



Die Datenschützer

Publikation des

Berufsverbandes der Datenschutzbeauftragten Deutschlands (BvD) e.V.

Das berufliche Leitbild des Datenschutzbeauftragten

vom 11.09.2009



Vorwort

Das vorliegende berufliche Leitbild ist die kontinuierliche Weiterentwicklung und Konkretisierung von beruflichen Kriterien zum Datenschutzbeauftragten innerhalb des BvD. Die vom Arbeitskreis Berufsbild herausgegebene und vom Vorstand im Februar 2009 angenommenen Berufsgrundsätze sind nun zur beruflichen Leitlinie weiter gestaltet wurden.

Die Herausgabe dieser Leitlinie wiederum markiert aber nur eine weitere Etappe im Entwicklungsprozess dieses Berufes und innerhalb des BvD. Die beruflichen Kriterien unterliegen einem dynamischen Wachstum und insbesondere im BvD einer fortwährenden Diskussion. Es ist Ziel, Aufgabe aber auch Verpflichtung des BvD, diese Leitlinie regelmäßig anzupassen und weiterzuentwickeln.

Für die bisherigen Hinweise, Anregungen und Vorschläge bedanken wir uns bei allen Mitgliedern. Jede weitere Empfehlung, Meinung und Stellungnahme zur Weiterentwicklung ist herzlich willkommen.

Der sprachlichen Vereinfachung wegen wurde im Text die männliche Bezeichnung „Datenschutzbeauftragter“ gewählt – die Regelungen umfassen und betreffen Personen beider Geschlechter.

Dieses Leitbild wurde von der Mitgliederversammlung in Ulm am 11.09.2009 verabschiedet.

Der Vorstand

Einleitung

Datenschutzbeauftragte vereinen in sich verschiedene Rollen. Sie beraten Unternehmen und Behörden und tragen zur Wahrung der Grundrechte bei.

Qualifizierte Datenschutzbeauftragte helfen, Risiken in Unternehmen und Behörden zu minimieren (z.B. Verhinderung Gesetzesverstöße, Bußgelder) sowie Imageverluste und Kosten als Folge von Datenschutzverstößen zu vermeiden. Sie stärken das Vertrauen von Bürgern, Kunden und Beschäftigten in die Datenverarbeitung des jeweiligen Unternehmens bzw. der Behörde.

Dieses Leitbild schafft einen Maßstab für die nachhaltige Ausführung der Tätigkeiten und für die notwendigen Qualifikationen der Datenschutzbeauftragten. Es macht die Tätigkeit der Datenschutzbeauftragten transparent und nachvollziehbar, konkretisiert die gesetzlichen Vorgaben zum Beruf des Datenschutzbeauftragten und schafft eine Orientierung.

In den gesetzlichen Vorgaben werden die Anforderungen an den Datenschutzbeauftragten lediglich mit „Fachkunde“ und „Zuverlässigkeit“ beschrieben. Das Verständnis des BvD von Einzelheiten der beruflichen Anforderungen wird in dem Leitbild erläutert.

Diese Leitlinie ist eine Handreichung um zu Erkennen, wie jemand seine Funktion als Datenschutzbeauftragter wahrnehmen kann.

Für die Berufsausübung ist jedoch mehr erforderlich als nur Grundkenntnisse zu besitzen (Grundkompetenzen generell). Ein Datenschutzbeauftragter muss nicht nur über die notwendigen Qualifikationen verfügen, sondern in der Lage sein, sie entsprechend einzusetzen und erkennen können, an welcher Stelle die Qualifikationen nicht ausreichen. Außerdem muss er in der Lage sein, Lösungen zu organisieren. Die Aufgabe des BvD ist es, den Datenschutzbeauftragten hierbei zu unterstützen und Empfehlungen zu geben.

Dieses Leitbild richtet sich an interne und externe Datenschutzbeauftragte gleichermaßen. Interne Datenschutzbeauftragte sind jene, die als Arbeitnehmer für den Arbeitgeber oder im Auftrag ihres Arbeitgebers für ein anderes Unternehmen bzw. eine andere Behörde als Datenschutzbeauftragter tätig sind. Externe Datenschutzbeauftragte sind jene, die gewerblich für Unternehmen bzw. Behörden als Datenschutzbeauftragte tätig sind.

Das Leitbild betrifft die fachliche Tätigkeit, nicht aber die arbeitsrechtlichen Gegebenheiten bei internen Datenschutzbeauftragten. Hier besteht Bedarf zur sinnvollen Ergänzung und Fortentwicklung gesetzlicher Regelungen zum Beruf des Datenschutzbeauftragten.

Übersicht

Vorwort	2	
Einleitung.....	3	
Übersicht	4	
KAPITEL 1	DIE PERSÖNLICHEN UND FACHLICHEN VORAUSSETZUNGEN	6
1.1. Voraussetzung für die Berufsausübung	6	
1.1.1. Anforderungen.....	6	
1.1.2. Praxiserfahrungen	6	
1.2. Fachkenntnisse (Kompetenzen).....	6	
1.2.1. Rechtliche Grundkompetenzen	6	
1.2.2. IT- und TK-Grundkompetenzen	7	
1.2.3. Erweiterte Fachkenntnisse	7	
1.2.4. Betriebswirtschaftliche und organisatorische Grundkompetenz	7	
1.2.5. Aktualität der Fachkunde (Weiterbildung).....	8	
1.3. Fertigkeiten und Fähigkeiten	8	
1.3.1. Managementfähigkeiten	8	
1.3.2. Koordinierungs- und Teamfähigkeit	8	
1.3.3. Kommunikationsfähigkeiten	8	
1.3.4. Didaktische Fähigkeiten.....	9	
1.3.5. Prüfungs- und Auditmethodik	9	
1.4. Weitere persönliche Voraussetzungen	9	
1.4.1. Persönliche Integrität	9	
1.4.2. Durchsetzungsfähigkeit des eigenen Status.....	9	
1.4.3. Haftungsfähig.....	9	
KAPITEL 2	AUFGABEN UND LEISTUNGEN DES DATENSCHUTZBEAUFTRAGTEN	10
2.1. Grundlegende Lösungskompetenz	10	
2.2. Leitkompetenz	10	
2.3. Prüfungsaufgaben	10	
2.3.1. Prüfungsmaßstäbe und -methoden	10	
2.3.2. Prüfung von Geschäftsprozessen und Regelungen	11	
2.3.3. Prüfung von IT-Systemen.....	11	
2.3.4. Prüfung von Verträgen.....	11	
2.3.5. Prüfung technischer und organisatorischer Maßnahmen.....	11	
2.3.6. Prüfung vor Einführung („Vorabkontrolle“).....	11	
2.3.7. Überprüfung von Beschwerden und Vorfällen	12	
2.4. Gestaltungsaufgaben	12	
2.4.1. Erstellung datenschutzrelevanter Unterlagen.....	12	
2.4.2. Erstellung und Weiterentwicklung eines Datenschutzkonzeptes.....	13	
2.4.3. Sicherung der Betroffenenrechte	13	
2.4.4. Hinwirken auf Transparenz der Verarbeitung.....	13	
2.5. Mitwirkung in Prozessen und Projekten der verantwortlichen Stelle.....	13	
2.5.1. Mitwirkung bei datenschutzrelevanten Entscheidungen	13	
2.5.2. Erarbeitung von Stellungnahmen	14	
2.5.3. Mitwirkung in einzelnen Projekten	14	
2.6. Berichten und Informieren	14	
2.6.1. Umfang und Grenzen.....	14	
2.6.2. Regelmäßige Unterrichtung der Unternehmens- bzw. Behördenleitung	14	

2.6.3.	Regelmäßige Berichte an Bereiche der verantwortlichen Stelle	15
2.6.4.	Kommunikation mit der Datenschutzaufsichtsbehörde.....	15
2.6.5.	Regelmäßige Tätigkeitsberichte	15
2.7.	Schulungs- und Sensibilisierungsaufgaben	16
2.7.1.	Schulungsinhalte	16
2.7.2.	Zielgruppen.....	16
2.7.3.	Umsetzung verschiedener Sensibilisierungsmaßnahmen	17
2.8.	Beratungsaufgaben	17
2.8.1.	Beratungsmaßstab	17
2.8.2.	Beratung der Unternehmens- bzw. Behördenleitung	18
2.8.3.	Beratung der Bereiche, insbesondere Fachabteilungen	18
2.8.4.	Beratung der Betroffenen	18
2.8.5.	Beratung der Mitarbeitervertretung.....	18
2.9.	Qualitätssicherung der Aufgabenerfüllung	18
KAPITEL 3 ANFORDERUNGEN AN DIE BERUFS AUSÜBUNG		19
3.1.	Bestellung zum Datenschutzbeauftragten	19
3.1.1.	Voraussetzung der Bestellung	19
3.1.2.	Sicherstellung der Voraussetzungen	19
3.1.3.	Bestellungsform und -verfahren	19
3.1.4.	Dauer, Laufzeiten	19
3.1.5.	Wirkung der Bestellung	19
3.1.6.	Beendigung.....	20
3.2.	Unabhängigkeit der Berufsausübung	20
3.2.1.	Unabhängigkeit durch Ausschluss zeitlicher Interessenkonflikte	20
3.2.2.	Unabhängigkeit durch Ausschluss fachlicher Interessenkonflikte	20
3.2.3.	Unabhängigkeit durch Ressourcenausstattung	20
3.3.	Organisation der Tätigkeiten	21
3.3.1.	Planung	21
3.3.2.	Dokumentation	21
3.3.3.	Zusammenarbeiten mit anderen internen Stellen	21
3.3.4.	Informationsbeschaffung	22
3.3.5.	Einbeziehung von Aufsichtsbehörden	22
3.4.	Weitere Aspekte der Berufsausübung.....	22
3.4.1.	Haftung und Versicherungspflicht	22
3.4.2.	Informationszugang	22
3.4.3.	Verschwiegenheit	22
3.4.4.	Organisatorische Einbindung	23
3.4.5.	Präsenz	23
3.5.	Vertragliche Regelungen zur Berufsausübung	23
3.5.1.	Allgemeine Vertragsregeln.....	23
3.5.2.	Regeln zur Vermeidung von Benachteiligungen.....	23

