



Vorschlag des Arbeitskreises
„Die zukünftige Entwicklung des Datenschutzrechts in
Deutschland“ des Berufsverbandes der Datenschutz-
beauftragten Deutschlands (BvD) e. V.

über wesentliche Inhalte des Datenschutz-Audit-
Gesetzes (DSAG) gemäß § 9 a Satz 2 BDSG

Bei dem Beitrag handelt es sich um ein Ergebnis des Arbeitskreises „Die zukünftige Entwicklung des Datenschutzrechts in Deutschland“ des Berufsverbandes der Datenschutzbeauftragten Deutschlands (BvD) e. V. Es spiegelt nicht notwendigerweise die Meinung des Vorstandes des BvD wider.

Mitglieder des Arbeitskreises des BvD

- Helmut Baudenbach, Datenschutzbeauftragter der MAN Nutzfahrzeuge AG,
- Dr. Lutz Bergmann, Regierungsdirektor a. D., Justiziar des BvD, Mitverfasser des Handkommentars Datenschutzrecht Bergmann/Möhrle/Herb, Vorsitzender des Arbeitskreises „Die zukünftige Entwicklung des Datenschutzrechts in Deutschland“ des BvD,
- Peter Deckers, Datenschutzbeauftragter der NBV/UGA GmbH,
- Wilhelm Deml, IT-Manager bei der DeTe Immobilien,
- Dieter Ehenschwender, Datenschutzberater der T-Systems International GmbH, stellv. Vorsitzender des Arbeitskreises,
- Peter Kaiser, Rechnungsprüfung/Datenschutz beim Landeswohlfahrtsverband Württemberg-Hohenzollern,
- Ass. jur. Uwe Meister, Datenschutzbeauftragter der Landwirtschaftlichen Sozialversicherung Baden-Württemberg,
- Dietrich Mildner, Datenschutzbeauftragter der Dornier GmbH,
- Lutz Neundorf, Konzerndaten- und Informationsschutzbeauftragter der ABB Deutschland und ALSTOM-Power Deutschland,
- Rolf Warthold, Datenschutzbeauftragter in der E.ON Energie-Gruppe und stellv. Vorsitzender des BvD.

	Seite
1. Allgemeine Bestimmungen	4
1.1 Zweck des Gesetzes.....	4
1.2 Anwendungsbereich	4
1.3 Begriffsbestimmungen	4
1.4 Freiwilligkeit der Teilnahme und Erfüllungsgrad der Datenschutzvorschriften.....	5
2. Audit-Verfahren.....	5
2.1 Erarbeitung und Aktualisierung eines Prüfkriterienkataloges.....	5
2.2 Grundsätze zur Durchführung	5
2.3 Datenschutz-Produkt-Audit	6
2.4 Internes Datenschutz-System-Audit	6
2.5 Externes Datenschutz-System-Audit	6
2.6 Mitwirkung des bestellten Datenschutzbeauftragten	7
2.7 Erteilung und Registrierung des Datenschutz-Audit-Zertifikats.....	7
2.8 Gültigkeit des Zertifikats.....	7
2.9 Werbung mit dem Datenschutz-Gütesiegel	8
3. Auswahl und Zulassung der Datenschutz-Auditoren	8
3.1 Auswahl der Datenschutz-Auditoren	8
3.2 Zulassung der Datenschutz-Auditoren.....	8
3.3 Ordnungswidrigkeiten	8
4. Anpassung/Änderung betroffener Gesetze	9

1. Allgemeine Bestimmungen

1.1 Zweck des Gesetzes

Dieses Gesetz regelt auf Grund von § 9 a Bundesdatenschutzgesetz (BDSG) die rechtliche Grundlage für die näheren Anforderungen an die Prüfung und Bewertung, das Verfahren sowie die Auswahl und Zulassung der Gutachter. Es definiert die Rahmenbedingungen zur Erteilung eines Datenschutzzertifikats für nach diesem Gesetz geprüfte Produkte (Datenschutz-Produkt-Audit) und/oder verantwortliche Stellen (Datenschutz-System-Audit).

Das Datenschutz-Audit dient der Stärkung der Eigenverantwortung der verantwortlichen Stellen und ist eine vertrauensbildende Maßnahme gegenüber Kunden und Betroffenen.

