



Der Bundesbeauftragte
für den Datenschutz und
die Informationsfreiheit



Die Datenschutzbeauftragten in Behörde und Betrieb

Info **4**

Die Datenschutzbeauftragten in Behörde und Betrieb

Impressum

Herausgeber:

Der Bundesbeauftragte für den Datenschutz
und die Informationsfreiheit

Postfach 14 68, 53004 Bonn

Hausanschrift: Husarenstraße 30, 53117 Bonn

Tel. +49 (0) 228 997799-0

Fax +49 (0) 228 997799-550

E-Mail: poststelle@bfdi.bund.de


Internet: <http://www.datenschutz.bund.de>

Auflage: 9. Auflage, Oktober 2011

Realisation: Diamond media GmbH

Bildnachweis: Bellemedia | Dreamstime.com,

Jürgen Fälchle - Fotolia.com

BfDI – Info 



Inhaltsverzeichnis

Vorwort 6

1 Bestellung 8

1.1 Rechtsgrundlage und Anwendungsbereich 8

1.2 Wann muss ein Datenschutzbeauftragter bestellt werden? 9

1.3 Wer kann Datenschutzbeauftragter werden? 11

1.3.1 Was bedeutet die Anforderung der Fachkunde? 11

1.3.2 Was bedeutet die Anforderung der Zuverlässigkeit? 12

1.4 Wo bestehen Unvereinbarkeiten? 13

1.5 Wie ist der Datenschutzbeauftragte zu bestellen? 14

2 Stellung und Befugnisse 16

2.1 Stellung in der Hierarchie 16

2.2 Rechte und Grenzen in der Tätigkeit als Datenschutzbeauftragter 17

2.3 Benachteiligungsverbot 18

2.4 Unterstützungspflicht der verantwortlichen Stellen 19

2.5 Direktes Vorspracherecht beim Beauftragten für den Datenschutz 20

2.6 Eigeninitiative des Beauftragten für den Datenschutz 21

3 Aufgaben 22

3.1 Beratung und Mitwirkung 23

3.2 Vorabkontrolle 27

3.3 Kontrolle 29

3.4 Schulung 30

3.5 Verfahrensverzeichnis 31

3.6 Mitwirkung beim Audit 34

3.7 Verbündete 35

3.8 Erfahrungsaustausch 36

3.9 „Fahrplan“ 36

Anhang 1: Bestellung zur/zum behördlichen
Datenschutzbeauftragten 41

Anhang 2: Bekanntmachung/Hausverfügung Datenschutz 42

Anhang 3: Verfahrensverzeichnis nach § 4g i.V.m. § 18 und § 4e BDSG 43

Anhang 4: Muster für die Vorabkontrolle 46

Anhang 5: Hinweise zu automatisierten Abrufverfahren i.S.v. § 10 BDSG 48

Anhang 6: Anschriften der Datenschutzbeauftragten des
Bundes und der Länder 51

Anhang 7: Anschriften der Aufsichtsbehörden für
den nicht-öffentlichen Bereich 54

Anhang 8: Internetadressen zum Datenschutz 56

Anhang 9: Elektronische Informationen zum Datenschutz 57

Anhang 10: Beschluss der obersten Aufsichtsbehörden für
den Datenschutz im nicht-öffentlichen Bereich
(Düsseldorfer Kreis) vom 24./25. November 2010 59



Das Bundesdatenschutzgesetz enthält in den §§ 4f und 4g einheitliche Regelungen zu Bestellung und Aufgaben von betrieblichen bzw. behördlichen Beauftragten für den Datenschutz, die in gleicher Weise für den öffentlichen Bereich des Bundes wie für nicht-öffentliche Stellen, also für Unternehmen, Vereine, Verbände etc. gelten.

Diese internen Datenschutzbeauftragten, die nicht zu verwechseln sind mit den unabhängigen Aufsichtsbehörden für den jeweiligen Bereich, haben eine wichtige Funktion bei der Verwirklichung des

Datenschutzes. Das Gesetz will sie in die Lage versetzen, die ihnen vom Gesetzgeber übertragenen Aufgaben optimal zu erfüllen.

Die internen Datenschutzbeauftragten sind Motor des Datenschutzes in ihrer Behörde oder in ihrem Betrieb und zugleich Koordinatoren für alle Datenschutzmaßnahmen. Sie sollen auf allen Ebenen die Mitarbeiter motivieren, sensibel mit den ihnen anvertrauten personenbezogenen Daten umzugehen, frühzeitig Entwicklung und den Einsatz der IT-Einrichtungen und der Software für die Verarbeitung personenbezogener Daten begleiten und auf ihre Datenschutztauglichkeit hin überprüfen und die Leitung der Behörde oder des Betriebes in den Stand setzen, ihre Verantwortung auf dem Gebiet des Datenschutzes problembewusst und informiert wahrzunehmen.

Um dieses Aufgabenspektrum bewältigen zu können, benötigen die internen Datenschutzbeauftragten die aktive Unterstützung der Leitung ihrer Behörde oder ihres Betriebes. Dies betrifft nicht nur die Ausstattung mit Sachmitteln und fachkundigen Mitarbeitern, etwa für den IT-Bereich, sondern vor allem auch die Entlastung von anderen Aufgaben, damit hinreichend Zeit für die Arbeit als Datenschutzbeauftragte bleibt. Auch dürfen sie keinen Interessenkonflikten ausgesetzt sein, die sich aus der Wahrnehmung anderer ihnen übertragener Tätigkeiten ergeben können.

In der Vergangenheit sind überall dort, wo bereits interne Datenschutzbeauftragte tätig waren, durchweg positive Erfahrungen gemacht worden. Nachdem durch die Änderung des Bundesdatenschutzgesetzes im Mai 2001 erstmals einheitliche Bestimmungen für die Institution des Beauftragten für den Datenschutz im öffentlichen wie im nicht-öffentlichen Bereich geschaffen worden sind, ist deren Position mit der im September 2009 in Kraft getretenen BDSG-Novelle durch einen verbesserten Kündigungsschutz und eine Verpflichtung der Behörde bzw. des Betriebs zur Übernahme von Kosten für Schulungs- und Fortbildungsmaßnahmen nochmals deutlich gestärkt worden. Für die Zukunft wird ihre Bedeutung auf dieser neuen gesetzlichen Grundlage weiter wachsen. Funktionierender Datenschutz und bürger- bzw. kundenfreundliche Verfahren in diesem Bereich werden immer wichtiger und entwickeln sich zu einem Wettbewerbsvorteil. Bürgerinnen und Bürger informieren sich zunehmend über die Achtung ihres Persönlichkeitsrechts und machen ihr Verhalten davon abhängig, ob ihnen überzeugende Datenschutzkonzepte angeboten werden. Auch das im § 9a des Bundesdatenschutzgesetzes bereits verankerte Datenschutzaudit wird hier weiter die Aufgabe und Bedeutung der internen Datenschutzbeauftragten deutlich stärken.

Alles in allem dient die Tätigkeit der internen Datenschutzbeauftragten somit ihrem Unternehmen oder ihrer Verwaltung. Diese Broschüre stellt die wichtigsten Rechtsvorschriften für interne Datenschutzbeauftragte vor, verbunden mit einführenden Erläuterungen und praktischen Hinweisen. Sie richtet sich an die internen Datenschutzbeauftragten, aber auch an die interessierten Bürger und Mitarbeiter in Unternehmen und Verwaltung. Ich hoffe, diese Schrift kann dazu beitragen, dieses so bedeutende Amt zu stärken.

Berlin, im Oktober 2011

Peter Schaar

Der Bundesbeauftragte für den
Datenschutz und die Informationsfreiheit

Die Datenschutzbeauftragten in Behörde und Betrieb

1

Bestellung

1.1 Rechtsgrundlage und Anwendungsbereich

Im Bundesdatenschutzgesetz (BDSG) vom 20. Dezember 1990¹ wurden durch die Änderung mit Gesetz vom 18. Mai 2001², in Kraft getreten am 23. Mai 2001, in den §§ 4 f und 4 g erstmals einheitliche Bestimmungen für die Institution eines Datenschutzbeauftragten im öffentlichen wie im nicht-öffentlichen Bereich geschaffen. Diese Bestimmungen wurden durch das Erste Mittelstandsentlastungsgesetz vom 22. August 2006³ sowie durch Artikel 1 des Gesetzes zur Änderung datenschutzrechtlicher Vorschriften vom 14. August 2009⁴ nochmals geändert.

Die Praxis des Datenschutzes in Deutschland wird wesentlich durch das Wirken der betrieblichen und behördlichen Datenschutzbeauftragten bestimmt. Sie sind wichtige Ansprechpartner in Fragen des Datenschutzes für die Bürgerinnen und Bürger sowie die Leitungen und Beschäftigten in Behörden und Unternehmen.

Die Datenschutzgesetze der Länder sehen für den öffentlichen Bereich im Rahmen der Zuständigkeit der Länder ebenfalls die Einrichtung von Datenschutzbeauftragten vor. Die Regelungen des BDSG betreffen zum einen die Bestellung von Datenschutzbeauftragten in der Privatwirtschaft. Zum anderen müssen alle Behörden und sonstigen öffentlichen Stellen im Anwendungsbereich des BDSG einen Beauftragten für den Datenschutz berufen. Je nach Art der öffentlichen Stelle genügt auch die Bestellung eines Beauftragten für mehrere Bereiche. Während vor der Gesetzesnovellierung aus-

¹ BGBl. I S. 2954

² BGBl. I S. 904, §§ ohne weitere Bezeichnung sind stets solche des BDSG

³ BGBl. I S. 1970

⁴ BGBl. I S. 2814

schließlich im Bereich der Sozialleistungsträger nach dem Sozialgesetzbuch (§§ 35 SGB I, 81 SGB X i.V.m. § 4 f BDSG – novellierte Fassung) Datenschutzbeauftragte zu berufen waren, trifft diese Verpflichtung jetzt alle öffentlichen Stellen des Bundes.

Soweit im Folgenden von behördlichen Datenschutzbeauftragten gesprochen wird, sind nicht nur Behörden im engeren Sinne gemeint, sondern z.B. auch öffentliche Stellen des Bundes angesprochen, die privatrechtlich organisiert sind.

Diese Broschüre hat die behördlichen und betrieblichen Datenschutzbeauftragten als Organ der datenschutzrechtlichen Selbstkontrolle zum Gegenstand. Nicht umfasst ist die Datenschutzaufsicht durch den Bundesbeauftragten für den Datenschutz und die Informationsfreiheit oder die Landesbeauftragten für den Datenschutz, die im allgemeinen Sprachgebrauch häufig auch als „Datenschutzbeauftragte“ bezeichnet werden.

1.2 Wann muss ein Datenschutzbeauftragter bestellt werden?

Wie in Kapitel 1.1 ausgeführt, müssen die Behörden und sonstigen öffentlichen Stellen im Anwendungsbereich des BDSG einen Beauftragten für den Datenschutz bestellen. Nicht-öffentliche Stellen wie juristische Personen (z. B. Aktiengesellschaften, GmbH's usw.), Personengesellschaften (z. B. Gesellschaften des bürgerlichen Rechts), auch nicht rechtsfähige Vereinigungen (z. B. Gewerkschaften, politische Parteien) ebenso wie natürliche Personen (z. B. Ärzte, Rechtsanwälte, Architekten) können nach dem BDSG grundsätzlich verpflichtet sein, Datenschutzbeauftragte zu bestellen.

Voraussetzung für die Anwendbarkeit des BDSG ist zunächst, dass diese nicht-öffentlichen Stellen personenbezogene Daten unter Einsatz von Datenverarbeitungsanlagen (d.h. automatisiert) oder in oder aus nicht automatisierten Dateien verarbeiten, nutzen oder dafür erheben. Nicht einschlägig ist das BDSG, wenn die Erhebung, Verarbeitung oder Nutzung der Daten ausschließlich für persönliche oder familiäre Tätigkeiten erfolgt (§ 1 Abs. 2 Nr. 3).

Die Stellen, die die genannten Kriterien erfüllen, müssen nach § 4f Abs. 1 einen Beauftragten für den Datenschutz stets bestellen, wenn sie personenbezogene Daten geschäftsmäßig zum Zweck der Übermittlung (z.B. Adresshandel, Auskunfteien etc.), zum Zweck der anonymisierten Übermittlung oder für Zwecke der Markt- oder Meinungsforschung erheben, verarbeiten oder nutzen. Stets ist auch dann ein Datenschutzbeauftragter zu bestellen, wenn automatisierte Verarbeitungen erfolgen, die nach § 4d Abs. 5 der Vorabkontrolle unterliegen. (Näheres hierzu in Kapitel 3.2).

Sind diese besonderen Voraussetzungen nicht gegeben, hängt die Pflicht zur Berufung eines Datenschutzbeauftragten im nicht-öffentlichen Bereich von der Zahl der Personen ab, die mit der Datenverarbeitung beschäftigt sind. Ein Datenschutzbeauftragter muss bestellt werden, wenn

- in der Regel mindestens zehn Personen ständig mit der automatisierten Verarbeitung, Nutzung oder Erhebung personenbezogener Daten
- oder
- in der Regel mindestens zwanzig Personen mit der Verarbeitung, Nutzung oder Erhebung personenbezogener Daten auf andere Weise (manuelle Verarbeitung) beschäftigt sind.

Dabei stellt sich die Frage, wann eine Person mit der Datenverarbeitung im Sinne des BDSG „beschäftigt“ ist. Unstreitig zählen hierzu auch Teilzeitkräfte und Leiharbeitnehmer, denen im Rahmen ihrer beruflichen Aufgabenstellung die Verarbeitung personenbezogener Daten übertragen ist, und auch Inhaber von Mischarbeitsplätzen. Ein völlig untergeordneter Anteil von Datenverarbeitung an der Aufgabenstellung eines Beschäftigten dürfte aber nicht genügen, so z.B. die vereinzelt Erstellung eines Schreibens mit personenbezogenen Daten. Da der Anwendungsbereich des novellierten Bundesdatenschutzgesetzes jegliche automatisierte Datenverarbeitung erfasst, mithin auch die bloße Textverarbeitung, würde sonst die Verpflichtung zur Bestellung eines Datenschutzbeauftragten in einem Maße ausgedehnt, wie es nicht der gesetzgeberischen Absicht entspricht.

Der Datenschutzbeauftragte muss von der nicht-öffentlichen Stelle innerhalb einer Frist von einem Monat nach Aufnahme ihrer Tätigkeit bestellt werden. Das BDSG enthält einen Ordnungswidrigkeitentatbestand, der, wenn ein betrieblicher Datenschutzbeauftragter nicht oder nicht rechtzeitig bestellt wird, eine Geldbuße von bis zu 50.000 € vorsieht.

1.3 Wer kann Datenschutzbeauftragter werden?

Das Gesetz bestimmt, dass zum Datenschutzbeauftragten nur bestellt werden darf, wer die zur Erfüllung seiner Aufgaben erforderliche Fachkunde und Zuverlässigkeit besitzt. Das Maß der erforderlichen Fachkunde bestimmt sich im konkreten Einzelfall insbesondere nach dem Umfang der Datenverarbeitung der verantwortlichen Stelle und dem Schutzbedarf der personenbezogenen Daten, die die verantwortliche Stelle erhebt oder verwendet.

Auch eine Person außerhalb der verantwortlichen Stelle kann mit dieser Aufgabe betraut werden. Bei öffentlichen Stellen kann nach dem BDSG externer Datenschutzbeauftragter nur ein Bediensteter aus einer anderen öffentlichen Stelle sein.

Der Düsseldorfer Kreis, in dem alle Datenschutzaufsichtsbehörden für den nicht-öffentlichen Bereich vertreten sind, hat in seinem Beschluss vom 24./25. November 2010 „Mindestanforderungen an Fachkunde und Unabhängigkeit des Beauftragten für den Datenschutz nach § 4f Abs. 2 und 3 Bundesdatenschutzgesetz“ (Anhang 10) für die betrieblichen Datenschutzbeauftragten in der Privatwirtschaft eine Art Leitbild erstellt.