Kapitel 1

Die persönlichen und fachlichen Voraussetzungen

1.1. Voraussetzung für die Berufsausübung

1.1.1. Anforderungen

Die Ausübung des Berufs „Datenschutzbeauftragter“ setzt voraus, dass derjenige

- a. eine (allgemeine) berufliche Ausbildung erfolgreich absolviert hat,
- b. angemessene Fachkenntnisse in einer der Kategorien Recht, IT/TK oder betriebswirtschaftliche Organisation besitzt,
- c. über eine mindestens 2-jährige allgemeine Berufserfahrung verfügt und
- d. eine anschließende Ausbildung zum Datenschutzbeauftragten absolviert hat.

Wer keine (allgemeine) berufliche Ausbildung nachweisen kann, soll vor der Ausbildung zum Datenschutzbeauftragten statt dessen eine Berufserfahrung in einem der Bereiche Recht, IT/TK oder betriebswirtschaftliche Organisation über mindestens 6 Jahre erworben haben.

1.1.2. Praxiserfahrungen

Wer zum Datenschutzbeauftragten bestellt wird, soll zusätzlich zur Qualifikation (Anforderungen) über praktische Erfahrungen im Datenschutz verfügen. Die Praxiserfahrungen können im Rahmen der Ausbildung erworben werden. Sie können ersatzweise durch externe Unterstützung, Coaching, Praktika oder ähnliche Maßnahmen erlangt werden.

1.2. Fachkenntnisse (Kompetenzen)

Jeder Datenschutzbeauftragte verfügt unabhängig von Branche und Größe des Unternehmens bzw. der Behörde über ein Mindestmaß an Fachwissen (Grundkompetenzen).

Darüber hinaus können je nach der konkreten Aufgabenstellung in dem Unternehmen bzw. der Behörde weitere individuelle Fachkenntnisse nötig sein.

1.2.1. Rechtliche Grundkompetenzen

Jeder Datenschutzbeauftragte verfügt über Grundkompetenzen im Datenschutzrecht. Er kennt die datenschutzrelevanten Vorschriften seines Fachbereiches/seiner Branche, des Telemedien- und Telekommunikationsrechtes, des Strafrechtes, der Grundzüge des Vertragsrechtes und des Arbeitsrechtes sowie die einschlägige Rechtsprechung und kann diese verstehen und anwenden.

Zu den Grundkompetenzen sollten Kenntnisse aus folgenden Bereichen gehören:

- Allgemeines Persönlichkeitsrecht und Verfassungsrechte mit Datenschutzbezug,
- Prinzipien im Datenschutzrecht,
- Einwilligung und allgemeine Rechtsgrundlagen der Erhebung, Verarbeitung und Nutzung,
- Rechtliche Anforderungen an die Übermittlung von personenbezogenen Daten,
- Auftragsdatenverarbeitung,
- Arbeitnehmerdatenschutzrecht inklusive der sozialversicherungsrechtlichen Regelungen,
- Rechtliche Anforderungen beim Einsatz von IT und TK,
- Grundlagen des europäischen Datenschutzrechtes.

Der Datenschutzbeauftragte sollte in der Lage sein, die für sein Aufgabengebiet geltenden Rechtsvorschriften anwenden zu können und diese gegebenenfalls zu erschließen. Hierzu muss er selbstständig die zu beachtenden Rechtsvorschriften und die Rechtsprechung ausfindig machen können, die geltenden Anforderungen herausarbeiten sowie Sachverhalte und Gegebenheiten vor Ort hinsichtlich der Erfüllung datenschutzrechtlicher Anforderungen beurteilen und bewerten können.

1.2.2. IT- und TK-Grundkompetenzen

Erforderlich sind Grundlagenkenntnisse der Informations- und Telekommunikationstechnologie (IT/TK). Der Datenschutzbeauftragte soll in der Lage sein, diejenigen Techniken zu identifizieren, mit denen personenbezogene Daten erhoben, verarbeitet und genutzt werden. Darüber hinaus muss er grundlegende Sicherheitsrisiken für personenbezogene Daten erkennen und beurteilen können. Dies erstreckt sich z.B. auf folgende Bereiche:

- Zutritts- und Kontrollsysteme,
- Netzwerktechnologie und -systeme,
- Telekommunikationsnetze und -systeme,
- Hardware und deren Architekturen,
- Betriebssysteme,
- Datenbanktechnologien,
- Anwendungssoftware und IT-Verfahren.

Die Grundlagenkenntnisse von organisatorischen und technischen Sicherheitsmaßnahmen für IT- und TK-Systeme umfassen insbesondere Grundbegriffe und Ziele der IT-Sicherheit, Berechtigungsstrukturen und -konzepte, Protokolldaten (Log-Daten) und deren Auswertungsmöglichkeiten, Schutz vor Spionage- und Schadprogrammen, Kontrolle und Absicherung der Datenübertragung (Netzicherheit, Firewall, etc.), Grundlagen kryptographischer Verfahren und deren Anwendung, Datensicherung (Backup) und Archivierung, Anwendbarkeit von Sicherheitsnormen und Standards (z.B. BSI-Grundschutz, ISO/IEC 2700x), Qualitätsmanagement sowie Möglichkeiten der physischen Sicherheit.

1.2.3. Erweiterte Fachkenntnisse

Zusätzlich zu den Grundlagenkompetenzen ist je nach Unternehmen und Einsatzbereich des Datenschutzbeauftragten eine weitergehende Spezialisierung auf Teilbereiche bestimmter Verfahren und Technologien erforderlich. Welche erweiterten Kenntnisse notwendig sind, bestimmt sich nach den im jeweiligen Unternehmen bzw. der Behörde eingesetzten Verarbeitungsverfahren.

Fachspezifische Kenntnisse sind in solchen Branchen zwingend, in denen es vorrangig zu berücksichtigende spezifische Datenschutzregelungen gibt. Dazu zählen beispielsweise medizinische Einrichtungen (wie Krankenhäuser), Banken und Versicherungen, Auskunftsteien, TK- oder Postunternehmen, Verlags- und Pressewesen, IT-Dienstleister oder öffentliche Verwaltung sowie Unternehmen mit internationalem Datentransfer, mit Konzernstruktur oder mit komplexen IT-Strukturen.

1.2.4. Betriebswirtschaftliche und organisatorische Grundkompetenz

Um die Bedeutung der betriebsinternen Informationsflüsse im Hinblick auf personenbezogene Daten einschätzen zu können, sind Grundkenntnisse u.a. aus folgenden Bereichen von Bedeutung:

- Finanzwesen und Controlling,
- Personalwirtschaft,
- Vertrieb,
- Marketing und Public Relations (PR),
- Unternehmens- bzw. Behördenorganisation.

Insbesondere über die standardisierten und individuellen Geschäftsprozesse in den jeweiligen Bereichen hat der Datenschutzbeauftragte Wissen zu erlangen.

Darüber hinaus ist es notwendig, die einschlägigen gesetzlichen Regularien und Anforderungen an diese Unternehmens- bzw. Behördenprozesse zu kennen, um die Notwendigkeit und Richtigkeit der Verarbeitung personenbezogener Daten beurteilen zu können. Der Datenschutzbeauftragte sollte anhand der eingesetzten Verfahren und Geschäftsprozesse die Risiken für die Betroffenen beurteilen können. Er soll darüber hinaus in der Lage sein, Maßnahmenvorschläge und Datenschutzprozesse so zu gestalten, dass sie die betrieblichen Prozesse unterstützen und fördern, aber nicht behindern.

Dazu ist es erforderlich, die Managementdokumentationen (z.B. Qualitätsmanagementhandbuch, Prozessdokumentationen) zu kennen, zu verstehen und mit der vorliegenden Konzeption die Datenschutzvorschläge dort zu integrieren.

1.2.5. Aktualität der Fachkunde (Weiterbildung)

Ein Datenschutzbeauftragter verfügt nur dann über ausreichende Fachkunde, wenn er sein Wissen regelmäßig aktualisiert und vertieft. Er informiert sich selbstständig über gesetzliche Änderungen und aktuelle Rechtsprechung zum Datenschutz sowie über neue technische Entwicklungen und trainiert die Anwendung dieses Wissen. Hierzu nimmt er an Weiterbildungsveranstaltungen teil und baut sein Wissen u.a. im Selbststudium aus. Darüber hinaus eignen sich zur Weiterbildung auch der Austausch mit Fachkollegen sowie die Lektüre von Fachzeitschriften und Fachliteratur.

