Der Bundesbeauftragte
für den Datenschutz

BfD-Info 4

Die Datenschutzbeauftragten in Behörde und Betrieb

Impressum

Herausgeber:
Der Bundesbeauftragte für den Datenschutz
Postfach 20 01 12, 53131 Bonn
Hausanschrift: Husarenstraße 30, 53117 Bonn
Tel: (01888) 7799-0, Telefax: (01888) 7799-5 50
E-Mail: poststelle@bfd.bund.de
Internet: http://www.datenschutz.bund.de

Auflage: 4. Auflage, Stand Januar 2004

Inhaltsverzeichnis

Vorwort.....

1 Bestellung.....
1.1 Rechtsgrundlage und Anwendungsbereich.....
1.2 Wann muss ein Datenschutzbeauftragter bestellt werden?.....
1.3 Wer kann Datenschutzbeauftragter werden?.....
1.3.1 Was bedeutet die Anforderung der Fachkunde?.....
1.3.2 Was bedeutet die Anforderung der Zuverlässigkeit?.....
1.4 Wo bestehen Unvereinbarkeiten?.....
1.5 Wie ist der Datenschutzbeauftragte zu bestellen?.....

2 Stellung und Befugnisse.....
2.1 Stellung in der Hierarchie.....
2.2 Rechte und Grenzen in der Tätigkeit als Datenschutzbeauftragter.....
2.3 Benachteiligungsverbot.....
2.4 Unterstützungspflicht der verantwortlichen Stellen.....
2.5 Direktes Vorspracherecht beim Beauftragten für den Datenschutz.....
2.6 Eigeninitiative des Beauftragten für den Datenschutz.....

3 Aufgaben.....
3.1 Beratung und Mitwirkung.....
3.2 Vorabkontrolle.....
3.3 Kontrolle.....
3.4 Schulung.....
3.5 Verfahrensverzeichnis.....
3.6 Mitwirkung beim Audit.....
3.7 Verbündete.....
3.8 Erfahrungsaustausch.....
3.9 „Fahrplan“.....

Anhang 1: *Bestellung zur/zum behördlichen Datenschutzbeauftragten.....*
Anhang 2: *Bekanntmachung/Hausverfügung Datenschutz.....*
Anhang 3: *Verfahrensverzeichnis nach § 4g i.V.m. § 18 und § 4e BDSG.....*
Anhang 4: *Muster für die Vorabkontrolle.....*
Anhang 5: *Hinweise zu automatisierten Abrufverfahren i.S.v. § 10 BDSG.....*
Anhang 6: *Organigramm des Bundesbeauftragten für den Datenschutz.....*

Anhang 7: *Anschriften der Datenschutzbeauftragten des Bundes und der Länder.....*
Anhang 8: *Anschriften der Aufsichtsbehörden für den nicht öffentlichen Bereich.....*
Anhang 9: *Internetadressen zum Datenschutz.....*
Anhang 10: *Weitere Informationsschriften.....*
Anhang 11: *Elektronische Informationen zum Datenschutz.....*

Vorwort

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. Durch die Änderung des Bundesdatenschutzgesetzes im Mai 2001 ist deren Position 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.

Bonn, im Januar 2004

Peter Schaar
Der Bundesbeauftragte für den Datenschutz

Die Datenschutzbeauftragten in Behörde und Betrieb

1 Bestellung

1.1 Rechtsgrundlage und Anwendungsbereich

Im Bundesdatenschutzgesetz (BDSG) vom 20. Dezember 1990,[1] wurden durch die Änderung mit Gesetz vom 18. Mai 2001[2], in Kraft getreten am 23. Mai 2001, in den §§ 4f und 4g erstmals einheitliche Bestimmungen für die Institution eines Datenschutzbeauftragten im öffentlichen wie im nicht öffentlichen Bereich geschaffen. 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 ausschließlich im Bereich der Sozialleistungsträger nach dem Sozialgesetzbuch (§§ 35 SGB I, 81 SGB X i.V.m. § 4f 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 oder die Landesbeauftragten für den Datenschutz, die im allgemeinen Sprachgebrauch häufig auch als „Datenschutzbeauftragte“ bezeichnet werden.

---

[1] BGBl. I S. 2954

[2] BGBl. I S. 904; §§ ohne weitere Bezeichnung sind stets solche des BDSG.

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.) oder zum Zweck der anonymisierten Übermittlung (Markt- und 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 Arbeitnehmer ab, die mit der Datenverarbeitung beschäftigt sind. Ein Datenschutzbeauftragter muss bestellt werden, wenn

- mindestens fünf Arbeitnehmer 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 ein Arbeitnehmer 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 vereinzelte 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 25.000 € 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.
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.