1.3.1 Was bedeutet die Anforderung der Fachkunde?

Die Fachkunde des Datenschutzbeauftragten soll sich am Umfang der Datenverarbeitung und dem Schutzbedarf der personenbezogenen Daten orientieren. Je mehr Daten die verantwortliche Stelle verarbeitet und je sensibler die personenbezogenen Daten sind, desto höhere Anforderungen sind an die Qualifikation und Fachkunde des Datenschutzbeauftragten zu stellen.

Fachkunde bedeutet zunächst, dass der Datenschutzbeauftragte die gesetzlichen Regelungen kennt und sicher anwenden kann. Dazu gehören die Grundrechte mit Datenschutzbezug, das BDSG, einschlägige spezielle datenschutzrechtliche Regelungen und die Spezialvorschriften seines Fachbereichs.

Er muss über gute organisatorische Kenntnisse und vertiefte Kenntnisse der Informationstechnik verfügen.

Die Anforderungen an die Fachkunde bei betrieblichen Datenschutzbeauftragten im privatwirtschaftlichen Bereich sind in einem Beschluss des Düsseldorfer Kreises beschrieben (vgl. 1.3 sowie Anhang 10).

Wenn der Datenschutzbeauftragte ausreichende Kenntnisse noch nicht besitzt, muss er die Bereitschaft und Befähigung besitzen, sie zu erwerben. Die Behörde oder der Betrieb haben ihm die Gelegenheit zur Teilnahme an geeigneten Fortbildungsveranstaltungen zu geben sowie deren Kosten zu übernehmen (vgl. § 4f Abs. 3 Satz 7).

Auch eine Unterstützung durch sachkundige Beschäftigte der eigenen Stelle oder durch Einholung von externem Sachverstand ist in Betracht zu ziehen.

Fortbildungsveranstaltungen zum Thema Datenschutz werden von einer Reihe von Institutionen und privaten Anbietern durchgeführt. Das Virtuelle Datenschutzbüro hat auf seiner Internetseite (<http://www.datenschutz.de>) unter „Fortbildungen“ einzelne Fortbildungsangebote im Bereich Datenschutz und Datensicherheit aufgelistet und Institutionen/Anbieter genannt, die Schulungen zu datenschutzrechtlichen Themen durchführen.

1.3.2 Was bedeutet die Anforderung der Zuverlässigkeit?

Der Datenschutzbeauftragte in Behörden und Betrieben ist entsprechend seiner Aufgabenstellung Vertrauensperson sowohl für die Behörden- bzw. Geschäftsleitung, als auch für die Beschäftigten seiner Organisation und, je nach Ansiedlung, auch für die Bürgerinnen und Bürger oder auch Kunden und Geschäftspartner.

Dieser Stellung muss er gerecht werden und dem Datenschutz, der immer noch gelegentlich als „lästige Behinderung“ empfunden wird, Geltung verschaffen. Er hat damit

oft eine Position „zwischen den Stühlen“ und muss manchmal unbequem sein, sich durchsetzen, aber auch offen sein für unterschiedliche Interessen und nach angemessenen Lösungen suchen. Neben einer generellen charakterlichen Stärke und Eignung erfordert dies die Fähigkeit, eine unabhängige Position zu behaupten und gleichzeitig offen und verständnisvoll für unterschiedliche Interessenlagen zu sein.

Vom Gesetz besonders benannt ist die Verschwiegenheitspflicht des Datenschutzbeauftragten. Er ist zur Verschwiegenheit über die Identität der Betroffenen (auch Beschwerdeführer) sowie über die Umstände, die Rückschlüsse auf den Betroffenen zulassen, verpflichtet, soweit dieser ihn nicht davon befreit hat. Die strikte Beachtung der Verschwiegenheitspflicht ist Grundvoraussetzung für die Stellung des Datenschutzbeauftragten als Vertrauensperson.

Die Anforderungen an die Zuverlässigkeit von betrieblichen Datenschutzbeauftragten im privatwirtschaftlichen Bereich sind in einem Beschluss des Düsseldorfer Kreises beschrieben (vgl. 1.3 sowie Anhang 10).

1.4 Wo bestehen Unvereinbarkeiten?

Wenn ein Datenschutzbeauftragter die Aufgabe nicht hauptamtlich wahrnimmt, muss bei der Übertragung anderer Aufgaben darauf geachtet werden, dass diese den Datenschutzbeauftragten nicht in einen Interessenkonflikt bringen können und damit seine unabhängige Stellung gefährden.

Insbesondere darf er als Datenschutzbeauftragter mit Kontrollfunktionen nicht in die Situation kommen, dass er sich selbst kontrollieren muss.

Interessenkonflikte können insbesondere dann auftreten, wenn der Datenschutzbeauftragte gleichzeitig Aufgaben in den Bereichen

- Personal,
- ADV/Informationstechnik (IT) oder in

- Organisationseinheiten mit besonders umfangreicher oder sensibler Verarbeitung von personenbezogenen Daten wahrnimmt oder
- Geheimschutzbeauftragter ist.

Möglich ist dagegen die Zusammenlegung der Funktionen des Datenschutzbeauftragten mit denen des IT-Sicherheitsbeauftragten. Ist der IT-Sicherheitsbeauftragte organisatorisch unabhängig von der für die IT verantwortlichen Organisationseinheit eingerichtet, ist die Zusammenfassung in einer Hand empfehlenswert. Auch die Kombination mit der Leitung oder der Mitarbeit im Bereich Organisation bietet sich für die Aufgabe an. Bei einer gleichzeitigen Mitarbeit im Bereich Justitiariat/Recht ist nicht generell von einer Unvereinbarkeit auszugehen, gleichwohl kann es problematisch sein, wenn der Datenschutzbeauftragte auch in Gerichtsprozessen gegen Mitarbeiterinnen und Mitarbeiter tätig wird.

1.5 Wie ist der Datenschutzbeauftragte zu bestellen?

Der Datenschutzbeauftragte muss durch die Leitung der Behörde, der Organisation oder des Unternehmens schriftlich bestellt werden. Ein Muster für die Bestellung eines Datenschutzbeauftragten im Bereich der öffentlichen Stellen, auf die das BDSG Anwendung findet, ist als Anhang 1 beigefügt.

Über die Bestellung des Datenschutzbeauftragten sollten alle Mitarbeiterinnen und Mitarbeiter informiert werden. Im öffentlichen Bereich, in dem die Datenschutzbeauftragten auch Ansprechpartner für die Bürgerinnen und Bürger sind, sollten auch diese hierüber in geeigneter Form unterrichtet werden. Im Organisationsplan und im Geschäftsverteilungsplan ihrer Behörden sollten die Datenschutzbeauftragten mit ihrer besonderen Stellung in der Hierarchie kenntlich sein. Eine Mitwirkungs- bzw. Mitbestimmungspflicht des Personalrates oder Betriebsrates bei der Bestellung des Datenschutzbeauftragten im Hinblick auf die Funktion – also außerhalb ohnehin bestehender Mitbestimmungsvorschriften bei Personalmaßnahmen wie z.B. Einstellung oder Versetzung – besteht nicht. Daraus hat das Bundesarbeitsgericht in einer Grundsatzenscheidung vom 11. November 1997 – 1 ABR 21/97 – (veröffentlicht u.a. in Recht der

Datenverarbeitung 1998, S.64 ff.), die eine nicht-öffentliche Stelle betraf, abgeleitet, dass der betriebliche Datenschutzbeauftragte der Arbeitgeberseite zuzuordnen sei und damit keine Befugnis zur Kontrolle des Betriebsrates habe.

Ungeachtet einer fehlenden Mitbestimmungspflicht für die Bestellung des Datenschutzbeauftragten kommt eine Beteiligung des Personalrates oder Betriebsrates aber im Rahmen der vertrauensvollen Zusammenarbeit in Betracht.

2

Stellung und Befugnisse

2.1 Stellung in der Hierarchie

Die unabhängige und organisatorisch herausgehobene Stellung ist für eine wirkungsvolle Tätigkeit des Datenschutzbeauftragten von ausschlaggebender Bedeutung. Er darf bei der Wahrnehmung seiner Aufgaben nicht den Weisungen der Organisationseinheiten unterliegen, die er zu kontrollieren hat. In seiner Funktion als Datenschutzbeauftragter ist er nach § 4f Abs. 3 Satz 1 dem Leiter der öffentlichen oder nicht-öffentlichen Stelle unmittelbar zu unterstellen. Dies kann in Form einer Stabsfunktion erfolgen. Möglich ist auch eine Klarstellung der besonderen Stellung in der Hierarchie, die für alle Mitarbeiter erkennbar sein muss, z.B. im Organigramm einer Behörde.

Die Unabhängigkeit des Datenschutzbeauftragten gibt ihm auch das Recht, sich nach § 4g Abs. 1 Satz 2 in Zweifelsfällen an die für die Datenschutzkontrolle bei der verantwortlichen Stelle zuständige Behörde zu wenden, um auf die Einhaltung des Bundesdatenschutzgesetzes und anderer Vorschriften über den Datenschutz hinzuwirken.

Eine Einschränkung dieser unabhängigen Stellung findet sich allerdings für die in § 6 Abs. 2 Satz 4 genannten Behörden. Es sind dies z.B. die Verfassungsschutzbehörden, der Bundesnachrichtendienst, der Militärische Abschirmdienst, Behörden aus dem Bereich des Bundesministeriums der Verteidigung, Polizeibehörden, Staatsanwaltschaften und weitere. Dort setzt das Anrufungsrecht des Datenschutzbeauftragten einer Bundesbehörde gegenüber dem Bundesbeauftragten für den Datenschutz und die Informationsfreiheit das Benehmen mit dem Behördenleiter voraus. Bei Unstimmigkeiten zwischen dem behördlichen Beauftragten für den Datenschutz und dem Behördenleiter entscheidet die oberste Bundesbehörde über die Zulässigkeit der Anrufung des Bundesbeauftragten für den Datenschutz und die Informationsfreiheit (§ 4g Abs. 3 Satz 2 BDSG).

Die Unabhängigkeit des internen Datenschutzbeauftragten wird auch durch den besonderen Abberufungsschutz aus § 4f Abs. 3 Satz 4 abgesichert. Danach kann die Bestellung zum Beauftragten für den Datenschutz nur in entsprechender Anwendung von § 626 des Bürgerlichen Gesetzbuches (BGB), bei nicht-öffentlichen Stellen auch auf Verlangen der Aufsichtsbehörde, widerrufen werden. Ein wichtiger Grund für den Widerruf entsprechend § 626 BGB liegt dann vor, wenn dem Leiter der öffentlichen oder nicht-öffentlichen Stelle die weitere Amtsausübung durch den Datenschutzbeauftragten unter Berücksichtigung aller Umstände des Einzelfalles nicht zugemutet werden kann.

Noch weiter gestärkt ist die Position und Unabhängigkeit des Datenschutzbeauftragten seit dem 01. September 2009 durch einen verbesserten Kündigungsschutz. Nach § 4f Abs. 3 Satz 5 und 6 ist, sofern für die verantwortliche Stelle eine Pflicht zur Bestellung eines Datenschutzbeauftragten nach § 4f Abs. 1 besteht, eine Kündigung nur zulässig, wenn Tatsachen vorliegen, die zur Kündigung aus wichtigem Grund ohne Einhaltung einer Kündigungsfrist berechtigen (z.B. Einstellungsbetrug, beharrliche Arbeitsverweigerung). Das gleiche gilt für den Zeitraum eines Jahres nach Beendigung der Bestellung zum Beauftragten für den Datenschutz.

2.2 Rechte und Grenzen in der Tätigkeit als Datenschutzbeauftragter

Der Datenschutzbeauftragte hat jederzeit ein direktes Vortragsrecht bei der Leitung; dies ergibt sich daraus, dass er dieser unmittelbar unterstellt ist. Er ist über alle für seine Tätigkeit relevanten Geschehnisse in seiner Organisation umfassend und frühzeitig zu unterrichten. Dies kann geschehen durch:

- Beteiligung an Leitungsbesprechungen,
- Beteiligung an allen Planungen, die den Umgang mit personenbezogenen Daten betreffen,
- Verpflichtung aller Organisationseinheiten, den Datenschutzbeauftragten an allen datenschutzrelevanten Vorgängen zu beteiligen.

Es ist zu empfehlen, dass der Datenschutzbeauftragte in Abstimmung mit der Leitung einen Beteiligungskatalog erstellt. Dabei sollten auch Regelungen über die Art und Weise der Einbindung und deren Zeitpunkt erfolgen. Die Unabhängigkeit des Datenschutzbeauftragten wird auch dadurch gestützt, dass er in der Ausübung seiner Fachkunde auf dem Gebiet des Datenschutzes weisungsfrei ist (§ 4f Abs. 3 Satz 2).

Der Datenschutzbeauftragte bestimmt pflichtgemäß selbst die Art und den Zeitpunkt seines Tätigwerdens. Niemand, auch nicht der Leiter der Stelle, kann ihm vorschreiben, für welche Rechtsauffassung er sich bei der Bewertung einer datenschutzrechtlichen Frage im Einzelfall entscheidet. Der Leiter der Stelle kann sich aber über das Votum des Datenschutzbeauftragten hinwegsetzen, denn letztlich trägt er die Verantwortung für die Daten verarbeitende Stelle.

2.3 Benachteiligungsverbot

Neben dem Kündigungsschutz und dem besonderen Widerrufsschutz hinsichtlich seiner Bestellung (vgl. 2.1) wird die Unabhängigkeit des Datenschutzbeauftragten auch durch ein generelles Benachteiligungsverbot geschützt (§ 4f Abs. 3 Satz 3).

Das Verbot, den Datenschutzbeauftragten wegen der Erfüllung seiner Aufgaben zu benachteiligen, ist weit gefasst. Unterhalb der Schwelle des Widerrufs- und Kündigungsschutzes sind damit alle denkbaren Benachteiligungen, sei es bei dem beruflichen Fortkommen, bei Fortbildungen, in finanzieller Hinsicht oder in sonstiger Weise gemeint.

Ein Problem bei der praktischen Durchsetzung des Benachteiligungsverbotes liegt darin, dass die Benachteiligung „wegen der Erfüllung seiner Aufgaben erfolgen muss“. Der Zusammenhang mit der Aufgabenwahrnehmung muss also nachgewiesen werden können.

2.4 Unterstützungspflicht der verantwortlichen Stellen

Nach § 4f Abs. 5 Satz 1 haben die öffentlichen und nicht-öffentlichen Stellen den Beauftragten für den Datenschutz bei der Erfüllung seiner Aufgaben zu unterstützen und ihm insbesondere, soweit dies zur Erfüllung seiner Aufgaben erforderlich ist, Hilfspersonal sowie Räume, Einrichtungen, Geräte und Mittel zur Verfügung zu stellen.

Der Datenschutzbeauftragte muss entsprechend seiner Verschwiegenheitspflicht die Möglichkeit haben, in geeignetem Büroraum vertrauliche Gespräche zu führen. Für die Wahrnehmung seiner Aufgabe, Mitarbeiterinnen und Mitarbeitern zu schulen, müssen entsprechende Räume zur Verfügung stehen. Ein durch den Datenschutzbeauftragten selbst zu verwaltendes Budget ist nicht erforderlich, möglicherweise von dem Datenschutzbeauftragten selbst auch nicht immer gewünscht. Es müssen ihm dann aber die Sachmittel, z.B. für die Anschaffung von Literatur und zur Weiterbildung, bereitgestellt werden. Hinweise auf einführende Literatur und Fortbildungsmöglichkeiten können bei den Aufsichtsbehörden nachgefragt werden.