Es fördert die Identifikation mit den besonderen Belangen des Datenschutzes und die Beseitigung von Defiziten in der Umsetzung des geltenden Datenschutzrechts, die Erhöhung des Datenschutzniveaus und die Datenschutzensensibilisierung durch kontinuierliche Umsetzung von Verbesserungsmaßnahmen und geprüfter Datensicherheit.

Das Audit gewährleistet Rechtssicherheit bezüglich der Einhaltung der Datenschutzvorschriften in der verantwortlichen Stelle gegenüber Aufsichtsbehörden und Öffentlichkeit sowie für die Betroffenen eine bessere Wahrung ihres Rechts auf informationelle Selbstbestimmung.

Das Datenschutz-Audit dient der Förderung datenschutzfreundlicher Techniken.

1.2 Anwendungsbereich

Der Anwendungsbereich ergibt sich aus § 1 Abs. 2 bis 5 des BDSG.

1.3 Begriffsbestimmungen

Folgende Arten von Datenschutz-Audits sind zu unterscheiden:

1. Datenschutz-Produkt-Audit:

Methode zur Zertifizierung von Produkten wie Hardware, Software, bestimmten Techniken und Verfahren der EDV sowie Kommunikation. Nach erfolgter Prüfung auf Verträglichkeit mit den Vorschriften über den Datenschutz kann die Zertifizierung mit dem Datenschutz-Produkt-Gütesiegel erfolgen.

2. Datenschutz-System-Audit:

Methode zur Bewertung von Systemen und Abläufen zur elektronischen Erhebung, Verarbeitung und Nutzung personenbezogener Daten bei der verantwortlichen Stelle oder Teilen derselben auf Verträglichkeit mit den Vorschriften über den Datenschutz, und zwar als

a) Internes Datenschutz-System-Audit

Die Feststellung der Datenschutzkonformität erfolgt durch den bestellten Datenschutzbeauftragten der verantwortlichen Stelle im Auftrag des Leiters und unter Einbeziehung datenschutzrechtlich fachkundiger Kräfte sowie der Mitarbeitervertretung - jedoch ohne Zertifizierung - und

b) Externes Datenschutz-System-Audit

Die Feststellung der Datenschutzkonformität erfolgt durch zugelassene Datenschutz-Auditoren unter Einbeziehung des Datenschutzbeauftragten sowie der Mitarbeitervertretung der verantwortlichen Stelle mit der Zielsetzung, der auditierten Stelle das Datenschutz-System-Gütesiegel zu erteilen.

1.4 Freiwilligkeit der Teilnahme und Erfüllungsgrad der Datenschutzvorschriften

Die Durchführung von Datenschutz-Audits ist freiwillig.

Das Datenschutz-Produkt-Audit soll Transparenz und Bewertbarkeit zwischen unterschiedlichen Angeboten schaffen. Damit wird für den Nutzer eine Vergleichbarkeit von Qualität und Preis hinsichtlich des Datenschutz-Niveaus von Produkten erreicht.

Beim Datenschutz-System-Audit wird die Erfüllung der Datenschutzvorschriften seitens der verantwortlichen Stelle bezüglich ihrer internen Organisation und der eingesetzten Verarbeitungsverfahren geprüft.

2. Audit-Verfahren

2.1 Erarbeitung und Aktualisierung eines Prüfkriterienkataloges

Unter der Leitung des Bundesbeauftragten für den Datenschutz wird ein Fachausschuss gebildet. Dem Fachausschuss gehören Vertreter des Bundesamtes für Sicherheit in der Informationstechnik sowie aus Wirtschaft und Verwaltung an. Der Fachausschuss erstellt und aktualisiert einen Prüfkriterienkatalog, auf dessen Grundlage das Datenschutz-Audit bei der verantwortlichen Stelle durchzuführen ist.

Dieser Katalog enthält insbesondere Kriterien zu folgenden Bereichen:

1. Datenschutzkonzept,
2. Datenschutzorganisation,
3. Datenschutzmanagementsystem und
4. Datenschutzkontrolle.

Die Erfüllung der Katalogkriterien gewährleistet, dass alle auditierten Stellen den gleichen Prüfungskriterien unterworfen werden und damit eine Vergleichbarkeit der Ergebnisse erreicht wird.

Der Katalog wird im Bundesanzeiger veröffentlicht.

2.2 Grundsätze zur Durchführung

Ein Datenschutz-Audit wird durch mindestens zwei zugelassene Auditoren durchgeführt und ist vom bestellten Datenschutzbeauftragten der verantwortlichen Stelle zu unterstützen.