1.3.1 Was bedeutet die Anforderung der Fachkunde?

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

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.

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 sensitiver 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 in den Bereichen Justitiariat/Recht oder Organisation bietet sich für die Aufgabe an.

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 Grundsatzentscheidung 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. Ausfluss der Unabhängigkeit des

Datenschutzbeauftragten ist auch sein 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 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 (§ 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. Unberührt davon bleibt die nach der bisher ergangenen Rechtsprechung ggf. mögliche ordentliche Kündigung eines Datenschutzbeauftragten, der noch mit anderen Aufgaben betraut ist, wenn die Kündigung nicht im Zusammenhang mit der Funktion als Datenschutzbeauftragter steht.

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 besonderen Widerrufsschutz hinsichtlich seiner Bestellung 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 Widerrufsschutzes 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 Mitarbeiter 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.

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 3 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 Verfahrensverzeichnisses.

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. Gleiches gilt auch für den Umgang mit Kundendaten im Unternehmen. Dies betrifft nicht nur die virtuelle Welt des Internets, in der die Ängste vor einem Missbrauch der persönlichen Daten besonders stark sind.

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 dessen 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 bisher weitgehend nur durch Rechtsprechung bestimmt ist. Der Datenschutzbeauftragte muss somit die Einhaltung der Datenschutzvorschriften von der Erhebung der Daten, über die Institutionalisierung von Unterrichtungspflichten gegenüber

Betroffenen (Benachrichtigungsroutinen, Unterrichtung über das Widerspruchsrecht, Schaffung von Transparenz in der Datenverarbeitung) bis hin zur ordnungsgemäßen Beachtung von Löschungsfristen beratend begleiten.

Die Sicherung des Datenschutzrechts durch Technik ist hier von immer größerer Bedeutung. Auch dort setzt die Beratungstätigkeit bereits bei der Planung von Datenverarbeitungsvorhaben an. Mit § 3a des novellierten Bundesdatenschutzgesetzes wurde der Grundsatz der Datenvermeidung und Datensparsamkeit gesetzlich verankert und der Systemdatenschutz gestärkt. 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 das IT-Grundschutzhandbuch eine wertvolle Hilfe (kostenlos erhältlich beim Bundesamt für Sicherheit in der Informationstechnik – BSI –, auch kostenlos herunterzuladen von der Webseite des BSI unter der Adresse www.bsi.de). Den Behörden des Bundes wurde es zuletzt mit der „Empfehlung zur Anwendung des IT-Grundschutzhandbuches“ nahegelegt (Gemeinsames Ministerialblatt 1995, S. 741). 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 auch in der Zukunft weiterhin sich 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.
Gleichermaßen 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. Der Datenschutzbeauftragte ist auch hier bereits bei der Planung der Auftragsdatenverarbeitung und der Vertragsgestaltung 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. 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 zum BDSG und zu anderen Themen oder die Broschüren der Datenschutzaufsichtsbehörden der Länder nehmen und diese mit einem Vorstellungs- 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 Beschäftigungsstelle 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 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 Beispielsfällen 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 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 Verfahrensverzeichnisses, 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, soweit nicht besondere Berufs- oder Amtsgeheimnisse, wie z.B. die ärztliche Schweigepflicht, entgegenstehen.
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 (s. Anhänge) 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 Verfahrensverzeichnis 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 Verfahrensverzeichnis

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 Verfahrensverzeichnis 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 Verfahrensverzeichnis eine wichtige Übersicht für den Datenschutzbeauftragten, wobei dieser natürlich nicht gehindert ist, über das öffentliche Verfahrensverzeichnis 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 Verfahrensverzeichnisses 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 Verfahrensverzeichnisses, aufgenommen.

Dies hilft nicht nur dem Datenschutzbeauftragten, sondern auch der Datenschutzaufsicht bei Prüfungen. Die Tätigkeit des Datenschutzbeauftragten kann durch den Einsatz geeigneter automatisierter Verfahrensverzeichnisse weiter erleichtert werden. Ein solches Programm wird für den Bereich der Bundesbehörden durch das Bundesministerium der Finanzen entwickelt. Auch im Landesbereich hat z.B. der Landesbeauftragte für den Datenschutz Thüringen (s. Anschriftenverzeichnis) eine entsprechende Entwicklung vorgenommen, ebenso wie private Firmen für die Privatwirtschaft.