Seit dem 1. September 2009 ist in § 4f Abs. 3 Satz 7 gesetzlich geregelt, dass die Behörden bzw. Betriebe dem Beauftragten für den Datenschutz zur Erhaltung seiner erforderlichen Fachkunde die Teilnahme an Fort- und Weiterbildungsveranstaltungen zu ermöglichen und deren Kosten zu übernehmen haben.

Für den Fall, dass der Datenschutzbeauftragte vertiefte rechtliche oder technische Beratung benötigt, sollten ihm – soweit vorhanden – geeignete Ansprechpartner der betreffenden Fachabteilungen benannt werden, auf die er bei Bedarf zurückgreifen kann.

Zur Unterstützungspflicht der verantwortlichen Stelle gehört auch, dem Datenschutzbeauftragten durch eine rechtzeitige und frühzeitige Einbindung und Beteiligung bei allen Planungen und Verfahren, die personenbezogene Daten betreffen, die Wahrnehmung seiner Aufgabe zu erleichtern oder gar erst zu ermöglichen.

Das Gesetz fordert speziell in § 4g Abs. 1 Satz 4 Nr. 1 die rechtzeitige Unterrichtung des Datenschutzbeauftragten über die Vorhaben der automatisierten Verarbeitung

personenbezogener Daten. Dem Datenschutzbeauftragten müssen auch Zugangs- und Einsichtsrechte gewährt werden, damit er seine Kontrollbefugnisse ausüben kann.

Von entscheidender Bedeutung hinsichtlich der Unterstützungspflicht der verantwortlichen Stelle gegenüber dem Datenschutzbeauftragten ist eine angemessene Entlastung von möglicherweise übertragenen anderen Aufgaben. Alle Rechte und Befugnisse können dem Datenschutzbeauftragten nur von Nutzen sein, wenn er ausreichend Zeit für die Wahrnehmung seiner Aufgabe hat. Bei größeren Behörden oder Unternehmen mit zahlreichen Mitarbeitern und PC-Arbeitsplätzen oder auch besonders umfangreicher oder sensibler personenbezogener Datenverarbeitung, die sich auch aus der Verarbeitung von Bürger- oder Kundendaten ergeben kann, kann die Bestellung eines hauptberuflichen Datenschutzbeauftragten geboten sein. Auch wenn ein gesetzlicher Freistellungsanspruch für den Datenschutzbeauftragten nicht gegeben ist, ergibt sich die Verpflichtung zu einer angemessenen Entlastung aus der Unterstützungspflicht für die Aufgabenwahrnehmung. Hinzu kommt die Verpflichtung aus dem Benachteiligungsverbot und nicht zuletzt auch die Fürsorgepflicht des Arbeitgebers.

2.5 Direktes Vorspracherecht beim Beauftragten für den Datenschutz

Gemäß § 4f Abs. 5 Satz 2 können sich Betroffene jederzeit an den Beauftragten für den Datenschutz wenden. Betroffene können nach der Definition in § 3 Abs. 1 sowohl die Mitarbeiterinnen und Mitarbeiter der Behörde oder des Unternehmens als auch z.B. Bürgerinnen und Bürger, die Kunden eines Unternehmens sind oder sich an eine Behörde gewandt haben oder sonstige Personen sein. Aufgrund der bereits erörterten Verschwiegenheitspflicht des Datenschutzbeauftragten über die Identität des Betroffenen sowie über Umstände, die Rückschlüsse auf den Betroffenen zulassen gemäß § 4f Abs. 4, müssen diese nicht befürchten, ohne ihr Einverständnis als Beschwerdeführer bekannt zu werden. Der Dienstweg im Behördenbereich muss daher nicht eingehalten werden. Auch insoweit bleibt die Vertraulichkeit für die Betroffenen gewahrt.

2.6 Eigeninitiative des Beauftragten für den Datenschutz

Im folgenden Kapitel werden die Aufgaben des Datenschutzbeauftragten, wie sie sich aus dem Gesetz unmittelbar ergeben oder ableiten lassen, beschrieben. Zu betonen ist hier, dass der Beauftragte für den Datenschutz sich keinesfalls darauf beschränken sollte, auf Anforderungen seitens seiner Organisation oder auf Beschwerden und Eingaben von Betroffenen zu reagieren. Gefordert ist vielmehr ein eigeninitiativ tätiger Datenschutzbeauftragter, der sich von sich aus bereits an datenschutzrelevanten Planungen – entsprechende Kenntnis über solche Planungen vorausgesetzt – beteiligt und unaufgefordert die Einhaltung der datenschutzrechtlichen Bestimmungen überwacht.

Auch Initiativen zur Schulung in Datenschutzfragen und zur begleitenden Kontrolle bestehender Datenverarbeitungen sind gefragt.

3

Aufgaben

Der Beauftragte für den Datenschutz wirkt gemäß § 4g auf die Einhaltung des Bundesdatenschutzgesetzes und anderer Vorschriften über den Datenschutz hin.

Unbeschadet der fortbestehenden Verantwortlichkeit der Leitung der verantwortlichen Stelle (Behörde, Unternehmen oder sonstige Stelle) trägt er damit zur Einhaltung der Vorschriften des Datenschutzes in seiner Organisation bei. Seine Aufgaben liegen in der Beratung, der datenschutzrechtlichen Schulung des Personals, der Kontrolle der Einhaltung der datenschutzrechtlichen Vorschriften, der Unterstützung von Betroffenen bei der Wahrnehmung ihrer Datenschutzrechte und der Schaffung von Transparenz in der Datenverarbeitung durch das „Verfügbarmachen“ des von ihm geführten Verfahrensverzeichnis.

Die vorrangige Aufgabe des Datenschutzbeauftragten ist die Beratung. Sie erfolgt gegenüber der Haus- bzw. Unternehmensleitung, aber auch gegenüber den Mitarbeitern und auf Wunsch auch gegenüber dem Personal- oder Betriebsrat.

Wenn Schwachstellen oder Versäumnisse im Datenschutz festgestellt werden, sollte der Datenschutzbeauftragte zunächst gemeinsam mit den Beteiligten nach konstruktiven Lösungen suchen. Wichtig ist dabei, den Mitarbeitern bewusst zu machen, dass Datenschutz positiv und nützlich ist. Bei angemessener Verwirklichung wird der Datenschutz Arbeitsabläufe im Ergebnis eher fördern als erschweren. Wenn nämlich eine Behörde oder ein Unternehmen zu viele Daten sammelt, Daten zu schnell oder zu spät löscht oder Daten unberechtigt übermittelt, wird nicht nur gegen Datenschutzrecht verstoßen, sondern es werden auch Bürokratie und Mehrkosten verursacht. Vor allem ist der Datenschutz ein wichtiges Element einer bürgerfreundlichen Verwaltung und als Markenzeichen eines Kunden und Mitarbeiter orientierten Unternehmens auch ein Wettbewerbsfaktor. Dabei geht es nicht mehr nur darum, negative Zwischenfälle zu vermeiden. Damit Bürger Vertrauen in die Angebote einer elektronischen Verwaltung setzen, müssen sie ihr Persönlichkeitsrecht im Umgang mit ihren Daten gewahrt sehen.

3.1 Beratung und Mitwirkung

Beratung als Schwerpunktaufgabe des Datenschutzbeauftragten richtet sich an unterschiedliche Zielgruppen. Diese Zielgruppen müssen mit jeweils für sie geeigneten Methoden erreicht werden. Die Beratung umfasst die wesentlichen Aufgabenbereiche des Datenschutzbeauftragten, die Wahrung des Datenschutzrechtes und die Verwirklichung und Absicherung durch den Einsatz datenschutzgerechter Technikgestaltung. Sie muss darauf zielen, den Einzelnen, seien es die Bürger, Kunden oder die Mitarbeiterinnen und Mitarbeiter, darin zu unterstützen, ihr Persönlichkeitsrecht zu schützen. Dabei genügt es nicht, nur im Einzelfall tätig zu werden, vielmehr müssen mit der unterstützenden Beratung des Datenschutzbeauftragten Strukturen so angelegt werden, dass sie – wie es auch das erklärte Ziel des Bundesdatenschutzgesetzes in § 1 Abs. 1 ist, den Einzelnen von vorneherein davor schützen, dass er durch den Umgang mit seinen personenbezogenen Daten in seinem Persönlichkeitsrecht beeinträchtigt wird. Beratung sollte daher unter Einbeziehung der Leitungsebene auf entsprechende Organisationsstrukturen ausgerichtet sein. Sie setzt bereits bei der Datenerhebung an und kann z.B. die Ausgestaltung und den Inhalt von Formularen zur Datenerhebung betreffen. Es kann hier um die Datenerhebung bei den Bürgerinnen und Bürgern, bei Kunden oder auch beim eigenen Personal gehen. Folgend betrifft sie dann die weitere Datenverarbeitung, was z.B. auch die Führung der Akten umfasst. Auch hier können wiederum alle genannten Personengruppen betroffen sein. Soweit es um die Mitarbeiter geht, muss der Datenschutzbeauftragte sich mit den bereichsspezifischen Bestimmungen des Datenschutzes auseinandersetzen, sei es im Personalaktenrecht oder beim Arbeitnehmerdatenschutz, der – abgesehen von der in § 32 BDSG neu geschaffenen besonderen Bestimmung zur Erhebung, Verarbeitung und Nutzung von Beschäftigtendaten – bisher weitgehend nur durch Rechtsprechung bestimmt ist.

Der Datenschutzbeauftragte muss somit die Einhaltung der Datenschutzvorschriften von der Erhebung der Daten, über die Institutionalisierung von Unterrichtspflichten gegenüber Betroffenen (Benachrichtigungsroutinen, Unterrichtung über das Widerspruchsrecht, Schaffung von Transparenz in der Datenverarbeitung) bis hin zur ordnungsgemäßen Beachtung von Lösungsfristen beratend begleiten. Besonders zu erwähnen ist in diesem Zusammenhang die seit dem 1. September 2009 geltende Vorschrift des § 42a BDSG, die nicht-öffentliche Stellen verpflichtet, die Aufsichtsbehörde und die Betroffenen unverzüglich zu benachrichtigen, wenn bestimmte sensible Daten unrechtmäßig Dritten zur Kenntnis gelangt sind und schwerwiegende Beeinträchtigungen für die Rechte oder schutzwürdigen Interessen der Betroffenen drohen. Der betriebliche Datenschutzbeauftragte muss von der verantwortlichen Stelle bei Ermittlung von Datenschutzpannen und deren Bewältigung sowie der notwendigen Information der Aufsichtsbehörde und der Betroffenen beteiligt werden. Hierauf hat der Gesetzgeber in der amtlichen Begründung zu § 42a BDSG ausdrücklich hingewiesen.

Die Sicherung des Datenschutzrechts durch Technik ist von immer größerer Bedeutung. Auch dort setzt die Beratungstätigkeit bereits bei der Planung von Datenverarbeitungsvorhaben an. Mit dem § 3a des novellierten Bundesdatenschutzgesetzes wurde der Grundsatz der Datenvermeidung und Datensparsamkeit gesetzlich verankert und der Systemdatenschutz bestärkt.

Der Datenschutzbeauftragte sollte daher bereits bei der Beschaffung der Hard- und Software beratend hinzugezogen werden, damit sich schon die Auswahl von Datenverarbeitungssystemen an dem Ziel ausrichtet, keine oder so wenig personenbezogene Daten wie möglich zu erheben, zu verarbeiten oder zu nutzen.

Zur Vermeidung von technischen Pannen und Lücken in der Datensicherheit sollte der Datenschutzbeauftragte auch bei der Erstellung eines IT-Sicherheitskonzeptes beteiligt werden.

Für die Frage der Datensicherheit ist der IT-Grundschutzkatalog des Bundesamtes für die Sicherheit in der Informationstechnik (BSI) eine wertvolle Hilfe (kostenlos herunter zu laden von der Webseite des BSI unter der Adresse www.bsi.de). Der Datenschutz wurde im IT-Grundschutzkatalog mit einem IT-Grundschutz-Baustein „Datenschutz“

verankert. Den Behörden des Bundes wird nahe gelegt (Gemeinsames Ministerialblatt 1995, S. 741), sich am Grundschutzkatalog zu orientieren.

Die Beratungsaufgabe des Datenschutzbeauftragten umfasst also sowohl die rechtliche als auch die technische Seite der Datenverarbeitung. Die denkbaren Fallgestaltungen sind vielfältig und einem ständigen Wandel unterworfen.

Exemplarisch sollen hier nur einige Bereiche genannt werden, die zunehmend an Bedeutung gewonnen haben und sich auch in der Zukunft weiterhin stark entwickeln werden. Zu nennen ist die Internetpräsenz von Behörden und Unternehmen, die eine Beratung durch den Datenschutzbeauftragten im bereichsspezifischen Recht der Tele- und Mediendienste, aber auch des Telekommunikationsrechts bedingt. Der zweite Schritt von der reinen Information hin zum interaktiven Handeln mit Bürgern und Kunden im E-Government und E-Commerce hat längst begonnen und wirft neue Fragestellungen auf. Gleichmaßen wirkt sich der Einsatz der neuen Technologien auch im Arbeitnehmerdatenschutz in der Beschäftigungsstelle aus. Dabei spielen die Fragen der Telearbeit und der Kontrollen im Bereich der E-Mail- und Internetnutzung durch Arbeitnehmer eine besondere Rolle. Die Beratung des Datenschutzbeauftragten muss aber auch den Bereich der externen Datenverarbeitung für die Behörde oder das Unternehmen im Wege der Auftragsdatenverarbeitung umfassen. Nach wie vor birgt die zunehmende Vergabe von Datenverarbeitungsaufgaben an externe Auftragsdatenverarbeiter erhöhte Risiken für das Persönlichkeitsrecht. Deshalb hat der Gesetzgeber in § 11 Abs. 2 des novellierten Bundesdatenschutzgesetzes nicht nur beispielhaft zehn Punkte genannt, die im Falle einer Auftragserteilung schriftlich festzuhalten sind. Der Auftraggeber ist nunmehr sogar ausdrücklich verpflichtet, die Einhaltung der vereinbarten Maßnahmen vor Beginn der Datenverarbeitung und sodann regelmäßig zu überprüfen und das Ergebnis dieser Überprüfung zu dokumentieren. Der Datenschutzbeauftragte ist auch hier bereits bei der Planung der Auftragsdatenverarbeitung, der Vertragsgestaltung und der regelmäßigen Kontrolle beratend gefordert.

Neben der Beratung, die auf die Schaffung geeigneter Strukturen abzielt, ist die Aufgabe des Datenschutzbeauftragten als Vertrauensperson für betroffene Mitarbeiter und Bürger sehr wichtig. Im nicht-öffentlichen Bereich müssen Beschäftigte bei der Aufnahme ihrer Tätigkeit auf das Datengeheimnis nach § 5 BDSG verpflichtet werden. Verschiedene

Muster einer solchen Verpflichtungserklärung sind auf der Website des Bundesbeauftragten für den Datenschutz und die Informationsfreiheit veröffentlicht (<http://www.bfdi.bund.de> unter Themen / BDSG Datenschutz allgemein / Einzelfragen / Datengeheimnis).

In einer kleineren Organisation kann dies eine Möglichkeit für den Datenschutzbeauftragten sein, sich neuen Mitarbeiterinnen und Mitarbeitern gleich zu Beginn der Tätigkeit persönlich bekannt zu machen. In größeren Organisationseinheiten könnte das z. B. auch so aussehen, dass der Datenschutzbeauftragte mit einer Broschüre über den Datenschutz informiert, zumal die bloße Unterschriftsleistung unter eine Verschwiegenheitsverpflichtung noch keine Schulung im Datenschutz beinhaltet. Auch muss das Rad gerade mit Blick auf die begrenzten Personalressourcen des Datenschutzbeauftragten nicht immer neu erfunden werden. Warum nicht vorhandenes Informationsmaterial, wie die Informationsbroschüren des Bundesbeauftragten für den Datenschutz und die Informationsfreiheit zum BDSG und zu anderen Themen oder die Broschüren der Datenschutzaufsichtsbehörden der Länder nehmen und dies mit einem Vorstellungsgespräch und Begrüßungsschreiben des Datenschutzbeauftragten verteilen?