Der interne Datenschutzbeauftragte fordert von der Unternehmens- bzw. Behördenleitung seine regelmäßige Fort- und Weiterbildung ein.

1.3. Fertigkeiten und Fähigkeiten

Jeder Datenschutzbeauftragte verfügt unabhängig von Branche und Größe des Unternehmens bzw. der Behörde über bestimmte Fertigkeiten und Fähigkeiten.

1.3.1. Managementfähigkeiten

An den Datenschutzbeauftragten werden aufgrund der unterschiedlichen Aufgaben und Ansprechpartner hohe Anforderungen bezüglich seiner Managementkompetenz gestellt. Er verfügt über Lösungskompetenz, Leitkompetenz und Koordinierungskompetenz.

Außerdem verfügt er über Grundlagenwissen bzw. Fertigkeiten der Planungstechniken, der kaufmännischen Planung und Steuerung, des zielorientiertes Zeitmanagements und des Projektmanagements. Insbesondere ist er fähig, Prioritäten zu setzen.

Seine Aufgaben erfordern Gründlichkeit, die Dokumentation seiner Arbeit und eine strukturierte Ablagesystematik.

Sind Beschäftigte dem Datenschutzbeauftragten fachlich oder disziplinarisch unterstellt, sind die Grundlagen der Mitarbeiterführung für seine Aufgabe unabdingbar. Der Datenschutzbeauftragte muss eigene Beschäftigte anleiten und motivieren können.

1.3.2. Koordinierungs- und Teamfähigkeit

Der Datenschutzbeauftragte ist in der Lage, in der konkreten Umgebung die Datenschutzerfordernungen zu koordinieren. Er ist fähig, zu erkennen, in welchen Situationen Unterstützungsbedarf erforderlich ist und kann die notwendige Unterstützung einholen und in ein Team einbinden.

Dies setzt voraus, dass er weiß, wann weitere Sachkompetenz zu Rate zu ziehen ist und wie diese einzusetzen ist.

1.3.3. Kommunikationsfähigkeiten

Der Datenschutzbeauftragte ist bei der Ausübung seiner Tätigkeit in hohem Maße auf Kommunikationsprozesse angewiesen. Zu seinen wichtigsten Kompetenzen gehören Gesprächsführung, Verhandlungsgeschick und die Fähigkeit, mit Konflikten umzugehen.

Um die Forderungen des Datenschutzes erfolgreich umzusetzen, muss er außerdem in der Lage sein, zu moderieren und zwischen Interessengegensätzen verschiedener Bereiche zu vermitteln.

Für eine erfolgreiche Vorstellung seiner Vorschläge und Maßnahmen benötigt er Kompetenzen in Rhetorik. Außerdem sollte er die wichtigsten Präsentationstechniken beherrschen.

1.3.4. Didaktische Fähigkeiten

Der Datenschutzbeauftragte soll die Gefahren von Datenschutzverletzungen und IT-Sicherheitsrisiken, den richtigen Umgang mit personenbezogenen Daten sowie technische und organisatorische Schutzmaßnahmen in praxisnahen Schulungen erläutern können.

Er sollte fähig sein, vor einer Gruppe von Menschen gut zu erklären, sich klar auszudrücken und die Teilnehmer aktiv einzubinden sowie Geduld und Einfühlungsvermögen besitzen.

Die Auswahl und Gestaltung der Lehrmaterialien bzw. der Schulungspräsentation nach diesen Kriterien ist ein weiterer wichtiger Schritt zur erfolgreichen Schulung.

1.3.5. Prüfungs- und Auditmethodik

Der Datenschutzbeauftragte sollte fähig sein, Prüfungen und Audits zu entwickeln, zu planen, sie durchzuführen und die Ergebnisse in entsprechende Maßnahmenvorschläge umzusetzen. Insbesondere beherrscht er die Fragetechniken im Audit. Darüber hinaus muss er die Eignung und die Wirksamkeit von Maßnahmen beurteilen können.

1.4. Weitere persönliche Voraussetzungen

1.4.1. Persönliche Integrität

Als Datenschutzbeauftragter ist ungeeignet, wer nicht über ausreichende persönliche Integrität verfügt. Ungeeignet zur Ausübung der Datenschutzbeauftragtentätigkeit sind ferner Personen, die rechtskräftig verurteilt wurden wegen

- a. Verletzungen des Geheimnisschutzes des persönlichen Lebensbereiches (15. Abschnitt Strafgesetzbuch) oder
- b. eines Verbrechens (§ 12 Abs.1 Strafgesetzbuch), sofern die Straftaten im Bundeszentralregister erfasst sind.

Die Tätigkeiten sollen außerdem nicht ausgeübt werden von Personen, denen innerhalb der letzten 2 Jahre wegen Verletzung von Datenschutzvorschriften rechtskräftig gekündigt wurde.

1.4.2. Durchsetzungsfähigkeit des eigenen Status

Der Datenschutzbeauftragte ist fähig, seine Aufgaben unabhängig auszuführen, seinen Status einzufordern und Einschränkungen abzuwehren. Zu seinem Status gehören u.a.

- die Unabhängigkeit,
- die Weisungsfreiheit,
- das Benachteiligungsverbot,
- das Recht auf Zugang zu Informationen,
- das Recht auf einen unmittelbaren Kontakt zur Unternehmens- bzw. Behördenleitung,
- das Recht auf einen unmittelbaren Kontakt zu allen Mitarbeitern,
- das Recht auf einen regelmäßigen Kontakt zur Aufsichtsbehörde,
- das Recht auf vollständige Aufgabenerfüllung.

1.4.3. Haftungsfähig

Ein Datenschutzbeauftragter muss rechtlich und wirtschaftlich in der Lage sein, die Verantwortung für die Richtigkeit seiner Tätigkeit zu gewährleisten (siehe auch 3.4.1).

Kapitel 2

Aufgaben und Leistungen des Datenschutzbeauftragten

2.1. Grundlegende Lösungskompetenz

Der Datenschutzbeauftragte etabliert betriebswirtschaftliche Positiveffekte und minimiert Risiken für das Unternehmen durch Optimierung von Prozessen. Er benennt die kritischen Punkte in der Unternehmens- bzw. Behördenorganisation, zieht bei Bedarf Fachkompetenzen hinzu und generiert Lösungen.

Rechtzeitig reagiert er auf Fehlentwicklungen, zeigt Alternativen auf und verhindert damit betriebswirtschaftlich relevante Negativeffekte.

Er nimmt alle datenschutzrelevanten Abläufe des Unternehmens bzw. der Behörde wahr.

2.2. Leitkompetenz

Der Datenschutzbeauftragte beantwortet Fragen nach Vorteilen für das Unternehmen- bzw. die Behörde zur Risikominimierung und Prozessoptimierung. Er behandelt Datenschutz lösungsorientiert als Qualitätsfaktor und Qualitätsmerkmal.

Bei der Ausgestaltung dieser Praxisaufgaben kann der BvD unterstützend für die Mitglieder tätig werden.

2.3. Prüfungsaufgaben

Der Datenschutzbeauftragte prüft die Verfahren und Geschäftsprozesse, die internen Regelungen und Verträge sowie die IT-Systeme (Prüfobjekte). Prüfungen können auch im Rahmen eines geeigneten Datenschutzmanagements organisiert sein.

Umfang und Tiefe der Prüfungen unterliegen der Weisungsfreiheit des Datenschutzbeauftragten. Sie haben sich am geltenden Datenschutzrecht und dem aktuellen Stand der Technik zu orientieren.

Prüfungsergebnisse werden strukturiert dokumentiert und der Unternehmens- bzw. Behördenleitung berichtet. Hierbei ist auf festgestellte Risiken gesondert hinzuweisen.

2.3.1. Prüfungsmaßstäbe und -methoden

Prüfungsmaßstäbe sind insbesondere:

- Rechtskonformität,
- aktuellen IT-Sicherheitsstandards (Orientierung am "Stand der Technik"),
- Aktualität, Vollständigkeit und Richtigkeit,
- interne Regelungen sowie die Unternehmenskultur.

Die Rechtskonformität richtet sich nach den für die verantwortliche Stelle geltenden Gesetzen, Verordnungen, Gerichtsurteilen, Tarifverträgen, Betriebs- bzw. Dienstvereinbarungen und weiteren Verträgen. Zu den IT-Sicherheitsstandards gehören z.B. die Regelungen des BSI IT-Grundschutz, ISO 27001 sowie die Grundsätze ordnungsgemäßer DV-gestützter Buchführungssysteme (GoBS).

Zur Durchführung einer Prüfung bestimmt der Datenschutzbeauftragte vorab die Prüfungsmaterie bzw. den zu prüfenden Sachverhalt. Er benennt eigenverantwortlich nach sachkundigem Ermessen die notwendigen Prüfungshandlungen und dokumentiert das Prüfungsergebnis in einem Abschlussdokument.

Angemessene Prüfungshandlungen sind die Inaugenscheinnahme und Begehung, die Befragung verantwortlicher und ausführender Personen, die Beobachtung von Aktivitäten und Arbeitsabläufen, die Durchführung von Testläufen, die Vornahme von Stichproben sowie die Auswertung von Protokollen, Dateien, Dokumenten.

2.3.2. Prüfung von Geschäftsprozessen und Regelungen

Geschäftsprozesse, die praktische Umsetzung und der Umsetzungsgrad interner Regelungen, soweit dies offenbart wird, sind auf Datenschutzkonformität zu prüfen.

