Kriterienkatalog mit Erläuterungen

Version 1.0

01.08.2015

Inhaltsverzeichnis

Auf ein Wort…

Die datenschutz cert GmbH bietet Unternehmen des interaktiven Handels, d.h. Online- und Versandhandelsunternehmen, ein Datenschutzzertifikat – das Datenschutzgütesiegel für den Interaktiven Handel – an. Ziel ist es, Unternehmen die Möglichkeit zu geben, das Thema Datenschutz pro-aktiv und positiv zu besetzen und dies durch ein Zertifikat nach außen hin zu dokumentieren.

Die datenschutz cert GmbH ist bundesweit als Dienstleister im Bereich von Datenschutz- und IT-Sicherheit tätig. Als akkreditierte Zertifizierungsstelle erteilt die datenschutz cert GmbH u.a. international gültige Zertifikate gemäß ISO/IEC 27001 für Informationssicherheits-Managementsysteme (ISMS).

In die Erarbeitung dieses Zertifizierungsprozesses sowie des Kriterienkatalogs ist die Fachexpertise des Branchenverbandes bevh e.V. eingeflossen, für die wir uns herzlich bedanken.

Geprüft und zertifiziert wird das Unternehmen, wenn ein vorbildlicher Datenschutz etabliert und umgesetzt wird und die einschlägigen gesetzlichen Anforderungen erfüllt sind. Die Grundidee zur Realisierung eines vorbildlichen Datenschutzes ist dabei, Datenschutz im Unternehmen nachhaltig als Prozess zu etablieren und die Umsetzung kontinuierlich aufrechtzuerhalten – kurz gesagt, ein Datenschutzmanagement zu betreiben. Das Datenschutzmanagement bewertet vor allem diejenigen Vorkehrungen, die der Verbraucher nicht „sieht“ bzw. die er selbst nicht überprüfen kann. Aus diesem Grunde kommt der Transparenz der Prüfungskriterien für die Prüfung (Auditierung) und Zertifizierung besondere Bedeutung zu.

Über die Einhaltung rechtlicher Anforderungen hinaus zeichnet sich ein datenschutzrechtlich vorbildliches Unternehmen dadurch aus, dass es mehr für den Datenschutz unternimmt, als ausdrücklich gesetzlich gefordert ist. Mit dem Datenschutzgütesiegel wird die Einhaltung dieser vorbildlichen Maßnahmen dem Kunden sowie anderen Dritten deutlich gemacht.

Die datenschutz cert GmbH ist bundesweit als Dienstleister im Bereich von Datenschutz- und IT-Sicherheit tätig. Als akkreditierte Zertifizierungsstelle erteilt die datenschutz cert GmbH u.a. international gültige Zertifikate gemäß ISO/IEC 27001 für Informationssicherheits-Managementsysteme (ISMS).

Berlin und Bremen, im August 2015

Dr. Irene Karper LL.M.Eur.

datenschutz cert GmbH

1. Ihr Weg zum Datenschutzgütesiegel – der Ablauf im Überblick

In diesem Kapitel möchten wir Ihnen den Ablauf des Auditierungs- und Zertifizierungsverfahrens für das Datenschutzgütesiegel für den Interaktiven Handel erläutern und wesentliche Begriffe erklären. Sodann finden Sie Erläuterungen zu den jeweiligen Fragen des Fragebogens und Auslegungshilfen und damit einen Eindruck, welche Themen auf Sie bei der Auditierung (Prüfung) zukommen können.

Bitte beachten Sie, dass dieser Kriterienkatalog lediglich Empfehlungen beinhaltet, die keine Rechtsberatung ersetzen. Eine genaue Bewertung der individuellen, rechtskonformen Umsetzung des Datenschutzes in Ihrem Unternehmen, z.B. durch Ihre Datenschutzbeauftragte oder Ihren Datenschutzbeauftragten[1], ist unumgänglich.

1.1 Was soll auditiert und zertifiziert werden?

Auditiert und zertifiziert wird das Datenschutzmanagement eines Unternehmens, welches interaktiven Handel betreibt, und damit Prozesse, welche die Einhaltung der Vorgaben des Datenschutzes gewährleisten und fördern sollen.

Zunächst einmal definieren wir mit Ihrer Hilfe den Gegenstand der Auditierung. Hierfür machen Sie in einem von uns zur Verfügung gestellten Fragebogen bitte die entsprechenden Angaben. Wichtig ist, hier bereits den Standort Ihres Unternehmens zu benennen, der später auch vor Ort geprüft und zertifiziert werden soll. Pro Unternehmen wird zunächst nur ein Standort geprüft und zertifiziert. Dies ist in der Regel der Hauptsitz des Unternehmens des Antragstellers. Sofern aus einer Firmengruppe oder einem Konzern mehrere juristische Personen das Datenschutzgütesiegel erhalten sollen, ist jeweils ein separater Antrag nebst Fragebogen auszufüllen.

Sollte Ihr Unternehmen mehrere Niederlassungen haben, so achten Sie bitte darauf, dass Sie die Fragen im Teil C des Kataloges (technisch-organisatorische Datenschutzmaßnahmen) abschließend für alle Niederlassungen (im Inland und im Ausland) gesondert ausfüllen. Je nach Anzahl der Standorte erweitert sich der Fragebogen entsprechend. Nur so können wir die ggf. in jeder Niederlassung anders umgesetzten Sicherheitsmaßnahmen bewerten und für das Unternehmen in seiner Gesamtheit ein Datenschutzgütesiegel vergeben.

Gegenstand der Prüfung und Vergabe des Datenschutzgütesiegels ist stets das gesamte Unternehmen, wobei ausschließlich der Kunden- und Verbraucherdatenschutz im Fokus steht. Das Datenschutzgütesiegel soll dem Verbraucher verdeutlichen, dass seine Daten in datenschutzkonformer Weise verarbeitet werden. Aufgrund des in der E-Commerce-Brache üblichen direkten Kundenkontaktes umfasst die Prüfung auch die Webseiten Ihres Unternehmens. Rechtliche Aspekte des Datenschutzes am Arbeitsplatz werden von diesem Zertifikat hingegen nicht erfasst.

[1] Mit den nachfolgenden männlichen Bezeichnungen möchten die Verfasser gleichsam weibliche und männliche Personen einbeziehen.

1.2 Antrag und Fragebogen

Der bei der datenschutz cert GmbH abrufbare Antrag samt Fragebogen ist die Grundlage für die spätere Prüfung durch unsere Auditoren. Mit Nutzung des Fragebogens erkennen Sie die Vergabe- und Nutzungsbedingungen des Datenschutzgütesiegels für den Interaktiven Handel an.

Bitte nehmen Sie sich Zeit für die Beantwortung. Ihre Angaben werden später im Audittermin vor Ort von den Auditoren gegengeprüft. Unzutreffende Angaben führen zur Versagung bzw. zum Entzug des Datenschutzgütesiegels oder zu einer kostenpflichtigen Wiederholungsprüfung.

Anhand des vollständig ausgefüllten Fragebogens können Sie sofort sehen, ob Ihr Antrag Aussicht auf Erfolg hätte. Füllen Sie Fragen nicht aus oder entsprechen Ihre Antworten nicht der Rechtslage bzw. unserem Kriterienkatalog, erhalten Sie ein negatives Ergebnis. Entsprechen Ihre Antworten den Vorgaben des Fragenkataloges und damit den gesetzlichen Grundanforderungen, erhalten Sie ein positives Ergebnis und können den ausgefüllten Bogen samt Antrag unterzeichnet an

datenschutz cert GmbH
z. Hd. Dr. Irene Karper
Konsul-Smidt-Str. 88a
28217 Bremen

übersenden.

Sollten Ihnen Fragestellungen unklar sein, stehen Ihnen in diesem Kriterienkatalog Auslegungshilfen zur Verfügung. Im Zweifelsfall helfen wir Ihnen gern weiter.

1.3 Auditierung des Unternehmens vor Ort

Nach Eingang Ihres Antrags samt Fragebogen prüfen unsere Auditoren diesen auf Schlüssigkeit. Für den Fall der Zertifizierungsfähigkeit werden die Dokumente an die Zertifizierungsstelle bei der datenschutz cert GmbH weitergeleitet.

Wir stellen Ihnen eine Auswahl möglicher fachkundiger und lizenzierter Auditoren gerne zur Verfügung, aus der Sie den für Sie zuständigen Auditor auswählen. Im Bedarfsfall können wir Empfehlungen aussprechen.

Alle Auditoren und Verfahrensbeteiligten sind vertraglich zur vollsten Verschwiegenheit verpflichtet.

Der oder die Auditoren (maximal zwei Personen) setzen sich dann mit Ihnen über die von Ihnen angegebenen Kontaktdaten in Verbindung und vereinbaren einen Termin für die Auditierung vor Ort (sogenannter Site Visit).

Sicherlich möchten Sie sich gut auf die Prüfung vorbereiten. Sie erhalten daher eine Agenda mit dem wesentlichen Ablauf des Audits. Ferner sollten Sie Dokumente, die Sie im Fragebogen als Referenz angegeben haben, parat halten.

Für einige wesentliche Dokumente hält übrigens auch der Branchenverbandes bevh e.V. ggf. Vorlagen für Mitglieder oder Preferred Business Partner bereit. Für die Vergabe des Datenschutzgütesiegels für den Interaktiven Handel ist eine Mitgliedschaft im bevh e.V. keine zwingende Voraussetzung, wenngleich empfehlenswert.

Der Auditor prüft, ob Ihre Angaben auch tatsächlich so im Unternehmen umgesetzt wurden und erfragt dabei z.B. das Verfahrensverzeichnis, Muster für die Verpflichtung von Beschäftigten auf das Datengeheimnis, angegebene Dokumentationen zum Datenschutz oder den Ablauf bei Fragen und Beschwerden zum Datenschutz. Unternehmensinterne Richtlinien, Anweisungen oder Vereinbarungen (z.B. Datenschutzkonzept, Passwortrichtlinien), die im Fragebogen bzw. Kriterienkatalog angesprochen sind, müssen ebenfalls vorgelegt werden.

Das Audit vor Ort ist eine Momentaufnahme zum Stand des Datenschutzes in Ihrem Unternehmen. Dabei richten sich die Fragen und Bewertungen der Auditoren neben dem Kriterienkatalog an der aktuellen Auslegung der rechtlichen und technischen Anforderungen aus.

1.4 Ergebnisse der Auditierung

Am Ende der Auditierung erstellt der Auditor ein Auditprotokoll mit den Ergebnissen. Die Auditierung dient zugleich der weiteren Optimierung der Datenschutzorganisation in Ihrem Unternehmen.

Sollte hierbei eine Hauptabweichung zum Kriterienkatalog festgestellt werden (bspw. fehlt ein gesetzlich vorgeschriebenes Verfahrensverzeichnis), endet das Auditverfahren mit dem Ergebnis, das kein Datenschutzgütesiegel erteilt werden kann. Wird die Hauptabweichung später behoben, kann ein neuer Antrag gestellt werden.

Möglich ist auch, dass eine sogenannte Nebenabweichung festgestellt wird; hierbei handelt es sich um eine geringe Abweichung von den Anforderungen des Kriterienkataloges, bei denen die Anforderungen an den Datenschutz jedoch insgesamt noch erfüllt sind (bspw. liegt ein Verfahrensverzeichnis vor, es fehlt darin aber eine Angabe zur Datenübermittlung an Dritte). Nebenabweichungen müssen ebenfalls behoben werden; allerdings stehen sie einer Gütesiegelvergabe nicht entgegen, wenn noch während des Audits vor Ort ein Plan dargereicht wird, welcher verbindlich Maßnahmen zur sinnvollen und wirkungsvollen Behebung der Nebenabweichung sowie einen Termin zu Umsetzung innerhalb von maximal zwei Wochen dokumentiert. Nachweise zur Umsetzung sind der Zertifizierungsstelle dann unaufgefordert innerhalb von maximal vier Wochen einzureichen. Wird die Frist nicht eingehalten oder sind die Nachweise nach Bewertung der Auditoren unzureichend, um die Nebenabweichung zu beheben, wird das Datenschutzgütesiegel nicht erteilt. Um später das Gütesiegel zu erhalten, kann dann ein neuer Antrag gestellt werden.

Ferner können im Audit Empfehlungen ausgesprochen werden, die der Optimierung des Datenschutzmanagements dienen (bspw. liegen die gesetzlich geforderten Dokumente vor, sind auch inhaltlich richtig, es fehlt aber eine Versionsnummer, um Änderungen besser nachvollziehen zu können). Diese Empfehlungen beeinträchtigen nicht die erfolgreiche Gütesiegelvergabe. Deren Umsetzung oder Gründe der Nichtumsetzung werden allerdings im Rahmen folgender Auditierungen i.d.R. abgefragt werden.

Anschließend wird das Auditprotokoll finalisiert und bei der Zertifizierungsstelle mit einem Votum des Auditors eingereicht. Sie erhalten eine Kopie des Auditprotokolls.

1.5 Zertifizierung und Gültigkeit

Die Zertifizierungsstelle der datenschutz cert GmbH prüft das Auditprotokoll samt Votum auf Schlüssigkeit und erteilt bei Vorliegen aller Voraussetzungen des Kriterienkataloges und der Vergabe- und Nutzungsbedingungen das Zertifikat. Hierüber erhalten Sie eine Urkunde. Ferner wird das Zertifikat mit dem Unternehmensnamen, der Zertifizierungs-Nummer und -Gültigkeit auf den Webseiten der datenschutz cert GmbH in einer Zertifizierungsliste veröffentlicht.