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 Verfahrensverzeichnisses 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 Verfahrensverzeichnis 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 Verfahrensverzeichnis muss immer aktuell und vollständig sein. Es ist sicherzustellen, dass neue Verfahren und Verfahrensänderungen unverzüglich zum Verfahrensverzeichnis 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 Verfahrensverzeichnis 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 Verfahrensverzeichnis besteht für die öffentlichen Stellen des Bundes die Verpflichtung fort, nach § 18 Abs. 2 Satz 1 ein Verzeichnis 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 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 kundig gemacht hat, welche Anforderungen an eine Datenschutzbeauftragte zu stellen sind, weiß sie, dass sie die notwendigen Informationstechnikkenntnisse 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 hinterhergehen. 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 Auskunftsersuchen 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 Beschäftigen 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 vom ..... bestelle 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 vom ..... wurde

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	

Anhang 3

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	ja ☐ 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 DV-Anlagen 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 ?	ja ☐ nein ☐ - Zutreffendes ankreuzen -

Hauptblatt und Anlage(n) sind mit der Unterschrift des/der Verantwortlichen (Datenschutzbeauftrager/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 sensitiven 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 Fristen für die Löschung (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 Löschfristen (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 unvertretbaren 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]

---

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

Anhang 5

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 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 erforderlich, 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 bekannt gegeben 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.

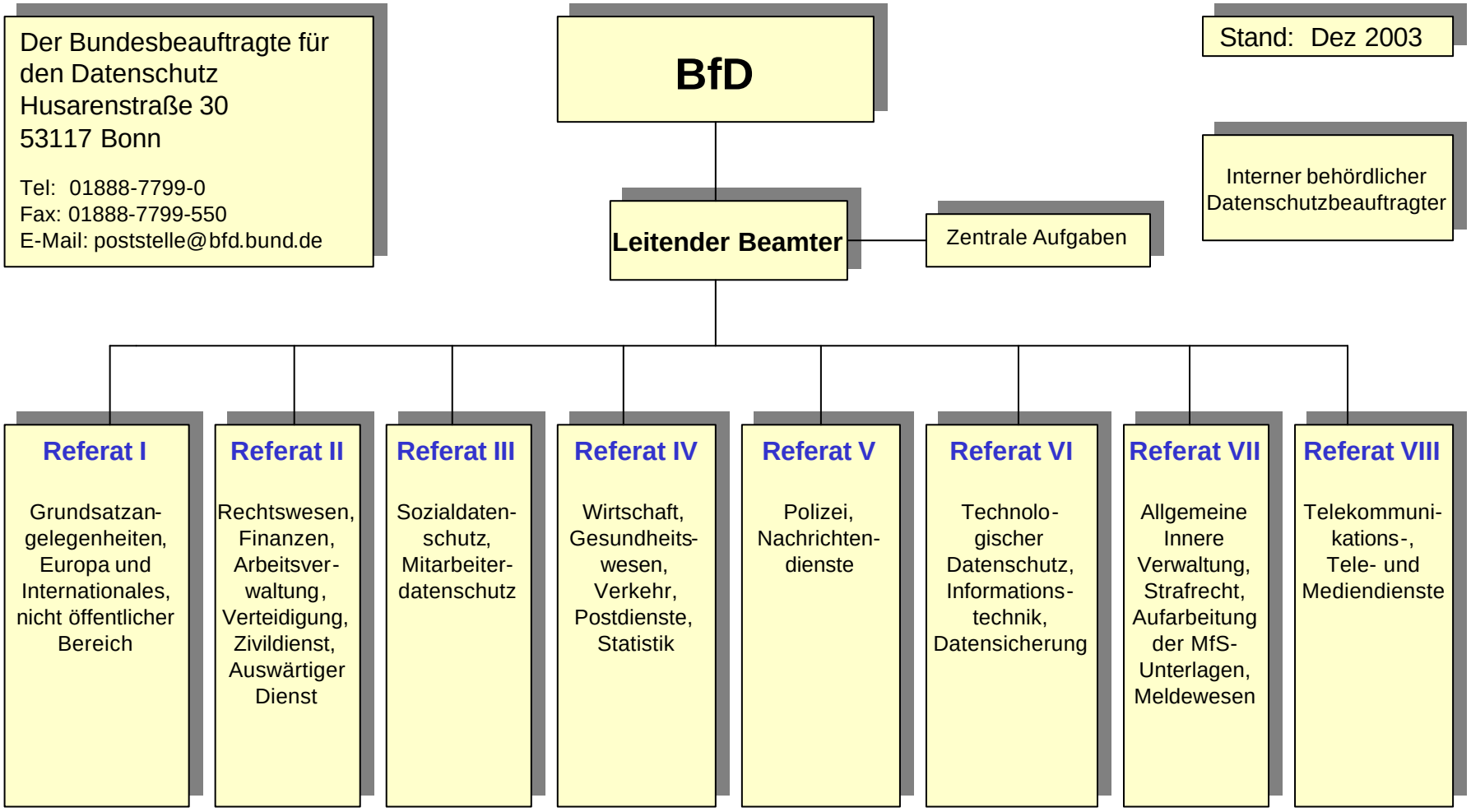
7. Bei der Auswertung der Protokolldaten steht das Ziel im Vordergrund, unzulässige und „problematische“ Abrufe zu erkennen, um geeignete Korrekturmaßnahmen einleiten zu

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 einzukreisen, 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.