Ein besonderes Augenmerk ist auf die Schnittstellen zwischen einzelnen Geschäftsprozessen zulegen, um die Datenintegrität, -authentizität und -sparsamkeit zu gewährleisten.

Hält der Datenschutzbeauftragte es für erforderlich, an Prüfungen im Rahmen anderer Prüfprozesse mitzuwirken, so kann er eigene Prüfprozesse integrieren.

2.3.3. Prüfung von IT-Systemen

Die Prüfung der IT-Systeme ist auf die Umsetzung und Ausgestaltung der technischen und organisatorischen Maßnahmen auszurichten. Die Prüfungsgrundlage wird durch interne Richtlinien zur IT-Sicherheit und andere interne IT-Regelungen erweitert.

Bei der Bewertung der einzelnen IT-Komponenten sind die Sicherheitsmaßnahmen auf technischer, wie auf organisatorischer Ebene zu prüfen.

2.3.4. Prüfung von Verträgen

Verträge sind an den Erfordernissen des Datenschutzes zu prüfen. Dabei sind bereits abgeschlossene Verträge und noch zu erstellende Verträge in die Betrachtung mit einzubeziehen.

Diese Prüfung umfasst insbesondere die Prüfung von Verbraucher- und Kundenverträgen einschließlich der AGB's, von Mitarbeiter- und Beschäftigtenverträgen sowie Verträgen mit Dienstleistern, wie z.B. Support- und Outsourcing-Verträge zur Pflege von Systemen, Programmen oder Diensten.

2.3.5. Prüfung technischer und organisatorischer Maßnahmen

Technische und organisatorische Maßnahmen zum Schutz der personenbezogenen Daten sind auf die Vollständigkeit und Wirksamkeit zu prüfen. Der Umfang der Prüfung hängt dabei von der Komplexität der Organisation und deren Datenverarbeitung ab.

2.3.6. Prüfung vor Einführung („Vorabkontrolle“)

Vor Einführung von Geschäftsprozessen oder IT-Systemen sowie bei Verfahren, die der Vorabkontrolle unterliegen, sind insbesondere zu prüfen:

- die Zweckbestimmung und die Rechtsgrundlage der vorgesehenen automatisierten Verarbeitung sowie die Zulässigkeit der Art der gespeicherten Daten- oder Datenkategorien, der geplanten Übermittlungen oder Übertragungen, der Zugriffsberechtigungen und der Regelfristen zur Löschung,
- die Einhaltung der materiellen Datenschutzbestimmungen – auch unter dem Gesichtspunkt der Datenvermeidung und Datensparsamkeit,
- die Umsetzung der Rechte der Betroffenen in der geplanten Verarbeitung und
- die Angemessenheit der geplanten technischen und organisatorischen Maßnahmen zum Schutz der personenbezogenen Daten.

2.3.7. Überprüfung von Beschwerden und Vorfällen

Betroffene haben das Recht, sich jederzeit an den Datenschutzbeauftragten zu wenden (z.B. gemäß § 4f Abs. 5 Satz 2 BDSG). In diesen Fällen geht er den Beschwerden ohne Verzögerung nach. Er ermittelt den Sachverhalt umfassend, prüft ihn unter Datenschutzgesichtspunkten und schlägt, sofern möglich, Lösungen vor. Am Ende der Prüfung soll er eine Bewertung des Sachverhaltes erstellen und entsprechend dokumentieren. Der verantwortlichen Stelle ist Gelegenheit zur Stellungnahme einzuräumen. Das Prüfungsergebnis ist dem Betroffenen mitzuteilen.

Der Datenschutzbeauftragte ist bei der Überprüfung von Beschwerden und Vorfällen zur Verschwiegenheit über die Identität der Person des Betroffenen verpflichtet. Lässt sich eine Überprüfung und Klärung nicht vollständig durchführen, ohne dass die Identität des Betroffenen preisgegeben werden muss, so ist der Datenschutzbeauftragte verpflichtet, den Betroffenen hierüber aufzuklären und die weitere Bearbeitung von seiner Zustimmung abhängig zu machen.

2.4. Gestaltungsaufgaben

Neben den nachfolgend beispielhaft genannten Gestaltungsaufgaben unterbreitet der Datenschutzbeauftragte auch Vorschläge für datenschutzfreundliche Unternehmensziele.

2.4.1. Erstellung datenschutzrelevanter Unterlagen

Der Datenschutzbeauftragte unterstützt die verantwortliche Stelle bei der Erarbeitung von Maßnahmen, die für die Umsetzung des Datenschutzes erforderlich sind. Er kann hierzu Entwürfe und Vorlagen erstellen. Dabei soll er Fachliteratur anwenden und kann auf Musterunterlagen zurückgreifen.

a.) Richtlinien und Dienst- bzw. Arbeitsanweisungen

Der Datenschutzbeauftragte entwirft Richtlinien, Dienst- und Arbeitsanweisungen oder wirkt bei deren Erstellung mit. Dabei soll ein unternehmensspezifisches Regelwerk entstehen. Die Richtlinien müssen die Unternehmensphilosophie, -kultur und -struktur berücksichtigen. Entsprechendes gilt für öffentliche Einrichtungen.

Richtlinien sind insbesondere dann zu erstellen, wenn sich der Gegenstand nicht durch Betriebs- bzw. Dienstvereinbarungen regeln lässt. Durch Richtlinien werden der Umgang mit und die Schutzmaßnahmen für personenbezogene Daten in den betroffenen Bereichen geregelt.

b.) Betriebs- bzw. Dienstvereinbarungen

Der Datenschutzbeauftragte wirkt bei der Erstellung von Betriebs- bzw. Dienstvereinbarungen mit. Er ergreift die Initiative zu deren Erstellung und zur datenschutzkonformen Gestaltung, außerdem prüft er sie unter Datenschutzgesichtspunkten und erstellt bei Bedarf Verbesserungsvorschläge.

c.) Öffentliches Verzeichnisse und interne Verarbeitungsübersicht

Der Datenschutzbeauftragte unterstützt die verantwortliche Stelle bei der Erstellung des öffentlichen Verzeichnisses sowie der internen Verarbeitungsübersicht.

Sofern eine verantwortliche Stelle kein Verzeichnis und keine Übersicht besitzt und sie den Datenschutzbeauftragten mit der Erstellung beauftragt, fordert er die Angaben ein und initiiert das Erstellen. Er wird hierbei zur treibenden Kraft. Darüber hinaus überwacht er die Aktualisierung der Angaben.

Auf Antrag macht er die Angaben des öffentlichen Verzeichnisses jedermann zugänglich. Der Umfang richtet sich dabei nach den für die verantwortliche Stelle geltenden Gesetzen und nach Gesichtspunkten von Amts-, Betriebs- und Geschäftsgeheimnissen (§ 203 StGB).

In der internen Verarbeitungsübersicht sind die Angaben eines Verzeichnisses sowie weitere Informationen über den Datenfluss, das Systemumfeld sowie über die Organisation und den Schutz der Datenverwendung zu dokumentieren.

d.) **Maßnahmenvorschläge**

Der Datenschutzbeauftragte unterbreitet geeignete Vorschläge für technische und organisatorische Schutzmaßnahmen. Hierzu gehören insbesondere Vorschläge zur Vermeidung von Daten, zur Pseudo- und Anonymisierung, zur Transparenz der Verarbeitung, zur Information über die Rechtsgrundlage und zur Wahrnehmung der Betroffenenrechte.

Die Maßnahmenvorschläge werden mit der Unternehmens- bzw. Behördenleitung bzw. je nach Organisation mit den betroffenen Stellen innerhalb der Einrichtung erörtert. Mit der Vorlage eines pragmatischen und sachgerechten Maßnahmenvorschlages hat der Datenschutzbeauftragte seine Aufgabe erfüllt.

Die Umsetzung der Maßnahmenvorschläge ist die Aufgabe der verantwortlichen Stelle. Es ist auszuschließen, dass ein Datenschutzbeauftragter eigene Maßnahmenvorschläge umsetzt; die Umsetzung und Prüfung von Maßnahmen durch dieselbe Person stellt einen Interessenkonflikt dar. Zur Vermeidung dieses Interessenkonfliktes entscheidet die verantwortliche Stelle, in welcher Form die Realisierung der Vorschläge des Datenschutzbeauftragten erfolgen kann und ordnet die Umsetzung an.

2.4.2. **Erstellung und Weiterentwicklung eines Datenschutzkonzeptes**

Über die einzelnen Maßnahmenvorschläge hinaus erstellt der Datenschutzbeauftragte eine strukturierte Gesamtschau aller Maßnahmen unter Berücksichtigung der unternehmens- bzw. behördenspezifischen Gegebenheiten als Datenschutzkonzept. Dieses beinhaltet die Beschreibung einer Datenschutzorganisation und ein Datenschutzhandbuch als Teil des Managementhandbuchs. Die Verantwortlichen des Unternehmens bzw. der Einrichtung finden dort alle wesentlichen Punkte, die im Rahmen der Verarbeitung personenbezogener Daten zu beachten sind.

Dabei sollen keine Papierberge entstehen, die aufwändig aktualisiert werden müssen, sondern Übersichtlichkeit und Anwendbarkeit der Dokumentation im Vordergrund stehen.