Das Datenschutzgütesiegel ist ab Ausstellung der Urkunde für zwei Jahre gültig, es sei denn, es wird vorzeitig entzogen, z.B. weil Tatsachen bekannt werden, nach denen einzelne Kriterien offensichtlich nicht mehr erfüllt werden. Bitte beachten Sie hierzu auch unsere **Vergabe und Nutzungsbedingungen,** die auf der Webseite der datenschutz cert GmbH unter http://www.datenschutz-cert.de abrufbar sind.

Nach Ablauf der Gültigkeitsdauer kann eine neue Auditierung mit dem Ziel der Re-Zertifizierung beauftragt werden. Das sich dann anschließende Verfahren ist in der Regel weniger aufwändig. Der Fragebogen wird hierzu von Ihnen aktualisiert. Im Audit können dann z.B. Stichproben vor Ort durchgeführt oder auch andere Niederlassungen/Standorte des Antragstellers geprüft werden.

2. Begriffsbestimmungen

Nachfolgend sind einige spezifische Begriffe des Fragenkataloges erläutert[2].

Verantwortliche Stelle	ist jede Person oder Stelle, die personenbezogene Daten für sich selbst erhebt, verarbeitet oder nutzt oder dies durch andere im Auftrag vornehmen lässt. In der Regel ist der Antragsteller verantwortliche Stelle, soweit er diese Voraussetzungen erfüllt.
Dritter	ist jede natürliche oder juristische Person oder Stelle außerhalb der verantwortlichen Stelle, die nicht Betroffener ist.
Betroffener	ist jede natürliche Person mit deren personenbezogenen oder personenbeziehbaren Daten umgegangen wird.
Verbraucher	ist jede natürliche Person, die ein Rechtsgeschäft zu einem Zwecke abschließt, der weder ihrer gewerblichen noch ihrer selbständigen beruflichen Tätigkeit zugerechnet werden kann.
Personenbezogene Daten	sind Einzelangaben über persönliche oder sachliche Verhältnisse einer bestimmten oder bestimmbaren natürlichen Person; als bestimmbar wird eine Person z.B. angesehen, die direkt oder indirekt identifiziert werden kann, insbesondere durch Zuordnung zu einer Kennnummer oder zu einem oder mehreren spezifischen Elementen, die Ausdruck ihrer physischen, physiologischen, psychischen, wirtschaftlichen, kulturellen oder sozialen Identität sind.
Besondere Arten personenbezogener Daten	sind Daten über die rassische oder ethnische Herkunft, politische Meinung, religiöse oder philosophische Überzeugung, Gewerkschafts-zugehörigkeit, Gesundheit oder das Sexualleben.
Verarbeitung personenbezogener Daten	ist jeder mit oder ohne Hilfe automatisierter Verfahren ausgeführte Vorgang, der der Erhebung im Sinne einer Datenbeschaffung, der Speicherung, der Organisation, der Aufbewahrung, der Anpassung, der Veränderung, der Abfrage, der Nutzung, der Weitergabe durch Übermittlung, der Verbreitung oder der Kombination bzw. dem Abgleich von Daten dient. Auch das Sperren, das Löschen oder das Vernichten werden umfasst.

[2] Begriffsdefinitionen können insbesondere den §§ 2 und 3 Bundesdatenschutzgesetz (BDSG) entnommen werden.

3. Teil A - Organisation des Datenschutzes

Nachfolgend werden die einzelnen Fragen des Fragebogens erklärt und Handlungshilfen für das Audit gegeben.

Teil A beschäftigt sich mit den Fragen der Organisation des Datenschutzes – auch „Datenschutzmanagement“ in Ihrem Unternehmen.

3.1 A1 - Beschäftigtenanzahl im Unternehmen: Mehr als neun

Sind in Ihrem Unternehmen mehr als neun Personen mit der automatisierten Verarbeitung von personenbezogenen Daten beschäftigt?

Sind mehr als neun Mitarbeiter eines Unternehmens mit der automatisierten Verarbeitung von personenbezogenen Daten befasst, hat das Unternehmen einen betrieblichen Datenschutzbeauftragten (bDSB) zu bestellen.

Anhand der Antwort auf die Frage soll festgestellt werden, ob eine Verpflichtung zur Bestellung eines Datenschutzbeauftragten überhaupt besteht oder nicht.

3.2 A2 - Beschäftigtenanzahl im Unternehmen: Mehr als 20

Falls A1 nein: Sind in Ihrem Unternehmen mehr als 20 Personen mit der Verarbeitung personenbezogener Daten beschäftigt?

Für Unternehmen, die mehr als 20 Personen mit der, auch nicht-automatisierten, Verarbeitung von personenbezogenen Daten beschäftigen, gilt die Verpflichtung zur Bestellung eines bDSB ohne jede Ausnahme.

Anhand der Antwort auf die Frage soll festgestellt werden, ob eine Verpflichtung zur Bestellung eines Datenschutzbeauftragten überhaupt besteht oder nicht.

3.3 A3 - Adresslistbroker, Markt- und Meinungsforschung

Falls A1 und A2 nein: Ist Ihr Unternehmen als Adresslistbroker oder Markt- und Meinungsforschungsunternehmen tätig?

Für Unternehmen, die personenbezogene Daten ausschließlich geschäftsmäßig zum Zweck der Übermittlung automatisiert verarbeiten, gilt die Verpflichtung zur Bestellung eines bDSB ohne jede Ausnahme.

Anhand der Antwort auf die Frage soll festgestellt werden, ob eine Verpflichtung zur Bestellung eines Datenschutzbeauftragten überhaupt besteht oder nicht.

3.4 A4 - Besondere Dienstleistungen

Falls A1-A3 nein: Unterhält Ihr Unternehmen Verfahren, die besondere Risiken für die Persönlichkeitsrechte der von der Datenverarbeitung betroffenen Personen beinhalten?

Unternehmen, die besonders risikoträchtige Datenverarbeitungsverfahren unterhalten (z.B. Videoanlagen, Gesundheitsdatenbanken), müssen einen Datenschutzbeauftragten bestellen, da solche Verfahren die sogenannte Vorabkontrollpflicht durch den bDSB auslösen (dazu sogleich). Anhand der Antwort auf die Frage soll festge-

stellt werden, ob eine Verpflichtung zur Bestellung eines Datenschutzbeauftragten überhaupt besteht oder nicht.

3.5 A5 - Bestellung eines Datenschutzbeauftragten

Falls einer der Fragen A1-A4 mit ja beantwortet wurden: Wurde ein betrieblicher Datenschutzbeauftragter (bDSB) gemäß Bundesdatenschutzgesetz (BDSG) bestellt?

Der bDSB hat gemäß § 4g Abs. 1 BDSG die Aufgabe, auf die Einhaltung des Bundesdatenschutzgesetzes sowie anderer Vorschriften über den Datenschutz hinzuwirken. Konkret hat er die ordnungsgemäße Anwendung von Datenverarbeitungsprogrammen zu überwachen und die Information der Beschäftigten zum Datenschutz (z.B. durch Schulungen) sicherzustellen. Er ist von dem Unternehmen rechtzeitig über geplante personenbezogene Datenverarbeitungsverfahren zu unterrichten und muss ggf. Vorabkontrollen durchführen. Vorabkontrollen sind immer dann durchzuführen, wenn ein Datenverarbeitungsverfahren besondere Risiken für die Persönlichkeitsrechte der Betroffenen aufweisen und zielen auf eine Analyse der Beherrschbarkeit des neu einzuführenden Verfahrens vor Aufnahme des eigentlichen Wirkbetriebes ab. Ferner ist dem bDSB das sog. Verfahrensverzeichnis gem. § 4e Satz 1 BDSG zur Verfügung zu stellen. Unter einem Verfahrensverzeichnis versteht man die Dokumentation aller Verfahren zur Verarbeitung personenbezogener Daten in einem Unternehmen in dem nach § 4e BDSG vorgegebenen Umfang.

Wurde trotz Bestellpflicht kein betrieblicher Datenschutzbeauftragter bestellt, endet das Audit mit nicht-bestanden.

3.6 A6 - Kontaktdaten des Datenschutzbeauftragten

Falls ja: Bitte geben Sie Name und Kontaktdaten des bDSB an.

Diese Angaben werden benötigt, um im Audit und bei Rückfragen mit der Person in Kontakt treten zu können.

3.7 A7 - Haupt-/Nebenberuf als Datenschutzbeauftragter

Falls ja: Ist der bDSB für Datenschutz haupt- oder nebenberuflich tätig?

Die Hauptberuflichkeit oder Nebenberuflichkeit dieser Person ist insofern relevant, als dass der Nebenberuf nicht mit den Aufgaben des Datenschutzbeauftragten kollidieren darf. Eine nebenberufliche Tätigkeit kann aber ebenso auch für die besondere Fachkunde und Integration des Datenschutzbeauftragten in den Betrieb sprechen. Mit Ihren Angaben soll später im Audit anhand des Einzelfalls überprüft werden, ob die bestellte Person tatsächlich unabhängig ist oder nicht.

3.8 A8 - Bestellurkunde

Falls ja: Liegt eine Bestellungsurkunde des bDSB vor?

Die Bestellung sollte nachweisbar und daher schriftlich (in der Regel durch eine Bestellungsurkunde) erfolgen. Ob auch der bDSB die Bestellungsurkunde unterschreiben muss, ist eine Frage des Einzelfalls. Das BDSG sieht ferner einen Kündigungsschutz für die bestellte Person vor.

Im Audit muss ein Dokument vorgelegt werden können, welches die Bestellung der Person bestätigt.

Ein Muster hierfür kann dem Fragenkatalog entnommen werden. Ist dies nicht gegeben, wird das Audit mit nicht-bestanden bewertet.

3.9 A9 - Unabhängigkeit des Datenschutzbeauftragten

Falls ja: Ist die Unabhängigkeit des bDSB u.a. dadurch sichergestellt, dass dieser nicht der Geschäftsleitung oder relevanten Leitungsfunktionen (etwa der Geschäfts-, IT-, Personal- oder Vertriebsabteilung) angehört?

Bestellt werden kann jede unabhängige Person. Dies kann auch eine externe Stelle oder betriebsfremde Person sein. Zum bDSB darf nicht benannt werden, wer wegen anderer in einem Unternehmen von ihm wahrzunehmender Funktionen in einen unzumutbaren Interessenkonflikt geraten würde. So dürfen Mitglieder der Geschäftsleitung sowie die Leiter der EDV, Personal- oder Vertriebsabteilung grundsätzlich nicht zugleich das Amt des bDSB begleiten. Sollte in Ausnahmefällen dennoch die Funktion des bDSB mit einer grundsätzlich unverträglichen Position zusammenfallen (dies kann insbesondere bei kleineren Unternehmen aufgrund eingeschränkter personeller Ressourcen der Fall sein), wird Sie der Auditor hierzu befragen und eine abschließende Entscheidung treffen. Der bDSB ist in seiner Funktion dem Geschäftsführer/Vorstand direkt zu unterstellen.

Ist dies nicht gegeben, wird das Audit mit nicht-bestanden bewertet.

3.10 A10 - Fachkundenachweise des Datenschutzbeauftragten

Falls ja: Kann der bDSB Erfahrungen oder Schulungen zum Thema Datenschutz nachweisen?

Der bDSB muss die für seine Aufgabe erforderliche Fachkunde und Zuverlässigkeit besitzen. Dies setzt u.a. voraus, dass er die notwendigen Kenntnisse über das Unternehmen und seine Organisation, Kenntnisse über die Datenverarbeitung, insbesondere über die eingesetzte Hard- und Software sowie Kenntnisse hinsichtlich der einschlägigen rechtlichen Vorschriften vorweist.

Eine gute Umsetzung der gesetzlichen Anforderungen an die Person und die Aufgabe des betrieblichen Datenschutzbeauftragten zeigt sich insbesondere an seiner kontinuierlichen Aus- und Fortbildung. Werden interne Mitarbeiter für diese Position eingesetzt, haben diese anfangs oftmals keine umfassenden Qualifikationen, sondern müssen sich diese im Laufe der Zeit erst aneignen. Unternehmen, die in diesem Bereich vorbildlich handeln, geben dem Datenschutzbeauftragten z.B. die Möglichkeit, sich durch regelmäßige Fortbildungsveranstaltungen weiterzubilden. Hier können auch datenschutz-spezifische Fachkreise angegeben werden, wie z.B. die Teilnahme am Arbeitskreis Datenschutz des bevh e.V. für Mitglieder.

Kann keine Erfahrung oder Schulung nachgewiesen werden, wird das Audit mit nicht-bestanden bewertet.

3.11 A11 - Weisungsfreiheit des Datenschutzbeauftragten

Falls ja: Ist der bDSB weisungsfrei bei der Ausübung der gesetzlich vorgesehenen Funktionen?

In der Aufgabenwahrnehmung ist der bDSB weisungsfrei (§ 4f Abs. 3 Satz 2 BDSG). Er kann also nicht von der Unternehmensleitung angewiesen werden, bestimmte Aufgaben nicht oder zu einem späteren Zeitpunkt anzugehen oder andere Aufgaben bevorzugt oder in bestimmter Weise zu erledigen.

Ist dies nicht gegeben, wird das Audit mit nicht-bestanden bewertet.

3.12 A12 - Sonstige Ansprechpartner für Datenschutz

Falls in Ihrem Unternehmen kein bDSB bestellt wurde: Gibt es einen Ansprechpartner für Kunden und Beschäftigte bei Fragen zum Datenschutz?

Sollte keine gesetzliche Pflicht zur Bestellung eines bDSB bestehen, obliegt die Kontroll- und Sensibilisierungspflicht der Unternehmensleitung selbst. In jedem Fall muss es daher zumindest einen Ansprechpartner für Fragen zum Datenschutz und zur IT-Sicherheit im Unternehmen geben.

