recht erscheint unter diesem Aspekt als zu kurz gedacht. In verbreiteten Normen, wie z. B. ISO 27001 oder auch zu Umweltaudits erstellen Sachverständige (Gutachter) in der Regel ein Gutachten (nicht: Zertifikat), einen Prüfbericht, in dem die Übereinstimmung des geprüften Obkjekts mit den jeweiligen Normen dargelegt wird.

Ein Zertifikat (oder Siegel) wird in der Regel bei erfolgreicher Prüfung (Audit) nach Prüfung des Auditberichts von der offiziell hierfür zuständigen Stelle vergeben. Es bescheinigt das positive Ergebnis offiziell und ist damit das Resultat eines erfolgreichen Auditverfahrens. Der im vorliegenden Entwurf implizierte Verzicht auf eine unabhängige Endüberprüfung durch die zuständige Stelle ist äußerst fragwürdig, weil sie die Zertifizierung durch (zumindest zeitweise) wirtschaftlich vom Antragsteller abhängige Personen vornehmen lässt.

Der Begriff des Datenschutzauditsiegels ist überflüssig oder sollte höchstens den Begriff des Zertifikats ersetzen.

Zusammenfassend erscheint nicht nachvollziehbar, aus welchem Grunde hier von etablierter Begriffsbildung und den damit verbundenen Verfahren abgewichen werden soll.

Der Begriff der „unveränderten Version“ ist nicht erläutert und daher in höchstem Maße missverständlich. Dem jetzigen Textvorschlag nach wäre eine Software zwar zertifizierbar, würde aber bei jeder Installation ihr Siegel verlieren, weil sie selbstverständlich bei der Installation durch den Anwender verändert wird (Konfiguration von Berechtigungen, Protokollen und sonstigen Einstellungen). Insbesondere bei Datenschutzkonzepten wäre eine zweijährige Weiterentwicklungspause unverantwortlich und geradezu kontraproduktiv. Ein Datenschutzkonzept muss ständig aktuellen Erfordernissen angepasst werden um einen datenschutzgerechten Umgang mit personenbezogenen Daten zu ermöglichen. Spätestens hier wird deutlich, dass der Begriff des Datenschutzkonzepts vermutlich weder verstanden noch ordentlich definiert wurde. Zertifizierbar im Sinne des Gesetzes könnten höchstens die Aspekte eines Datenschutzmanagement-Systems sein, die nach Art einer Leitlinie die organisatorische Verankerung grundlegender Datenschutzprozesse im Unternehmen beschreiben. Auf eine tragfähige Definition des hier verwendeten Begriffs „Datenschutzkonzept“ kann daher keinesfalls verzichtet werden.

4. Rolle der Aufsichtsbehörde

Die Rolle der Aufsichtsbehörden selbst und Rahmenbedingungen für die von ihnen durchzuführenden Verfahren sind unzureichend formuliert. Unabhängig von der generellen Frage nach föderaler Zuständigkeit sind ergibt es keinen Sinn, den Aufsichtsbehörden keine „Endabnahmemöglichkeit“ im Einzelfall einzuräumen, ihnen aber gleichwohl die Aufgabe von Rücknahme und Widerruf (vermutlich: des Zertifikats?)zuzuordnen, also gewissermaßen eine nachlaufende Endabnahme vorzusehen.Es wird eben gerade nicht, wie in der Begründung angeführt, eine einheitliche Vergabepraxis erzielt, sondern ein länderorientierter Flickenteppich geschaffen, der durch die Vergabepraxis durch die Sachverständigen weiter an Uneinheitlichkeit zunimmt.

5. Fazit

Der vorliegende Entwurf ist nicht dazu geeignet, den in § 9a BDSG erteilten Auftrag des Gesetzgebers angemessen und praxisgeeignet umzusetzen. Er vermittelt vielmehr den Eindruck, als habe der Autor ohne große Kenntnis in der Sache einen wenig durchdachten Vorschlag entwickelt.

Auch in der Begrifflichkeit scheint der Autor nicht sattelfest zu sein: Der Rückfall in alte Zeiten durch Bezugnahme auf die automatisierte Verarbeitung personenbezogener Daten in Dateien erscheint anachronistisch. Spätestens seit der EU-RiLi wurde auf den Bezug zum Dateibegriff verzichtet.

Ein nach dem vorliegenden Gesetzentwurf durchgeführtes Audit würde voraussichtlich nach einem kurzen Zeitraum an Wert verlieren, weil die Art und Weise seiner Erteilung bei den Verbrauchern nicht als objektiv und einheitlich begründete Entscheidung wahrgenommen würde.

Wenn sich dies für Unternehmen, was anzunehmen ist, ebenso darstellt, wäre das Interesse an der Durchführung von Audits voraussichtlich sehr gering. Die Folge wäre, dass erneut die Chance auf ein marktgerechtes Instrument für Datenschutz vertan wurde und lediglich ein weiterer Papiertiger sein Leben fristet.

Einem solchen staatlich reglementierten Audit wäre ein ausschließlich auf international anerkannten Normen basierendes Verfahren jedenfalls vorzuziehen.

Nicht zuletzt ist zu kritisieren, dass nach sechsjähriger Verzögerung der Gesetzentwurf den Verbänden zur Kommentierung nun innerhalb der Herbstferien und mit einer Antwortfrist von nur 4 Wochen zugestellt wird. Eine angemessene, innerhalb der Organisation abgestimmte Kommentierung ist gerade für ehrenamtlich arbeitende Verbände so nur unter größten Schwierigkeiten möglich. Man kann sich des Eindrucks nicht ganz erwehren, dass durch das Prozedere kritische Stimmen von vorneherein möglichst vermieden werden sollen.

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 38 470, schuler@datenschutzverein.de