Der Bundesbeauftragte für
den Datenschutz
Husarenstraße 30
53117 Bonn
Tel: 01888-7799-0
Fax: 01888-7799-550
E-Mail: poststelle@bfd.bund.de
BfD
Stand: Dez 2003
Interner behördlicher Datenschutzbeauftragter
Leitender Beamter
Zentrale Aufgaben
Referat I
Grundsatzan-gelegenheiten, Europa und Internationales, nicht öffentlicher Bereich
Referat II
Rechtswesen, Finanzen, Arbeitsver-waltung, Verteidigung, Zivildienst, Auswärtiger Dienst
Referat III
Sozialdaten-schutz, Mitarbeiter-datenschutz
Referat IV
Wirtschaft, Gesundheits-wesen, Verkehr, Postdienste, Statistik
Referat V
Polizei, Nachrichten-dienste
Referat VI
Technolo-gischer Datenschutz, Informations-technik, Datensicherung
Referat VII
Allgemeine Innere Verwaltung, Strafrecht, Aufarbeitung der MfS-Unterlagen, Meldewesen
Referat VIII
Telekommuni-kations-, Tele- und Mediendienste

Anhang 7

Anschriften der Datenschutzbeauftragten des Bundes und der Länder

Bund	Der Bundesbeauf-trag für den Datenschutz	Dr. Joachim Jacob Postfach 20 01 12 53131 Bonn Friedrich-Ebert-Str. 1 53173 Bonn	Tel.: 02 28 / 8 19 95-0 Fax: 02 28 / 8 19 95-5 50 E-Mail: poststelle@bfd.bund.de Internet: http://www.bfd.bund.de
Baden-Württemberg	Der Landesbeauf-tragte für den Daten-schutz Baden-Württemberg	Peter Zimmermann Postfach 10 29 32 70025 Stuttgart Marienstr. 12 70178 Stuttgart	Tel.: 07 11 / 61 55 41-0 Fax: 07 11 / 61 55 41-15 E-Mail: poststelle@lfd.bwl.de Internet: http://www.baden-wuerttemberg.datenschutz.de
Bayern	Der Bayerische Landesbeauftragte für den Datenschutz	Reinhard Vetter Postfach 22 12 19 80502 München Wagmüllerstr. 18 80538 München	Tel.: 0 89 / 21 26 72-0 Fax: 0 89 / 21 26 72-50 E-Mail: poststelle@datenschutz-bayern.de Internet: http://www.datenschutz-bayern.de
Berlin	Berliner Beauftragter für Datenschutz und Informationsfreiheit	Prof. Dr. Hansjürgen Garstka Pallasstr. 25/26 10781 Berlin	Tel.: 030 / 75 60 78 09 Fax: 030 / 2 15 50 50 E-Mail: mailbox@datenschutz-berlin.de Internet: http://www.datenschutz-berlin.de
Brandenburg	Der Landesbeauf-tragte für den Daten-schutz und für das Recht auf Akteneinsicht	Dr. Alexander Dix Stahnsdorfer Damm 77 14532 Kleinmachnow	Tel.: 03 32 03 / 3 56-0 Fax: 03 32 03 / 3 56-49 E-Mail: poststelle@lda.brandenburg.de Internet: http://www.lda.brandenburg.de
Bremen	Landesbeauftragter für den Datenschutz	Sven Holst Postfach 10 03 80 27503 Bremerhaven Arndtstr. 1 27570 Bremerhaven	Tel.: 04 71 / 92 46 10 Fax: 04 71 / 9 24 61 31 E-Mail: office@datenschutz.bremen.de Internet: http://www.datenschutz.bremen.de
Hamburg	Der Hamburgische Datenschutz-beauftragte	Dr. Hans-Hermann Schrader Baumwall 7 20459 Hamburg	Tel.: 0 40 / 4 28 41-20 44 Fax: 0 40 / 4 28 41 23 72 E-mail: mailbox@datenschutz.hamburg.de Internet: www.hamburg.datenschutz.de
Hessen	Der Hessische Da-tenschutz-beauftragte	Prof. Dr. Friedrich von Zezschwitz Postfach 31 63 65021 Wiesbaden Uhlandstr. 4 65189 Wiesbaden	Tel.: 06 11 / 14 08-0 Fax: 06 11 / 14 08-9 00 E-Mail: poststelle@datenschutz.hessen.de Internet: http://www.datenschutz.hessen.de
Mecklen-burg-Vorpommern	Landesbeauftragter für den Datenschutz	Dr. Werner Kessel Schloß Schwerin 19053 Schwerin	Tel.: 03 85 / 5 94 94-0 Fax: 03 85 / 5 94 94-58 E-Mail: datenschutz@mvnet.de Internet: http://www.lfd.m-v.de
Niedersach-sen	Der Landesbeauf-tragte für den Daten-schutz Niedersach-sen	Burckhard Nedden Postfach 2 21 30002 Hannover Brühlstr. 9 30169 Hannover	Tel.: 05 11 / 1 20-45 00 Fax: 05 11 / 1 20 45 99 E-Mail: poststelle@lfd.niedersachsen.de Internet: http://www.lfd.niedersachsen.de