Der Datenschutzbeauftragte wirkt außerdem darauf hin, dass die Datenschutzkriterien auch in die Konzepte anderer Prüfbereiche wie (z.B. dem Qualitätsmanagement) mit einfließen.

2.4.3. **Sicherung der Betroffenenrechte**

Wenden sich Betroffene an die verantwortliche Stelle, um ihre Rechte wie z.B. Auskunftsrechte, Widerspruchsrechte oder das Recht auf Sperrung in Anspruch zu nehmen, so wirkt der Datenschutzbeauftragte auf die ordnungsgemäße Abwicklung hin.

Der Datenschutzbeauftragte überprüft das Begehren und gibt eine Stellungnahme ab. Er wirkt auf eine zeitnahe Verwirklichung der Rechte, insbesondere eine schnelle Beantwortung von Auskunftsbegehren hin.

2.4.4. **Hinwirken auf Transparenz der Verarbeitung**

Der Datenschutzbeauftragte wirkt auf eine umfassende Transparenz der Datenverarbeitung in der verantwortlichen Stelle hin. Er entwickelt Konzepte und Vorschläge, in welcher Art und Weise und in welchem Umfang Betroffene über die Verarbeitungsvorgänge informiert werden sollen. Darüber hinaus achtet er auf Vollständigkeit und Richtigkeit der Informationen.

2.5. **Mitwirkung in Prozessen und Projekten der verantwortlichen Stelle**

Der Datenschutzbeauftragte wirkt bei der datenschutzgerechten Gestaltung von Betriebs- bzw. Behördenprozessen mit.

2.5.1. **Mitwirkung bei datenschutzrelevanten Entscheidungen**

Der Datenschutzbeauftragte nimmt als unabhängiger Sachverständiger zu Datenschutzfragen an Beratungen aller relevanten internen und einschlägigen externen Gremien teil. Darüber hinaus beteiligt er sich beispielsweise an

- den Verhandlungen zwischen Unternehmens- bzw. Behördenleitung und Mitarbeitervertretung als Sachverständiger,
- der Festlegung von Kriterien bei der Investitionsplanung,
- der Gestaltung von IT-Sicherheitsprozessen,

- IT-Revisionsprozessen zur Wahrnehmung der Datenschutzkontrollaufgaben,
- der Einführung neuer IT-Systeme mittels Vorabkontrolle und Beratung,
- der Gestaltung und der Überwachung der Qualitätsmanagementprozesse.

Sofern er eigene Prozesse anstößt, beteiligt er die relevanten Stellen der verantwortlichen Stelle entsprechend.

Ist der Datenschutzbeauftragte in Prozesse einbezogen, hat er seine Unabhängigkeit zu gewährleisten. So kann er einen Prozess beratend oder prüfend begleiten.

2.5.2. Erarbeitung von Stellungnahmen

Durch eine Stellungnahme beurteilt der Datenschutzbeauftragte Sachverhalte und beschreibt die Gründe für das Wertungsergebnis. Insbesondere bewertet er Abläufe, Unternehmensprozesse, Verfahren, Anwendungen, IT-Infrastruktur, Formulare, Investitionen oder Verträge, die geplant oder geändert werden.

Eine Stellungnahme sollte vom Datenschutzbeauftragten auch immer dann abgegeben werden, wenn er Verbesserungsmöglichkeiten im Datenschutz erkannt hat, wenn Anfragen an den Datenschutzbeauftragten gerichtet werden oder auf Anforderung.

Die Stellungnahme bewertet zum einen die datenschutzrechtliche Zulässigkeit und zum anderen die Vollständigkeit und Wirksamkeit von Schutzmaßnahmen. Sie enthält die bestimmenden Faktoren des Sachverhaltes, ein zusammenfassendes Ergebnis sowie eine umfassende Bewertung. Maßstab für die Bewertung sind gesetzliche Vorschriften und interne Regelungen. Sofern der Datenschutzbeauftragte zu einem negativen Ergebnis kommt (z.B. Unzulässigkeit, Verbesserungspotenzial), sollte die Stellungnahme zugleich Lösungsansätze (z.B. Maßnahmenvorschläge zur Umsetzung der technisch-organisatorischen Maßnahmen nach § 9 BDSG) enthalten.

2.5.3. Mitwirkung in einzelnen Projekten

Neben der Beteiligung des Datenschutzbeauftragten in den Regelabläufen wirkt er in Einzelprojekten mit.

2.6. Berichten und Informieren

Der Datenschutzbeauftragte informiert und berichtet gegenüber internen Stellen. Dies geschieht regelmäßig oder anlassbezogen. Adressaten sind insbesondere Unternehmens- bzw. Behördenleitung und Mitarbeitervertretungen. Darüber hinaus können anlassbezogen Aufsichtsbehörden, Betroffene und Dritte Adressaten sein.

2.6.1. Umfang und Grenzen

Die Weisungsfreiheit des Datenschutzbeauftragten entbindet ihn nicht vom Berichten.

Die gesetzliche Vertraulichkeitsverpflichtung (wie gegenüber dem Betroffenen) begrenzen seine Berichtspflicht. Die Verpflichtung zur Verschwiegenheit besteht auch dann, wenn fahrlässige Datenschutzverletzungen durch Beschäftigte verursacht wurden. Er kann sachbezogen berichten, eine Pflicht zum personenbezogenen berichten besteht nicht.

2.6.2. Regelmäßige Unterrichtung der Unternehmens- bzw. Behördenleitung

Die Unternehmens- bzw. Behördenleitung ist als Hauptverantwortlicher für den Datenschutz erster Empfänger der Berichte und Informationen des Datenschutzbeauftragten. Er unterrichtet die Unternehmens- bzw. Behördenleitung über

- a. die Datenschutzsituation in der verantwortlichen Stelle im Allgemeinen,
- b. mögliche Risiken,
- c. Verstöße gegen gesetzliche, vertragliche und interne Vorschriften sowie Anforderungen der Datenschutzaufsichtsbehörde,
- d. festgestelltes Verbesserungspotenzial und Umsetzungshindernisse,

- e. Umsetzungsstatus des Aktivitäten- und Maßnahmenplans,
- f. durchgeführte und geplante Tätigkeiten als Datenschutzbeauftragter,
- g. Änderungen von einschlägigen rechtlichen oder technischen Rahmenbedingungen.

2.6.3. Regelmäßige Berichte an Bereiche der verantwortlichen Stelle

Der Datenschutzbeauftragte berichtet direkt gegenüber weiteren internen Bereichen, sofern dies die Unternehmens- bzw. Behördenleitung festlegt hat. So können und sollten Kommunikationsstränge insbesondere zur IT-Abteilung, IT-Revision, Personalabteilung, sowie zum Qualitätsmanagement, Vertrieb, Marketing und branchenspezifischen operativen Bereichen bestehen.

Bei Unstimmigkeiten oder wenn Entscheidungen herbeizuführen sind, bleibt die Unternehmens- bzw. Behördenleitung weiterhin Ansprechpartner.

2.6.4. Kommunikation mit der Datenschutzaufsichtsbehörde

Der Datenschutzbeauftragte informiert die jeweilige Aufsichtsbehörde

- a. auf Verlangen der Aufsichtsbehörde,
- b. auf Verlangen der Unternehmens- bzw. Behördenleitung,
- c. bei unlösbaren Konflikten um die Rechtmäßigkeit von Verfahren und Maßnahmen zwischen verantwortlicher Stelle und Datenschutzbeauftragten,
- d. nach pflichtgemäßen Ermessen wenn Zweifelsfälle bestehen,
- e. bei Konflikten um die Unabhängigkeit des Datenschutzbeauftragten.

Stellt der Datenschutzbeauftragte besonders schwerwiegende Verstöße gegen die gesetzlichen Datenschutzvorschriften fest und hat die Unternehmens- bzw. Behördenleitung trotz Kenntnis der Rechtswidrigkeit wiederholt erklärt, diese nicht abstellen zu wollen, ist nach sorgfältiger Ermessensentscheidung die Aufsichtsbehörde in Kenntnis setzen. Besonders schwerwiegend sind Verstöße, wenn

- bei Kenntnis der Rechtswidrigkeit dauerhaft bzw. über einen langen Zeitraum mehrere Vorschriften verletzt werden und viele Personen betroffen sind,
- schwerwiegende Verletzungen des Persönlichkeitsrechtes festgestellt wurden,
- sensible Daten wiederholt ohne rechtliche Erlaubnis an Dritte übermittelt werden, ohne dass Gegenmaßnahmen ergriffen wurden,
- Auskunftsansprüche an Betroffene bewusst nicht oder bewusst wahrheitswidrig erteilt werden.

2.6.5. Regelmäßige Tätigkeitsberichte

a.) Ziele und Zweck

Unabhängig von den vorstehenden Kommunikationspflichten sollte der Datenschutzbeauftragte durch einen regelmäßigen Tätigkeitsbericht gegenüber der Unternehmens- und Behördenleitung über seine Tätigkeit berichten.