Auch die Bürgerinnen und Bürger sowie Kunden eines Unternehmens können über die Person des Datenschutzbeauftragten und die Verwirklichung des Datenschutzes in seiner Beschäftigungsstelle informiert werden und ein allgemeines Beratungsangebot bekommen. Neben den Printmedien sollte hier in jedem Fall auch das Internet für solche Informationen genutzt werden. Allgemein gilt, dass die Beratungsaufgabe des Datenschutzbeauftragten und seine entsprechenden Angebote bekannt und den Betroffenen leicht zugänglich sein müssen.

Der Beteiligungskatalog, den der Datenschutzbeauftragte mit der Leitung seiner Organisation abgestimmt hat, sollte daher in seiner Organisation publik gemacht werden, ebenso wie die Serviceangebote des Datenschutzbeauftragten. Dies kann in vielfältiger Weise geschehen. Eine behörden- bzw. unternehmensinterne Zeitung kann für Informationen genutzt werden. In einer Zeit, in der fast alle Arbeitsplätze mit vernetzten Computern ausgestattet sind, bietet sich auch das Intranet (organisationsinternes Netz) für Informationen an. Für nach außen gerichtete Angebote sollte immer auch das Internet benutzt werden. Aber auch herkömmliche Verbreitungswege wie das „Schwarze Brett“ und Aushänge kommen in Frage.

Es ist zu empfehlen, dass der Datenschutzbeauftragte regelmäßig (ggf. jährlich) seiner Leitung einen Bericht über Datenschutzfragen abgibt. Dabei geht es nicht nur darum, den Datenschutz in das Bewusstsein zu rücken, sondern auch darum, Probleme und Entwicklungen aufzuzeigen und auf mögliche Fehlentwicklungen frühzeitig hinzuweisen. Auch ein solcher Bericht hat daher eine Beratungsfunktion und sollte keine „Geheimsache“ sein.

3.2 Vorabkontrolle

Eine weitere dem Datenschutzbeauftragten ausdrücklich gemäß § 4d Abs. 6 Satz 1 zugewiesene Aufgabe ist die Vorabkontrolle. Wann eine Vorabkontrolle durchzuführen ist, ergibt sich aus § 4d Abs. 5:

„Soweit automatisierte Verarbeitungen besondere Risiken für die Rechte und Freiheiten der Betroffenen aufweisen, unterliegen sie der Prüfung vor Beginn der Verarbeitung (Vorabkontrolle). Eine Vorabkontrolle ist insbesondere durchzuführen, wenn

1. besondere Arten personenbezogener Daten (§ 3 Abs. 9) verarbeitet werden oder
2. die Verarbeitung personenbezogener Daten dazu bestimmt ist, die Persönlichkeit des Betroffenen zu bewerten einschließlich seiner Fähigkeiten, seiner Leistung oder seines Verhaltens,

es sei denn, dass eine gesetzliche Verpflichtung oder eine Einwilligung des Betroffenen vorliegt oder die Erhebung, Verarbeitung oder Nutzung der Zweckbestimmung eines Vertragsverhältnisses oder vertragsähnlichen Vertrauensverhältnisses mit dem Betroffenen dient.“

Die in § 4d Abs. 5 Satz 2 genannten Beispiele sind Regelbeispiele. Das bedeutet, dass eine Vorabkontrolle auch in anderen, nicht genannten Beispielfällen, erforderlich sein kann. Sie sollte stets durchgeführt werden, wenn ein automatisiertes Abrufverfahren nach § 10 eingeführt werden soll. Um prüfen zu können, ob die Voraussetzungen einer Vorabkontrolle gegeben sind, muss der Datenschutzbeauftragte, wie zuvor schon erwähnt, im Rahmen seines Beteiligungskataloges von allen geplanten automatisierten

Verfahren zur Verarbeitung personenbezogener Daten frühzeitig Kenntnis erhalten. In Zweifelsfällen hinsichtlich der Erforderlichkeit einer Vorabkontrolle muss er sich an die zuständige Aufsichtsbehörde für den nicht-öffentlichen Bereich bzw. bei den Post- und Telekommunikationsunternehmen und den öffentlichen Stellen des Bundes an den Bundesbeauftragten für den Datenschutz und die Informationsfreiheit wenden (§ 4d Abs. 6 Satz 3).

Zeitlich ist die Vorabkontrolle nach Empfang der Übersicht nach § 4g Abs. 2 Satz 1 vorzunehmen. Sie umfasst inhaltlich sowohl die materiell-rechtliche Prüfung der geplanten Verarbeitung wie auch die Beurteilung der technischen und organisatorischen Maßnahmen. Aus Gründen der Beweissicherheit ist sie schriftlich oder in gesicherter elektronischer Form zu dokumentieren. Die Dokumentation gehört sinnvoller Weise in den nicht öffentlichen Teil des Verfahrensverzeichnis, wenn das Verfahren dort aufgenommen wird. Das Muster einer Vorabkontrolle nach dem BDSG ist als Anhang 4 abgedruckt. Dabei handelt es sich um die Abwandlung eines vom Hessischen Landesbeauftragten für den Datenschutz entwickelten ersten Musters einer Checkliste für die Durchführung einer Vorabkontrolle entsprechend den Vorschriften für den Bundesbereich. Das Muster darf jedoch nicht schematisch angewandt werden. Es ist vielmehr bei jeder Vorabkontrolle zu prüfen, ob zusätzliche Aspekte einbezogen werden müssen. In den in § 4d Abs. 5 Satz 2 genannten Ausnahmefällen (gesetzliche Verpflichtung, Einwilligung des Betroffenen oder wenn die Erhebung, Verarbeitung oder Nutzung der Zweckbestimmung eines Vertragsverhältnisses oder vertragsähnlichen Vertrauensverhältnisses mit dem Betroffenen dient) besteht keine Rechtspflicht zur Durchführung der Vorabkontrolle.

3.3 Kontrolle

Wie in Kapitel 3 ausgeführt hat der Datenschutzbeauftragte auch nachträglich die Einhaltung der datenschutzrechtlichen Vorschriften zu überprüfen. Die ihm eingeräumten Zugangs- und Einsichtsrechte sollten deswegen auch das Recht auf jederzeitige – auch unangekündigte – Kontrolle beinhalten. Hierzu muss der Datenschutzbeauftragte Zugang zum Rechenzentrum sowie den Dienst- bzw. Geschäftsräumen haben. Ferner muss er alle Unterlagen einsehen können, die mit der Verarbeitung personenbezogener Daten im Zusammenhang stehen. Ihm steht auch Einblick in die gespeicherten personenbezogenen Daten zu. Eine Kontrollbefugnis gegenüber dem Betriebs- bzw. Personalrat besteht, wie bereits dargelegt, jedoch nicht.

Der Datenschutzbeauftragte ist frei darin, zu bestimmen, wann und in welcher Form er die Kontrollen durchführt. Neben dem Nachgehen von Beschwerden, die Anlass zu einer gezielten Kontrolle in dem betroffenen Bereich geben, müssen regelmäßige Kontrollen stattfinden.

Für die Durchführung von Prüfungen gibt es verschiedene Ansätze. In Betracht kommt eine gezielte Prüfung der technisch-organisatorischen Maßnahmen und ihrer Einhaltung. Denkbar ist auch, sich auf die Kontrolle einer der in der Anlage zu § 9 Satz 1 benannten Maßnahmenbereiche zu konzentrieren. Die Prüfung kann auch ausgerichtet werden auf die Kontrolle eines bestimmten Verfahrens oder das Verfolgen eines Bearbeitungsvorganges einschließlich der materiell-rechtlichen Prüfung, Einhaltung der Zweckbindung, Beachtung der Rechtsgrundlage etc. oder auch auf eine Kombination der angesprochenen Vorgehensweisen.

Für die praktische Durchführung in speziellen Bereichen gibt es zahlreiche Checklisten. Es wird insoweit auf die Veröffentlichungen der Datenschutzaufsichtsbehörden verwiesen. Auch das Grundschutzhandbuch des BSI bietet eine gute Arbeitshilfe für die Durchführung von Prüfungen.

3.4 Schulung

Eine weitere wichtige Aufgabe, die das Gesetz dem Datenschutzbeauftragten gemäß § 4g Abs. 1 Satz 3 Nr. 2 zuweist, ist die Schulung der bei der Verarbeitung personenbezogener Daten tätigen Mitarbeiter. Auch hier gilt – ebenso wie bei der Beratung – dass die Schulung unterschiedliche Zielgruppen hat, die in geeigneter Weise mit auf sie abgestimmten Methoden erreicht werden müssen. Schulung darf daher nicht nach dem Prinzip „Gießkanne“ erfolgen. Wer bereits seit Jahren mit der Verarbeitung personenbezogener Daten zu tun und sich hier auch schon hinsichtlich der datenschutzrechtlichen Vorschriften kundig gemacht hat, bedarf keiner Einführungsschulung. Wer ganz frisch mit datenschutzrechtlichen Fragen konfrontiert wird, ist ggf. mit speziellen Fragestellungen überfordert. Auch knappe personelle Ressourcen des Datenschutzbeauftragten oder begrenzte Sachmittel für externe und interne Schulungen erfordern Prioritätensetzung.

Eine grundlegende Schulung benötigen die Personen, die in der EDV mit der Datenverarbeitung beschäftigt sind, auch diejenigen, die in der Personaldatenverarbeitung eingesetzt sind. Im übrigen sollten alle Mitarbeiterinnen und Mitarbeiter mit den wichtigsten Bestimmungen im Umgang mit personenbezogenen Daten vertraut gemacht werden. Dabei können die Schwerpunkte sehr unterschiedlich sein, je nach dem, wo der Mitarbeiter eingesetzt ist, sei es in der Gesundheitsbehörde, in der Arztpraxis oder in der Direktmarketingabteilung eines Unternehmens. Je nach Standort und Erfahrung kommen daher

- die Einweisung neuer Mitarbeiterinnen und Mitarbeiter,
- Schulungen im Rahmen der allgemeinen Aus- und Fortbildung der Beschäftigten,
- Vorträge oder Referate für einzelne Abteilungen oder Mitarbeitergruppen,
- Ausgabe von Merkblättern, die nach Bedarf aktualisiert werden können,
- Mitteilungen am Schwarzen Brett,
- Mitteilungen in Besprechungen,
- Berichte bei Mitarbeiterversammlungen,
- Beiträge in Hauszeitschriften und sonstigen internen Mitteilungsblättern,

- Verteilung von Informationsmaterial sowie die Nutzung des behörden- oder unternehmenseigenen Intranets in Betracht.

Sinnvoll ist es, einen Fortbildungsplan, abgestimmt auf die jeweiligen Zielgruppen, zu entwickeln. Die Herstellung von Bezügen zum aktuellen Geschehen ist erfahrungsgemäß geeignet, Interesse an datenschutzrechtlichen Fragestellungen zu wecken. Dies können Bezüge zu allgemeinen aktuellen politischen und gesellschaftlichen Entwicklungen, aber auch aktuelle Bezüge zur Tätigkeit der Mitarbeiter sein.

Um eine Optimierung der Schulungsangebote zu erreichen, empfiehlt es sich auch, wie in anderen Fortbildungsbereichen üblich, Feedback-Systeme einzuführen. Die Einbeziehung der Mitarbeiter und die Aufnahme ihrer Verbesserungsvorschläge sollten dann dazu führen, dass ein Fortbildungssystem nicht statisch bleibt, sondern angemessen weiterentwickelt wird.

3.5 Verfahrensverzeichnis

Die Behörden und öffentlichen Stellen des Bundes führen ebenso wie die verantwortlichen Stellen im nicht-öffentlichen Bereich eine Übersicht über ihre Verfahren automatisierter Verarbeitungen, in denen personenbezogene Daten gespeichert werden. Diese kann, soweit die Angaben öffentlich sind (§ 4e Satz 1 Nr. 1 bis 8), von jedermann eingesehen werden.

Ausgenommen sind die Verzeichnisse folgender Behörden

- Verfassungsschutzbehörden,
- Bundesnachrichtendienst,
- Militärischer Abschirmdienst,
- andere Behörden des Bundesministers der Verteidigung, soweit die Sicherheit des Bundes berührt wird,

- Staatsanwaltschaft und Polizei,
- öffentliche Stellen der Finanzverwaltung, sobald sie personenbezogene Daten in Erfüllung ihrer gesetzlichen Aufgaben im Anwendungsbereich der Abgabenordnung zur Überwachung und Prüfung speichern.

Dieses Verzeichnisses erfüllt mehrere Funktionen. Wie sich aus dem genannten Einsichtsrecht für jedermann ergibt, dient es zunächst der Schaffung von Transparenz in der Datenverarbeitung. Die Bürgerinnen und Bürger gewinnen aus dem Verzeichnisses Anhaltspunkte, ob und wo sie ggf. von ihrem Auskunftsrecht Gebrauch machen wollen. Sehr bedeutsam ist auch die Festlegung der Zweckbestimmung der Datenerhebung, Verarbeitung oder Nutzung des Verfahrens. Da die Zweckbestimmung bereits bei der Erhebung der Daten festzulegen und im Verzeichnisses für das gesamte Verfahren erkennbar zu bestimmen ist, kann man die Zweckbindung der jeweiligen Verarbeitung nachvollziehen und so ihre Einhaltung bei der weiteren Verarbeitung prüfen.

Zugleich ist das Verzeichnisses eine wichtige Übersicht für den Datenschutzbeauftragten, wobei dieser natürlich nicht gehindert ist, über das öffentliche Verzeichnisses hinaus, für das nur der gesetzliche Mindestinhalt vorgeschrieben ist, eine eigene weitere Übersicht mit zusätzlichen Angaben zu führen, die er für seine Aufgabenerfüllung benötigt.

Das Muster eines Verzeichnisses für die Bundesbehörden ist im Anhang 3 abgedruckt. Die Bundesbehörden haben hierzu weitere Ausfüllhinweise erhalten. In dieses Muster wurden auch freiwillige Angaben, wie z. B. die Kennzeichnung der Auftragsdatenverarbeitung im nicht-öffentlichen Teil des Verzeichnisses, aufgenommen.

Dies hilft nicht nur dem Datenschutzbeauftragten, sondern auch der Datenschutzaufsicht bei Prüfungen. Die Tätigkeit des Datenschutzbeauftragten kann durch den Einsatz geeigneter automatisierter Verzeichnisse weiter erleichtert werden. Das Bundesministerium der Finanzen hat in fachlicher Zusammenarbeit mit dem Bundesbeauftragten für den Datenschutz und die Informationsfreiheit eine menügesteuerte IT-Anwendung zur Führung eines elektronischen Verzeichnisses für den Bereich der

Bundesverwaltung entwickelt und stellt dieses Produkt „DATSCHA“ (Datenschutzanwendung in der Bundesfinanzverwaltung) auch anderen Behörden des Bundes kostenfrei zur Verfügung. Informationen zum Verfahren finden Sie auf der Website des Bundesministeriums der Finanzen (www.bundesfinanzministerium.de) unter Service/Dienstleistungen. Entsprechende Entwicklungen haben auch private Firmen für den nicht-öffentlichen privatwirtschaftlichen Bereich vorgenommen.