Anhang 7

Nordrhein-Westfalen	Die Landesbeauftragte für den Datenschutz Nordrhein-Westfalen	Bettina Sokol Postfach 20 04 44 40102 Düsseldorf Reichsstr. 43 40217 Düsseldorf	Tel.: 02 11 / 38 42 40 Fax: 02 11 / 3 84 24 10 E-Mail: datenschutz@lfd.nrw.de Internet: http://www.lfd.nrw.de
Rheinland-Pfalz	Der Landesbeauftragte für den Datenschutz Rheinland-Pfalz	Prof. Dr. Walter Rudolf Postfach 30 40 55020 Mainz Deutschhausplatz 12 55116 Mainz	Tel.: 0 61 31 / 2 08 24 49 Fax: 0 61 31 / 2 08 24 97 E-Mail: poststelle@datenschutz.rlp.de Internet: http://www.datenschutz.rlp.de
Saarland	Der Landesbeauftragte für Datenschutz	Karl Albert Postfach 10 26 31 66026 Saarbrücken Fritz-Dobisch-Str. 12 66111 Saarbrücken	Tel.: 06 81 / 9 47 81-0 Fax: 06 81 / 9 47 81 29 E-Mail: lfd-saar@t-online.de Internet: http://www.lfd.saarland.de
Sachsen	Der Sächsische Datenschutzbeauftragte	Dr. Thomas Giesen Postfach 12 09 05 01008 Dresden Bernhard-von-Lindenau-Platz 1 01067 Dresden	Tel.: 03 51 / 49 35-4 01 Fax: 03 51 / 49 35-4 90 Internet: www.datenschutz.de
Sachsen-Anhalt	Landesbeauftragter für den Datenschutz Sachsen-Anhalt	Klaus-Rainer Kalk Postfach 19 47 39009 Magdeburg Berliner Chaussee 9 39114 Magdeburg	Tel.: 03 91 / 8 18 03-0 Fax: 03 91 / 8 18 03 33 Internet: http://www.datenschutz.sachsen-anhalt.de
Schleswig-Holstein	Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein	Dr. Helmut Bäumler Postfach 71 16 24171 Kiel Holstenstraße 98 24103 Kiel	Tel.: 04 31 / 9 88 12 00 Fax: 04 31 / 9 88 12 23 E-Mail: mail@datenschutzzentrum.de Internet: http://www.datenschutzzentrum.de
Thüringen	Der Thüringer Landesbeauftragte für den Datenschutz	Silvia Liebaug Postfach 10 19 51 99019 Erfurt Johann-Sebastian-Bach-Straße 1 99096 Erfurt	Tel.: 03 61 / 3 77 19 00 Fax: 03 61 / 3 77 19 04 E-Mail: poststelle@datenschutz.thueringen.de Internet: http://www.datenschutz.thueringen.de

