# Neuer Datenschutzstandard ist Basis für Prüfsiegel

## Dr. Niels Lepperhoff über das neue Angebot von BvD und GDD

Ein gutes Datenschutzniveau in einem Unternehmen ist unsichtbar. Es lässt sich weder an Produkteigenschaften noch an Kennzahlen wie Umsatz oder Mitarbeiteranzahl festmachen. Der BvD e.V. und die Gesellschaft für Datenschutz und Datensicherheit e.V. (GDD) haben deshalb ein Datenschutzsiegel basierend auf dem Datenschutzstandard „DS-BvD-GDD-01" speziell für die Auftragsdatenverarbeitung entwickelt. BvD-News-Redakteur Michael Braun sprach mit Dr. Niels Lepperhoff, dem Geschäftsführer der von BvD und GDD gegründeten DSZ Datenschutz Zertifizierungsgesellschaft mbH, über den neuen Standard, das neue Siegel und den Hintergrund des neuen BvD-Angebotes.

*BvD-News: Herr Dr. Lepperhoff, BvD und GDD haben sich zusammengetan, um gemeinsam einen Standard zur Auftragsdatenverarbeitung zu entwickeln, der von Auditoren überprüft und der mit einem Prüfsiegel bestätigt wird. Wie läuft das Verfahren kurz zusammengefasst ab?*

**Dr. Niels Lepperhoff:** Der Datenschutzstandard „DS-BvD-GDD-01" ist Grundlage zur Erteilung des von BvD und GDD entwickelten Datenschutzsiegels. Vergeben wird dieses Siegel von der DSZ Datenschutz Zertifizierungsgesellschaft mbH, einem gemeinsamen Unternehmen von BvD und GDD. Vor Erteilung des Siegels wird die Auftragsdatenverarbeitung von einem von der DSZ zertifizierten Auditor geprüft.

*BvD-News: Welche Beweggründe für die Formulierung des Standards gab es?*

**Dr. Niels Lepperhoff:** Das Angebot von BvD und GDD ist dazu da, um einen Mangel zu beheben, der sich aus § 11 BDSG (Auftragsdatenverarbeitung) ergibt. Er ist sehr unklar formuliert, es gibt viele Unsicherheiten, wie die Ausführungen des § 11 gemeint sind. Niemand weiß mit Sicherheit, was er tun muss, und das macht die Praxis enorm schwierig. Der neue Standard wurde von Datenschutz-Experten aus der Praxis heraus entwickelt. Der Standard ist offen und für jedermann einsehbar. Die Einhaltung dieses Standards wird durch die Vergabe eines Siegels bescheinigt. Die Konzeption aus öffentlich zugänglichem Standard sowie neutraler und transparenter Zertifizierung mit ausgewiesenen Datenschutzexperten überzeugt aus unserer Sicht.

*BvD-News: Was genau ist denn an Unsicherheiten vorhanden?*

**Dr. Niels Lepperhoff:** Der Gesetzgeber stellt zwar klar, dass vor Auftragsvergabe eine Überprüfung zur Auftragsdatenverarbeitung erfolgen muss – und dass es sie auch danach geben muss. Er spricht jedoch nur von einer regelmäßigen Kontrolle, ohne konkrete Zeiträume zu benennen. Unklar ist auch, in welcher Form kontrolliert werden soll.

*BvD-News: Es gibt ja bereits Prüfsiegel und Zertifikate am Markt. Warum jetzt das Siegel von BvD und GDD?*

**Dr. Niels Lepperhoff:** Die bisherigen Segel hatten Schwächen – sie waren intransparent und vor allem – sie hatten nicht die Unterstützung durch eine Aufsichtsbehörde.

*BvD-News: Und das ist jetzt anders?*

**Dr. Niels Lepperhoff:** Genau. Mit dem Standard DS-BvD-GDD-01 und dem damit verbundenen Siegel liegt erstmals eine Gesamtkonzeption aus Standard und Zertifizierungsablauf vor, die von einer Aufsichtsbehörde – in dem Fall durch den Landesbeauftragten für Datenschutz und Informationsfreiheit Nordrhein-Westfalen (LDI NRW) – befürwortet wird (siehe https://www.ldi.nrw.de/mainmenu_Datenschutz/submenu_Datenschutzrecht/Inhalt/Wirtschaft/Inhalt/Modellvorhaben_Datenschutzsiegel/Modellvorhaben_Datenschutzsiegel.pdf).

Der neue Standard beschreibt zudem konkret und transparent, welche Pflichten Auftraggeber wie Auftragnehmer in der Auftragsdatenverarbeitung haben. Er berücksichtigt die Betriebswirklichkeit und funktioniert dabei vollkommen unabhängig: Jede Technik und jede standardisierte Leistung wird unterstützt. Der neue Datenschutzstandard ist zudem öffentlich verfügbar und einsehbar. Dazu kommt wie gesagt die Qualitätsaussage der Behörde.