Der Tätigkeitsbericht dient der Information der Unternehmens- bzw. Behördenleitung, der reversionssicheren Dokumentation und als Aktivitätennachweis des Datenschutzbeauftragten. Er dient darüber hinaus der Gewährleistung der ordnungsgemäßen Übergabe beim Wechsel des Datenschutzbeauftragten, als Nachweis gegenüber der Aufsichtsbehörde und der Nachvollziehbarkeit und Messbarkeit der Datenschutzentwicklung in der verantwortlichen Stelle.

b.) Inhalt

Der Bericht soll folgende Punkte enthalten:

- eine Beschreibung der Datenschutzsituation in der verantwortlichen Stelle,
- festgestellte Verstöße gegen gesetzliche, vertragliche und interne Vorschriften sowie Anforderungen der Datenschutzaufsichtsbehörde,
- festgestellte Risiken,
- eine Zusammenfassung von Aktivitäten und Maßnahmen mit Darstellung des jeweiligen Umsetzungsstatus,
- eine Einschätzung der mittel- und langfristigen Entwicklung des Datenschutzes in der verantwortlichen Stelle und Vorschläge für entsprechende Unternehmensziele.

Empfehlenswert ist ein mindestens jährlicher Bericht, wenn nicht die Anforderungen in der verantwortlichen Stelle ein anderes Berichtsintervall verlangen.

2.7. Schulungs- und Sensibilisierungsaufgaben

Die Schulung und Sensibilisierung von Verantwortlichen und Beschäftigten in der verantwortlichen Stelle ist eine grundlegende Voraussetzung für ein funktionierendes Datenschutzmanagement in der verantwortlichen Stelle und gehört zu den zentralen Aufgaben des Datenschutzbeauftragten.

Er führt Schulungen zeitlich und inhaltlich eigenverantwortlich und nach sachlichem Ermessen durch. Dabei legt er Wissensinhalte und Umfang fest. Die Schulungen müssen praxisnah und zielgruppengerecht aufgebaut sein. Sie sind außerdem didaktisch aufzubereiten.

Die Durchführung der Schulung kann auf Dritte übertragen werden. In diesem Fall überwacht der Datenschutzbeauftragte die Durchführung der Schulung, die Dokumentation und den Nachweis der durchgeführten Schulungen.

Die Schulungsorganisation, wie z.B. Freistellung und Einladung der Beschäftigten, ist Aufgabe des Unternehmens. Werden die Rahmenbedingungen für Schulungen dem Datenschutzbeauftragten nicht zur Verfügung gestellt, so statuiert er einen Zweifelsfall.

2.7.1. Schulungsinhalte

Der Datenschutzbeauftragte vermittelt grundlegendes Basiswissen und Vertiefungswissen.

Zum Basiswissen gehören insbesondere Begrifflichkeiten im Datenschutz, Hintergründe und Entstehung, Prinzipien im Datenschutz, Stellung und Aufgaben des Datenschutzbeauftragten, Datenschutzorganisation des Unternehmens bzw. der Behörde und Grundlagen der IT-Sicherheit.

Das zu vermittelnde Vertiefungswissen umfasst insbesondere Unternehmens- bzw. behördenspezifische Kenntnisse, zielgruppenspezifische Kenntnisse (z.B. Vertrieb, Marketing, aber auch Beauftragtenwesen sowie Betriebsarzt), Beschäftigten-/Arbeitnehmerdatenschutz, Kundendatenschutz sowie technische und organisatorische Maßnahmen zum Datenschutz.

2.7.2. Zielgruppen

a.) Unternehmens- bzw. Behördenleitung und Führungskräfte

Der Datenschutzbeauftragte schult die Unternehmens- bzw. Behördenleitung und die Führungskräfte. Hierbei sind die rechtlichen und technischen Anforderungen der Datenschutzvorschriften sowie die Risiken bei Datenschutzverstößen besonders hervorzuheben. Außerdem sind die Notwendigkeit und die Arbeitsweise einer Datenschutzorganisation und die Verantwortung der Führungsebene zur Anleitung im datenschutzgerechten Handeln zu vertiefen.

b.) Fachverantwortliche

Fachverantwortlichen ist über das Basiswissen hinaus zusätzlich das Wissen zu vermitteln, dass für die datenschutzgerechte Gestaltung der fachspezifischen Prozesse und Verfahren notwendig ist. Insbesondere sind die technischen und organisatorischen Maßnahmen, die im jeweiligen Fachbereich ergriffen werden müssen, zu vertiefen.

c.) Beschäftigte

Alle Beschäftigten des Unternehmens, die mit personenbezogenen Daten arbeiten sind im Basiswissen zu unterweisen. Darüber hinaus sind Beschäftigte fachspezifisch vertieft zu schulen, insbesondere Beschäftigte der Bereiche Personalverwaltung, IT-Betreuung und Kundenbetreuung. Außerdem ist Beschäftigten das Wissen über die richtige Anwendung der technischen und organisatorischen Schutzmaßnahmen zu vermitteln.

d.) Mitarbeitervertretung

Die Mitarbeitervertretung ist durch die Vorschriften über die Mitbestimmung für die Überwachung des Schutzes der Arbeitnehmerdaten mit verantwortlich; eine ergänzende Schulung über das Basiswissen hinaus ist daher notwendig.

Andererseits ist die Mitarbeitervertretung als regelmäßiger Empfänger höchst sensibler personenbezogener Daten auch hinsichtlich des korrekten Umganges mit diesen Daten zu sensibilisieren und über die weiteren gesetzlichen Pflichten zu schulen.

e.) Betriebsarzt

Der Betriebsarzt unterliegt der ärztlichen Schweigepflicht und ist darüber hinaus hinsichtlich des Datenschutzes zu schulen. Insbesondere ist dabei zu verdeutlichen, welche Risiken durch den Einsatz der EDV in der betriebsärztlichen Praxis entstehen können und unter welchen Voraussetzungen er Daten erheben, verarbeiten und weitergeben darf. Dabei sind nicht nur das BDSG, sondern auch die Gesetzgebung zur Arbeitssicherheit und die Sozialgesetzgebung zu berücksichtigen. Insbesondere ist darauf hinzuweisen, dass Informationen über den Gesundheitszustand der Arbeitnehmer zu den besonders geschützten Daten gehören.

2.7.3. Umsetzung verschiedener Sensibilisierungsmaßnahmen

Neben der reinen Datenschutzbildung bzw. über diese Schulung hinaus ist der Datenschutzbeauftragte für die angemessene Sensibilisierung der Beschäftigten und Führungskräfte für Datenschutzthemen verantwortlich. Um die Aufnahme der Schulungsinhalte und deren Verständnis zu verbessern, aber auch um die Mitarbeiter und Führungskräfte aktueller informieren zu können, ist der Datenschutzbeauftragte angehalten, geeignete Maßnahmen zur Sensibilisierung in der verantwortlichen Stelle zu erarbeiten. Diese Maßnahmen sind speziell auf die verantwortliche Stelle oder die Organisation zuzuschneiden. Dies kann von Sensibilisierungsworkshops für bestimmte Personenkreise bis hin zu Awarenesskampagnen für das gesamte Unternehmen gehen. Vorteilhaft ist dabei, dass die unternehmensspezifischen Bedürfnisse aber auch z.B. die Erfordernisse der IT-Sicherheit eingearbeitet werden können.

2.8. Beratungsaufgaben

Der Datenschutzbeauftragte berät alle Bereiche der verantwortlichen Stelle sowie anlassbezogen auch Betroffene bei allen Fragen zum Datenschutz, bei der Ausgestaltung von Maßnahmen zum Datenschutz, sowie bei der Risikoabschätzung.

2.8.1. Beratungsmaßstab

Der Datenschutzbeauftragte berät bei der Erstellung und Implementierung von technischen und organisatorischen Maßnahmen zum Datenschutz. Die Maßstäbe dafür sind Wirksamkeit, Wirtschaftlichkeit, Praktikabilität, Angemessenheit sowie Akzeptanz der Maßnahmen. Dazu gehört auch eine enge Zusammenarbeit mit dem Qualitätsmanagement und der IT-Abteilung. Ziel der Beratung soll auch sein, durch ein hohes Datenschutzniveau zu einem Wettbewerbsvorteil für die verantwortliche Stelle beizutragen.

2.8.2. Beratung der Unternehmens- bzw. Behördenleitung

Der Datenschutzbeauftragte berät die Unternehmens- bzw. Behördenleitung in allen Angelegenheiten (z.B. bei Projekten), die den Datenschutz tangieren oder tangieren könnten. Er gibt Hinweise auf die notwendige Festlegung der Zwecke der Verarbeitung personenbezogener Daten, auf Benachrichtigungspflichten, Pflichten zur Vorabkontrolle, Meldepflichten, sowie auf die Rechtskonformität geplanter Verfahren. Bei der Festlegung der technischen oder organisatorischen Schutzmaßnahmen wirkt er im Rahmen der Angemessenheitsfestlegung der Unternehmens- bzw. Behördenleitung auf die datenschutzfreundlichste Alternative hin.

2.8.3. Beratung der Bereiche, insbesondere Fachabteilungen

Der Datenschutzbeauftragte berät alle von den Datenschutzregelungen betroffenen Bereiche der Einrichtung. Er berät sie insbesondere bei der Durchführung der vorgegebenen technischen und organisatorischen Maßnahmen zum Datenschutz.

2.8.4. Beratung der Betroffenen

Wenden sich Betroffene an den Datenschutzbeauftragten, berät er jene umfassend und vertraulich. Er eröffnet ihnen Alternativen über Vorgehensweisen und informiert, wenn er Beschwerden, nicht ohne die Identität des Betroffenen zu offenbaren, nachgehen kann.