Die im Rahmen des Datenschutz-Audits erforderlichen Unterlagen sind den Auditoren zur Einsicht zur Verfügung zu stellen. Dabei kann auch auf die Unterlagen interner Datenschutz-Audits zurück gegriffen werden.

Das zu befragende Personal ist für das Datenschutz-Audit, soweit erforderlich, freizustellen.

Die Mitarbeitervertretung ist als Teil der verantwortlichen Stelle mit zu auditieren. Zur Wahrung der Vertraulichkeit der Belange der Mitarbeitervertretung wird jedoch der Audit-Bericht für den Bereich der Mitarbeitervertretung nicht dem Leiter der verantwortlichen Stelle übergeben, sondern mit dem Vorsitzenden der Mitarbeitervertretung besprochen und ihm übergeben.

Die zugelassenen Datenschutz-Auditoren prüfen die Einhaltung des deutschen Datenschutzrechts, europäischer oder internationaler sowie anderer bereichsspezifischer Datenschutz-Vorschriften, sowohl für das Datenschutz-Produkt-Audit gemäß Ziffer 2.3 als auch für das Datenschutz-System-Audit gemäß Ziffer 2.5.

Das Ergebnis des Datenschutz-Audits ist zu dokumentieren und in einem Bericht zusammen zu fassen. Der Bericht ist sowohl der Datenschutz-Zertifizierungsstelle als auch dem Leiter der verantwortlichen Stelle, dem bestellten Datenschutzbeauftragten und gegebenenfalls dem Vorsitzenden der Mitarbeitervertretung, zusammen mit Handlungsempfehlungen zu erläutern und zu übergeben. Der Bericht kann - auch in

Teilen - veröffentlicht werden. Eine teilweise Veröffentlichung darf nicht zur Verfälschung des Prüfergebnisses führen.

Die zugelassenen Auditoren sprechen eine Empfehlung zur Erteilung des Datenschutz-Zertifikats gegenüber der Datenschutz-Zertifizierungsstelle aus.

2.3 Datenschutz-Produkt-Audit

Die Auditierung wird durch zugelassene Datenschutz-Auditoren durchgeführt.

Durch das Audit wird das zu prüfende Produkt hinsichtlich der Umsetzung technischer Möglichkeiten und eventueller Mängel in der Handhabung des Datenschutzes beurteilt und bewertet.

Ansonsten erfolgt die Auditierung analog zu Ziffer 2.5.

2.4 Internes Datenschutz-System-Audit

Das interne Datenschutz-System-Audit ist an den unter Ziffer 2.5 angeführten Kriterien zu orientieren. Es wird von der verantwortlichen Stelle selbst durchgeführt.

Über die Ergebnisse ist dem Leiter der verantwortlichen Stelle schriftlich zu berichten.

Das interne Audit dient als Vorstufe eines externen Audits.

2.5 Externes Datenschutz-System-Audit

Die Auditierung wird durch zugelassene Datenschutz-Auditoren in folgenden Schritten durchgeführt:

1. In einer Einführungsbesprechung erfolgt die Festlegung von Umfang, Vorgaben und Zielen der Auditierung mit dem Leiter, dem Datenschutzbeauftragten und der Mitarbeitervertretung der verantwortlichen Stelle.
2. Durch das Audit wird das zu prüfende System hinsichtlich Umsetzung und eventueller Mängel in der Handhabung des Datenschutzes beurteilt und bewertet.
3. In einem Abschluss-/prüfbericht werden Art und Umfang der von der verantwortlichen Stelle vorzunehmenden Verbesserungen dokumentiert.

Die Bewertung des Systems durch die zugelassenen Datenschutz-Auditoren wird an Hand folgender Merkmale durchgeführt, soweit sie gesetzlich erforderlich sind:

1. die Ordnungsmäßigkeit der Bestellung des Datenschutzbeauftragten,
2. das Vorliegen und die ordnungsgemäße Führung des Verfahrensregisters,
3. die ordnungsgemäße Anwendung der Datenverarbeitungsprogramme, mit deren Hilfe personenbezogene Daten verarbeitet werden,
4. die datenschutzgerechte Planung und Einführung neuer und die Änderung bestehender Verfahren der automatisierten Verarbeitung personenbezogener Daten,
5. die Gewährleistung der Unterrichtung und der korrekten Einwilligung Betroffener bei der Verarbeitung besonderer Arten von Daten (§ 3 Abs. 9 BDSG),
6. die ordnungsgemäße Durchführung und Dokumentation der Vorabkontrolle,
7. die ordnungsgemäße Information und Belehrung der Mitarbeiter durch geeignete Maßnahmen über ihre Rechte und Pflichten und die Einhaltung der Datenschutzvorschriften,
8. die Zusammenarbeit des Leiters der verantwortlichen Stelle und der Mitarbeitervertretung in den Belangen des Datenschutzes mit dem bestellten Datenschutzbeauftragten,
9. die ordnungsgemäße und vollständige Verpflichtung auf das Datengeheimnis nach § 5 BDSG,