*BvD-News: Sie betonen die öffentliche Verfügbarkeit und die Transparenz. Können Sie diese Aspekte genauer ausführen?*

**Dr. Niels Lepperhoff:** Das Siegel ist sozusagen zweifach neutral: Scharfe Regeln zur Interessensfreiheit geben zum einen vor, dass weder der Auditor noch Mitglieder des Zertifizierungsausschusses mit dem zu prüfenden Unternehmen wirtschaftlich verbunden sein dürfen. Das gilt für Vergangenheit und Zukunft: Es ist ihnen untersagt, in den folgenden 12 Monaten Aufträge des Unternehmens anzunehmen. Der Zertifizierungsausschuss, bestehend aus unabhängigen zertifizierten Experten, prüft die Empfehlung des Auditors und entscheidet über die Siegelvergabe. Hier greift das Multi-Augen-Prinzip. Die Prüfberichte, die sich daraus ergeben, sind öffentlich zugänglich und geben so zu jeder Zeit den Prüfungsumfang und das Prüfungsergebnis wieder.

*BvD-News: Was haben Auftragnehmer und Auftraggeber konkret davon?*

**Dr. Niels Lepperhoff:** Auftraggeber und Auftragnehmer profitieren durch die Zertfizierung in mehrfacher Hinsicht: Es fallen nur geringe Kosten für Datenschutzkontrollen an, es ergibt sich mehr Sicherheit durch zertifizierte Auftragnehmer und die Prüfung erfolgt unabhängig, transparent und offen nachvollziehbar.

*BvD-News: Die Prüfung nehmen Auditoren ab. Einfach gefragt: Wie wird man zertifizierter Auditor?*

**Dr. Niels Lepperhoff:** Wer sich als Auditor zertifizieren lassen möchte, muss bestimmte Bedingungen erfüllen. Dies haben BvD und GDD zur Bedingung gemacht, um dem hohen Anspruch des neu entwickelten Datenschutzstandards zur Auftragsdatenverarbeitung gerecht zu werden.

***Dr. Niels Lepperhoff ist Geschäftsführer der von BvD und GDD neu gegründeten DSZ Datenschutz Zertifizierungsgesellschaft mbH.***

Konkret bedeutet das: Zertifizierte Auditoren müssen über eine Ausbildung zum Datenschutzbeauftragten nach der zwischen dem BvD und der GDD abgestimmten Ausbildung von 2008 oder einer in Inhalt und Umfang vergleichbaren Ausbildung verfügen. Erwartet wird eine einschlägige Berufserfahrung als Datenschutzbeauftragter oder Mitarbeiter eines Datenschutzbeauftragten von mindestens sechs Jahren. Vier Jahre reichen bei vorliegendem Magister, Bachelor-Abschluss oder dem ersten juristischen Staatsexamen an einer staatlich anerkannten Hochschule aus. Wer zugelassen werden möchte, muss eine Ausbildung zum Auditor in einem beliebigen Feld oder Berufserfahrung als Auditor in einem beliebigen Feld vorweisen. Obligatorisch ist eine Teilnahme an der Fortbildung


zum Auditor nach DS-BvD-GDD-01, die ab Frühjahr 2014 von BvD und GDD angeboten werden. Weiterer Aspekt: Eine innerhalb der letzten zwölf Monate bestandene Prüfung zum Auditor nach DS-BvD-GDD-01. Erst dann kann der Auditor Prüfungen im Rahmen dieses Zertifizierungsprozesses durchführen.

*BvD-News: Gibt es schon Datenschutzbeauftragte, die als Auditoren tätig werden können?*
**Dr. Niels Lepperhoff:** Ja. Erste Auditoren sind zertifiziert, so dass Unternehmen ab sofort ein Siegel beantragen können.

*BvD-News: Was haben externe Datenschutzbeauftragte als BvD-Mitglied davon, Auditor zu sein?*
**Dr. Niels Lepperhoff:** Für den Auditor ergeben sich gewisse Vorteile: Er kann mit der Verleihung der Zertifizierung als Auditor werben und er wird in eine zentrale Auditorenliste eingetragen. Damit sich der Auditor regelmäßig weiterbildet und seine Unternehmensprüfungen stets auf dem neuesten Stand des Datenschutzstandards verlaufen, ist das Zertifikat drei Jahre ab Ausstellungsdatum gültig. Es kann jeweils um weitere drei Jahre verlängert werden, sofern die Zertifizierungsvoraussetzungen, wie nachgewiesene Fortbildungen, erfüllt werden.

# Datenschutzkonforme Wege ins Web 2.0

## Fortbildung Social Media für Datenschutzbeauftragte am 4. November

Am 4. November findet im NH Hotel Frankfurt-Mörfelden die ganztägige BvD Fortbildung „Social Media für Datenschutzbeauftragte“ statt. Wir werfen einen Blick auf die social media Basics und Twitter & co. Ebenso werden rechtliche Betrachtungen hinsichtlich der Mitarbeiter-Rekrutierung im Web, aber auch für das Marketing relevante Aspekte beleuchtet. Referenten für diese Fortbildung sind Christoph Heyn und Stefan Bachmann. Anmeldungen hierfür nimmt die Geschäftsstelle gerne entgegen.