Den Begriff des „Verfahrens“ definiert das Gesetz selbst nicht. Abgeleitet aus Art. 18 Abs. 1 der EU-Richtlinie 95/46 EG des Europäischen Parlaments und des Rates vom 24. Oktober 1995 hat sich die folgende Definition durchgesetzt:

„Unter Verfahren ist die Gesamtheit an Verarbeitungen zu verstehen, mit denen eine oder mehrere miteinander verbundene Zweckbestimmung(en) realisiert werden sollen. Ein Verfahren kann danach eine Vielzahl von Datenverarbeitungsdateien umfassen“.

Als Beispiele für Verfahren können danach Personalverwaltungs-, Betreuungs- und Abrechnungssysteme, Verfahren zur Abwicklung von Kundenaufträgen, Telekommunikationssysteme, Teledienste und sonstige Systeme, die eine geschlossene Struktur von Verarbeitungen umfassen, genannt werden.

Der Inhalt des Verzeichnisses ergibt sich aus § 4e Nr. 1 bis 9. Für den Bereich der Bundesverwaltung ist die Vorschrift des § 18 Abs. 2 zu berücksichtigen. Danach ist auch die Rechtsgrundlage der Verarbeitung schriftlich festzulegen. Auch müssen bestimmte, allgemeinen Verwaltungszwecken dienende automatisierte Verarbeitungen nicht in das Verzeichnisses aufgenommen werden.

Vom Einsichtsrecht nicht umfasst werden die Angaben nach § 4e Nr. 9 zu den technisch-organisatorischen Maßnahmen nach § 9 zur Gewährleistung der Sicherheit der Verarbeitung.

Die Übersicht mit den in § 4e Satz 1 genannten Angaben ist nach dem eindeutigen Wortlaut des Gesetzes dem Datenschutzbeauftragten von der verantwortlichen Stelle zur Verfügung zu stellen. Es ist also nicht seine Aufgabe, sich aus den Fachabteilungen die erforderlichen Informationen zu besorgen. Das Verzeichnisses muss immer

aktuell und vollständig sein. Es ist sicherzustellen, dass neue Verfahren und Verfahrensänderungen unverzüglich zum Verzeichnisse gemeldet werden. Ohnehin muss aber der Datenschutzbeauftragte, wie bereits an anderer Stelle ausgeführt, schon frühzeitig in der Planungsphase neuer Verfahren beteiligt werden, um die Frage einer etwaigen Vorabkontrolle prüfen zu können.

Aufgabe des Datenschutzbeauftragten ist es hingegen, das Verzeichnisse auf Antrag jedermann in geeigneter Weise verfügbar zu machen. In welcher Form dieses „Verfügbarmachen“ zu erfolgen hat, schreibt das Gesetz nicht vor. Es kann dies daher auch durch Gewährung von Einsichtnahme erfolgen. Eine Einstellung des Verzeichnisses in das Internet verlangt das Gesetz nicht. Unter Abwägung der Vor- und Nachteile kann jede Behörde und jedes Unternehmen selbst entscheiden, ob – auch – Transparenz in dieser Weise geschaffen werden soll. Möglich ist ebenso die Übersendung von Kopien. Neben dem Verzeichnisse besteht für die öffentlichen Stellen des Bundes die Verpflichtung fort, nach §18 Abs. 2 Satz 1 ein Verzeichnisse der eingesetzten Datenverarbeitungsanlagen zu führen, da diese Vorschrift nicht geändert worden ist.

3.6 Mitwirkung beim Audit

Schließlich könnte als neue, zukunftsgerichtete Aufgabe die Mitwirkung beim Datenschutzaudit für ihre Organisationen auf die behördlichen und betrieblichen Datenschutzbeauftragten zukommen.

§ 9a sieht vor, dass zur Verbesserung des Datenschutzes und der Datensicherheit Anbieter von Datenverarbeitungssystemen und Programmen und Daten verarbeitende Stellen ihr Datenschutzkonzept sowie ihre technischen Einrichtungen durch unabhängige und zugelassene Gutachter prüfen und bewerten lassen können. Ferner können sie das Ergebnis dieser Prüfung veröffentlichen. Ein Ausführungsgesetz zum Datenschutzaudit, das in § 9a Satz 2 angekündigt ist, liegt bisher noch nicht vor. Auf Bundesebene gibt es daher noch keine gesetzlichen Regeln für die Durchführung eines Audits. Auch ist das Audit freiwillig. Es dient als datenschutzrechtliches Gütesiegel dazu, Datenschutz

zum Wettbewerbsfaktor für miteinander konkurrierende Unternehmen und auch für Behörden werden zu lassen, die miteinander in einem fruchtbaren Wettbewerb um eine „bürgerfreundliche, moderne und dementsprechend auch datenschutzgerechte“ Verwaltung stehen. § 9a sieht eine Prüfung durch externe – unabhängige und zugelassene – Gutachter vor. Dessen ungeachtet hat sich für die künftige Regelung eines Audits die Vorstellung durchgesetzt, dass dieses in engem Zusammenwirken von externen Gutachtern und internen behördlichen oder betrieblichen Datenschutzbeauftragten entwickelt werden sollte. Dies ist nachdrücklich als zutreffender Ansatz zu unterstützen. Ein kompetenter Datenschutzbeauftragter kennt seine Organisation und kann und muss bei einem Audit mitwirken. Seine Stellung als Ansprechpartner für Fragen des Datenschutzes soll hierdurch eine zusätzliche Stärkung erfahren. Auch wenn das Ausführungsgesetz zum Audit auf Bundesebene noch aussteht, können Datenschutzbeauftragte durchaus bereits jetzt ein Datenschutzkonzept und Datenschutzmanagementsystem anstreben und einrichten, das für ein künftiges Datenschutzaudit tauglich ist.

3.7 Verbündete

Um den Datenschutz in ihren Beschäftigungsstellen erfolgreich und effizient voranzubringen, benötigen die Datenschutzbeauftragten Verbündete. Eine enge Zusammenarbeit mit dem IT-Sicherheitsbeauftragten, der die Aufgabe hat, für die Datensicherheit zu sorgen, ist tunlich. Zusammenarbeit mit dem Organisationsreferat in der Behörde oder der Revision im Unternehmen ist zu empfehlen. Z.B. können auch Datenschutzkontrollen – nach Vorgabe des Datenschutzbeauftragten – in Prüfungen der Revisionsabteilungen einbezogen werden. Vorausgesetzt ist, dass der Datenschutzbeauftragte sich seiner Aufgabe nicht im wesentlichen durch Delegation entledigen darf und auch der erforderliche Abstand (Unabhängigkeit) gegenüber den zu Kontrollierenden bei den Prüfungen gewahrt bleibt. Eine gute Zusammenarbeit sollte der Datenschutzbeauftragte mit dem Personal- oder Betriebsrat suchen, der ebenso wie der Datenschutzbeauftragte der Wahrung der Datenschutzrechte der Beschäftigten gesetzlich verpflichtet ist.

3.8 Erfahrungsaustausch

Unbedingt zu empfehlen ist die Teilnahme des Datenschutzbeauftragten an einem Erfahrungsaustausch mit Kolleginnen und Kollegen. Hierfür bieten sich vielfältige Möglichkeiten. Im Bereich der Bundesbehörden findet ein Erfahrungsaustausch zwischen den Datenschutzbeauftragten der Obersten Bundesbehörden mit dem Bundesbeauftragten für den Datenschutz und die Informationsfreiheit statt. Gleiches ist auch für die nachgeordneten Behörden auf ihrer Ebene sinnvoll. In der Privatwirtschaft gibt es ebenfalls verschiedene Erfahrungsaustauschkreise über die Gesellschaft für Datenschutz und Datensicherung e.V., z. T. auch über Industrie- und Handelskammern und andere Stellen.

3.9 „Fahrplan“

Anliegender Fahrplan geht auf den vielfach geäußerten Wunsch von Teilnehmerinnen und Teilnehmern in Datenschutzseminaren zurück und soll – „nicht ganz ernst und wörtlich zu nehmen“ – eine kleine Anregung geben:

1. Station: Ein schöner Frühlingstag in der Fa. Müller

Frau Schmitz trifft auf dem Flur ihre Chefin, Frau Müller. Frau Müller bittet zum Gespräch in ihr Büro. „Nach dem neuen Bundesdatenschutzgesetz brauchen wir eine Datenschutzbeauftragte. Frau Schmitz, Sie haben doch schon in der IT-Abteilung gearbeitet und gute Kenntnisse in der Informationstechnik. Sie sollen unsere neue Datenschutzbeauftragte werden. Überlegen Sie sich bitte, ob Sie bereit sind, die Aufgabe zu übernehmen.“

Frau Schmitz geht in sich und erkundigt sich zunächst bei der Aufsichtsbehörde, was die Aufgaben einer Datenschutzbeauftragten sind. Schließlich sagt sie zu.

2. Station: Frau Schmitz bildet sich

Nachdem Frau Schmitz sich kündigt gemacht hat, welche Anforderungen an eine Datenschutzbeauftragte zu stellen sind, weiß sie, dass sie die notwendigen Informationstechnikenkenntnisse durch ihre frühere Tätigkeit in der Firma bereits mitbringt. Auch die Struktur der Organisation ist ihr als langjährigem Firmenmitglied vertraut. Was ihr nach ihrer Feststellung noch fehlt, sind die datenschutzrechtlichen Kenntnisse. Sie erkundigt sich nach fundierten Fortbildungsangeboten und findet eine geeignete Schulung, die sie wahrnimmt.

3. Station: Eine Datenschutzbeauftragte wird geboren

Frau Schmitz fühlt sich jetzt gerüstet und nimmt von ihrer Chefin das schriftliche Bestellungsschreiben entgegen. Bekannt für ihre Ordnungsliebe hat Frau Schmitz sich für ihre Fortbildungsaktivitäten bereits einen entsprechenden Ordner angelegt und nimmt jetzt zunächst die organisatorischen Fragen ihrer künftigen Tätigkeit in Angriff. Sie sorgt dafür, dass ihr für ihre vertraulichen Besprechungen als Datenschutzbeauftragte ein Einzelzimmer zur Verfügung steht. Ein eigenes Postfach wird für sie eingerichtet, damit ihre Post als Datenschutzbeauftragte nicht mit der übrigen Firmenpost geöffnet wird. In der Fortbildung hat sie auch einige Anstöße für die Beschaffung von Fachliteratur erhalten. Mit dem Budgetverantwortlichen klärt sie die Anschaffung von Literatur und Fachzeitschriften ab, auf die sie künftig in ihrer Arbeit zurückgreifen möchte.

4. Station: Jetzt sollen es alle wissen

Als Ansprechpartnerin für die Kolleginnen und Kollegen, aber auch für die Kunden und Geschäftspartner der Firma in Datenschutzfragen soll Frau Schmitz jetzt bekannt gemacht werden. Zunächst gibt die Chefin eine Hausmitteilung heraus, mit der jetzt offiziell bekannt gemacht wird, dass Frau Schmitz zur neuen Datenschutzbeauftragten der Firma bestellt wurde. Die Hausmitteilung wird auch in das firmeninterne Netz eingestellt. Frau Schmitz lässt es sich nicht nehmen, sich in der Firmenzeitung als neue Datenschutzbeauftragte den Kollegen und Kolleginnen persönlich vorzustellen. Ein Aushang am „Schwarzen Brett“ soll noch die letzten Kollegen informieren.

Sobald Frau Schmitz sich eingearbeitet hat, soll eine Information für die Kunden erstellt werden, natürlich auch auf der firmeneigenen Internetseite.

5. Station: Verbündete gesucht

Frau Schmitz will keine reine Einzelkämpferin sein und sucht sich Verbündete. Auch der Betriebsrat hat die Aufgabe, über den Datenschutz für die Arbeitnehmer zu wachen. Frau Schmitz geht zum Betriebsrat und bekundet ihre Bereitschaft und ihren Wunsch nach einer guten Zusammenarbeit. Auch in der IT-Abteilung, beim IT-Sicherheitsbeauftragten der Firma, in der Revisionsabteilung und den Fachabteilungen stellt sie sich vor.

6. Station: An ihr geht kein Weg vorbei

Frau Schmitz, die nach ihrem jüngsten Antrittsbesuch in ihrer früheren IT-Abteilung konkretere Vorstellungen darüber hat, welche personenbezogenen Datenverarbeitungen aktuell in der Firma vorhanden sind, geht jetzt daran, einen Beteiligungskatalog aufzustellen. Bei der Vorabkontrolle besonders risikoreicher Datenverarbeitungen muss sie bereits in der Planungsphase beteiligt werden, ebenso bei der Anschaffung neuer DV-Technik und Software, aber auch sonst möchte sie bei allen wesentlichen Verfahren frühzeitig eingeschaltet werden. Nachdem die Geschäftsleitung ihrem Vorschlag für einen Beteiligungskatalog zugestimmt hat, wird dieser der IT-Abteilung und den anderen Fachabteilungen als verbindlich bekannt gegeben. Im Organigramm der Firma ist dargestellt, dass Frau Schmitz der Chefin unmittelbar unterstellt ist. An Frau Schmitz geht so leicht kein Weg mehr vorbei.

7. Station: Das Verfahrensverzeichnis

Frau Schmitz hat von der IT-Abteilung eine Übersicht über die personenbezogenen Verfahren der automatisierten Datenverarbeitung, die Hard- und Software sowie die vorhandenen Zugriffsberechtigungen erhalten. Manchen Informationen muss sie doch noch hinterher gehen. Für die Zukunft beschließt sie, entsprechende Vordrucke für die Meldung der Verfahren einzusetzen. Da es in der Firma doch eine Vielzahl automatisierter personenbezogener Verfahren gibt, will Frau Schmitz sich über die im Handel erhältlichen automatisierten Programme zur Führung von Verfahrensverzeichnissen informieren. Sie überlegt auch, Muster zu übernehmen und gegebenenfalls anzupassen, die mit Vordrucken für die Wahrnehmung des Einsichtsrechtes in das öffentliche Verfahrensverzeichnis, zu Auskunftersuchen u.a. eine organisatorische Arbeitserleichterung bewirken.

8. Station: Das Rad ist schon erfunden

Frau Schmitz sucht den Erfahrungsaustausch mit den Datenschutzbeauftragtenkolleginnen und -kollegen. Sie vermittelt der Chefin, wie wichtig die Teilnahme an einem solchen Austausch für ihre Arbeit ist und dass es letztlich auch Zeit spart, von den Erfahrungen anderer profitieren zu können.

9. Station: Jetzt sind andere an der Reihe zu lernen

Frau Schmitz hat sich inzwischen einen guten Überblick sowohl über die datenschutzrechtlichen Bestimmungen als auch über die konkret anstehenden Datenschutzfragen in ihrer Firma verschafft. Sie fühlt sich jetzt stark, ihre Aufgabe zur Schulung der Mitarbeiter anzugehen. Sie beginnt mit der Erstellung eines Schulungskonzeptes. Hier bindet sie die Chefin mit ein, denn Schulung muss auch die Leitungsebene und die Abteilungsleiterinnen und Abteilungsleiter umfassen. Auch der Betriebsrat wird beteiligt. Ideen aus dem Betriebsrat, welche Datenschutzthemen für die Kolleginnen und Kollegen besonders wichtig sind und wie man deren Interesse am besten wecken kann, fließen in das Konzept ein.

10. Station: Jetzt wird geplant, geschult und geprüft

Frau Schmitz ist jetzt in der Situation, ihre künftige Arbeit über einen längeren Zeitraum planen zu können. Sie überlegt: Wann sollen Schulungen stattfinden? Wann und wo sehe ich stichprobenweise Prüfungen der Datenverarbeitung vor? In der Revisionsabteilung hat Frau Schmitz Unterstützung gefunden. Neben von ihr selbst durchgeführten Prüfungen sollen datenschutzrechtliche Fragestellungen mit ihrer Unterstützung auch von der Revisionsabteilung mit aufgegriffen werden.