Anhang 8

Anschriften der Aufsichtsbehörden für den nicht öffentlichen Bereich

Land	oberste Aufsichtsbehörde	regional zuständige Aufsichtsbehörden
Baden-Württemberg	Innenministerium Baden-Württemberg Postfach 10 24 43 70020 Stuttgart Dorotheenstr. 6 70173 Stuttgart Tel.: 07 11 / 2 31-4 Fax: 07 11 / 2 31-32 99	Innenministerium Baden-Württemberg Postfach 10 24 43 70020 Stuttgart Dorotheenstr. 6 70173 Stuttgart Tel.: 07 11 / 2 31-4 Fax: 07 11 / 2 31-32 99
Bayern	Bayerisches Staatsministerium des Innern Odeonsplatz 3 80539 München Tel.: 0 89 / 21 92-01 Fax: 0 89 / 2 19 2-122 66	Regierung von Mittelfranken Aufsichtsbehörde für den Datenschutz Promenade 27 (Schloß) 91522 Ansbach Tel.: 09 81 / 53-301 Fax: 09 81 / 53-206
Berlin	Berliner Beauftragter für Datenschutz und Informationsfreiheit Pallasstr. 25/26 10781 Berlin Tel.: 0 30 / 75 60 78 09 Fax: 0 30 / 2 15 50 50 E-Mail: mailbox@datenschutz-berlin.de Internet: http://www.datenschutz-berlin.de	Berliner Beauftragter für Datenschutz und Informationsfreiheit Pallasstr. 25/26 10781 Berlin Tel.: 0 30 / 75 60 78 09 Fax: 0 30 / 2 15 50 50 E-Mail: mailbox@datenschutz-berlin.de Internet: http://www.datenschutz-berlin.de
Brandenburg	Ministerium des Innern Henning-von-Tresckow-Str. 9 - 13 14467 Potsdam Tel.: 03 31 / 8 66 23 60 Fax: 03 31 / 8 66 23 02 E-Mail: Lfd-bbg@t-online.de Internet: http://www.mi.brandenburg.de	Ministerium des Innern Henning-von-Tresckow-Str. 9-13 14467 Potsdam Tel.: 03 31 / 8 66 23 60 Fax: 03 31 / 8 66 23 02 E-Mail: Lfd-bbg@t-online.de Internet: http://www.mi.brandenburg.de
Bremen	Der Landesbeauftragte für den Daten-schutz Postfach 10 03 80 27503 Bremerhaven Arndtstr. 1 27570 Bremerhaven Tel.: 04 71 / 92 46 10 Fax: 04 71 / 9 24 61 31 E-Mail: office@datenschutz.bremen.de Internet: http://www.datenschutz.bremen.de	Der Landesbeauftragte für den Daten-schutz Postfach 10 03 80 27503 Bremerhaven Arndtstr. 1 27570 Bremerhaven Tel.: 04 71 / 92 46 10 Fax: 04 71 / 9 24 61 31 E-Mail: office@datenschutz.bremen.de Internet: http://www.datenschutz.bremen.de

Anhang 8

Land	oberste Aufsichtsbehörde	regional zuständige Aufsichtsbehörden
Hamburg	Der Hamburgische Datenschutzbeauftragte Baumwall 7 20459 Hamburg Tel.: 0 40 / 4 28 41-20 45 Fax: 0 40 / 4 28 41-23 72 E-Mail: mailbox@datenschutz.hamburg.de Internet: http://www.hamburg.datenschutz.de	Der Hamburgische Datenschutzbeauftragte Baumwall 7 20459 Hamburg Tel.: 0 40 / 4 28 41-20 44 Fax: 0 40 / 4 28 41-23 72 E-Mail: mailbox@datenschutz.hamburg.de Internet: http://www.hamburg.datenschutz.de
Hessen	Hessisches Ministerium des Innern und für Sport Friedrich-Ebert-Allee 12 65185 Wiesbaden Tel.: 06 11 / 3 53-0 Fax: 06 11 / 3 53-13 43 Internet: http://www.hmdi.hessen.de	Regierungspräsidium Gießen Landgraf-Philipp-Platz 3-7 35390 Gießen Tel.: 06 41 / 3 03-1 Fax: 06 41 / 3 03-25 09 Internet: http://www.rp-giessen.de Regierungspräsidium Darmstadt Wilhelminenstraße 1-3 64283 Darmstadt Tel.: 0 61 51 / 12-0 Fax: 0 61 51 / 12 68 34 E-Mail: datenschutz@rpda.hessen.de Internet: http://www.rpda.de Regierungspräsidium Kassel Steinweg 6 34117 Kassel Tel.: 05 61 / 1 06-0 Fax: 05 61 / 1 06 10 12 Internet: http://www.rp-kassel.de
Mecklenburg-Vorpommern	Innenministerium des Landes Mecklenburg-Vorpommern Arsenal am Pfaffenteich 19048 Schwerin Tel.: 03 85 / 5 88 22 50 Fax: 03 85 / 5 88 29 78	Innenministerium des Landes Mecklenburg-Vorpommern Arsenal am Pfaffenteich 19048 Schwerin Tel.: 03 85 / 5 88 22 50 Fax: 03 85 / 5 88 29 78