Ist dies nicht gegeben, wird das Audit mit nicht-bestanden bewertet.

3.13 A13 - Verpflichtung von Beschäftigten auf das Datengeheimnis

Sind Beschäftigte, die mit personenbezogenen Daten umgehen, gemäß § 5 BDSG auf das Datengeheimnis verpflichtet worden?

Gemäß § 5 BDSG sind alle mit der Verarbeitung personenbezogener Daten Beschäftigten bei Aufnahme ihrer Tätigkeit auf das Datengeheimnis zu verpflichten. Das Datengeheimnis besteht auch nach Beendigung ihrer Tätigkeit fort. Einer (Selbst)-Verpflichtung der Geschäftsführung bedarf es hingegen nicht.

Im Audit ist den Auditoren hierzu ein Beispiel vorzulegen. Im Fragenkatalog können Sie hierzu ein Muster abrufen.

Ist dies nicht gegeben, wird das Audit mit nicht-bestanden bewertet.

3.14 A14 - Informationen zum Thema Datenschutz für Beschäftigte

Werden mit der Datenverarbeitung betraute Beschäftigte regelmäßig, mindestens 1x jährlich, über Themen zum Datenschutz oder zur Datensicherheit informiert (z.B. in Schulungen, Merkblättern, Rundschreiben, Fachsitzungen, persönlichen Gesprächen)?

Von besonderer Bedeutung für ein funktionierendes Datenschutzmanagement im Unternehmen ist die Sensibilisierung der Beschäftigten für das Thema. Gerade an der Schnittstelle von Unternehmen und Verbraucher aber auch von Personalverantwortlichen und der Belegschaft muss die Einhaltung datenschutzrechtlicher Standards sichergestellt werden. Aus diesem Grund hat der bDSB gemäß § 4e BDSG die Aufgabe, die bei der Verarbeitung personenbezogener Daten tätigen Beschäftigten durch geeignete Maßnahmen mit Vorschriften über den Datenschutz und mit den jeweiligen besonderen Erfordernissen des Datenschutzes vertraut zu machen.

Dies kann durch Schulungen aber auch durch Richtlinien, Anweisungen, Merkblätter o.Ä. geschehen. Z.B. kann es auch sinnvoll sein, Erinnerungen per Run-E-Mail oder Mitteilungen am Schwarzen Brett eines Unternehmens zum Thema Datenschutz zu verbreiten. Hier sind verschiedene Möglichkeiten denkbar, die im Audit abgefragt werden.

Liegen gar keine Anhaltspunkte für entsprechende Maßnahmen vor, wird das Audit mit nicht-bestanden bewertet.

3.15 A15 - Vorliegen eines rechtskonformen Verfahrensverzeichnisses

Liegt ein Verfahrensverzeichnis mit den gesetzlich geforderten Mindestangaben gemäß § 4g Abs. 2 Satz 2 i.V.m. § 4 e Satz 1 Nr. 1-9 BDSG vor?

Gemäß § 4g Abs. 2 Satz 2 i.V.m. § 4 e Satz 1 Nr. 1-9 BDSG müssen für jedes Verfahren automatisierter Datenverarbeitung bestimmte Angaben in einem sogenannten Verfahrensverzeichnis zusammengefasst werden. Das Verfahrensverzeichnis besteht aus einem Deckblatt und genau der Anzahl Anlagen, die der Anzahl der automatisierten Datenverarbeitungsverfahren in Ihrem Unternehmen entsprechen. Im Fragenkatalog steht Ihnen eine Vorlage zur Verfügung. Folgende Mindestangaben müssen im Verfahrensverzeichnis erfasst sein:

- Name oder Firma der verantwortlichen Stelle,
- Inhaber, Vorstände, Geschäftsführer oder sonstige gesetzliche oder nach der Verfassung des Unternehmens berufene Leiter und die mit der Leitung der Datenverarbeitung beauftragten Personen,
- Anschrift der verantwortlichen Stelle,
- Zweckbestimmungen der Datenerhebung, -verarbeitung oder -nutzung,
- Beschreibung der betroffenen Personengruppen und der diesbezüglichen Daten oder Datenkategorien; Als betroffene Personengruppen kommen beispielsweise Kunden oder Arbeitnehmer in Betracht. Insbesondere soll auch ersichtlich sein, ob es sich um Daten nach § 3 Abs. 9 BDSG handelt. Eine möglichst detaillierte Angabe (Datenfeldbezeichnung) ist dafür erforderlich;
- Empfänger oder Kategorien von Empfängern, denen die Daten mitgeteilt werden können; Empfänger ist nach der Definition des § 3 Abs. 8 BDSG jede Person oder Stelle, die Daten erhält. Dazu gehören beispielsweise auch Auftragnehmer im Rahmen eines Auftragsverhältnisses nach § 11 BDSG;
- Regelfristen für die Löschung der Daten, z.B.
  - steuerlich relevante Dokumente: 10 Jahre (§ 147 Abs. 3 AO)
  - Handelsbriefe: 6 Jahre (§ 147 Abs. 3 AO i.V.m. § 257 Abs. 2 HBG)
  - Verbraucherdaten ohne steuerliche Relevanz: Löschung, sofern die Daten für den ursprünglichen Zweck oder einen anderen legitimen Zweck nicht mehr erforderlich sind (§ 35 Abs. 2 Nr. 3 BDSG)
  - Aufbewahrungsfristen aus Spezialnormen (GOBS, GDPdU, Lebensmittelrecht,...)
- eine geplante Datenübermittlung in Drittstaaten,

--- eine allgemeine Beschreibung, die es ermöglicht, vorläufig zu beurteilen, ob die Maßnahmen nach § 9 BDSG zur Gewährleistung der Sicherheit der Verarbeitung angemessen sind.

Für jedes Verfahren automatisierter Datenverarbeitung, das unterschiedlichen Zwecken dient, wie etwa Vertragsverarbeitungen, Werbedateien, Personaldatenverarbeitung, Finanzbuchhaltung etc., sind im Anlagenteil des Verfahrensverzeichnisses gesondert entsprechende Angaben zu dokumentieren und ggf. – im Rahmen der Meldepflicht – der Datenschutz-Aufsichtsbehörde zu melden.

Ist dies nicht gegeben, wird das Audit mit nicht-bestanden bewertet.

3.16 A16 - Einsichtsmöglichkeit in das Verfahrensverzeichnis

Kann das Verzeichnis von jedermann auf Anfrage eingesehen werden?

Aus § 4g Abs. 2 Satz 2 BDSG ergibt sich die Verpflichtung des betrieblichen Datenschutzbeauftragten, die Angaben des § 4e Satz 1 Nr. 1-8 BDSG „auf Antrag jedermann in geeigneter Weise verfügbar“ zu machen. Bis auf die Beschreibung der technisch-organisatorischen Maßnahmen müssen alle sonstigen Angaben des Verfahrensverzeichnisses auf Nachfrage zur Verfügung gestellt werden. Der Begriff „in geeigneter Weise verfügbar zu machen“ bedeutet dabei allerdings nicht zwangsläufig, dass die Angaben schriftlich zu machen sind. Denkbar ist auch eine mündliche Auskunft oder die Möglichkeit zur Einsichtnahme vor Ort, oder auch eine Veröffentlichung des Verfahrensverzeichnisses im Internet. Die Einsicht darf nicht erschwert werden (z.B. durch eine Kostenpflicht).

Das Verzeichnis sämtlicher Verfahren muss vor dem Vor-Ort-Termin der Auditoren in Ihrem Unternehmen dem Antrag beigefügt oder zumindest durch Inhaltsverzeichnis nachgewiesen werden. Es wird im Vor-Ort-Termin von den Auditoren eingesehen.

Kann es nicht vorgelegt oder eingesehen werden, endet das Audit mit nicht-bestanden.

3.17 A17 - Aktualität des Verfahrensverzeichnisses

Ist das Verfahrensverzeichnis älter als zwei Jahre?

Da sich die Hard- und Softwarelandschaft im Unternehmen ständig ändert, ist es sinnvoll, das Verfahrensverzeichnis regelmäßig zu aktualisieren, z.B. mindestens alle zwei Jahre. Bei älteren Verzeichnissen ist gegenüber den Auditoren zu begründen, warum das Verzeichnis nicht aktualisiert wurde.

Wurden Verfahren zwischenzeitlich geändert, ohne dass das Verzeichnis aktualisiert wurde und liegt dies mehr als zwei Jahre zurück, so endet das Audit mit nicht-bestanden.

3.18 A18 - Vorabkontrolle von Verfahren

Werden neue IT-Systeme oder Anwendungen, in denen personenbezogene Daten verarbeitet werden, vor Einführung datenschutzrechtlich und datensicherheitstechnisch überprüft?

Gemäß § 4d Abs. 5 BDSG unterliegen automatisierte Verarbeitungen einer Prüfung vor Beginn der Verarbeitung (Vorabkontrolle), wenn sie besondere Risiken für die Rechte und Freiheiten der Betroffenen aufweisen. Eine Vorabkontrolle ist insbesondere durchzuführen, wenn besondere Arten personenbezogener Daten verarbeitet werden (z.B. Gesundheitsdaten) oder wenn die Verarbeitung personenbezogener Daten dazu bestimmt ist, die Persönlichkeit des Betroffenen zu bewerten einschließlich seiner Fähigkeiten, seiner Leistung oder seines Verhaltens. Ein weiteres Beispiel ist der Einsatz von Videotechnik im Unternehmen. Ausnahmen der Vorabkontrollpflicht sind in § 4 Abs. 5 BDSG definiert. Es muss daher grundsätzlich gewährleistet sein, dass Vorabkontrollen durchgeführt werden können. Im Audittermin werden die Auditoren z.B. abfragen, ob ein Prozess zur Einbindung des bDSB bei Einführung risikoträchtiger Datenverarbeitungsverfahren im Unternehmen etabliert ist, ob Vorabkontrollen stattgefunden haben und falls nein, warum nicht.

Die Durchführung von Vorabkontrollen, zumindest aber deren Ergebnis, ist schriftlich zu dokumentieren, z.B. durch Freigaben, Bestellungsbestätigungen etc. Ein Formular kann dem Fragebogen entnommen werden.

Liegen Anhaltspunkte dafür vor, dass trotz eines relevanten Verfahrens keine Vorabkontrolle durchgeführt wurde, endet das Audit als nicht-bestanden.

3.19 A19 - Regelmäßige Kontrollen von Verfahren

Wird regelmäßig überprüft, ob bestehende IT-Systeme oder Anwendungen den datenschutzrechtlichen und datensicherheitstechnischen Bestimmungen entsprechen?

Liegt keine gesetzliche Verpflichtung für eine Vorabkontrolle vor, so kann es sich trotzdem empfehlen, bei Einführung neuer Systeme, Techniken oder Software eine datenschutzrechtliche Verfahrenskontrolle durchzuführen: Nicht selten lassen sich datenschutzrechtliche Risiken erst im Rahmen einer professionellen Begutachtung durch den bDSB identifizieren.

Im Audit muss nachgewiesen werden können, dass solche Prüfungen durchgeführt werden (können), z.B. durch regelmäßige Audits, Revisionen, Softwarepflege etc. Ist dies nicht der Fall, endet das Audit als nicht-bestanden.

3.20 A20 – Zertifikate / Gütesiegel bzgl. Datenschutz / IT-Sicherheit

Liegen für eingesetzte Software, Verfahren oder Dienstleister ein Gütesiegel oder Zertifikate vor, die sich auf Datenschutz oder IT-Sicherheit beziehen (ein anerkanntes Datenschutzgütesiegel für Software oder Online-Shop, ein ISO 27001-Zertifikat für ein Rechenzentrum)?

Falls ja, bitte benennen Sie das Siegel/ Zertifikat, den Geltungsbereich, die Gültigkeit und die erteilende Stelle.

Verfahrenskontrollen können auch durch externe Stellen durchgeführt werden, z.B. in Form von Begutachtungen, Auditierungen oder auch Zertifizierungen. Kann das Unternehmen für eingesetzte Software, Verfahren oder Dienstleister Gütesiegel oder Zertifikate vorweisen, die sich auf Datenschutz oder IT-Sicherheit beziehen (z.B. ein anerkanntes Gütesiegel für Online-Shops, ein Datenschutzgütesiegel für Software,

ein ISO 27001-Zertifikat für ein Rechenzentrum), so unterstützt dies die Vorabkontrolle – und zugleich diese Auditierung. Es ist allerdings optional und keine Bedingung für die Erlangung des Datenschutzgütesiegels.

Ob ein glaubwürdiges Zertifikat vorliegt, kann nur nachgewiesen werden, wenn Name, Adressat, Gültigkeit und ausstellende Stelle konkret dargelegt werden können. Nachweise werden hierzu in der Regel dann – soweit hier angegeben – auch im Audittermin abgefragt und sollten zur Einsicht bereit gelegt werden.

4. Teil B - Zulässigkeit von Datenverarbeitungsverfahren

Im Rahmen des Audits kann und soll nicht geklärt werden, ob ein konkret eingesetztes Verfahren, in welchem personenbezogene Daten verarbeitet werden, zulässig ist oder nicht. Das Unternehmen muss aber zumindest generell gewährleisten können, dass ein solches Verfahren rechtskonform ist. Im Rahmen des Audits vor Ort werden dazu Fragen gestellt und stichprobenartig Einblicke in wesentliche Datenverarbeitungsverfahren genommen, um festzustellen, ob das Datenschutzmanagement des Unternehmens über Mechanismen verfügt, welche die eine Zulässigkeit der Datenverarbeitung angemessen sicherstellen können.