10. die ordnungsgemäße und vollständige Belehrung über und Verpflichtung auf das Fernmeldegeheimnis für die betreffenden Mitarbeiter nach § 89 TKG,
11. das Vorliegen und die Umsetzung von Konzepten und Maßnahmen zur Informations- und Katastrophensicherheit,
12. die technische Aktualität, die ordnungsgemäße Einhaltung und Wirksamkeit der IT-Sicherheitsmaßnahmen zur Verarbeitung personenbezogener Daten,
13. die Berücksichtigung datenschutzrechtlicher Belange in Betriebsvereinbarungen und Verträgen besonders im Rahmen der Auftragsdatenverarbeitung gemäß § 11 BDSG,
14. die Vorkehrungen zur Information der Betroffenen,
15. die ordnungsgemäße Handhabung von Übermittlungen personenbezogener Daten an Dritte, insbesondere in Drittstaaten ohne angemessenes Datenschutzniveau,
16. des Kriterienkataloges gemäß Ziffer 2.1.

2.6 Mitwirkung des bestellten Datenschutzbeauftragten

Interne Audits sind unter der fachlichen Leitung und der aktiven Teilnahme des bestellten Datenschutzbeauftragten der verantwortlichen Stelle durchzuführen.

Die Aufgabe und Stellung des bestellten Datenschutzbeauftragten darf durch die Durchführung von Datenschutz-Audits nicht beeinträchtigt werden.

Vorschläge der zugelassenen Auditoren zur Verbesserung des Datenschutzes, der Datensicherheit und zum Systemdatenschutz (§ 3 a BDSG) sind zu dokumentieren. Der bestellte Datenschutzbeauftragte überprüft die Umsetzung der vereinbarten Maßnahmen.

2.7 Erteilung und Registrierung des Datenschutz-Audit-Zertifikats

Für die Erteilung des Datenschutz-Audit-Zertifikats und des Datenschutz-Gütesiegels ist als Datenschutz-Zertifizierungsstelle eine zentrale und unabhängige Stelle einzurichten oder eine bereits bestehende zu beauftragen.

Vorstellbar ist ein „Unabhängiges Bundeszentrum für Datenschutz (UBD)“ analog dem Modell des „Unabhängigen Landesentrums für Datenschutz Schleswig-Holstein (ULD)“ oder die Industrie- und Handelskammer (IHK) in Berlin¹.

Diese Stelle erteilt der verantwortlichen Stelle bei positiver Bewertung ein Datenschutz-Audit-Zertifikat und veröffentlicht dieses in einem öffentlichen Verzeichnis. Das Datenschutz-Audit-Zertifikat berechtigt zur Führung des Datenschutz-Gütesiegels.

Mit der Erteilung des Datenschutz-Audit-Zertifikats entfällt die Kontrolle durch die Aufsichtsbehörde gemäß § 38 Abs. 1 BDSG für den auditierten Bereich während des Gültigkeitszeitraums des Zertifikats.

2.8 Gültigkeit des Zertifikats

Das erteilte Datenschutz-Produkt-Zertifikat gilt für geprüfte Produkte in der jeweilig auditierten Version. Bei Versionsänderungen ist ein Wiederholungsaudit zum Erhalt des Zertifikats erforderlich, wobei sich die Prüfung auf die geänderten Teile und ihre Einfügung in das Gesamtprodukt beschränken kann.

Das erteilte Datenschutz-System-Zertifikat gilt zwei Jahre und kann in einem Wiederholungs-Audit, das sich auf die Prüfung der Veränderungen beschränken kann, um weitere zwei Jahre verlängert werden. Sind erhebliche Veränderungen im auditierten System zu beurteilen, so ist eine erneute Zertifizierung des Gesamtsystems erforderlich.