Anhang 8

Land	oberste Aufsichtsbehörde	regional zuständige Aufsichtsbehörden
Niedersachsen	Niedersächsisches Innenministerium Lavesallee 6 30169 Hannover Tel.: 05 11 / 1 20-0 Fax: 05 11 / 1 20-65 50	Der Landesbeauftragte für den Datenschutz Niedersachsen Postfach 2 21 30002 Hannover Brühlstraße 9 30169 Hannover Tel.: 05 11 / 1 20 45 00 Fax: 05 11 / 1 20 45 99 E-Mail: poststelle@lfd.niedersachsen.de Internet: http://www.lfd.niedersachsen.de
Nordrhein-Westfalen	Innenministerium des Landes Nordrhein-Westfalen Haroldstr. 5 40190 Düsseldorf Tel.: 02 11 / 8 71 01 Fax: 02 11 / 8 71 33 55	Die Landesbeauftragte für den Datenschutz Nordrhein-Westfalen Bettina Sokol Postfach 20 04 44 40102 Düsseldorf Reichsstraße 43 40217 Düsseldorf Tel.: 02 11 / 38 42 40 Fax: 02 11 /3 84 24 10 E-Mail: datenschutz@lfd.nrw.de Internet: http://www.lfd.nrw.de
Rheinland-Pfalz	Ministerium des Innern und für Sport Schillerplatz 3-5 55116 Mainz Tel.: 0 61 31 / 16 32 59 Fax: 0 61 31 / 16 33 69	Aufsichts- und Dienstleistungsdirektion (ADD) Trier Willy-Brandt-Platz 3 54290 Trier Tel.: 06 51 / 94 94-0 Fax: 06 51 / 94 94-1 70 E-Mail: poststelle@add.rlp.de Internet: http://www.add.rlp.de
Saarland	Ministerium des Innern und für Sport - Abt. B - Mainzer Str. 136 66121 Saarbrücken Tel.: 06 81 / 9 62-0 Fax: 06 81 / 9 62-16 05	Ministerium des Innern und für Sport - Abt. B - Mainzer Str. 136 66121 Saarbrücken Tel.: 06 81 / 9 62-0 Fax: 06 81 / 9 62-16 05
Sachsen	Sächsisches Staatsministerium	Regierungspräsidium Chemnitz

Anhang 8

Land	oberste Aufsichtsbehörde	regional zuständige Aufsichtsbehörden
	des Innern Referat 26 - Datenschutz Wilhelm-Buck-Straße 2 01097 Dresden Tel.: 03 51 / 5 64-32 60 Fax: 03 51 / 5 64-31 99 E-Mail: datenschutz@smi.sachsen.de	Altchemnitzer Str. 41 09120 Chemnitz Tel.: 03 71 / 5 32-11 49 Fax: 03 71 / 5 32-11 59 E-Mail: post@rpc.sachsen.de Regierungspräsidium Dresden Postfach 10 06 53 01076 Dresden Stauffenbergallee 2 01099 Dresden Tel.: 03 51 / 8 25-14 20 Fax: 03 51 / 8 25-99 99 Regierungspräsidium Leipzig Braustr. 2 04107 Leipzig Tel.: 03 41 / 9 77-14 70 Fax: 03 41 / 9 77-11 99
Sachsen-Anhalt	Ministerium des Innern des Landes Sachsen-Anhalt Halberstädter Str. 2 39112 Magdeburg Tel.: 03 91 / 5 67 54 04 Fax: 03 91 / 5 67 52 90	Regierungspräsidium Halle Willy-Lohmann-Str. 7 06114 Halle Tel.: 03 45 / 51 40 Fax: 03 45 / 5 14 14 44 E-Mail: poststelle@rph.mi.lsa.net.de
Schleswig-Holstein	Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein Postfach 71 16 24171 Kiel Holstenstraße 98 24103 Kiel Tel.: 04 31 / 9 88 12 00 Fax: 04 31 / 9 88 12 23 E-Mail: mail@datenschutzzentrum.de Internet: www.datenschutzzentrum.de	Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein Postfach 71 16 24171 Kiel Holstenstraße 98 24103 Kiel Tel.: 04 31 / 9 88 12 00 Fax: 04 31 / 9 88 12 23 E-Mail: mail@datenschutzzentrum.de Internet: www.datenschutzzentrum.de
Thüringen	Thüringer Innenministerium Steigerstr. 24 99096 Erfurt Tel.: 03 61 / 3 79 00 Fax: 03 61 / 3 79 31 11 E-Mail: poststelle@tim.thueringen.de	Thüringer Landesverwaltungsamt Weimarplatz 4 99423 Weimar Tel.: 03 61 / 37 73 72 58 Fax: 03 61 / 37 73 73 46 E-Mail: poststelle@tlva.thueringen.de