Nachfolgend sollen einige Aspekte der Zulässigkeit der Datenverarbeitung im Teil B des Fragenkatalogs genannt werden, die zwar nicht abschließend sind, jedoch im Rahmen der Auditierung angesprochen werden können.

Die Erhebung, Verarbeitung, Nutzung, Speicherung oder Übermittlung von personenbezogenen Daten (i.w.S. als „**Datenverarbeitung**“ zu bezeichnen) ist gemäß § 4 Abs. 1 BDSG zulässig, soweit eine **Rechtsvorschrift dies erlaubt** oder der Betroffene **eingewilligt** hat.

Die Verarbeitung von *Verbraucher- bzw. Kundendaten* richtet sich zunächst nach den Vorgaben des Bundesdatenschutzgesetzes. So ist beispielsweise die Verarbeitung von Kundendaten **zu eigenen Geschäftszwecken** nach § 28 Abs. 1 S. 1 Nr. 1 BDSG zulässig, wenn diese für die Begründung, Durchführung oder Beendigung eines Schuldverhältnisses erforderlich ist. Hierzu gehört z.B. die Verarbeitung der Postanschrift für die Zusendung von bestellten Waren. Werden Name oder Anschrift für Zwecke der postalischen Direktwerbung genutzt, ist § 28 Abs. 3 BDSG einschlägig. Danach können unter bestimmten Voraussetzungen u.a. Titel, Name, Postanschrift, Beruf, Geburtsjahr sowie ein Gruppenmerkmal (z.B. „Schuhliebhaber“) auch ohne eine Einwilligung für Marketingzwecke genutzt werden, sofern der Kunde gemäß § 28 Abs. 4 BDSG jederzeit der Nutzung widersprechen kann und er hierüber sowie über den konkreten Verwendungszweck im Zeitpunkt der Erhebung des Datums und sodann bei jeder werblichen Ansprache erneut informiert wurde. Für personenbezogene Auswertungen müssen die Vorgaben von § 28b BDSG erfüllt sein.

Daneben bestehen ggf. weitere **spezialgesetzliche Regelungen** zum Umgang mit personenbezogenen Daten, wie etwa zum Umgang mit Sozialversicherungsdaten für Beschäftigte anhand der Sozialgesetzbücher, zum Umgang mit Telekommunikationsdaten gemäß Telekommunikationsgesetz (TKG), zum Umgang mit Nutzerdaten bei Telemedien gemäß Telemediengesetz (TMG) oder zum Umgang mit werblicher, elektronischer Kommunikation (z.B. E-Mail, Telefon) gemäß § 7 des Gesetzes gegen den unlauteren Wettbewerb (UWG). Ferner können betriebliche Regelungen (Betriebsvereinbarungen) den Datenschutz im Beschäftigungsverhältnis spezifizieren.

Existiert keine gesetzliche Grundlage, ist die Datenverarbeitung nur zulässig, wenn sie auf einer **Einwilligung des Betroffenen** beruht. Die Betroffene muss im Zeitpunkt der Einwilligung über Inhalt und Tragweite derselben informiert sein und freiwillig in die Verwendung der Daten einwilligen.

Ferner ist die Zulässigkeit einer **Datenübermittlung an Dritte** zu prüfen. Hier muss z.B. sichergestellt sein, dass die Weitergabe der Daten rechtmäßig erfolgt und der Betroffene in der Regel hierüber informiert wurde. Davon abzugrenzen ist die weisungsgebundene Datenverarbeitung im Auftrag gemäß § 11 BDSG, die vor allem bei den technisch-organisatorischen Datenschutzmaßnahmen Bedeutung erlangt (siehe Teil C des Fragenkataloges).

Werden im **Print-Bereich** außerhalb des sog. **Listenprivilegs** personenbezogene Daten für Werbezwecke genutzt, ist dies allein auf Grundlage einer Einwilligung des Betroffenen zulässig. Listenprivileg bedeutet, dass die in § 28 Abs. 3 Satz 2 BDSG genannten Datenarten (Personengruppe, Berufs-, Branchen- oder Geschäftsbezeichnung, Name, Titel, akademischer Grad, Anschrift und Geburtsjahr) unter den dort genannten Vorgaben auch ohne Einwilligung für Werbezwecke genutzt werden können. Gehen die erfassten und verarbeiteten Daten über die dort Genannten hinaus, ist eine Einwilligung notwendig. Dies ist z.B. der Fall, sofern das vollständige Geburtsdatum für Werbezwecke genutzt werden soll. Gemäß § 28 Abs. 3a BDSG muss die Einwilligung schriftlich bestätigt werden, sofern sie in anderer Form als der Schriftform erteilt wird. Eine Ausnahme gilt, wenn die Einwilligung elektronisch erklärt wurde (z.B. per Anklicken einer Checkbox) und dies protokolliert und jederzeit abrufbar ist. Zudem muss die Einwilligungserklärung hervorgehoben werden, sofern sie zusammen mit anderen Erklärungen abgegeben wird.

Bei erstmaliger Datenerfassung und sodann bei jeder werblichen Ansprache ist der Betroffene über diesen Verarbeitungszweck sowie über sein jederzeitiges Widerrufs- bzw. Widerspruchsrecht zu informieren.

Im Bereich **elektronischen Marketings** existiert ein Listenprivileg nicht. E-Mail Adressen dürfen deshalb regelmäßig nur auf Grundlage der **Einwilligung** des Betroffenen zum Zwecke der Werbung genutzt werden. Als einzige Ausnahme von diesem Grundsatz dürfen Bestandskunden bei Berücksichtigung der engen Vorgaben des § 7 Abs. 3 UWG auch ohne Vorliegen einer konkreten Einwilligung werblich angesprochen werden.

Für die werbliche Ansprache von Neukunden – also bei erstmaliger Registrierung für den Erhalt eines **Newsletters** – gelten demnach folgende Regelungen:

- Es muss eine nachweisbare, protokollierte, freiwillige und rechtlich wirksame Einwilligung des Empfängers vorliegen.
- Der Empfänger muss im Rahmen jeder werblichen Ansprache die einfache und kostenfreie Möglichkeit haben, dieser mit Wirkung für die Zukunft zu widersprechen („unsubscribe“).
- Ferner muss der Empfänger bei der erstmaligen Erhebung der E-Mail-Adresse und bei jeder werblichen Ansprache darauf hingewiesen werden, dass der Verwendung der Daten für Werbung jederzeit widersprochen werden kann.
- Der kommerzielle Charakter ist schon in der Betreffzeile der E-Mail oder des Anschreibens hervorzuheben, der tatsächliche Absender zu nennen und ein Impressum einzubinden.

Hinsichtlich der Aufnahme eines Interessenten in den Newsletterverteiler hat sich bereits aus Gründen der Nachweisbarkeit das sog. Double-Opt-In-Verfahren durchgesetzt. Hierbei erteilt der Verbraucher seine Einwilligung durch Eingabe seiner E-Mail-Adresse und/oder Anklicken eines Einwilligungsfeldes bzw. Absenden der Anfrage (1. Opt-In). Sodann erhält er eine Bestätigungs-E-Mail an die angegebene Adresse mit der Aufforderung, den Bestellvorgang zu bestätigen (zumeist per Link eingebunden). Mit der Bestätigung erfolgt das 2. Opt-In. Der Empfänger wird dadurch weitestgehend vor unerwünschten E-Mails abgesichert. Infolge der jüngeren Rechtsprechung zum Double-Opt-In Verfahren sind an die Protokollierung bestimmte Anforderungen zu stellen. Als best practice empfiehlt sich danach:

- Schriftliche Definition des Double-Opt-in-Verfahrens als Unternehmensstandard bei Darstellung, wie (und gegebenenfalls unter Nutzung welchen Dienstleisters) die Erhebung und Verifizierung der E-Mail-Adressen erfolgt
- Protokollierung des Zeitpunkts der Newsletteranfrage sowie der IP-Adresse des Anfragenden (ausdruckbares Dokument)
- Beschränkung des Inhalts der E-Mail auf den Bestätigungslink, Verzicht auf weiterführende Informationen zum Unternehmen, zu Produkten, etc.
- Protokollierung der IP-Adresse des Klicks auf den Bestätigungslink und des Zeitpunkt des Klicks (ausdruckbares Dokument, Aufbewahrung bis zur Beendigung des Newsletterabonnements)
- Aufnahme des Datenerhebungs- und Verarbeitungsprozesses in die Datenschutzerklärung

Zudem ist sicherzustellen, dass der Widerspruch eines Kunden gegen die Datenverarbeitung zu Werbezwecken auch entsprochen wird. Widersprüche gegen werbliche E-Mails können unter Beachtung des Grundsatzes der Datensparsamkeit in einer Blacklist gespeichert und gegengeprüft werden. Möglich ist auch, die Daten mit der sogenannten Robinsonliste abzugleichen, um von vorneherein dem Wunsch des Verbrauchers, keine Werbung zu erhalten, zu entsprechen.

Denkbar ist auch, dass die Personendaten gemäß § 28 Abs. 1 Satz 1 Nr. 1 BDSG **zur Erfüllung von Vertragszwecken ausgewertet** werden. Welche Zwecke das sei können, hängt von der vertraglichen Ausgestaltung ab. Auch gilt es, Grundsätze wie Erforderlichkeit und Datensparsamkeit angemessen zu berücksichtigen.

Datenverarbeitungen können alternativ auch im **berechtigten Interesse** des Datenverarbeiters liegen und gemäß § 28 Abs. 1 Satz 1 Nr. 2 BDSG zulässig sein, sofern nicht schutzwürdige Interessen des Betroffenen überwiegen. Ob das Interesse der verantwortlichen Stelle an einer Verarbeitung berechtigt ist, hängt von der Datenart und der Zweckbestimmung ab. Beispielsweise liegt es im Interesse des Anwenders, die Bonität eines Konsumenten zu prüfen, um im Falle der Zahlungsunfähigkeit Schaden abzuwenden. Zur Bonitätsprüfung können gemäß § 28 BDSG jedoch nur solche Angaben genutzt werden, die tatsächlich nachgewiesen werden können, also z.B. die Abgabe einer eidesstattlichen Versicherung, nicht aber einseitige Angaben über die Zahlungsunwilligkeit (z.B. über die Einleitung eines Mahnverfahrens, dieses könnte ja auch unberechtigt sein).

Das sogenannte **Scoring** ist an den engen Zulässigkeitsvoraussetzungen von § 28b BDSG zu messen. Danach wäre die Auswertung von Daten beispielsweise unzulässig, wenn

- einzelne Kunden ausschließlich auf Grundlage schlechter Scoringwerte ohne individuelle Einzelfallprüfung abgelehnt würden (§ 6a BDSG),
- Merkmale genutzt würden, die einem Nutzungs- oder Diskriminierungsverbot unterliegen (Geschlecht, Rasse, sexuelle Orientierung, Behinderung, Religion, Weltanschauung, ggf. Alter),

Legitimiert werden kann die Auswertung oder Bewertung verschiedener personenbezogener Daten aber auch über eine Einwilligung. An die Einwilligung sind die bereits genannten Anforderungen zu stellen.

Zu den im Teil B des Fragenkatalogs genannten Grundanforderungen an die Zulässigkeit sind die nachfolgenden Fragen und Erörterungen relevant.

4.1 B1 - Verfahren, in denen Verbraucherdaten verarbeitet werden

Bitte nennen Sie Name und Version der eingesetzten Verfahren, mit denen in Ihrem Unternehmen im Wesentlichen Verbraucherdaten verarbeitet werden (insbesondere ein CRM-System), ggf. bitte auf das Verfahrensverzeichnis verweisen.

Um eine Einschätzung zu erhalten, ob das zu zertifizierende Unternehmen generell die Zulässigkeit der Datenverarbeitung gewährleisten kann, müssen den Auditoren zunächst die eingesetzten, wesentlichen Verfahren bekannt sein. Da das Unternehmen verpflichtet ist, diese im Verfahrensverzeichnis aufzuführen, kann an dieser Stelle auch auf das Verfahrensverzeichnis verwiesen werden.

Als wesentlich betrachtet werden Verfahren des Customer Relationship Managements, Kundendatenverwaltungsprogramme, Newsletterkundendatenbanken, Marketingdatenbanken. Im Audittermin beziehen sich Fragen der Auditoren auf einige der hier genannten Verfahren.

4.2 B2 - Dokumentation im Verfahrensverzeichnis

Sind die o.g. Systeme im Verfahrensverzeichnis enthalten?

Die genannten Verfahren müssen im gesetzlich vorgesehenen Verfahrensverzeichnis aufgeführt werden.

Ist dies nicht der Fall, endet das Audit als nicht-bestanden.

4.3 B3 - Hinweis auf Widerspruchsrecht bei Werbung

B.4 Werden Verbraucher in jedem Fall auf die Möglichkeit zum Widerspruch gegen eine Datennutzung zu Werbezwecken hingewiesen?

Eine Datenverarbeitung zu Werbezwecken ist prinzipiell unzulässig, wenn der Betroffene gegen diese Form der Verwendung widersprochen hat. Auf dieses Recht ist der Betroffene immer hinzuweisen.

Ist dies nicht der Fall, endet das Audit als nicht-bestanden.

4.4 B4 - Umsetzung des Einwilligungserfordernisses bei Werbung

Wird eine Einwilligung des Betroffenen eingeholt, sofern für Marketing oder Werbung mehr Angaben erfasst werden als Personengruppe, Berufs-, Branchen- oder Geschäftsbezeichnung, Name, Titel, akademischer Grad, Anschrift und Geburts*jahr*? Z.B. ist eine Einwilligung notwendig, wenn das vollständige Geburtsdatum für Werbung erfasst wird, siehe § 28 Abs. 3 Satz 2 BDSG.