11. Station: Wo der Datenschutz in der Firma steht, was erreicht wurde

Ein erstes Jahr als Datenschutzbeauftragte geht dem Ende zu. Frau Schmitz zieht Bilanz, was sich im Datenschutz getan hat. Sie schreibt einen Tätigkeitsbericht für die Firmenleitung. Darin gibt sie einen Überblick, was sich verbessert hat, aber auch, wo es mit dem Datenschutz noch hapert. Den Beschäftigten stellt Frau Schmitz den Tätigkeitsbericht auf der Betriebsversammlung ebenfalls vor.

12. Station: Ausblick auf ein Datenschutzkonzept

Die Bestandsaufnahme im Tätigkeitsbericht hat gezeigt, dass sich in der Firma im Datenschutz einiges positiv entwickelt hat, was sowohl das Wissen und Umsetzen bei Vorgesetzten und Mitarbeitern betrifft, als auch die technische Seite angeht. Manches läuft noch unkoordiniert nebeneinander. Für die zukünftige Arbeit denkt Frau Schmitz daran, mit der entsprechenden Unterstützung ihrer Chefin, aber auch mit den Kolleginnen und Kollegen aus dem Betriebsrat und der IT-Abteilung ein Gesamtkonzept für den Datenschutz in Angriff zu nehmen. Vielleicht wird das Unternehmen auch ein „Gütesiegel“ im Datenschutz anstreben?

Ihr Fahrplan sieht ganz anders aus?

Vielmehr Verspätungen, Umleitungen, Umwege, Sie mussten sogar einmal zurückfahren?

Auch Rom wurde nicht an einem Tag erbaut, so hört man jedenfalls...



Anhang 1

Bestellung zur/zum behördlichen Datenschutzbeauftragten

Sehr geehrte(r) Frau/Herr,

mit Wirkung vombestelle ich Sie zur/zum behördlichen Datenschutzbeauftragten. In dieser Funktion sind Sie der Behördenleitung unmittelbar unterstellt.

Ihre Aufgabe ist es, unbeschadet der eigenen Datenschutzverantwortung der jeweiligen Organisationseinheiten, durch Beratung und jederzeitige auch unangemeldete Kontrolle auf die Einhaltung des Bundesdatenschutzgesetzes sowie anderer Rechtsvorschriften über den Datenschutz hinzuwirken.

Im Einzelnen ergibt sich die Aufgabe aus § 4g BDSG. Sie sind bei der Erfüllung Ihrer Aufgabe von allen Mitarbeiterinnen und Mitarbeitern zu unterstützen.

Alle Mitarbeiterinnen und Mitarbeiter der Behörde können sich in Angelegenheiten des Datenschutzes ohne Einhaltung des Dienstweges an Sie wenden.

Mit freundlichen Grüßen.

.....
(Unterschrift)



Anhang 2

Bekanntmachung/Hausverfügung Datenschutz

Bestellung einer/s behördlichen Datenschutzbeauftragten sowie einer/s Vertreterin/Vertreters

Mit Wirkung vomwurde

Frau/Herr

zur/zum behördlichen Datenschutzbeauftragten sowie

Frau/Herr

zur/zum Vertreterin/Vertreter der/des behördlichen Datenschutzbeauftragten bestellt. Die/der behördliche Datenschutzbeauftragte sowie ihre/ sein/e Vertreter/in sind in dieser Eigenschaft der Leitung der Behörde unmittelbar unterstellt. Ihre/seine Aufgabe ist es, unbeschadet der eigenen Datenschutzverantwortung der jeweiligen Organisationseinheiten, durch Beratung und jederzeitige auch unangemeldete Kontrolle auf die Einhaltung des Bundesdatenschutzgesetzes sowie anderer Rechtsvorschriften über den Datenschutz hinzuwirken. Im Einzelnen ergibt sich die Aufgabe aus § 4g BDSG.

Sie sind bei der Erfüllung ihrer Aufgabe von allen Mitarbeiterinnen und Mitarbeitern zu unterstützen. Soweit sie personenbezogene Daten verarbeiten, sind die Mitarbeiterinnen und Mitarbeiter der Behörde verpflichtet, bei der Einführung neuer Verfahren sowie bei der Erarbeitung behördeninterner Regelungen und Maßnahmen zur Verarbeitung personenbezogener Daten die/den Datenschutzbeauftragte/n frühzeitig zu beteiligen. Alle Mitarbeiterinnen und Mitarbeiter der Behörde können sich in Angelegenheiten des Datenschutzes ohne Einhaltung des Dienstweges an die/den behördliche/n Datenschutzbeauftragte/n sowie im Vertretungsfall an die/den Vertreter/in wenden.

Mit freundlichen Grüßen

.....

(Unterschrift)



Anhang 3

Verfahrenverzeichnis nach § 4g i.V.m. § 18 und § 4e BDSG Hauptblatt

- Das Verzeichnis ist nur teilweise zur Einsichtnahme bestimmt (§ 4g Abs. 2 BDSG)
- Das Verzeichnis ist nicht zur Einsichtnahme bestimmt (§4g Abs.3 Satz 1 BDSG); [z.B. Verfassungsschutzbehörden, Bundesnachrichtendienst, Militärischer Abschirmdienst, Behörden aus dem Bereich des Bundesministeriums der Verteidigung, Polizeibehörden, Staatsanwaltschaften etc.]

1. Verantwortliche Stelle

1.1 Name / Bezeichnung der verantwortlichen Stelle	
1.2 Organisationskennziffer, Ministerium / Amt, Abteilung, ggf. Sachgebiet	
Straße	
PLZ / Ort	
Telefon / Telefax*	
E-Mail-Adresse*	
Internet-Adresse / URL*	

2. Vertretung

2.1 Leitung der verantwortlichen Stelle (einschl. Vertreter)	
2.2 mit der Leitung der Datenverarbeitung beauftragte Person (en):	

3. Angaben zur Person des Datenschutzbeauftragten*

Name (n)	
Straße	
PLZ / Ort	
Telefon / Telefax	
E-Mail-Adresse	
Internet-Adresse / URL	

* = freiwillige Angaben

© 2002, BfD, Bonn

Anlage Nr.:

(für jedes Verfahren automatisierter Verarbeitung ist eine separate Anlage zum Hauptblatt auszufüllen!)

Name/Bezeichnung der verantwortl. Stelle (Übernahme der Nr. 1.1 aus Hauptblatt)

Das Verfahren ist Teil eines gemeinsamen oder verbundenen Verfahrens nach § 10 BDSG	<input type="checkbox"/> ja <input type="checkbox"/> nein – Zutreffendes ankreuzen –
wenn ja, Bezeichnung der verantwortl. Stelle	

4. Zweckbestimmung, Verfahrensbezeichnung, Rechtsgrundlage

4.1 Zweckbestimmung der Datenerhebung, -verarbeitung oder -nutzung
4.2 ggf. Bezeichnung des Verfahrens
4.3 Rechtsgrundlage (ggf. nach Art der Datenverarbeitung unterschieden)

5. Betroffene Personengruppen und Daten oder Datenkategorien

5.1 Beschreibung der betroffenen Personengruppen
5.2 Beschreibung der diesbezüglichen Daten oder Datenkategorien

6. Empfänger oder Kategorien von Empfängern, denen die Daten mitgeteilt werden können; bei Datentransfers in Drittstaaten siehe Nr. 8

--

7. Regelfristen für die Löschung der Daten, Zeitraum

--

8. Geplante Übermittlung in Drittstaaten

8.1 Name des Drittstaates
8.2 Empfänger oder Kategorien von Empfängern
8.3 Art der Daten oder Datenkategorien

Behördeninterner Teil

– nicht zu veröffentlichen (nach § 4g Abs. 2 S. 2 BDSG) –

9. Angaben zur Beurteilung der Angemessenheit getroffener Sicherheitsmaßnahmen

9.1 Art der eingesetzten DVAnlagen und Software
9.2 Maßnahmen nach § 9 BDSG i.V.m. der Anlage dazu

Erläuterungen zu 9.2:

Zutrittskontrolle
Zugangskontrolle
Zugriffskontrolle
Weitergabekontrolle
Eingabekontrolle
Auftragskontrolle
Verfügbarkeitskontrolle
Trennungsgebot

(Sind zu einem der vorstehenden Punkte keine Maßnahmen zu treffen, brauchen keine Angaben gemacht zu werden)

10. Begründetes Ergebnis der Vorabkontrolle gem. § 4d Abs. 5 BDSG

--

11. Auftragsdatenverarbeitung * (Angabe freiwillig)

Handelt es sich um eine Auftragsdatenverarbeitung im Sinne von § 11 BDSG?	<input type="checkbox"/> ja <input type="checkbox"/> nein – Zutreffendes ankreuzen –
---	---

Hauptblatt und Anlage (n) sind mit der Unterschrift des/der Verantwortlichen (Datenschutzbeauftragter/EDV-Leiter) zu versehen.



Anhang 4

Muster

Checkliste für die Vorabkontrolle

Folgender Ablauf ist zu durchlaufen:

(Die als Klammerzusatz angegebenen Nummern beziehen sich jeweils auf die Nummerierung im Formular „Verfahrensverzeichnis“-Muster).

1. Grundangaben

- zur datenverarbeitenden Stelle (Nr. 1)
- zur Zweckbestimmung (Nr. 4.1)
- zur Rechtsgrundlage (Nr. 4.3)
- zur Art der gespeicherten Daten (Nr. 5.2)
- zur Schutzbedürftigkeit der Daten, insbesondere bei sensiblen Daten im Sinne von § 3 Abs. 9 BDSG oder sonst besonders schutzbedürftigen Daten
- zum Kreis der Betroffenen (Nr. 5.1)
- zur Übermittlung (Nr. 6 und 8)
- zu den zugriffsberechtigten Personengruppen (Nr. 9.2)
- zu den für die Löschung maßgeblichen Fristen (Nr. 7).

2. Prüfung, ob

- die Art der gespeicherten Daten (Nr. 5.2)
- die Übermittlungen (Nr. 6 und 8)
- die Eingrenzung der Zugriffsberechtigten (Nr. 9.2)
- die Löschrufen (Nr. 7)

von der angegebenen Zweckbestimmung und Rechtsgrundlage (Nr. 4.1 und Nr. 4.3) gedeckt sind, insbesondere auch unter Berücksichtigung des Grundsatzes der Datenvermeidung und Datensparsamkeit nach § 3a BDSG. Ist dies nicht der Fall, muss geprüft werden, ob Änderungen im Verfahren möglich sind, die zu einem positiven Fortgang der Prüfung führen. Falls dies nicht möglich ist, ist die Datenverarbeitung nicht zulässig.

3. Prüfung, ob die Rechte der Betroffenen nach §§ 19, 19a, 20 BDSG gewahrt sind.

- Können die erforderlichen Auskünfte, Berichtigungen, Sperrungen und Löschungen durchgeführt werden?

- Ist sichergestellt, dass der Betroffene in den Fällen des § 4g Abs. 2 Satz 2 BDSG seine Rechte ohne unverhältnismäßigen Aufwand geltend machen kann?

Auch hier ist im Negativfall die Nachbesserungsmöglichkeit zu prüfen.

4. Risikofaktoren für einen Missbrauch der Daten sind zu ermitteln. Dies sind Gefahren für

- die Vertraulichkeit
- die Integrität
- die Verfügbarkeit

der Daten. Dazu gehören z.B. die Gefahr, dass Datenträger oder „Computerlisten“ während des Transports gestohlen werden, Virenbefall, Gefahr von unbefugten Zugriffen.

5. Beurteilung der möglichen Folgen bei missbräuchlicher Verwendung der Daten, z.B.

- Gefahren oder Nachteile für die Betroffenen
- Schadensersatzansprüche
- finanzielle Schäden
- „Vertrauensschaden“

6. Angaben zur Technik des Verfahrens

- Einzelplatzrechner
- bei vernetzten Rechnern auch Angaben zur Netzstruktur und Datenhaltung (Nr. 9.1)
- eingesetzte Software (Nr. 9.1)
- sowie zu den technischen und organisatorischen Maßnahmen nach § 9 BDSG und seiner zugehörigen Anlage (Nr. 9.2)

7. Abgleich der Risikofaktoren unter besonderer Berücksichtigung der Schutzbedürftigkeit der personenbezogenen Daten mit den getroffenen Sicherheitsmaßnahmen und Entscheidung, ob das Restrisiko unter Anwendung des Verhältnismäßigkeitsgrundsatzes tragbar ist. Ist das Restrisiko zu hoch, ist zu prüfen, ob eine Nachbesserung der Technik des Verfahrens oder der technischen und organisatorischen Maßnahmen eine positive Bewertung ergibt. Ist dies nicht der Fall, ist die Datenverarbeitung nicht zulässig. Bei vertretbarem Restrisiko endet die Vorabkontrolle des geprüften Verfahrens mit positivem Ergebnis.

Das Ergebnis der Vorabkontrolle ist aufzuzeichnen.¹

¹Das Muster der Vorabkontrolle wurde mit freundlicher Unterstützung des Hessischen Datenschutzbeauftragten, der ein erstes Modell einer Vorabkontrolle entwickelt hatte, den Vorschriften des Bundesdatenschutzgesetzes angepasst.

Hinweise zu automatisierten Abrufverfahren i.S.v. § 10 BDSG

1. Ein automatisiertes Abrufverfahren (§ 10 BDSG) ist ein Datenverarbeitungsverfahren, in dem Einzeldaten oder ganze Datenbestände durch Abruf an einen Dritten (§ 3 Abs. 8) übermittelt (§ 3 Abs. 4 Nr. 3) werden. Die Verantwortung für die Zulässigkeit des einzelnen Abrufs trägt die abrufende Stelle (§ 10 Abs. 4). Von mehreren Stellen gemeinsam betriebene Dateien mit wechselseitiger Schreibbefugnis fallen nicht unter § 10.
2. Wesentlich für den Abruf ist das Moment der „Selbstbedienung“. Werden Art und Umfang der zu übermittelnden Daten allein von der übermittelnden Stelle bestimmt und kann der Empfänger nur den Zeitpunkt festlegen, liegt daher kein Abruf im Sinne des § 10 vor, so etwa bei der regelmäßigen Übermittlung der Kfz-Zulassungsdaten von den Gemeinden an das Kraftfahrtbundesamt im automatisierten Verfahren. Ein Abruf kann der Abruf eines Datensatzes, des Teils eines Datensatzes oder mehrerer Datensätze (eines Datenbestandes) sein. Gegenstand eines Abrufs kann auch das Ergebnis einer Datenverarbeitung sein, z.B. des Vergleichs oder Abgleichs zweier Datenbestände.
3. Die beteiligten Stellen legen die Einzelheiten des vereinbarten Verfahrens gemäß § 10 Abs. 2 S. 2 schriftlich fest:
 - Anlass und Zweck des Verfahrens,
 - Dritte, an die übermittelt wird,
 - Art der zu übermittelnden Daten,
 - nach § 9 erforderliche technische und organisatorische Maßnahmen.
4. Das Abrufverfahren ist schriftlich zu dokumentieren. Die in § 10 Abs. 2 genannten Informationen sind in geeigneter Weise übersichtlich in einer eigenen Dokumentation zusammenzustellen. Dazu reicht die technische Entwicklungsdokumentation (Programmdokumentation) allein in der Regel nicht aus.
5. Ist an dem Verfahren eine öffentliche Stelle i.S.v. § 12 Abs. 1 beteiligt, ist der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit über das Abrufverfahren zu unterrichten. Dabei sind ihm die gem. § 10 Abs. 2 S. 2 festgelegten Einzelheiten des Verfahrens (s.o. Nr. 3) mitzuteilen.
6. Die speichernde Stelle hat zu gewährleisten, dass die Übermittlung personenbezogener Daten zumindest durch geeignete Stichprobenverfahren festgestellt und überprüft werden kann (§ 10 Abs. 4). Dazu ist eine Protokollierung der Abrufe erforder-

lich, deren Umfang für das einzelne Abrufverfahren festzulegen ist. Zumindest für einen Teil der Abrufe werden Zeitpunkt und Inhalt (Anfragetext und Antworttext) sowie abrufende Stelle und abrufender Benutzer dokumentiert. Eine Vollprotokollierung, d.h. eine lückenlose Protokollierung aller Abrufe mit allen genannten Details, ist vom Gesetz nicht gefordert. Gleichwohl kann sie unter Umständen geboten sein. Solche Umstände können sich aus der Sensibilität der gespeicherten Daten (§ 3 Abs. 9), der Art des Übertragungsweges, aus dem Benutzerkreis oder aus allen drei Kriterien ergeben. Selbst wenn alle Anforderungen des § 9 nebst Anlage erfüllt sind, ist ein Eindringen über die online-Verbindung in den Datenbestand durch Hacker nicht auszuschließen. Zwar dient die Einrichtung geeigneter Stichprobenverfahren der Gewährleistung der Kontrolle (durch den Bundesbeauftragten oder die Aufsichtsbehörden), es ist aber vor allem Sache der speichernden Stelle zu überprüfen, ob unbefugt auf ihre gespeicherten Daten zugegriffen wird.