Kennt der Betroffene seine Betroffenheit nicht, so informiert der Datenschutzbeauftragte ihn darüber.

2.8.5. Beratung der Mitarbeitervertretung

Der Datenschutzbeauftragte berät die Mitarbeitervertretung in allen Fragen bei bestehenden und geplanten Verfahren mit personenbezogenen Daten. Eine der Aufgaben der Mitarbeitervertretung ist der Schutz der Beschäftigten durch die Überwachung des Arbeitnehmerdatenschutzes. Hier ergibt sich eine Überschneidung, die eine enge Zusammenarbeit von Mitarbeitervertretung und Datenschutzbeauftragten impliziert.

2.9. Qualitätssicherung der Aufgabenerfüllung

Die Qualitätssicherung der vollständigen und richtigen Aufgabenerfüllung wird in erster Linie durch Eigenkontrolle gewährleistet. Zu den Instrumenten der Qualitätssicherung gehören insbesondere:

- Festhalten und Abarbeiten der hier beschriebenen Aufgaben,
- Dokumentation der eigenen Arbeit,
- Wahrnehmung der Berichtspflichten (siehe Abschnitt 2.6).

Der Datenschutzbeauftragte dokumentiert seine Arbeit revisionssicher. Dieser Dokumentation sollte zu entnehmen sein, welche Aufgaben erledigt und welche offen sind. Bei den offenen Aufgaben sind die Verantwortlichkeit für den nächsten Schritt und die Erledigungstermine festzuhalten.

Die Dokumentation dient der kontinuierlichen Verbesserung der eigenen Tätigkeit, des Nachweises einer fachkundigen Tätigkeitserfüllung gegenüber Unternehmensführung und Aufsichtsbehörden sowie der Übergabe an einen Nachfolger. Bei einem Wechsel müssen sämtliche Dokumentationen dem Nachfolger übergeben werden. Dies gilt nicht für den Fall der Verschwiegenheitspflicht gegenüber Betroffenen.

Zur Sicherstellung einer qualitativen Aufgabenerfüllung kann sich der Datenschutzbeauftragte auch eines externen Audits (privat, Aufsichtsbehörde) bedienen.

Kapitel 3

Anforderungen an die Berufsausübung

3.1. Bestellung zum Datenschutzbeauftragten

3.1.1. Voraussetzung der Bestellung

Zum Datenschutzbeauftragten darf sich nur eine natürliche Person bestellen lassen, die die persönlichen und fachlichen Voraussetzungen zur Berufsausübung erfüllt.

Zum Datenschutzbeauftragten kann sich sowohl ein Beschäftigter als auch eine Person außerhalb der verantwortlichen Stelle bestellen lassen.

3.1.2. Sicherstellung der Voraussetzungen

Der zu Bestellende soll bei der Bestellung sicherstellen, dass die folgenden Voraussetzungen vorliegen:

- a. die erfolgreiche Qualifizierung zum Datenschutzbeauftragten; bei internen Datenschutzbeauftragten ist dies vom Arbeitgeber sicherzustellen ist,
- b. bei einem mehr als 3 Jahren zurückliegendem Qualifizierungsabschluss zum Datenschutzbeauftragten zusätzlich Weiterbildungsmaßnahmen,
- c. bei externen Datenschutzbeauftragten eine abgeschlossene Berufshaftpflicht oder eine anderweitige Schadensabsicherung bzw. entsprechende vertragliche Regelung.

3.1.3. Bestellungsform und -verfahren

Der Datenschutzbeauftragte lässt sich ausschließlich durch die jeweilige Unternehmens- bzw. Behördenleitung bestellen. Die Bestellung erfolgt schriftlich.

Soll die Beauftragtenfunktion für mehrere rechtlich selbstständige Einheiten ausgeübt werden, muss für jede Einheit eine eigene Bestellung erfolgen. Dabei kann ein Datenschutzbeauftragter für mehrere miteinander verbundene und nicht verbundene Unternehmen oder Behörden die Aufgaben wahrnehmen, so lange dies nicht den Regeln der Unabhängigkeit widerspricht.

Es können ein oder mehrere Stellvertreter bestellt werden.

3.1.4. Dauer, Laufzeiten

Beauftragtenverhältnisse können zeitlich befristet werden. Langfristige Bestellungen werden empfohlen. Die Laufzeit für die Erstbestellung sollte fünf Jahre, die für Wiederbestellungen drei Jahre nicht unterschreiten.

3.1.5. Wirkung der Bestellung

Der Datenschutzbeauftragte arbeitet auf dem Gebiet des Datenschutzes weisungsfrei.

Wer als Beschäftigter des Unternehmens bestellt wird, führt die Beauftragtentätigkeiten eigenständig neben oder statt dem ursprünglichen Tätigkeitsbereich aus. Ist der Datenschutzbeauftragte zugleich ein Beschäftigter eines anderen Unternehmens, so ist er bei der fachlichen Ausführung seiner Aufgaben im Rahmen jeder Bestellung auch gegenüber seinem eigenen Arbeitgeber weisungsfrei tätig. Gegenüber der Einrichtung, die ihn bestellt, ist er unabhängig tätig gemäß den Ausführungen dieser Berufsgrundsätze.

Er steuert das ihm zugeordnete Personal fachlich.

3.1.6. Beendigung

Die Bestellung endet außer in den gesetzlich festgelegten Fällen (Widerruf, Abberufung, außerordentliche Kündigung) auch durch Zeitablauf oder Rücktritt des Bestellten.

Zur Vermeidung von Schwierigkeiten achtet der externe Beauftragte darauf, dass Art und Zeitpunkt des Bestellsendes mit dem Ende des zu Grunde liegenden Dienstvertrages zusammenfallen.

3.2. Unabhängigkeit der Berufsausübung

Der Datenschutzbeauftragte muss unabhängig tätig sein und sein können. Unabhängig ist er, wenn er frei von Interessenkonflikten und frei von der Weisungsfreiheit entgegenstehenden Beeinflussungen ist und über ausreichende Ressourcen verfügt.

Interessenkonflikte liegen vor, wenn die Tätigkeit des Datenschutzbeauftragten mit anderen Aufgaben z.B. in einem zeitlichen oder fachlichen Widerspruch steht.

Sind die Voraussetzungen für die Unabhängigkeit der Berufsausübung nicht erfüllt, kann der Beruf des Datenschutzbeauftragten nicht ausgeübt werden.

3.2.1. Unabhängigkeit durch Ausschluss zeitlicher Interessenkonflikte

Für eine unabhängige Ausführung der Funktion des Datenschutzbeauftragten sind die Datenschutzaufgaben vorrangig vor anderen Verpflichtungen zu erfüllen. Die anderen Verpflichtungen treten in den Hintergrund. Kann die andere Verpflichtung nicht in den Hintergrund treten, ist eine Bestellung zum Datenschutzbeauftragten nicht möglich. Für die Erfüllung der Datenschutztätigkeiten ist eine Freistellung sicherzustellen.

3.2.2. Unabhängigkeit durch Ausschluss fachlicher Interessenkonflikte

Darüber hinaus sind die Tätigkeiten im Unternehmen bzw. der Behörde mit den Aufgaben des Datenschutzbeauftragten unvereinbar, bei denen ein fachlicher Interessenkonflikt besteht. Diese Tätigkeiten sind nicht in Personalunion auszuüben. Dazu zählen insbesondere die folgenden Tätigkeiten:

- a. schwerpunktmäßige Verarbeitung oder Nutzung personenbezogener Daten, wie z.B. administrative Aufgaben im IT-Bereich, Personalsachbearbeitung, Kundendatenbearbeitung,
- b. konzeptionelle und strategische Tätigkeiten im IT-Bereich,
- c. operative Tätigkeiten zur Gewährleistung der IT-Sicherheit,
- d. Unternehmens- bzw. Behördenleitung, Mitarbeiterführung und deren Assistenz,
- e. Rechtliche Beratungen als Justiziere, Rechtsabteilungsleiter, Rechtsanwälte und anderer Berater, die das Unternehmen bzw. die Behörde vertreten,
- f. Leitungsfunktionen der Mitarbeitervertretung,
- g. Wirtschaftsprüfung.

3.2.3. Unabhängigkeit durch Ressourcenausstattung

Der Datenschutzbeauftragte ist unabhängig, wenn er im erforderlichen Umfang über Kommunikationsmittel, Büroausstattung, Fachliteratur sowie Berechtigungen, die ihm die uneingeschränkte Erfüllung seiner Aufgaben ermöglichen, verfügt.

Die Ausstattung ist eine gesetzliche Bringschuld des bestellenden Unternehmens bzw. der Behörde. Kommt das bestellende Unternehmen bzw. die Behörde dieser Pflicht nicht nach, fordert der Datenschutzbeauftragte diese ein.

Die für seine Berufsausübung erforderlichen sachlichen, personellen und organisatorischen Voraussetzungen stimmt er einvernehmlich mit der bestellenden Stelle ab.

3.3. Organisation der Tätigkeiten

3.3.1. Planung

Der Datenschutzbeauftragte plant und organisiert seine Tätigkeit eigenverantwortlich.

Er stellt für alle wesentlichen Tätigkeiten einen schriftlichen Aktivitätenplan auf und führt diesen fort. Der Aktivitätenplan ist Bestandteil des Berichtswesens an die Unternehmens- bzw. Behördenleitung und Grundlage aller Abstimmungen zum Datenschutz in der verantwortlichen Stelle.