Nutzt Ihr Unternehmen diese Werbemöglichkeiten, dann wird im Audit ein Beispiel einer solchen Einwilligungserklärung eingesehen werden. Alternativ können Muster vorgelegt oder das Verfahren beschrieben werden. Eine Hilfestellung zur Erstellung einer rechtskonformen Einwilligungserklärung kann dem Fragenkatalog entnommen werden.

Entspricht die Einwilligungserklärung nicht den gesetzlichen Anforderungen, endet das Audit als nicht-bestanden.

4.5 B5 - Einwilligung bei Werbung per Telefon

Falls Ihr Unternehmen Telefonnummern von Verbrauchern zu werblichen Zwecken (z.B. Telefonumfragen, SMS-Werbeversand) verarbeitet: Erfolgt dies nur mit einer nachweisbaren, wirksamen Einwilligung?

Gemäß § 7 UWG ist hierfür immer eine nachweisbare Einwilligung notwendig. Nutzt Ihr Unternehmen diese Werbemöglichkeiten, dann wird im Audit ein Beispiel einer solchen Einwilligungserklärung eingesehen werden. Alternativ können Muster vorgelegt oder das Vorgehen beschrieben werden. Eine Hilfestellung zur Erstellung einer rechtskonformen Einwilligungserklärung kann dem Fragenkatalog entnommen werden.

Entspricht die Einwilligungserklärung nicht den gesetzlichen Anforderungen, endet das Audit als nicht-bestanden.

4.6 B6 - Einwilligung bei Werbung per E-Mail

Falls Ihr Unternehmen E-Mail-Adressen von Verbrauchern zu werblichen Zwecken nutzt: Erfolgt dies nur unter Beachtung des § 7 Abs. 3 UWG oder mit einer nachweisbaren, wirksamen Einwilligung?

Gemäß § 7 UWG ist für elektronische Werbung immer eine nachweisbare Einwilligung notwendig. Für Bestandskunden gilt daneben § 7 Abs. 3 UWG. Nutzt Ihr Unternehmen diese Werbemöglichkeiten, dann wird im Audit ein Beispiel einer solchen Einwilligungserklärung eingesehen werden. Alternativ können Muster vorgelegt oder das Vorgehen beschrieben werden. Eine Hilfestellung zur Erstellung einer rechtskonformen Einwilligungserklärung kann dem Fragenkatalog entnommen werden.

Entspricht die Einwilligungserklärung nicht den gesetzlichen Anforderungen, endet das Audit als nicht-bestanden.

4.7 B7 - Online-Shop

Für den Bereich des Webauftritts eines Unternehmens (z.B. eines Online-Shops) sind die Vorgaben des Telemedienrechts zu beachten. Daher zielen die nachfolgenden

Fragen auf spezielle Anforderungen ab, deren Umsetzung im Audit auch nachgewiesen werden muss (z.B. durch Besichtigung der Webseiten durch die Auditoren, Vorlegen von Dokumenten durch das Unternehmen, Beschreibung des Verfahrens im Audittermin).

Führt Ihr Unternehmen einen Online-Shop?

Wird diese Frage mit nein beantwortet, entfallen einige weitere Fragen. Falls ja, ist es notwendig, die URL / Webadresse zu benennen, die die Auditoren einsehen können.

4.8 B8 - Hauptwebseite des Unternehmens

Führt Ihr Unternehmen eine (Haupt-) Unternehmenswebseite?

Falls ja, wären spezielle Anforderungen des Telemedienrechts für Webseiten hier zu beachten. Die URL / Webadresse muss hier benannt werden, damit die Auditoren diese einsehen können.

4.9 B9 - Impressumspflicht

Falls eine Webseite / Online-Shop geführt wird: Ist eine rechtskonforme Anbieterkennzeichnung (Impressum) gemäß § 5 Telemediengesetz vorhanden?

Die nach § 5 TMG erforderlichen Angaben zum Betreiber der Webseite sowie – soweit erforderlich – weitere Informationen gemäß § 6 TMG müssen gut erreichbar auf der Webseite vorgehalten werden.

Ist dies nicht der Fall, endet das Audit als nicht-bestanden.

4.10 B10 - Datenschutzerklärung auf Webseiten

Falls eine Webseite / Online-Shop geführt wird: Ist eine rechtskonforme Datenschutzerklärung gemäß § 13 Telemediengesetz vorhanden?

Weitere (Transparenz-)Pflichten von Anbietern von Telemedien werden durch § 13 TMG vorgegeben. Danach ist der Webseiten-Nutzer (der Besucher) zu Beginn des Nutzungsvorgangs umfassend über die Verarbeitung personenbezogener Daten zu unterrichten. Häufig ist für den Nutzer nicht ohne weiteres erkennbar, dass bereits im Zeitpunkt des Aufrufens einer Website (ggf. personenbezogene) Daten erhoben werden. Beispiele hierfür sind IP-Adresse, Browsertyp, Uhrzeit und Dauer der Nutzung sowie Informationen über gesetzte Cookies. Es ist aus datenschutzrechtlicher Sicht daher umso wichtiger, den Nutzer zu Beginn der Nutzung über die Identität des Webseitenbetreibers sowie über Art und Umfang der erhobenen personenbezogenen Daten zu informieren. Mit der Offenlegung der Verarbeitungsabsichten und der Konsequenzen der Erhebung und Speicherung personenbezogener Daten durch den Anbieter eines Dienstes soll erreicht werden, dass der Nutzer zu einem möglichst frühen Zeitpunkt Entscheidungsmöglichkeiten hinsichtlich des weiteren Datenverarbeitungsprozesses erhält. Im Fragenkatalog werden Bausteine für eine rechtskonforme Datenschutzerklärung zur Verfügung gestellt.

Liegt keine rechtskonforme Datenschutzerklärung vor, endet das Audit als nicht-bestanden.

4.11 B11 - Datensparsame Webformulare

Falls eine Webseite / Online-Shop geführt wird: Wurden Online-Formulare und Dateneingabemasken so gestaltet, dass so wenig Daten wie möglich und nur so viel wie notwendig erfasst werden (Grundsatz der Datenvermeidung und Datensparsamkeit)?

Auch in Webformularen sind so wenig personenbezogene Daten wie möglich und nur so viel wie notwendig zu erfassen. Etwa ist für die Bestellung eines Newsletters, der nur per E-Mail verschickt wird, keine Angabe der Postadresse notwendig.

Sollen weitergehende – zweckmäßige – Daten erfasst werden, sind diese z.B. als optional oder als freiwillige Angabe unter Hinweis auf deren Verwendungszweck zu kennzeichnen.

Ist dies nicht der Fall, endet das Audit als nicht-bestanden.

4.12 B12 - Umsetzung von Einwilligungen in Webformularen

Sofern in Formularen oder Dateneingabemasken besonders sensible personenbezogene Daten (z.B. Gesundheitsdaten) erfasst werden: Wird hierzu eine nachweisbare und wirksame Einwilligung eingeholt?

Die Erfassung und Verarbeitung besonderer personenbezogener Daten erfordert immer eine Einwilligung unter Hinweis auf den konkreten Verwendungszweck.

Ist dies nicht der Fall, endet das Audit als nicht-bestanden.

4.13 B13 - Verwendung und Transparenz von Cookies auf Webseiten

Falls eine Webseite / Online-Shop geführt wird: Werden die Vorgaben der sog. Cookie-Richtlinie 2002/58/EG entsprechend der Vorgaben des deutschen Gesetzgebers umgesetzt?

Auch Cookies unterliegen den Bestimmungen des BDSG und des TMG, insbesondere, wenn sie personenbeziehbare Daten, wie z.B. eine User-ID enthalten. Über den Einsatz von Cookies ist gemäß § 13 Abs. 1 Satz 2 TMG zu informieren (z.B. in der Datenschutzerklärung).

Zudem ist die sogenannte „Cookie-Richtlinie“ der Europäischen Union (Richtlinie 2009/136/EG) zu beachten. Danach ist das Setzen von Cookies – je nach Art des Cookies - grundsätzlich nur zulässig, wenn der Nutzer darüber unterrichtet wurde und er einwilligt.

Werden Cookies dafür genutzt, das Surf- oder Klickverhalten der Webseitenbesucher zu analysieren („Online Behavioural Advertising“), sind ggf. die Regelung des Artikels 5 Absatz 3 der europäischen Datenschutzrichtlinie für elektronische Kommunikation (RL 2002/58/EG) zu beachten.

Die Auditoren prüfen hierzu die angegebene Webseite des Unternehmens und die dazugehörige Information (Datenschutzerklärung, Vorlage im Fragenkatalog verfügbar). Bei der Anwendung dieser Rechtsvorschriften ziehen die Auditoren die aktuelle Auslegung durch Rechtsprechung, Aufsichtsbehörden und Fachliteratur heran. Sind die genannten Vorgaben nicht eingehalten, endet das Audit als nicht-bestanden.

4.14 B14 - Tracking-Tools auf Webseiten

Falls auf der Webseite / im Online-Shop sog. Trackingtools eingesetzt werden: Werden Vorkehrungen getroffen, dass keine personenbezogenen Daten ohne Einwilligung gespeichert werden?

Soweit bei Aufruf von Webseiten sog. Trackingtools zum Einsatz kommen und hierbei personenbezogene Daten erfasst werden, sind unterschiedliche rechtliche Anforderungen sowie Vorgaben der Datenschutzaufsichtsbehörden zu beachten. Wird danach die IP-Adresse des Rechners des Webseitenbesuchers nicht anonymisiert (verkürzt um die letzten vier Ziffern), ist dem Webseitenbesucher ein Widerspruchsrecht einzuräumen und zu verdeutlichen (z.B. durch ein Add-On-Verfahren zur Deaktivierung von Cookies oder der Ausführung eines Skriptes).

Orientiert an den Vorgaben der Datenschutzaufsichtsbehörden von Bund und Ländern sollten bei Einsatz für Google Analytics oder Adobe Analytics/Site Catalyst die nachfolgenden Aspekte berücksichtigt werden. Auf andere Trackingverfahren sind diese Grundsätze zu übertragen.

Google Analytics

- --- Hinweis in Datenschutzerklärung auf Einsatz von Google Analytics und die Möglichkeit der Deaktivierung (Opt-Out) unter Einbindung eines Opt-Out-Cookies-Links
- --- Verlinkung in Datenschutzerklärung auf Downloadmöglichkeit des Browser-Add-On zu Google Analytics
- --- Abschluss eines schriftlichen Vertrags zur Auftragsdatenverarbeitung gem. § 11 BDSG mit der Google Germany GmbH
- --- Veranlassung der Löschung des letzten Oktett der IP-Adresse (anonymizeIP)
- --- Löschung der Altdaten

Adobe Analytics/ Site Catalyst

- --- Hinweis in Datenschutzerklärung auf Einsatz von Google Analytics und die Möglichkeit der Deaktivierung (Opt-Out)
- --- Abschluss eines schriftlichen Vertrags zur Auftragsdatenverarbeitung gem. § 11 BDSG mit der Adobe Systems GmbH
- --- Veranlassung der Löschung des letzten Oktett der IP-Adresse (Obfuscate IP-Removed)
- --- Laufzeit der Cookies: 2 Jahre

Zudem dürfen gemäß § 15 Abs. 3 S. 3 TMG Bestandsdaten des Webseitenbesuchers (z.B. Name. Adresse) nicht mit seinen Nutzungsdaten zusammengeführt werden, es sei denn, der Nutzer hat seine Einwilligung erklärt.

Die Auditoren prüfen hierzu die angegebene Webseite des Unternehmens und die dazugehörige Information (Datenschutzerklärung). Bei der Anwendung dieser Rechtsvorschriften ziehen die Auditoren die aktuelle Auslegung durch Rechtsprechung, Aufsichtsbehörden und Fachliteratur heran. Sind die genannten Vorgaben nicht eingehalten, endet das Audit als nicht-bestanden.

4.15 B15 - Social-Plug-Ins

Falls auf einer Webseite / Online-Shop sogenannte Social-Plug-Ins eingesetzt werden z.B. von facebook, google+): Wurden Maßnahmen getroffen, die den datenschutzkonformen Einsatz der Plug-Ins sicherstellen?

Erfolgt die Datenverarbeitung durch einen Dritten, kann zudem ein Fall der Auftragsdatenverarbeitung vorliegen, die z.B. gemäß § 11 BDSG zu beurteilen ist. Erfolgt die Datenverarbeitung im Ausland, insbesondere in einem Staat außerhalb der EU oder des Europäischen Wirtschaftsraumes (EWR), ist zu überprüfen, ob hierfür eine Übermittlungsbefugnis besteht und ein angemessenes Datenschutzniveau gewährleistet ist.

Die Auditoren prüfen hierzu die angegebene Webseite des Unternehmens und die dazugehörige Information (Datenschutzerklärung). Bei der Anwendung dieser Rechtsvorschriften ziehen die Auditoren die aktuelle Auslegung durch Rechtsprechung, Aufsichtsbehörden und Fachliteratur heran. Sind die genannten Vorgaben nicht eingehalten, endet das Audit als nicht-bestanden.

4.16 B16 - Double-Opt-In bei Newsletteranmeldung

Falls per E-Mail Newsletter oder Werbung an Verbraucher verschickt wird: Wird bei Erhebung der E-Mail-Adresse ein Double-Opt-In-Verfahren mit Nachweisen zu den einzelnen Bestellschritten durchgeführt?

Durch das Double-Opt-In-Verfahren wird sichergestellt, dass die Person, die das Bestellformular ausfüllt, auch der Inhaber der E-Mail-Adresse ist. Dadurch wird sichergestellt, dass die Vorgaben des § 7 UWG eingehalten werden und der Versand werblicher E-Mails nicht als rechtswidriger Spam gewertet wird.