Neben der Vollprotokollierung kann, wenn keine besonderen Umstände vorliegen, auch eine Blockprotokollierung vorgenommen werden. Hierbei werden für beliebige Zeiträume alle Abrufe protokolliert, wobei die Festlegung der Zeiträume den Benutzern nicht bekanntgegeben wird. Die Auswahl, welche Protokollierung vorgenommen wird, sollte flexibel und situationsangemessen sein. Eine statistisch gleichmäßige (repräsentative) Berücksichtigung des Gesamtaufkommens der Abrufe ist nicht geboten. Eine gezielte Auswahl nach bestimmten Kriterien, zu denen auch Zufallskriterien gehören können, wird meist wirkungsvoller sein. Von entscheidender Bedeutung für die Missbrauchsprävention ist, dass die Art und Weise der Protokollierung für die Benutzer nicht vorhersehbar ist; für sie muss immer das Risiko einer Protokollierung und Nachprüfung bestehen. Die Protokolldaten müssen nicht in Papierform vorliegen; es reicht aus, wenn sie maschinenlesbar und durch Softwareunterstützung auswertbar sind. Eine allgemeine Aussage, wie lange die Protokolle aufzubewahren sind, ist nicht möglich. Im allgemeinen wird eine Aufbewahrungsdauer von einem Jahr angemessen sein. Für alle Protokolldateien gilt die besondere Zweckbindung des § 14 Abs. 4 BDSG.

7. Bei der Auswertung der Protokolldaten steht das Ziel im Vordergrund, unzulässige und „problematische“ Abrufe zu erkennen, um geeignete Korrekturmaßnahmen einleiten zu können. Ebenso ist es Ziel der Auswertung, eine möglichst hohe Gewissheit zu erreichen, dass unzulässige Abrufe nicht stattfinden. Hierzu ist es notwendig, einzelne protokollierte Abrufe auf ihre Rechtmäßigkeit zu überprüfen, insbesondere

an Hand der Unterlagen der abrufenden Stelle. Welche Fälle in die konkrete Überprüfung einbezogen werden, richtet sich nach dem Kontrollzweck. Eine für den gesamten protokollierten Bestand repräsentative Auswahl ist nicht geboten und für sich allein nicht der optimale Ansatz. Vielmehr ist es zweckmäßig, durch Auswertung des Protokollbestandes diejenigen Teilmengen ein zukreisen, bei denen eine erhöhte Wahrscheinlichkeit kritischer Abrufsfälle besteht. Hierzu können Auswertungen nach Tageszeiten, nach abrufberechtigten Personen oder Stellen, nach regionalen Gesichtspunkten, nach Nutzungsfrequenz, nach verwendeten Abrufarten oder nach abgerufener Datenart in Betracht kommen. Erweisen sich bestimmte Teilmengen von Abrufen als besonders fehlerträchtig, ist es angezeigt, für diese eine intensivere Protokollierung und Auswertung vorzunehmen. Umgekehrt kann die Kontrolldichte für Bereiche zurückgenommen werden, für die sich erwiesen hat, dass keine Fehler (mehr) auftreten. Die Zwischen- und Endergebnisse der Auswertung unterliegen ebenso wie der Inhalt der Protokolldateien der besonderen Zweckbestimmung des § 14 Abs. 4. Es ist Aufgabe der verantwortlichen Stelle, den einzelnen Benutzer (jede einzelne Person) der abrufenden Stelle zu identifizieren und zu authentisieren (Anl. zu § 9). Einzelheiten dieser und aller weiteren Maßnahmen zur Sicherheit des Verfahrens sind bei der Vereinbarung des Abrufverfahrens von den beteiligten Stellen festzulegen. Erforderlich sind solche Maßnahmen, die in angemessenem Verhältnis zu dem angestrebten Schutzzweck stehen (§ 9 Satz 2). Passwörter sind in Abrufsystemen durch kryptographische Verfahren zu schützen. Die Identifikation und Authentisierung vom Benutzer sollte über geeignete Verfahren sichergestellt werden; bei besonders sensiblen Daten ist der Einsatz von Digitalen Signaturen zu prüfen. Die Gestaltung von Passwörtern muss nach den allgemein anerkannten Regeln erfolgen (14. Tätigkeitsbericht (Anl. 13)). Gruppenidentifikationen sind bei Abrufen nach § 10 nicht zulässig.

8. Wegen der prinzipiellen Angreifbarkeit des öffentlichen Wählnetzes, insbesondere Internetübergänge über das Telefonnetz, sind bei besonders sensiblen Daten (§ 3 Abs. 9) kryptographische Verfahren zur Sicherung der Vertraulichkeit und Integrität erforderlich.
9. Die Anforderungen des § 9 BDSG mit Anlage werden durch § 10 nicht eingeschränkt.



Anhang 6

Anschriften der Datenschutzbeauftragten des Bundes und der Länder

Bund	Der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit Husarenstraße 30 53117 Bonn Verbindungsbüro Berlin: Friedrichstr. 50 10117 Berlin	Tel.: 0228/997799-0 Fax: 0228/997799-550 E-Mail: poststelle@bfdi.bund.de Internet: www.datenschutz.bund.de
Baden-Württemberg	Der Landesbeauftragte für den Datenschutz Baden-Württemberg Postfach 10 29 32 70025 Stuttgart Urbanstraße 32 70182 Stuttgart	Tel.: 0711/615541-0 Fax: 0711/615541-15 E-Mail: poststelle@lfd.bwl.de Internet: www.baden-wuerttemberg.datenschutz.de
Bayern	Der Bayerische Landesbeauftragte für den Datenschutz Postfach 22 12 19 80502 München Wagmüllerstr. 18 80538 München	Tel.: 089/212672-0 Fax: 089/212672-50 E-Mail: poststelle@datenschutz-bayern.de Internet: www.datenschutz-bayern.de
Berlin	Berliner Beauftragter für Datenschutz und Informationsfreiheit An der Urania 4-10 10787 Berlin	Tel.: 030/13889-0 Fax: 030/2155050 E-Mail: mailbox@datenschutz-berlin.de Internet: www.datenschutz-berlin.de
Brandenburg	Die Landesbeauftragte für den Datenschutz und für das Recht auf Akteneinsicht Stahnsdorfer Damm 77 14532 Kleinmachnow	Tel.: 033203/356-0 Fax: 033203/356-49 E-Mail: poststelle@lda.brandenburg.de Internet: www.lda.brandenburg.de
Bremen	Die Landesbeauftragte für Datenschutz und Informationsfreiheit der Freien Hansestadt Bremen Postfach 10 03 80 27503 Bremerhaven Arndtstr. 1 27570 Bremerhaven	Tel.: 0471/596-2010 oder 0421/361-2010 Fax: 0421/469-18495 E-Mail: office@datenschutz.bremen.de Internet: www.datenschutz-bremen.de
Hamburg	Der Hamburgische Beauftragte für Datenschutz und Informationsfreiheit Klosterwall 6 (Block C) 20095 Hamburg	Tel.: 040/42854-4040 Fax: 040/42854-4000 E-Mail: mailbox@datenschutz.hamburg.de Internet: www.hamburg-datenschutz.de

Hessen	Der Hessische Datenschutz-beauftragte Postfach 31 63 65021 Wiesbaden Gustav-Stresemann-Ring 1 65189 Wiesbaden	Tel.: 0611/1408-0 Fax: 0611/1408-900 oder -901 E-Mail: poststelle@datenschutz.hessen.de Internet: www.datenschutz.hessen.de
Mecklenburg-Vorpommern	Der Landesbeauftragte für Daten-schutz und Informationsfreiheit Mecklenburg-Vorpommern Schloss Schwerin 19053 Schwerin	Tel.: 0385/59494-0 Fax: 0385/59494-58 E-Mail: datenschutz@mvnet.de Internet: www.lfd.m-v.de
Niedersachsen	Der Landesbeauftragte für den Datenschutz Niedersachsen Postfach 2 21 30002 Hannover Brühlstraße 9 30169 Hannover	Tel.: 0511/120-4500 Fax: 0511/120-4599 E-Mail: poststelle@lfd.niedersachsen.de Internet: www.lfd.niedersachsen.de
Nordrhein-Westfalen	Landesbeauftragter für Daten-schutz und Informationsfreiheit Nordrhein-Westfalen Postfach 20 04 44 40102 Düsseldorf Kavalleriestr. 2-4 40213 Düsseldorf	Tel.: 0211/38424-0 Fax: 0211/38424-10 E-Mail: poststelle@ldi.nrw.de Internet: www.ldi.nrw.de
Rheinland-Pfalz	Der Landesbeauftragte für den Datenschutz Rheinland-Pfalz Postfach 3040 55020 Mainz Hintere Bleiche 34 55116 Mainz	Tel.: 06131/208-2449 Fax: 06131/208-2497 E-Mail: poststelle@datenschutz.rlp.de Internet: www.datenschutz.rlp.de
Saarland	Landesbeauftragte für Datenschutz und Informationsfreiheit Postfach 102631 66026 Saarbrücken Fritz-Dobisch-Str. 12 66111 Saarbrücken	Tel.: 0681/94781-0 Fax: 0681/94781-29 E-Mail: poststelle@datenschutz.saarland.de Internet: www.datenschutz.saarland.de
Sachsen	Der Sächsische Datenschutz-beauftragte Postfach 12 09 05 01008 Dresden Bernhard-von-Lindenau-Platz 1 01067 Dresden	Tel.: 0351/493-5401 Fax: 0351/493-5490 E-Mail: saechsdsb@slt.sachsen.de Internet: www.saechsdsb.de/
Sachsen-Anhalt	Landesbeauftragter für den Datenschutz Sachsen-Anhalt Postfach 19 47 39009 Magdeburg Leiterstraße 9 39104 Magdeburg	Tel.: 0391/81803-0 Fax: 0391/81803-33 E-Mail: poststelle@lfd.sachsen-anhalt.de Internet: www.datenschutz.sachsen-anhalt.de

Schleswig-Holstein	Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein Postfach 71 16 24171 Kiel Holstenstraße 98 24103 Kiel	Tel.: 0431/988-1200 Fax: 0431/988-1223 E-Mail: mail@datenschutzzentrum.de Internet: www.datenschutzzentrum.de
Thüringen	Thüringer Landesbeauftragter für den Datenschutz Postfach 90 04 55 99107 Erfurt Jürgen-Fuchs-Straße 1 99096 Erfurt	Tel.: 0361/377-1900 Fax: 0361/377-1904 E-Mail: poststelle@datenschutz.thueringen.de Internet: www.thueringen.de/datenschutz

Anhang 7

Anschriften der Aufsichtsbehörden für den nicht-öffentlichen Bereich

Baden-Württemberg	Der Landesbeauftragte für den Datenschutz Baden-Württemberg Postfach 10 29 32 70025 Stuttgart Urbanstraße 32 70182 Stuttgart	Tel.: 0711/615541-0 Fax: 0711/615541-15 E-Mail: poststelle@lfd.bwl.de Internet: www.baden-wuerttemberg.datenschutz.de
Bayern	Landesamt für Datenschutzaufsicht Promenade 27 (Schloss) 91522 Ansbach	Tel.: 0981/53-1300 Fax: 0981/53-5300 E-Mail: poststelle@lda.bayern.de Internet: www.lda.bayern.de
Berlin	Berliner Beauftragter für Datenschutz und Informationsfreiheit An der Urania 4 - 10 10787 Berlin	Tel.: 030/13889-0 Fax: 030/2155050 E-Mail: mailbox@datenschutz-berlin.de Internet: www.datenschutz-berlin.de
Brandenburg	Die Landesbeauftragte für den Datenschutz und für das Recht auf Akteneinsicht Stahnsdorfer Damm 77 14532 Kleinmachnow	Tel.: 033203/356-0 Fax: 033203/356-49 E-Mail: poststelle@lda.brandenburg.de Internet: www.lda.brandenburg.de
Bremen	Die Landesbeauftragte für Datenschutz und Informationsfreiheit der Freien Hansestadt Bremen Postfach 10 03 80 27503 Bremerhaven Arndtstr. 1 27570 Bremerhaven	Tel.: 0471/596-2010 oder 0421/361-2010 Fax: 0421/496-18495 E-Mail: office@datenschutz.bremen.de Internet: www.datenschutz-bremen.de
Hamburg	Der Hamburgische Beauftragte für Datenschutz und Informationsfreiheit Klosterwall 6 (Block C) 20095 Hamburg	Tel.: 040/42854-4040 Fax: 040/42854-4000 E-Mail: mailbox@datenschutz.hamburg.de Internet: www.hamburg-datenschutz.de
Hessen	Der Hessische Datenschutzbeauftragte Postfach 31 63 65021 Wiesbaden Gustav-Stresemann-Ring 1 65189 Wiesbaden	Tel.: 0611/1408-0 Fax: 0611/1408-900 oder -901 E-Mail: poststelle@datenschutz.hessen.de Internet: www.datenschutz.hessen.de
Mecklenburg-Vorpommern	Der Landesbeauftragte für Datenschutz und Informationsfreiheit Mecklenburg-Vorpommern Schloss Schwerin 19053 Schwerin	Tel.: 0385/59494-0 Fax: 0385/59494-58 E-Mail: datenschutz@mvnet.de Internet: www.lfd.m-v.de

Niedersachsen	Der Landesbeauftragte für den Datenschutz Niedersachsen Postfach 221 30002 Hannover Brühlstraße 9 30169 Hannover	Tel.: 0511/120-4500 Fax: 0511/120-4599 E-Mail: poststelle@lfd.niedersachsen.de Internet: www.lfd.niedersachsen.de
Nordrhein-Westfalen	Landesbeauftragter für Datenschutz und Informationsfreiheit Nordrhein-Westfalen Postfach 200444 40102 Düsseldorf Kavalleriestr. 2-4 40213 Düsseldorf	Tel.: 0211/38424-0 Fax: 0211/38424-10 E-Mail: poststelle@ldi.nrw.de Internet: www.ldi.nrw.de
Rheinland-Pfalz	Der Landesbeauftragte für den Datenschutz Rheinland-Pfalz Postfach 3040 55020 Mainz Hintere Bleiche 34 55116 Mainz	Tel.: 06131/208-2449 Fax: 06131/208-2497 E-Mail: poststelle@datenschutz.rlp.de Internet: www.datenschutz.rlp.de
Saarland	Unabhängiges Datenschutzzentrum Saarland Postfach 102631 66026 Saarbrücken Fritz-Dobisch-Str. 12 66111 Saarbrücken	Tel.: 0681/94781-0 Fax: 0681/94781-29 E-Mail: poststelle@datenschutz.saarland.de Internet: www.datenschutz.saarland.de
Sachsen	Der Sächsische Datenschutzbeauftragte Postfach 12 09 05 01008 Dresden Bernhard-von-Lindenau-Platz 1 01067 Dresden	Tel.: 0351/493-5401 Fax: 0351/493-5490 E-Mail: saechsdsb@slt.sachsen.de Internet: www.saechsdsb.de
Sachsen-Anhalt	Landesverwaltungsamt Sachsen-Anhalt Referat 106 (Justizariat) Ernst-Karmith-Straße 2 06114 Halle (Saale) Postanschrift Postfach 20 02 56 06003 Halle (Saale)	Tel.: 0345/514-0 Fax: 0345/514-3799 E-Mail: poststelle@lvwa.sachsen-anhalt.de Internet: www.sachsen-anhalt.de
Schleswig-Holstein	Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein Postfach 71 16 24171 Kiel Holstenstraße 98 24103 Kiel	Tel.: 0431/9881200 Fax: 0431/9881223 E-Mail: mail@datenschutzzentrum.de Internet: www.datenschutzzentrum.de
Thüringen	Thüringer Landesverwaltungsamt - Referat 200 - Weimarplatz 4 99423 Weimar	Tel.: 0361/3770-0 Fax: 0361/3773-7190 E-Mail: poststelle@tlvwa.thueringen.de Internet: www.thueringen.de/de/tlvwa/