Anhang 9

Internetadressen zum Datenschutz

	www.
Der Bundesbeauftragte für den Datenschutz	bfd.bund.de
Datenschutzaufsichtsbehörden der Länder	siehe Anschriftenliste, S. ...
Virtuelles Datenschutzbüro	datenschutz.de
Gesetzessammlung von IURIS und BMI (ca. 600 Gesetze)	staat-modern.de/gesetze
Deutscher Bundestag	bundestag.de
Das Informationssystem für parlamentarische Vorgänge	http://dip.bundestag.de
Bundesamt für Sicherheit in der Informationstechnik	bsi.de
EPIC Electronic Privacy Information Center	epic.org
Oberste Bundesgerichte:	
Bundesverfassungsgericht	bverfg.de
Bundesverwaltungsgericht	bverwg.de
Bundesarbeitsgericht	bundesarbeitsgericht.de
Bundesgerichtshof	bundesgerichtshof.de
Europäische Datenschutzinstitutionen	bfd.bund.de/anschriften/dsb_euro.html
Internationale Datenschutzinstitutionen	bfd.bund.de/anschriften/dsb_inter.html
Europäische und Internationale Datenschutzinstitutionen s.a.	datenschutz.de/institutionen
Europarat	coe.int/dataprotection
Europäische Kommission	europa.eu.int/comm/internal_market/de/dataprot/index.htm

Anhang 10

Weitere Informationsschriften des BfD zum Datenschutz

Beim Bundesbeauftragten für den Datenschutz können folgende Schriften kostenlos angefordert werden:

- **BfD-Info 1 – Bundesdatenschutzgesetz – Text und Erläuterung –**
  Die Broschüre enthält den Gesetzestext und erläutert die Gesetzesvorschriften. (Stand: Dezember 2002)

- **BfD-Info 2 – Der Bürger und seine Daten –**
  Die Broschüre gibt einen Überblick über die Stellen, die möglicherweise personenbezogene Daten über Bürger erheben, verarbeiten und nutzen und bei denen die Datenschutzrechte geltend gemacht werden können. (Stand: Juli 1999)

- **BfD-Info 3 – Schutz der Sozialdaten –**
  Die Broschüre stellt den besonderen Datenschutz im Bereich der Sozialversicherung – also der Kranken-, Unfall- und Rentenversicherung sowie der Arbeitslosen- und der Pflegeversicherung – und auch anderer Sozialleistungen, wie z.B. Sozialhilfe, nach dem Sozialgesetzbuch dar. (Stand: November 1994)

- **BfD-Info 5 – Datenschutz in der Telekommunikation –**
  Die Broschüre gibt einen Überblick über die Datenschutzrechte der Bürger im Zusammenhang mit der Nutzung von Telekommunikationsdiensten (z.B. Inhalt von Vertragsvordrucken oder Nutzung der Daten für Werbezwecke). Diejenigen, die beruflich im Bereich der Telekommunikation mit personenbezogenen Daten umgehen, erhalten Hinweise zu einzelnen Rechtsvorschriften (Stand: September 2001)

- **Tätigkeitsberichte – soweit vorhanden –**
  Ab dem 16. Tätigkeitsbericht (für die Jahre 1995 bis 1996) sind diese auch auf CD-Rom erhältlich.

- **Bundesdatenschutzgesetz in englischer** Sprache

- **Bundesdatenschutzgesetz in französischer** Sprache

Die Informationsbroschüren des BfD sowie die Tätigkeitsberichte ab dem 16. Tätigkeitsbericht werden auch im Internet angeboten unter der Adresse http://www.datenschutz.bund.de .

Anhang 11

Elektronische Informationen zum Datenschutz

Vor dem Hintergrund der steigenden Bedeutung des Internets als Kommunikationsmedium ist der Bundesbeauftragte für den Datenschutz auch dort mit einem Angebot vertreten. Die Homepage ist unter der Adresse http://www.datenschutz.bund.de erreichbar. Das Angebot umfasst neben den Rubriken „Bürger fragen“ und „Datenschutz von A-Z“ u.a.

- aktuelle Hinweise und Pressemitteilungen zum Datenschutz,
- umfangreiche Materialien wie Tätigkeitsberichte, alle BfD-Informationsbroschüren, Gesetzes- und Verordnungstexte (z.T. auch in englischer Sprache), Entschließungen der Datenschutzkonferenzen,
- Informationen zum europäischen Datenschutz und zur internationalen Zusammenarbeit der Datenschutzbeauftragten,
- Informationen zum Thema „Datenschutz und Technik“, darunter ein Beitrag „Datenschutzfreundliche Technologien in der Telekommunikation“,
- Anschriften und weitere interessante Links.

Daneben können Informationen zum Datenschutz auch beim **Virtuellen Datenschutzbüro** unter der Adresse http://www.datenschutz.de abgerufen werden. Das Projekt „Virtuelles Datenschutzbüro“ 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 auch die Datenschutzbeauftragten der meisten Bundesländer, der Norddeutschen Bistümer der Katholischen Kirche und Datenschutzbeauftragte aus der Schweiz, den Niederlanden und Kanada.
Die seit Ende 2000 bestehende neue Einrichtung 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.