Beim Double-Opt-In-Verfahren erhält der Verbraucher nach Mitteilung seiner E-Mail-Adresse eine E-Mail an die von ihm angegebene E-Mail-Adresse mit der Aufforderung, die Newsletterbestellung zu bestätigen (in der Regel per Klick auf einen beigefügten Link). Diese Aufforderungs-E-Mail muss frei von Werbung sein. Erst nach Aktivierung des Links und der daraus folgenden Bestätigung wird der Verbraucher in den Newsletterverteiler aufgenommen.

Alternativ dazu kann die Bestätigung, dass an eine angegebene E-Mail-Adresse Werbung oder ein Newsletter geschickt werden darf, auch auf anderem Wege dokumentiert werden. Erforderlich ist stets, dass das Vorliegen der Einwilligung des Betroffenen im Zweifel eindeutig nachgewiesen werden kann (z.B. als schriftliche Bestätigung oder als nachvollziehbare Notiz über Einwilligung, Person und Widerspruchshinweis in einem CRM-System).

Im Audit kann die Bestellung des Newsletters von den Auditoren getestet werden. fehlt ein Double-Opt-In-Verfahren oder ein vergleichbarer Prozess, endet das Audit als nicht-bestanden.

4.17 B17 - Sperrvermerke bei Widersprüchen und Widerruf von Einwilligungen

Sofern Verbraucher Einwilligungen widerrufen: Kann die Umsetzung eines Widerrufs nachvollzogen werden?

Es muss gewährleistet sein, dass dem Widerspruch des Betroffenen auch entsprochen werden kann, z.B. indem die Daten des Betroffenen in eine Sperrdatei (Blacklist) aufgenommen werden; die Versendung des Newsletters erfolgt erst dann, wenn ein Abgleich mit der Sperrdatei stattgefunden hat.

Im Audit erfragen die Auditoren, wie sichergestellt wird, dass ein Widerspruch gegen bzw. der Widerruf der Einwilligung in die werbliche Datennutzung Berücksichtigung findet.

Können keine Anhaltspunkte dafür gefunden werden, endet das Audit als nicht-bestanden.

5. Teil C - Technisch – organisatorische Sicherheitsmaßnahmen

Neben der inhaltlichen Gestaltung der Datenverarbeitungsprozesse kommt es darauf an, die verwendeten technischen Systeme so zu gestalten und zu betreiben, dass die Daten nur in einem zulässigen Rahmen verwendet werden. Dies ist durch technisch-organisatorische Maßnahmen abzusichern. Die Anlage zu § 9 BDSG auferlegt Unternehmen acht Kontrollziele zur Einrichtung von technischen und organisatorischen Sicherheitsmaßnahmen. Hinsichtlich der konkreten Ausgestaltung dieser Maßnahmen lässt das Gesetz mit Rücksicht auf die jeweiligen Ressourcen einen gewissen Spielraum. Die Vorgaben zu den Sicherheitsmaßnahmen sind aus diesem Grunde allgemein gefasst, die konkrete Ausgestaltung obliegt der verantwortlichen Stelle.

Bei den nachfolgend aufgeführten technisch-organisatorischen Sicherheitsmaßnahmen sind im Gegensatz zu den bisherigen gesetzlichen Anforderungen aufgrund der Vielzahl möglicher Szenarien die Mindestanforderungen nicht explizit genannt. Die Bewertung der tatsächlich getroffenen oder auch nicht getroffenen Maßnahmen liegt daher im Ermessen der Auditoren. Die Bewertung der Auditoren richtet sich allerdings an Grundsätzen aus, welche von Aufsichtsbehörden, dem Bundesamt für Sicherheit in der Informationstechnik sowie anderen anerkannten Stellen als angemessen bewertet werden.

Liegen sicherheitsrelevante, anerkannte und gültige Zertifikate vor (z.B. ISO 27001, IT-Grundschutz), dann kann auf die nachweisbaren Ergebnisse im Audit verwiesen werden.

Auch hier ist die Auditierung nur eine Momentaufnahme der Sicherheitsmaßnahmen, die zum Auditzeitpunkt festgestellt werden konnten.

5.1 C1 - Standorte

Bitte geben Sie an, auf welchen Standort der später zu prüfenden juristischen Person sich die nachfolgenden Antworten beziehen. Sollen mehrere Standorte in die Prüfung und Zertifizierung einbezogen werden, füllen Sie bitte jeweils das Kapitel C in den folgenden Tabellenblättern aus.

Geben Sie bitte zunächst alle Standorte an, für die die nachfolgend gemachten Angaben zutreffen. Bei mehreren Standorten füllen Sie bitte die Fragen zu C. entsprechend mehrfach aus.

Dies kann z.B. notwendig sein, wenn Ihr Unternehmen am Hauptsitz geprüft wird aber die IT-Systeme in einem Rechenzentrum an einem anderen Niederlassungsort betrieben werden. In diesem Fall wären sowohl für den Hauptsitz als auch für das Rechenzentrum entsprechende Angaben zu Kapitel C zu machen.

Ebenfalls ist dies notwendig, wenn personenbezogene Daten zwar durch Ihr Unternehmen verarbeitet werden, die Datenhaltung aber insgesamt oder zum Teil auf einen externen Dienstleister ausgelagert wurde. Auch hier müssten dann die Maßnahmen pro relevanten Standort beschrieben werden, wobei im Falle einer externen Datenhaltung durch Dienstleister eine Bezugnahme auf den insoweit erforderlichen Auftragsdatenverarbeitungsvertrag angezeigt ist.

Hingegen genügt eine gemeinsame Darstellung, wenn die Datenverarbeitung zwar an mehreren Niederlassungen Ihres Unternehmens stattfindet, die getroffenen Sicherheitsmaßnahmen aber stets identisch sind.

Die Auditoren können Nachweise hierzu verlangen oder Stichproben während des Audittermins vor Ort durchführen.

Sollte im Audittermin festgestellt werden, dass auch andere Standorte für die Umsetzung der Datensicherheit relevant sind, ohne dass diese im Fragebogen aufgeführt wurden, kann das Audit mit nicht-bestanden bewertet werden. Alternativ dazu wird die Gültigkeit des Datenschutzgütesiegels – sofern möglich – auf den geprüften und nachweisbar rechtskonform aufgestellten Standort begrenzt.

5.2 C2 - Zutrittskontrolle bei Gebäuden, Räumen, Serverräumen

Sind Gebäude, Räumlichkeiten und Serverräume mit Sicherheitsschlössern versehen?

Unternehmen haben Maßnahmen zu treffen, durch die Unbefugten der physische Zutritt zu Datenverarbeitungsanlagen verwehrt wird. Nr. 1 der Anlage zu § 9 BDSG erfasst damit Sicherheitsmaßnahmen, um den räumlichen Bereich rund um Datenverarbeitungsanlagen vor dem körperlichen Zutritt Unbefugter zu schützen.

Die o.g. Maßnahmen stellen einen Mindeststandard dar, den es zu erfüllen gilt. Anderenfalls endet das Audit mit nicht-bestanden.

5.3 C3 - Zutrittskontrolle beim Serverraum im Speziellen

Ist der Serverraum grundsätzlich abgeschlossen?

Unternehmen haben Maßnahmen zu treffen, durch die Unbefugten der physische Zutritt zu Datenverarbeitungsanlagen verwehrt wird. Nr. 1 der Anlage zu § 9 BDSG erfasst damit Sicherheitsmaßnahmen, um den räumlichen Bereich rund um Datenverarbeitungsanlagen vor dem körperlichen Zutritt Unbefugter zu schützen.

Die o.g. Maßnahmen stellen einen Mindeststandard dar, den es zu erfüllen gilt. Anderenfalls endet das Audit mit nicht-bestanden.

5.4 C4 - Zutrittskontrolle – Weitere Maßnahmen

Welche der nebenstehenden Sicherheitsmaßnahmen sind umgesetzt?

- ☐ **Gebäude, Räumlichkeiten und / oder Serverraum sind alarmgesichert.**
- ☐ **Gebäude, Räumlichkeiten und / oder Serverraum sind durch ein Spezialschloss (z.B. Kartenleser, biometrischer Scan) gesichert.**
- ☐ **Das Gebäude wird außerhalb der Betriebszeiten von einem Wachdienst geschützt.**
- ☐ **Gebäude und / oder Serverraum sind videoüberwacht.**
- ☐ **Das Gebäude kann nur per Durchlass eines Pförtners betreten werden.**
- ☐ **Es werden Besucherlisten geführt.**

- ☐ **Betriebsfremde Personen dürfen sich nur in Begleitung von Betriebszugehörigen im Gebäude aufhalten.**
- ☐ **Racks im Serverraum sind verschlossen.**
- ☐ **Es existieren Fensterschlösser.**
- ☐ **Es existiert eine dokumentierte Schlüssel-Ordnung.**
- ☐ **Sonstiges:**

Unternehmen haben Maßnahmen zu treffen, durch die Unbefugten der physische Zutritt zu Datenverarbeitungsanlagen verwehrt wird. Nr. 1 der Anlage zu § 9 BDSG erfasst damit Sicherheitsmaßnahmen, um den räumlichen Bereich rund um Datenverarbeitungsanlagen vor dem körperlichen Zutritt Unbefugter zu schützen. Die o.g. Maßnahmen stellen exemplarisch Möglichkeiten dar, personenbezogene Daten im Wege einer Zutrittskontrolle zu schützen. Welche Maßnahmen letztendlich zu erfüllen sind, lässt sich anhand des potentiellen Risikos bei einem Datenverlust nur für den individuellen Sachverhalt Ihres Unternehmens ermitteln. Gefordert wird daher an dieser Stelle ein Standard an Maßnahmen, über die die gesetzlich geforderte Zutrittskontrolle angemessen sichergestellt werden kann; mehrere Antworten sind möglich und verbessern das Sicherheitsniveau.

5.5 C5 - Zugangskontrolle – Passwortschutz

Wird zum Starten des Arbeitsplatz-Rechners die Eingabe eines Passwortes verlangt?

Für Datenverarbeitungssysteme drohen aus verschiedenen Richtungen Risiken für die Sicherheit und Vertraulichkeit der personenbezogenen Daten: Durch Einschleusen von Viren, Trojanischen Pferden und ähnlicher Schadsoftware oder durch das bloße Eindringen (Hacken) in die Datenverarbeitungsanlagen von außen können Daten unbefugt gelöscht, verändert, gelesen oder vervielfältigt werden, dies unter Umständen sogar ohne oder erst mit verspäteter Kenntnis der verantwortlichen Stelle. Aus diesem Grund sind an die gem. Nr. 2 der Anlage zu § 9 BDSG geforderte Zugangskontrolle aus Datensicherheitsgründen hohe Anforderungen zu stellen. Die Qualität der Zugangskontrolle bestimmt im Wesentlichen die Qualität der Datensicherheit im Unternehmen insgesamt. Die Zugangskontrolle umfasst jedoch nicht nur Schutzmaßnahmen gegen Gefahren, die von „außen“ drohen, sondern erfordert daneben auch Sicherheitsvorkehrungen gegen den internen unbefugten Zugang. Auch wenn Schäden durch internen Missbrauch nicht in der gleichen Weise publik werden wie das Eindringen oder Lahmlegen von EDV-Systemen bekannter Unternehmen durch Angriffe von außen, sind die bestehenden Risiken durch internen Missbrauch mindestens ebenso hoch.

Die nachfolgend aufgezählten Maßnahmen stellen einen Mindeststandard dar, den es zu erfüllen gilt. Ist dies nicht der Fall, endet das Audit mit nicht-bestanden.

5.6 C6 - Zugangskontrolle – Weitere Maßnahmen

Welche der nebenstehenden Sicherheitsmaßnahmen sind umgesetzt?

- ☐ Bei Abwesenheit von mehr als 12 Minuten wird ein Bildschirmschoner mit Passwortschutz aktiviert.
- ☐ Das Passwortkonzept ist dokumentiert.
- ☐ Fernwartungen werden erst nach mündlicher Rücksprache mit dem Dienstleister freigeschaltet.
- ☐ IT-Systeme sind durch eine Firewall geschützt.
- ☐ IT-Systeme sind durch Anti-Viren- und Anti-Trojaner-Programme geschützt
- ☐ Es existiert eine Demilitarisierte Zone (DMZ).
- ☐ Es existiert ein Sicherheitskonzept für den Betrieb der Server.
- ☐ Es existiert ein Change-Management zur Verwaltung von Änderungen.
- ☐ Es erfolgen regelmäßig Systemrevisionen.
- ☐ Sonstiges:

Die o.g. Maßnahmen stellen exemplarisch Möglichkeiten dar, personenbezogene Daten im Sinne einer Zugangskontrolle zu schützen. Welche Maßnahmen letztendlich zu erfüllen sind, lässt sich anhand des potentiellen Risikos bei einem Datenverlust nur für den individuellen Sachverhalt Ihres Unternehmens ermitteln. Gefordert wird an dieser Stelle ein Standard an Maßnahmen, über die die gesetzlich geforderte Zugangskontrolle angemessen sichergestellt werden kann; mehrere Antworten sind möglich und verbessern das Sicherheitsniveau.

5.7 C7 - Zugangskontrolle – Passwortkonvention

Sind die Passwörter mindestens acht Zeichen lang und enthalten sie Ziffern und Sonderzeichen?

Passwörter dürfen nicht leicht zu erraten sein. Daher müssen im Unternehmen bestimmte Passwortkonventionen gelten.

Die o.g. Maßnahme stellt einen Mindeststandard für einen Zugangsschutz dar, den es zu erfüllen gilt. Anderenfalls endet das Audit mit nicht-bestanden.