Anhang 8

Internetadressen zum Datenschutz

	WWW.
Der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit	datenschutz.bund.de
Datenschutzaufsichtsbehörden der Länder	siehe Anschriften in Anhang 6 und Anhang 7
Virtuelles Datenschutzbüro	datenschutz.de
Gesetzessammlung von BMJ und juris GmbH	gesetze-im-internet.de
Elektronischer Bundesanzeiger	ebundesanzeiger.de
Deutscher Bundestag	bundestag.de
Das Informationssystem für parlamentarische Vorgänge	dipbt.bundestag.de
Parlamentsspiegel (Landesparlamente)	parlamentsspiegel.de
Bundesamt für Sicherheit in der Informationstechnik	bsi.bund.de
EPIC Electronic Privacy Information Center	epic.org
Verbraucherzentrale Bundesverband e.V.	vzbv.de/go/
Verbraucherzentralen	verbraucherzentrale.de/
Europäische und Internationale Datenschutzbehörden	datenschutz.bund.de/DE/AnschriftenUndLinks/AuslaendischeDatenschutzbeauftragte/AuslaendischeDS_node.html
Europäische und Internationale Datenschutzinstitutionen	datenschutz.de/institutionen
Europarat	coe.int/t/dghl/standardsetting/DataProtection/default_en.asp
Europäische Kommission	ec.europa.eu/justice/policies/privacy/index_en.htm
Artikel 29 Gruppe	ec.europa.eu/justice_home/fsj/privacy/index_de.htm
Europäisches Verbraucherzentrum Deutschland	euroinfo-kehl.eu/

Anhang 9

Elektronische Informationen zum Datenschutz

Vor dem Hintergrund der steigenden Bedeutung des Internets als Kommunikationsmedium ist der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit auch dort mit einem Angebot vertreten. Die Homepage ist unter der Adresse <http://www.datenschutz.bund.de> oder <http://www.bfdi.bund.de> erreichbar.

Der Internetauftritt wurde Anfang 2006 grundlegend umgestaltet und entspricht nun dem aktuellen Aufgabenkreis. Der Besucher kann zwischen den Beiträgen zum Datenschutz oder zur Informationsfreiheit wählen. Die Datenschutz-Seite bietet eine Auswahl an Schwerpunktthemen von besonderer Aktualität oder Bedeutung an. Eng verknüpft mit den Schwerpunktthemen dokumentieren umfangreiche Themenbeiträge die Inhalte der datenschutzrechtlichen Tätigkeit. Die Internetseite hält zudem eine Sammlung bedeutsamer Rechtsprechung zum Datenschutz und zur Informationsfreiheit vor. Es lassen sich auch Informationen wie Pressemitteilungen, Reden, Arbeitshilfen oder die Tätigkeitsberichte nachlesen. Ebenso können die herausgegebenen Informationsbroschüren und Faltblätter online abgerufen werden. Ferner werden Entschließungen der internationalen, europäischen und nationalen Datenschutzkonferenzen, Informationen zum europäischen Datenschutz und zur internationalen Zusammenarbeit der Datenschutzbeauftragten sowie Anschriften und weitere interessante Links bereitgehalten.

Seit dem 1. Juli 2009 ist auf der Internetseite auch ein interaktives Diskussionsforum freigeschaltet (http://www.bfdi.bund.de/bfdi_forum/index.php). Das Datenschutzforum, in dem der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit, Peter Schaar, auch mit einem eigenen Blog vertreten ist, soll als Plattform für alle am Thema Datenschutz Interessierten dienen. Das Forum ist nicht nur für Fachleute gedacht, sondern soll bei allen Bürgerinnen und Bürgern Interesse daran wecken, Meinungen, Erfahrungen und Erwartungen zu Themen und Problemen des Datenschutzes einzubringen und hierüber miteinander zu diskutieren. Im Forum sind auch Themen eröffnet worden, die für Datenschutzbeauftragte besonders interessant sind.

Informationen zum Datenschutz können auch beim Virtuellen Datenschutzbüro unter der Adresse <http://www.datenschutz.de> abgerufen werden. Das Virtuelle Datenschutzbüro ist eine im Internet betriebene zentrale Informations- und Anlaufstelle für

Datenschutzfragen, die von zahlreichen offiziellen Datenschutzinstitutionen (Projektpartnern) mitgetragen wird. Das Projekt wurde vom Unabhängigen Landeszentrum für Datenschutz Schleswig-Holstein initiiert und aufgebaut. Es ist Portal und Ansprechstelle im Internet für alle Bürgerinnen und Bürger, Experten und Datenschutzinstitutionen. Projektpartner sind neben dem Bundesbeauftragten für den Datenschutz und die Informationsfreiheit auch die Datenschutzbeauftragten der meisten Bundesländer, die Datenschutzbeauftragten der Evangelischen Kirche sowie der Norddeutschen Bistümer der Katholischen Kirche, Rundfunkdatenschutzbeauftragte sowie Datenschutzbeauftragte aus Kanada, der Schweiz, Liechtenstein und Polen.

Das Virtuelle Datenschutzbüro bietet u.a.:

- Informationen zu allen Fragen rund um den Datenschutz,
- Diskussionsforen zu aktuellen Datenschutzthemen,
- Antworten zu den häufigsten Fragen von Anwendern,
- Eine Plattform für die Zusammenarbeit der Datenschützer weltweit.



Anhang 10

Beschluss der obersten Aufsichtsbehörden für den Datenschutz im nicht-öffentlichen Bereich (Düsseldorfer Kreis) vom 24./25. November 2010

Mindestanforderungen an Fachkunde und Unabhängigkeit des Beauftragten für den Datenschutz nach § 4f Abs. 2 und 3 Bundesdatenschutzgesetz (BDSG)

Die obersten Aufsichtsbehörden für den Datenschutz im nicht-öffentlichen Bereich haben bei der Kontrolle verantwortlicher Stellen festgestellt, dass Fachkunde und Rahmenbedingungen für die Arbeit der Beauftragten für den Datenschutz (DSB) in den verantwortlichen Stellen angesichts zunehmender Komplexität automatisierter Verfahren zum Umgang mit personenbezogenen Daten nicht durchgängig den Anforderungen des BDSG genügen. Die obersten Aufsichtsbehörden für den Datenschutz im nicht-öffentlichen Bereich weisen darauf hin, dass die Aus- und Belastung der DSB maßgeblich beeinflusst wird durch die Größe der verantwortlichen Stelle, die Anzahl der zu betreuenden verantwortlichen Stellen, Besonderheiten branchenspezifischer Datenverarbeitung und den Grad der Schutzbedürftigkeit der zu verarbeitenden personenbezogenen Daten. Veränderungen bei den vorgenannten Faktoren führen regelmäßig zu einer proportionalen Mehrbelastung der DSB. Nachfolgende Mindestanforderungen sind zu gewährleisten:

I. Erforderliche Fachkunde gemäß § 4f Abs. 2 Satz 1 BDSG

§ 4 f Abs. 2 Satz 1 BDSG legt fest, dass zum Beauftragten für den Datenschutz (DSB) nur bestellt werden darf, wer die erforderliche Fachkunde und Zuverlässigkeit besitzt. Weitere Ausführungen dazu enthält das Gesetz nicht. Vor dem Hintergrund der gestiegenen Anforderungen an die Funktion des DSB müssen diese mindestens über folgende datenschutzrechtliche und technisch-organisatorische Kenntnisse verfügen:

1. Datenschutzrecht allgemein – unabhängig von der Branche und der Größe der verantwortlichen Stelle
 - Grundkenntnisse zu verfassungsrechtlich garantierten Persönlichkeitsrechten der Betroffenen und Mitarbeiter der verantwortlichen Stelle und

- umfassende Kenntnisse zum Inhalt und zur rechtlichen Anwendung der für die verantwortlichen Stellen einschlägigen Regelungen des BDSG, auch technischer und organisatorischer Art,
 - Kenntnisse des Anwendungsbereiches datenschutzrechtlicher und einschlägiger technischer Vorschriften, der Datenschutzprinzipien und der Datensicherheitsanforderungen insbesondere nach § 9 BDSG.
2. Branchenspezifisch – abhängig von der Branche, Größe oder IT-Infrastruktur der verantwortlichen Stelle und der Sensibilität der zu verarbeitenden Daten
- Umfassende Kenntnisse der spezialgesetzlichen datenschutzrelevanten Vorschriften, die für das eigene Unternehmen relevant sind,
 - Kenntnisse der Informations- und Telekommunikationstechnologie und der Datensicherheit (physische Sicherheit, Kryptographie, Netzwerksicherheit, Schadsoftware und Schutzmaßnahmen, etc.),
 - betriebswirtschaftliche Grundkompetenz (Personalwirtschaft, Controlling, Finanzwesen, Vertrieb, Management, Marketing etc.),
 - Kenntnisse der technischen und organisatorischen Struktur sowie deren Wechselwirkung in der zu betreuenden verantwortlichen Stelle (Aufbau- und Ablaufstruktur bzw. Organisation der verantwortlichen Stelle) und
 - Kenntnisse im praktischen Datenschutzmanagement einer verantwortlichen Stelle (z. B. Durchführung von Kontrollen, Beratung, Strategieentwicklung, Dokumentation, Verzeichnisse, Logfile-Auswertung, Risikomanagement, Analyse von Sicherheitskonzepten, Betriebsvereinbarungen, Videoüberwachungen, Zusammenarbeit mit dem Betriebsrat etc.).

Grundsätzlich müssen die erforderlichen rechtlichen, technischen sowie organisatorischen Mindestkenntnisse **bereits zum Zeitpunkt der Bestellung** zum DSB im ausreichenden Maße vorliegen. Sie können insbesondere auch durch den Besuch geeigneter Aus- und Fortbildungsveranstaltungen und das Ablegen einer Prüfung erlangt sein. Um eventuell zu Beginn der Bestellung noch bestehende Informationsdefizite auszugleichen, empfiehlt sich der Besuch von geeigneten Fortbildungsveranstaltungen. Der Besuch solcher Veranstaltungen ist auch nach der Bestellung angezeigt, um auf dem aktuellen, erforderlichen Informationsstand zu bleiben, und um sich Kenntnisse über die sich ändernden rechtlichen und technischen Entwicklungen anzueignen.

II. Anforderungen an die Unabhängigkeit der/des Beauftragten gem. § 4f Abs. 3 BDSG

Gemäß § 4f Abs. 3 Satz 2 BDSG sind DSB in Ausübung ihrer Fachkunde auf dem Gebiet des Datenschutzes weisungsfrei. Um die Unabhängigkeit der DSB zu gewährleisten, sind eine Reihe betriebsinterner organisatorischer Maßnahmen erforderlich:

1. DSB sind dem Leiter/der Leiterin der verantwortlichen Stelle organisatorisch unmittelbar zu unterstellen (§ 4f Abs. 3 Satz 1 BDSG). Sie müssen in der Lage sein, ihre Verpflichtungen ohne Interessenkonflikte erfüllen zu können. Dieses ist durch entsprechende Regelungen innerhalb der verantwortlichen Stelle bzw. vertragliche Regelungen sicher zu stellen und sowohl innerhalb der verantwortlichen Stelle als auch nach außen hin publik zu machen. Den DSB ist ein unmittelbares Vortragsrecht beim Leiter der Stelle einzuräumen.
2. DSB dürfen wegen der Erfüllung ihrer Aufgaben in Hinblick auf ihr sonstiges Beschäftigungsverhältnis, auch für den Fall, dass die Bestellung zum DSB widerrufen wird, nicht benachteiligt werden (vgl. § 4f Abs. 3 Satz 3 ff BDSG). Analog muss bei der Bestellung von externen DSB der Dienstvertrag so ausgestaltet sein, dass eine unabhängige Erfüllung der gesetzlichen Aufgaben durch entsprechende Kündigungsfristen, Zahlungsmodalitäten, Haftungsfreistellungen und Dokumentationspflichten gewährleistet wird. § 4f Abs. 3 BDSG schränkt insoweit die grundsätzliche Vertragsfreiheit ein. Empfohlen wird grundsätzlich eine Mindestvertragslaufzeit von 4 Jahren, bei Erstverträgen wird wegen der Notwendigkeit der Überprüfung der Eignung grundsätzlich eine Vertragslaufzeit von 1 – 2 Jahren empfohlen.
3. Datenschutzbeauftragte sind zur Verschwiegenheit über die Identität des Betroffenen sowie über Umstände, die Rückschlüsse auf den Betroffenen zulassen, verpflichtet, soweit sie nicht davon durch die Betroffenen befreit wurden. Dies gilt auch gegenüber der verantwortlichen Stelle und deren Leiter (§ 4f Abs. 4 BDSG).

III. Erforderliche Rahmenbedingungen innerhalb der verantwortlichen Stelle zur Fachkunde und Unabhängigkeit des DSB

1. Die Prüfpflichten der DSB (vgl. § 4g BDSG) setzen voraus, dass ihnen die zur Aufgabenerfüllung erforderlichen Zutritts- und Einsichtsrechte in alle betrieblichen Bereiche eingeräumt werden.

2. DSB müssen in alle relevanten betrieblichen Planungs- und Entscheidungsabläufe eingebunden werden. Sie führen das Verzeichnis (§ 4g Abs. 2 BDSG) und haben hierfür die erforderlichen Unterlagen zu erhalten.
3. Zur Erhaltung der zur Erfüllung seiner Aufgaben erforderlichen Fachkunde haben die verantwortlichen Stellen den DSB die Teilnahme an Fort- und Weiterbildungsveranstaltungen zu ermöglichen und deren Kosten zu übernehmen. Bei der Bestellung von externen DSB kann die Fortbildung Bestandteil der vereinbarten Vergütung sein und muss nicht zusätzlich erbracht werden.
4. Internen DSB muss die erforderliche Arbeitszeit zur Erfüllung ihrer Aufgaben und zur Erhaltung ihrer Fachkunde zur Verfügung stehen. Bei Bestellung eines externen DSB muss eine bedarfsgerechte Leistungserbringung gewährleistet sein. Sie muss in angemessenem Umfang auch in der beauftragenden verantwortlichen Stelle selbst erbracht werden. Ein angemessenes Zeitbudget sollte konkret vereinbart und vertraglich festgelegt sein.
5. Die verantwortlichen Stellen haben DSB bei der Erfüllung ihrer Aufgaben insbesondere durch die zur Verfügung Stellung von Personal, Räumen, Einrichtung, Geräten und Mitteln zu unterstützen (§ 4f Abs. 5 BDSG).