In dem Aktivitätenplan organisiert er eigenverantwortlich seine Aufgaben, Maßnahmen inklusive der Schulungen und Schulungsthemen, Audits und Termine. Der Plan gibt Auskunft über Ziele und Vorgehensweise sowie den Erledigungsstand der Aktivitäten zum Datenschutz in der verantwortlichen Stelle.

Der Umfang und der Detaillierungsgrad der Planungen sollten im angemessenen Verhältnis zur Größe, Komplexität und Aufgabenstellung der verantwortlichen Stelle stehen.

3.3.2. Dokumentation

Der Datenschutzbeauftragte dokumentiert seine Tätigkeiten. Ziel der Dokumentation ist die Nachvollziehbarkeit seiner Tätigkeit.

Gegenstand der Dokumentation sind insbesondere die folgenden Tätigkeiten:

- Planung der Aktivitäten,
- Schulungen, Sensibilisierungsmaßnahmen,
- Prüfungen,
- Berichterstattung und Stellungnahmen,
- Beratungen,
- Vorabkontrollen,
- Bearbeitung von Vorfällen und Beschwerden,
- Mitwirkung bei Richtlinien oder Betriebs- bzw. Dienstvereinbarungen,
- Gespräche und Schriftverkehr mit der Aufsichtsbehörde,
- Feststellungen sonstiger datenschutzrelevanter Sachverhalte.

Richtlinien über die Dokumentationspflichten insbesondere der Bereiche Revision, IT-Revision, IT-Sicherheit oder Qualitätsmanagement können diese Dokumentationspflichten allgemein oder auch branchen- und unternehmensspezifisch erweitern.

Der Datenschutzbeauftragte sorgt für einen angemessenen Schutz der ihm anvertrauten Informationen.

3.3.3. Zusammenarbeiten mit anderen internen Stellen

Der Datenschutzbeauftragte nutzt und unterstützt die gemeinsame Abstimmung von Prozessen, Aktivitäten und Terminen mit anderen internen Stellen und nutzt die Synergien. So sollte z.B. mit dem Qualitätsmanagement bei der Erstellung eines Handbuchs oder bei der Datenschutzorganisation sowie auch bei der Gestaltung und Durchführung von Audits zusammengearbeitet werden.

Darüber hinaus sucht er die Unterstützung durch weitere Stabsstellen und gegebenenfalls Beauftragte in der verantwortlichen Stelle (z.B. Revision, IT-Sicherheit, Qualitätsmanagement, Arbeitssicherheit), die bei der Wahrnehmung ihres Auftrages die Umsetzung der Datenschutzvorschriften besonders fördern oder berücksichtigen können. Diese Stellen können durch ihren jeweils speziellen Blick auf die Organisation den Datenschutzbeauftragten unterstützen und als Multiplikatoren wirken.

3.3.4. Informationsbeschaffung

Zur sachgerechten Erfüllung seiner Aufgaben nutzt der Datenschutzbeauftragte alle Aktivitäten zur Informationsbeschaffung. Bestehen im Unternehmen bzw. der Behörde Datenschutzkoordinatoren, sind diese in die Informationsbeschaffung einzubeziehen. Er fordert alle notwendigen Informationen von der Unternehmens- bzw. Behördenleitung ein. Er ist verpflichtet, Sachverhalte objektiv und umfassend aufzuklären; hierzu muss er die erforderlichen Wege der Informationsbeschaffung nutzen. Dazu gehören insbesondere das Führen von Gesprächen mit Jedermann, das Sichten von Archiven und Dokumenten sowie Recherchen im Internet.

3.3.5. Einbeziehung von Aufsichtsbehörden

Die Aufsichtsbehörde kann im Einzelfall zur Beratung, in Zweifelsfällen oder zur Klärung von Sachfragen durch den Datenschutzbeauftragten einbezogen werden, wenn die Möglichkeiten zur Klärung in der verantwortlichen Stelle nicht zum Erfolg geführt haben.

Ein Zweifelsfall liegt auch vor, wenn der Datenschutzbeauftragte feststellt, dass ihm wichtige Informationen fehlen und die Beschaffung von der Unternehmens- bzw. Behördenleitung nicht weiter unterstützt wird.

Beziehen sich die Zweifel auf die Vorabkontrolle, muss die Aufsichtsbehörde einbezogen werden.

Bei der Einbeziehung der Aufsichtsbehörde hat er darauf zu achten, über vertrauliche Vorgänge nur die erforderlichen Einzelheiten in der verantwortlichen Stelle kundzutun.

3.4. Weitere Aspekte der Berufsausübung

3.4.1. Haftung und Versicherungspflicht

Der Datenschutzbeauftragte haftet für die Richtigkeit seiner Beratung und Prüfungsergebnisse. Er haftet für Personen-, Sach- und Vermögensschäden, die er schuldhaft verursacht hat.

Vertragliche Haftungsbeschränkungen können vereinbart werden, sie bedürfen der Schriftform. Es ist zu berücksichtigen, dass ein vollständiger Haftungsausschluss rechtlich nicht möglich ist.

Der Datenschutzbeauftragte schließt eine Berufshaftpflichtversicherung zur Deckung der sich aus seiner Berufstätigkeit ergebenden Haftpflichtgefahren für Vermögensschäden ab und hält die Versicherung während der Dauer seiner Bestellung aufrecht; für den internen Datenschutzbeauftragten gelten übliche arbeits- oder dienstrechtliche Haftungsprivilegierungen.

3.4.2. Informationszugang

Der Datenschutzbeauftragte achtet darauf, dass er einen freien Informationszugang zu allen Unternehmens- bzw. Behördenbereichen inklusive des Zugangs zu den internen Netzwerken erhält und an innerbetrieblichen Kommunikations- und Informationsmitteln und -verteiltern beteiligt ist. Bei Bedarf fordert er dies ein.

3.4.3. Verschwiegenheit

Der Datenschutzbeauftragte ist zur Verschwiegenheit verpflichtet. Diese Pflicht bezieht sich auf alles, was ihm in Ausübung seines Berufes bekannt geworden ist. Dies gilt nicht für Tatsachen, die offenkundig sind oder ihrer Bedeutung nach keiner Geheimhaltung bedürfen.

Der zum Datenschutzbeauftragten Bestellte schweigt über die Einzelheiten von Beschwerden, Datenschutzverletzungen oder Informanten. Er behandelt die Identität der Beschwerdeführer vertraulich, sofern diese nicht ausdrücklich mit der Offenbarung ihrer Identität einverstanden sind.

Darüber hinaus ist er zur Verschwiegenheit über alle personenbezogenen Informationen sowie Amts-, Betriebs- und Geschäftsgeheimnisse, über die er während seiner Tätigkeit Kenntnis erlangt, verpflichtet. Dies gilt auch über das Ende seiner Tätigkeit als Datenschutzbeauftragter hinaus.

Beschäftigt der Beauftragte Mitarbeiter, so verpflichtet er diese zur gleichen Verschwiegenheit.

3.4.4. Organisatorische Einbindung

Der Datenschutzbeauftragte wirkt darauf hin, dass er in alle datenschutzrelevanten Gremien des Unternehmens- bzw. der Behörde eingebunden wird und dass er beim Bekanntwerden und in der Öffentlichkeitsarbeit unterstützt wird. Ist er nicht als Stabsstelle und im Organigramm ausgewiesen, fordert er dies ein.

3.4.5. Präsenz

Der Datenschutzbeauftragte soll seine Tätigkeiten überwiegend in dem Unternehmen bzw. der Behörde ausüben, das ihn bestellt.

3.5. Vertragliche Regelungen zur Berufsausübung

3.5.1. Allgemeine Vertragsregeln

Die Details der Ausübung vereinbart der zu Bestellende in einem Dienstvertrag mit dem Unternehmen bzw. der Behörde. In der vertraglichen Vereinbarung sollen neben der Beschreibung der Leistung die folgenden Punkte festgelegt werden:

- der zeitliche Aufwand für die Beauftragentätigkeiten,
- Art und Umfang der sachlichen Ausstattung (inkl. Arbeitsmittel),
- Art und Umfang der personellen Unterstützung,
- Ansprechpartner und unmittelbare Kommunikation zur Unternehmens- bzw. Behördenleitung,
- Budgetmittel und Reiseaufwendungen,
- evtl. Einschränkungen der Haftung.

Umfang und Detaillierungsgrad der Ausführungen können von der Größe des Unternehmens bzw. der Behörde abhängig gemacht werden.

3.5.2. Regeln zur Vermeidung von Benachteiligungen

Sofern der Datenschutzbeauftragte auch Beschäftigter des Unternehmens bzw. der Behörde ist, sollten auch die folgenden Punkte zur Vermeidung einer Benachteiligung geregelt werden:

- Die Weiterbeschäftigung, sofern die Bestellung zeitlich befristet ist oder durch Rücktritt endet,
- Weiterbildung/Fortbildung nach Ablauf der Bestellung,
- Gehaltsentwicklung,
- Kündigungsschutz,
- Verschwiegenheitspflichten.

Herausgeber:

Berufsverband der Datenschutzbeauftragten Deutschlands (BvD) e.V.

Budapester Strasse 31

10787 Berlin

fon: +49 30 21964397

fax: +49 30 21964392

mail: bvd-geschaefsstelle@bvdnet.de

www.bvdnet.de