5.8 C8 - Zugangskontrolle – Updates von Systemen/EDV

Werden regelmäßig Updates der Betriebssysteme eingespielt?

Updates können Sicherheitslücken schließen und sind daher für die Datensicherheit notwendig.

Die o.g. Maßnahme stellt einen Mindeststandard für einen Zugangsschutz dar, den es zu erfüllen gilt. Anderenfalls endet das Audit mit nicht-bestanden.

5.9 C9 - Zugriffskontrolle – Differenziertes Berechtigungskonzept

Sind Berechtigungen für Zugriffe differenziert nach den jeweiligen Aufgaben der Beschäftigten?

Die Zugriffskontrolle, Nr. 3 der Anlage zu § 9 BDSG betrifft die Einrichtung von Sicherheitsmaßnahmen, welche die durch eine Datenverarbeitungsanlage verarbeiteten Daten gegen unbefugten Zugriff schützen. Zentrales Merkmal solcher Schutzmaßnahmen sind Berechtigungskonzepte (abgestufte Zugangskennungen mit entsprechendem Passwort).

Die o.g. Maßnahme stellt einen Mindeststandard für einen Zugriffsschutz dar, den es zu erfüllen gilt. Anderenfalls endet das Audit mit nicht-bestanden.

5.10 C10 - Zugriffskontrolle – Weitere Maßnahmen

Welche der nebenstehenden Sicherheitsmaßnahmen sind umgesetzt?

- ☐ **Die relevanten Anwendungen zur Verarbeitung personenbezogener Daten erfordern die Eingabe eines Passwortes.**
- ☐ **Ein Berechtigungs- und Rollenkonzept ist dokumentiert.**
- ☐ **Zugriffe werden protokolliert.**
- ☐ **Logfiles werden regelmäßig überprüft.**
- ☐ **Es existiert ein Security-Monitoring.**
- ☐ **Sonstiges:**

Die o.g. Maßnahmen stellen Möglichkeiten dar, personenbezogene Daten im Sinne einer Zugriffskontrolle zu schützen. Welche Maßnahmen letztendlich zu erfüllen sind, lässt sich anhand des potentiellen Risikos bei einem Datenverlust nur für den individuellen Sachverhalt Ihres Unternehmens ermitteln. Gefordert wird an dieser Stelle ein Standard an Maßnahmen, über die die gesetzlich geforderte Zugriffskontrolle angemessen sichergestellt werden kann; mehrere Antworten sind möglich und verbessern das Sicherheitsniveau.

5.11 C11 - Zugriffskontrolle – Zuweisung von Rollen / Prüfung der Berechtigung

Gibt es ein rollenbasiertes Berechtigungskonzept und ist sichergestellt, dass die Rollen verträglich sind?

Für jedes Verfahren, in denen personenbezogene Daten verarbeitet werden, sollten die Berechtigungen für Lesen, Schreiben, Löschen etc. genau definiert werden (z.B. anhand von Funktionen/Tätigkeitsbereichen). Dabei sollte nicht jede Rolle „alles“ können. Es ist in der Regel z.B. ausreichend, wenn Praktikanten lesende Zugriffe auf ein System erhalten und nur in Ausnahmefällen auch schreibende Rechte. In jedem Fall muss dies vor einem Zugriff definiert sein – und möglichst dokumentiert sein. Oftmals bieten auch IT-Systeme Möglichkeiten für eine nachweisbare Umsetzung.

Die o.g. Maßnahme stellt einen Mindeststandard für einen Zugriffsschutz dar, den es zu erfüllen gilt. Anderenfalls endet das Audit mit nicht-bestanden.

5.12 C12 - Zugriffskontrolle – ordnungsgemäße Datenträgervernichtung

Existieren Vorgaben zur Datenträgervernichtung sowie ein Löschkonzept?

Die Vernichtung von personenbezogenen Daten muss ordnungsgemäß abgesichert sein, so dass Zugriffe auf diese Daten nicht mehr möglich sind. Die Umsetzung kann z.B. dadurch erfolgen, dass ein zertifiziertes Entsorgungsunternehmen damit beauftragt wurde oder dass Mitarbeiter einen DIN-geprüften Aktenvernichter nutzen können. Idealerweise ist ein Konzept hierfür dokumentiert, zumindest aber nachweisbar im Audit.

Die o.g. Maßnahme stellt einen Mindeststandard für einen Zugriffsschutz dar, den es zu erfüllen gilt. Anderenfalls endet das Audit mit nicht-bestanden.

5.13 C13 - Weitergabekontrolle – Verschlüsselung bei Webformularen

Sofern sensible personenbezogene Daten über Webseiten erfasst werden (z.B. Bankdaten): Erfolgt die Übertragung verschlüsselt (z.B. per https / ssl)?

Durch die Weitergabekontrolle gemäß Nr. 4 der Anlage zu § 9 BDSG soll sichergestellt werden, dass die Daten bei der elektronischen Übertragung bzw. bei der Speicherung oder während ihres physischen Transports auf Datenträgern nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können. Die Maßnahmen sind vom Versender bzw. von demjenigen zu treffen, der den Transport initiiert oder für die Speicherung der Daten verantwortlich ist. Die Weitergabekontrolle erfasst nicht nur die mittels elektronischer Übertragung weitergegeben Daten, sondern auch die auf portablen Datenträgern (DVD, USB-Stick, externe Festplatten etc.) gespeicherten Daten.

Die o.g. Maßnahme stellt einen Mindeststandard für eine Weitergabekontrolle dar, den es zu erfüllen gilt. Anderenfalls endet das Audit mit nicht-bestanden.

5.14 C14 - Weitergabekontrolle – Weitere Maßnahmen

Welche der nebenstehenden Sicherheitsmaßnahmen sind umgesetzt?

- ☐ **Datenbanken sind verschlüsselt.**
- ☐ **Festplatten oder andere Datenträger sind verschlüsselt.**
- ☐ **Sonstiges:**

Die o.g. Maßnahmen stellen Möglichkeiten dar, personenbezogene Daten im Sinne einer Weitergabekontrolle zu schützen. Welche Maßnahmen letztendlich zu erfüllen sind, lässt sich anhand des potentiellen Risikos bei einem Datenverlust nur für den individuellen Sachverhalt Ihres Unternehmens ermitteln. Gefordert wird an dieser Stelle ein Standard an Maßnahmen, über die die gesetzlich geforderte Weitergabekontrolle angemessen sichergestellt werden kann; mehrere Antworten sind möglich und verbessern das Sicherheitsniveau.

5.15 C15 - Eingabekontrolle – Protokollierung

Ist eine Protokollierung aller schreibenden bzw. ändernden oder löschenden Zugriffe bei den Verfahren, die personenbezogene Daten verarbeiten, sichergestellt?

Maßnahmen zur Gewährleistung der Eingabekontrolle gemäß Nr. 5 der Anlage zu § 9 BDSG sollen sicherstellen, dass zu jedem Zeitpunkt nachvollzogen werden kann, wer welche Daten wann eingegeben und wie verändert hat. Eine solche Kontrolle kann nur durch eine lückenlose, detaillierte Protokollierung der schreibenden, ändernden und löschenden Zugriffe erreicht werden, wobei die Protokolldaten selbst wiederum vor unbefugtem Zugriff zu schützen sind.

Die o.g. Maßnahme stellt einen Mindeststandard für einen Zugangsschutz dar, den es zu erfüllen gilt. Anderenfalls endet das Audit mit nicht-bestanden.

5.16 C16 - Eingabekontrolle – Auswertung von Protokollen

Kann durch (ggfls. automatisierte) Auswertungen festgestellt werden, ob die Benutzer befugt waren, die aufgezeichneten Aktivitäten auszuführen?

Es muss eine Möglichkeit bestehen, Eingaben auf IT-Systemen zu kontrollieren, um dadurch Verstöße oder irreguläre Vorgänge feststellen zu können.

Die o.g. Maßnahme stellt einen Mindeststandard für eine Eingabekontrolle dar, den es zu erfüllen gilt. Anderenfalls endet das Audit mit nicht-bestanden.

5.17 C17 - Eingabekontrolle – Weitere Maßnahmen

Welche der nebenstehenden Sicherheitsmaßnahmen sind umgesetzt?

- ☐ **Protokolldaten werden regelmäßig stichprobenartig ausgewertet.**
- ☐ **Der Zugriff auf Protokolldaten ist geregelt und eingeschränkt.**
- ☐ **Protokolldaten sind vor Veränderungen geschützt.**
- ☐ **Es werden Tools zur Protokollauswertung eingesetzt.**
- ☐ **Sonstiges:**

Die o.g. Maßnahmen stellen Möglichkeiten dar, personenbezogene Daten im Sinne einer Eingabekontrolle zu schützen. Welche Maßnahmen letztendlich zu erfüllen sind, lässt sich anhand des potentiellen Risikos bei einem Datenverlust nur für den individuellen Sachverhalt Ihres Unternehmens ermitteln. Gefordert wird daher an dieser Stelle ein Standard an Maßnahmen, über die die gesetzlich geforderte Eingabekontrolle angemessen sichergestellt werden kann; mehrere Antworten sind möglich und verbessern das Sicherheitsniveau.

5.18 C18 - Auftragskontrolle – Bestimmung von Dienstleistern

Werden Dienstleister eingesetzt, die personenbezogene Daten im Auftrag verarbeiten oder diese zur Kenntnis nehmen könnten (vgl. § 11 BDSG)?

Durch eine Auftragskontrolle gemäß Nr. 6 der Anlage zu § 9 BDSG soll gewährleistet werden, dass auch bei einer Auslagerung der Datenverarbeitung auf Andere die Anforderungen an Datenschutz und Datensicherheit gewährleistet sind.

Gemäß § 11 BDSG sind in dem Fall, dass personenbezogene Daten im Auftrag durch andere Stellen verarbeitet werden, konkrete Vorgaben sowohl durch den Auftraggeber (AG), als auch durch den Auftragnehmer (AN) zu beachten. Eine solche Auftragsdatenverarbeitung liegt vor, wenn die beauftragte Stelle die Daten ausschließlich für fremde Zwecke verarbeitet. Hiervon abzugrenzen ist eine Datenverarbeitung, bei der die beauftragte Stelle die Daten eigenverantwortlich für bestimmte eigene Zwecke verarbeitet (Funktionsübertragung). Bei der Auftragsdatenverarbeitung verbleibt die datenschutzrechtliche Verantwortlichkeit beim Aufraggeber, während bei der Funktionsübertragung die datenschutzrechtliche Verantwortlichkeit (auch oder ausschließlich) bei der Stelle liegt, der die Aufgabenwahrnehmung übertragen wurde. Ob es sich im konkreten Fall um eine Auftragsdatenverarbeitung oder um eine Funktionsübertragung handelt, hängt sowohl von den tatsächlichen Verhältnissen als auch von der Vertragsgestaltung zwischen den beteiligten Stellen ab. In der Regel handelt es sich bei beauftragten Lettershops, Callcentern, Hostingdienstleistern oder Anbietern von Software as a Service oder von webbasierenden, virtuellen Datenräumen oder Speicherplätzen, in welche Daten hochgeladen, gespeichert, verwaltet und ausgetauscht werden können (auch sogenannte „Cloud“-Anbieter) um Auftragsdatenverarbeiter.

Dies gilt übrigens auch für Fälle, in denen die vorgenannten Dienstleistungen, im Auftrag durch eine Konzerntochter oder durch die Konzernmutter durchgeführt werden. Da hier kein „Konzernprivileg“ gilt, haben auch Unternehmensgruppen untereinander entsprechende Verträge sowie Kontrollen gemäß § 11 BDSG zu regeln.

Bei der Auftragsdatenverarbeitung trifft den Auftraggeber die Pflicht, den Auftragnehmer sorgfältig unter Berücksichtigung der bei ihm gegebenen technischen und organisatorischen Sicherheitsmaßnahmen auszuwählen und ihn während der Dauer des Auftrags zu überwachen (Auftragskontrolle). Die Kontrolle ist vor der erstmaligen Datenverarbeitung des Auftragnehmers und sodann regelmäßig durchzuführen. Die Kontrollen sind zudem zu dokumentieren. Hierbei kann auch auf vorhandene, aussagekräftige Zertifikate zum Datenschutz und zur Datensicherheit (z.B. ISO 27001 oder ein Zertifikat zur Auftragsdatenverarbeitung) zurückgegriffen werden.

Da der Auftraggeber trotz der Delegation für die ordnungsgemäße Datenverarbeitung verantwortlich bleibt, hat er gegenüber dem Auftragnehmer ein umfassendes Weisungsrecht (§ 11 Abs. 3 BDSG). Zudem sind die Datenschutzmaßnahmen gemäß § 11 BDSG schriftlich zu regeln.

Eine gute bzw. vorbildliche Umsetzung der Vorschriften des BDSG zur Auftragsdatenverarbeitung in der Praxis drückt sich durch eine vertrauensvolle Zusammenarbeit zwischen Auftragnehmer und Auftraggeber aus. Dies beinhaltet u.a., dass der Auftraggeber nicht nur über die Datenverarbeitungsvorgänge und entsprechenden Si-

cherheitsvorkehrungen beim Auftragnehmer informiert ist, sondern auch aktiv darauf Einfluss nehmen kann, sei es durch konkrete Vorgaben gegenüber dem Auftragnehmer oder durch gemeinsame Maßnahmen zur Verbesserung des Datenschutzes.

Kommen in Ihrem Unternehmen Auftragsdatenverarbeiter zum Einsatz, wird im Audit vor Ort ein Nachweis gefordert, dass ein Vertrag gemäß § 11 BDSG zwischen den relevanten Parteien vorliegt und dass Kontrollen durchgeführt wurden und regelmäßig durchgeführt werden.