¹ Dieser Vorschlag wird aus folgenden Gründen gemacht: 1. Bei der IHK handelt es sich um eine allseits anerkannte Körperschaft des öffentlichen Rechts. 2. Da ein bundeseinheitliches Register sinnvoll ist, schlagen wir die Konzentration auf die Bundeshauptstadt Berlin vor.

2.9 Werbung mit dem Datenschutz-Gütesiegel

Mit der Erteilung des Datenschutz-Zertifikats ist die auditierte Stelle berechtigt, das Datenschutz-Gütesiegel zu Werbe- und Marketingzwecken zu verwenden. Das Datenschutz-Gütesiegel enthält die Registrierungsnummer sowie das Gültigkeitsdatum und verweist auf die Eintragung in der Liste der zertifizierten verantwortlichen Stellen. Das Datenschutz-Gütesiegel wird zum zertifizierten Produkt und/oder zum zertifizierten System erteilt.

3. Auswahl und Zulassung der Datenschutz-Auditoren

3.1 Auswahl der Datenschutz-Auditoren

Ein Sachverständigenausschuss bei der für die Erteilung des Datenschutz-Audit-Zertifikats und des Datenschutz-Gütesiegels zuständigen Stelle entscheidet über Auswahl und Zulassung von Datenschutz-Auditoren. Dieser Ausschuss setzt sich paritätisch zusammen aus mindestens je einem Vertreter aus folgenden drei Bereichen:

1. Vertreter des Bundes- und/oder der Landes-Datenschutzbeauftragten und/oder der Aufsichtsbehörden,
2. Experten des Datenschutzes und der IT-Sicherheit aus dem Hochschulbereich,
3. Erfahrene Praktiker des Datenschutzes und der IT-Sicherheit aus Privatwirtschaft und öffentlichem Bereich.

Die Namen der Mitglieder des Ausschusses werden in geeigneter Weise veröffentlicht.

Voraussetzung für die Zulassung als Datenschutz-Auditor ist die nachgewiesene Qualifikation zum fachkundig geprüften Datenschutzbeauftragten und eine mindestens fünfjährige Berufserfahrung als Datenschutzbeauftragter oder eine qualifizierte technische oder juristische Ausbildung mit mindestens fünfjähriger Berufserfahrung auf dem Gebiet des Datenschutzes.

Die Auswahl und Zulassung erfolgt insbesondere auf der Grundlage folgender, im Detail durch den Ausschuss festzulegenden Kriterien:

1. Fachkompetenz,
2. Vertrauenswürdigkeit,
3. Zuverlässigkeit und
4. Unabhängigkeit.

Bei Stimmgleichheit des Ausschusses entscheidet die Stimme des Vorsitzenden.

3.2 Zulassung der Datenschutz-Auditoren

Die Zulassung zum Datenschutz-Auditor ist auf drei Jahre befristet. Die Verlängerung der Zulassung ist daran gebunden, dass der Auditor mindestens zwei durchgeführte Datenschutz-Audits pro Jahr nachweist. Eine erneute Zulassung ist an ein wiederholtes Verfahren vor dem Ausschuss gebunden.

Ein Datenschutz-Auditor darf nicht mehr als höchstens drei aufeinanderfolgende Audits bei derselben verantwortlichen Stelle durchführen.

3.3 Ordnungswidrigkeiten

Der Missbrauch des Gütesiegels wird mit Bußgeld bis zu 100.000 Euro bestraft. Missbrauch ist:

1. die Verwendung ohne erteiltes Zertifikat oder
2. die Weiterverwendung des Siegels nach Ablauf der Gültigkeit.

4. Anpassung/Änderung betroffener Gesetze

Soweit die IHK Berlin als zentrale Stelle für die Datenschutz-Zertifizierung und die Einrichtung des Ausschusses für die Zulassung der Datenschutz-Auditoren bestimmt wird, ist das „Gesetz zur vorläufigen Regelung des Rechts der Industrie- und Handelskammern“ anzupassen bzw. zu ändern.

Ferner ist die für die Datenschutz-Zertifizierung und die Einrichtung des Ausschusses für die Zulassung der Datenschutz-Auditoren zuständige Stelle zu ermächtigen, durch Satzung einen Gebührenkatalog zu erlassen über:

1. die Kosten für die Zulassung zum externen Datenschutz-Auditor
2. die Kosten für die Erteilung des Datenschutz-Audit-Zertifikats in Verbindung mit der entsprechenden Veröffentlichung.

Bei der unter Ziffer 2.7 Abs. 2 genannten 1. Alternative kann die Regelung im DSAG selbst erfolgen.