5.19 C19 - Auftragskontrolle – Auflistung der Auftragsdatenverarbeiter

Falls ja: Bitte listen Sie die wesentlichen Dienstleister und eine Beschreibung ihrer Tätigkeit auf (z.B. Hosting des CRM-Systems im Rechenzentrum durch die YX GmbH; Callcenter mit Anbindung an das CRM durch die XY GmbH, Vernichtung von Datenträgern durch die XY GmbH; Fernwartung des Webservers durch die XY GmbH…).

Hier sind solche Auftragsdatenverarbeitungsverhältnisse gefragt, die für die Verarbeitung von Kundendaten von Bedeutung sind. Typischerweise sind dies Rechenzentren, in denen IT-Systeme des Unternehmens gehostet oder gewartet werden, Dienstleister, die zu Wartungszwecken einen Fernzugriff oder Zugriff vor Ort auf die IT-Systeme erhalten, externe Callcenter oder auch Entsorgungsunternehmen, die mit der Aktenvernichtung beauftragt sind.

Die relevanten externen Dienstleister sollen an dieser Stelle zusammengestellt werden. Später wird im Rahmen des Audits bezogen auf diese Dienstleister geprüft, ob Verträge konform zu § 11 BDSG sowie entsprechende Kontrollen vorliegen. Nachweise über Verträge oder die Beschreibung von Kontrollen müssen daher im Audit für die Auditoren zur stichprobenartigen Einsicht bereitgehalten werden.

5.20 C20 - Auftragskontrolle – Verträge gemäß § 11 BDSG

Falls Auftragnehmer i.S.d. § 11 BDSG eingesetzt werden: Liegen zu allen Auftragnehmern Verträge konform zu § 11 BDSG vor?

Gemäß § 11 BDSG sind diese Verträge zwingend schriftlich mit den im Gesetz benannten Mindestinhalten zu regeln.

Im Rahmen des Audits können die Auditoren stichprobenartig Verträge hierzu einsehen. Sie müssen daher bereitgehalten werden. Liegen diese nicht vor, endet die Auditierung mit nicht-bestanden.

5.21 C21 - Auftragskontrolle – Kontrollen der Dienstleister

Falls Auftragnehmer i.S.d. § 11 BDSG eingesetzt werden: Wurden diese zu Beginn und werden diese regelmäßig und nachweisbar kontrolliert (inkl. technisch-organisatorischer Maßnahmen nach § 9 BDSG)?

Hier ist nachzuweisen, dass die Auftragsdatenverarbeiter kontrolliert wurden und werden. Eine Vor-Ort-Kontrolle kann durch eine dokumentierte Auswahlentscheidung ersetzt werden, wenn hierbei definierte Auswahlkriterien zugrunde gelegt wurden, z.B. Zertifizierungen des Dienstleisters.

Liegen keine Nachweise vor oder kann dies den Auditoren nicht schlüssig dargelegt werden, endet das Audit mit nicht-bestanden.

5.22 C22 - Verfügbarkeitskontrolle – Backupkonzept

Gibt es ein Konzept zur Datensicherung (Backup)?

Die Verfügbarkeitskontrolle erfordert gem. Nr. 7 der Anlage zu § 9 BDSG Sicherheitsmaßnahmen, die die Daten gegen die zufällige Zerstörung bzw. Verlust schützen. Gefahren in diesem Bereich können durch Blitzschlag, Stromausfall, Wasserschaden

und ähnliche Einflüsse von außen drohen. Die zur Gewährleistung der Verfügbarkeitskontrolle zu treffenden Maßnahmen betreffen damit sowohl technische, als auch organisatorische Vorkehrungen zur Abwehr der o.g. Gefahren.

Die o.g. Maßnahme stellt einen Mindeststandard für die Verfügbarkeit von personenbezogenen Daten dar, den es zu erfüllen gilt. Anderenfalls endet das Audit mit nicht-bestanden.

5.23 C23 - Verfügbarkeitskontrolle – Weitere Maßnahmen

Welche der nebenstehenden Sicherheitsmaßnahmen sind umgesetzt?

- ☐ Der Serverraum wird über eine Klimaanlage gekühlt.
- ☐ Der Serverraum ist frei von Wasserleitungen.
- ☐ Der Serverraum ist mit einem Hochwasserschutz ausgestattet.
- ☐ Der Serverraum ist mit einer Brandmeldeanlage ausgestattet.
- ☐ Es ist eine unterbrechungsfreie Stromversorgung (USV) installiert.
- ☐ Der Serverraum ist mit einer Gaslöschanlage ausgestattet.
- ☐ Im Gebäude und im Serverraum stehen aktuell geprüfte Feuerlöscher zur Verfügung.
- ☐ Es befinden sich keine Brandlasten im Serverraum (z.B. Papier).
- ☐ Die Tür zum Serverraum ist eine Brandschutztür.
- ☐ Es werden täglich Backups aller relevanten Systeme erstellt.
- ☐ Backup-Bänder werden in einem anderen Brandabschnitt aufbewahrt.
- ☐ Backup-Bänder werden in einem feuerfesten Tresor aufbewahrt.
- ☐ Relevante Daten werden in zwei Rechenzentren gespiegelt.
- ☐ Es existiert eine dokumentierte Notfallregelung für den Schadensfall.
- ☐ Es existieren Stellvertretungsregelungen für Administratoren.
- ☐ Sonstiges:

Die o.g. Maßnahmen stellen Möglichkeiten dar, personenbezogene Daten im Sinne einer Verfügbarkeit zu schützen. Welche Maßnahmen letztendlich zu erfüllen sind, lässt sich anhand des potentiellen Risikos bei einem Datenverlust nur für den individuellen Sachverhalt Ihres Unternehmens ermitteln. Gefordert wird daher an dieser Stelle ein Standard an Maßnahmen, über die die gesetzlich geforderte Verfügbarkeitskontrolle angemessen sichergestellt werden kann; mehrere Antworten sind möglich und verbessern das Sicherheitsniveau.

5.24 C24 - Trennungsgebot – Datenbanktrennung/Mandantentrennung

Werden personenbezogene Daten, abhängig von dem Zweck ihrer Nutzung, in unterschiedlichen (logischen) Datenbanken verarbeitet?

Das Trennungsgebot gemäß Nr. 8 der Anlage zu § 9 BDSG fordert, dass Daten, die für unterschiedliche Zwecke erhoben werden, grundsätzlich jedenfalls logisch getrennt verarbeitet werden sollen.

Die o.g. Maßnahme stellt einen Mindeststandard zur Sicherstellung des Trennungsgebotes schutz dar, den es zu erfüllen gilt. Anderenfalls endet das Audit mit nicht-bestanden.

5.25 C25 - Trennungsgebot – Weitere Maßnahmen

Welche der nebenstehenden Sicherheitsmaßnahmen sind umgesetzt?

- ☐ **Daten werden pseudonymisiert, um eine Zusammenführung zu verhindern.**
- ☐ **Daten werden in getrennten Datenbanken geführt.**
- ☐ **Daten werden hardwareseitig getrennt geführt.**
- ☐ **Die Zwecktrennung ist über das Berechtigungskonzept umgesetzt.**
- ☐ **Sonstiges:**

Die o.g. Maßnahmen stellen Möglichkeiten dar, personenbezogene Daten im Sinne eines Trennungsgebotes zu schützen. Welche Maßnahmen letztendlich zu erfüllen sind, lässt sich anhand des potentiellen Risikos bei einem Datenverlust nur für den individuellen Sachverhalt Ihres Unternehmens ermitteln. Gefordert wird daher an dieser Stelle ein Standard an Maßnahmen, über die das gesetzlich geforderte Trennungsgebot angemessen sichergestellt werden kann; mehrere Antworten sind möglich und verbessern das Sicherheitsniveau.

6. Umsetzung von Rechten der Betroffenen

Zu einem vorbildlichen Datenschutzmanagement gehört neben den Sicherheitsvorkehrungen zum Schutz vor Risiken durch internen wie externen Missbrauch der Daten auch die Einrichtung von technischen und organisatorischen Maßnahmen zur effizienten Gewährleistung der gesetzlichen Betroffenenrechte. Nur wenn die Betroffenen ihre Rechte gegenüber der verantwortlichen Stelle einfach und unkompliziert geltend machen können, kann sich das Unternehmen im Bereich Datenschutz auszeichnen. Das Bild, welches der Betroffene von der Qualität des in dem Unternehmen praktizierten Datenschutzes erhält, wird dabei in hohem Maße davon bestimmt, wie dieses auf Anfragen, seien es solche allgemeiner Art zum Thema Datenschutz, spezielle Auskunftsersuchen zu personenbezogenen Daten oder bei der Geltendmachung von Sperrungs-, Löschungs-, Berichtigungs- oder Widerspruchsrechten, reagiert. Ein gut organisiertes „Auskunftsmanagement" kann dabei für viele Unternehmen ein Aushängeschild für vorbildlichen Datenschutz sein.

6.1 D1 - Beschwerdestelle

Existiert im Unternehmen eine Stelle, an die sich Verbraucher bei Fragen und Beschwerden zum Datenschutz wenden können (bitte benennen)?

Eine solche Stelle ist unumgänglich, damit der Betroffene überhaupt seine Rechte geltend machen kann. Dies kann ein professioneller Beschwerdemanager sein oder auch eine im Unternehmen definierte Person. In der Regel wird dies auch vom betrieblichen Datenschutzbeauftragten wahrgenommen.

Liegt keine solche Stelle vor, endet das Audit mit nicht-bestanden.

6.2 D2 - Auskünfte für Betroffene zur Speicherung von Daten

Werden Auskünfte zur Speicherung personenbezogener Daten gegenüber Betroffenen erteilt?

Betroffene haben z.B. gemäß § 34 BDSG ein Recht auf Auskunft. Daher endet das Audit mit nicht-bestanden, sofern nicht nachgewiesen werden kann, wie mögliche Auskunftsersuchen bearbeitet und erteilt werden.

6.3 D3 - Recht auf Löschung, Sperrung, Berichtigung von Daten

Wird dem Betroffenen ein Recht auf Löschung oder Sperrung sowie Berichtigung seiner gespeicherten Daten unter Berücksichtigung gesetzlicher Aufbewahrungsfristen eingeräumt?

Betroffene haben unter bestimmten Voraussetzungen ein Recht auf Löschung, Sperrung oder Berichtigung von personenbezogenen Daten, z.B. gemäß § 35 BDSG. Auf der anderen Seite kann die datenverarbeitende Stelle zur Speicherung personenbezogener Daten verpflichtet sein, etwa aus steuerlichen oder handelsrechtlichen Gründen.

Das Audit endet mit nicht-bestanden, sofern nicht nachgewiesen werden kann, wie mögliche Betroffenenersuchen bearbeitet und erteilt werden.

6.4 D4 - Datenlöschung nach Ablauf gesetzlicher Fristen

Werden personenbezogene Daten mit Ablauf gesetzlicher Aufbewahrungsfristen gelöscht?

Daten sind nach Ablauf von gesetzlichen Aufbewahrungsvorgaben unverzüglich zu löschen, z.B. gemäß § 35 BDSG. Der Gesetzgeber hat vielfältige Aufbewahrungsfristen geregelt, die hier nicht abschließend aufgeführt werden können. Beispielsweise sind für gewerbe- und steuerrechtliche Dokumente Aufbewahrungsfristen im Handelsgesetzbuch sowie in der Abgabenordnung geregelt. Die jeweilige Zweckbestimmung der Datenverarbeitung gibt dabei grundsätzlich den Beginn der Frist vor. Idealerweise wird die Löschung systemseitig automatisiert unterstützt, sie kann aber auch manuell erfolgen. Die Löschvorgaben beziehen sich nicht nur auf produktive Systeme sondern auch auf Backups.

Im Audit werden hierzu z.B. Löschkonzepte abgefragt und ggf. auch eine Stichprobe in einem wesentlichen Datenverarbeitungssystem gemacht. Das Audit endet mit nicht-bestanden, sofern nicht nachgewiesen werden kann, wie die Einhaltung der Löschvorgaben im Unternehmen umgesetzt wird.

7. Förderung des Datenschutzes

Mit dem Datenschutzgütesiegel soll nicht nur die Einhaltung des Datenschutzrechts zum Auditzeitpunkt bescheinigt werden; es soll darüber hinaus auch insbesondere Kunden und den von der Verarbeitung der Daten Betroffenen zeigen, dass ihre personenbezogenen Daten bei dem antragstellenden und ggf. zertifizierten Unternehmen gut aufgehoben sind.

Sind im Unternehmen Maßnahmen umgesetzt, die den Datenschutz besonders fördern oder in besonderer Weise die Rechte der Betroffenen gewährleisten? Bitte nennen Sie Beispiele.

Neben den genannten gesetzlichen Vorgaben muss das Unternehmen nachweisen können, dass es den Datenschutz insgesamt fördert. Dies kann auf vielfältige Weise bewerkstelligt werden, so dass anstelle von Fragen hier nur Beispiele genannt werden sollen:

- Für Datenschutzprüfungen wird ein Audittool eingesetzt.
- Das Verfahrensverzeichnis wird auf den Unternehmenswebseiten veröffentlicht.
- Es gibt zahlreiche transparente Hinweise und Merkblätter, die den Datenschutz verdeutlichen.
- Das Unternehmen kann bereits andere anerkannte Zertifikate in den Bereichen Datenschutz oder Datensicherheit vorweisen (diese sind oben angegeben).

Das Audit endet mit nicht-bestanden, sofern die Auditoren keine Anhaltspunkte dafür haben, dass der Datenschutz besonders gefördert wird.

Möglichkeit für Ihre Notizen:

Ende des Kriterienkataloges mit Erläuterungen