



BVD Arbeitskreis
Berufsbild

DAS BERUFSBILD DES DATENSCHUTZBEAUFTRAGTEN

Kapitel 1: Aufgaben des Datenschutzbeauftragten

DAS BERUFSBILD DES DATENSCHUTZBEAUFTRAGTEN

**Kapitel 1:
Die Aufgaben des Datenschutzbeauftragten**



Die Aufgabenliste des Datenschutzbeauftragten wurde erarbeitet vom
Arbeitskreis „Berufsbild“ im Berufsverband der Datenschutzbeauftragten Deutschlands

An der Ausarbeitung haben mitgewirkt :

Marco Biewald, Dieter Ehenschwender, Heike Gehrke, Werner Hülsmann, Thomas Küpker, Ilse Römer, Roland Schäfer, Thomas Spaeing.

Für die zahlreichen Hinweise und Anregungen während der Ausarbeitung möchten wir uns bei allen BVD Mitgliedern recht herzlich bedanken.

Für weitere Fragen und Anregungen finden Sie Kontakt per E-Mail ak-berufsbild@biewald.de

Bamberg, 23.02.2007



1.1. Organisation der Arbeit des Datenschutzbeauftragten	4
1.1.1. Planung	4
1.1.2. Dokumentationsaufgaben	4
1.1.3. Personelle und sachliche Unterstützung	5
1.1.4. Zusammenarbeiten mit anderen internen Stellen	5
1.1.5. Informationsbeschaffung	5
1.1.6. Einbeziehung von Aufsichtsbehörden	5
1.2. Prüfungsaufgaben	6
1.2.1. Prüfungsmaßstäbe und -methoden	6
1.2.2. Prüfung von Geschäftsprozessen und Regelungen	6
1.2.3. Prüfung von IT Systemen	7
1.2.4. Verträge	7
1.2.5. Prüfung technischer und organisatorischer Maßnahmen	7
1.2.6. Prüfungen vor Einführung („Vorabkontrolle“)	8
1.2.7. Überprüfung von Beschwerden und Vorfällen	8
1.3. Gestaltungsaufgaben	8
1.3.1. Erstellung datenschutzrelevanter Unterlagen	8
1.3.2. Datenschutzkonzept	9
1.3.3. Sicherung der Betroffenenrechte	10
1.3.4. Aufklärungspflichten	10
1.4. Mitwirkung in Prozessen und Projekten der verantwortlichen Stelle	10
1.4.1. Beteiligungen	10
1.4.2. Stellungnahmen	10
1.4.3. Projektmitarbeit	11
1.5. Berichts- und Informationspflichten	11
1.5.1. Umfang und Grenzen	11
1.5.2. Unternehmens- bzw. Behördenleitung	11
1.5.3. Bereiche der verantwortlichen Stelle	11
1.5.4. Mitarbeitervertretung	12
1.5.5. Datenschutzaufsichtsbehörde	12
1.5.6. Tätigkeitsbericht	12
1.6. Schulungs- und Sensibilisierungsaufgaben	13
1.6.1. Schulungsinhalte	13
1.6.2. Zielgruppen	14
1.6.3. Sensibilisierungsmaßnahmen	14
1.7. Beratung	15
1.7.1. Beratungsmaßstab	15
1.7.2. Unternehmens- bzw. Behördenleitung	15
1.7.3. Bereiche, insbesondere Fachabteilungen	15
1.7.4. Betroffene	15
1.7.5. Mitarbeitervertretung	15
1.8. Qualitätssicherung der Aufgaben	16



Einleitung

Der Datenschutzbeauftragte wirkt auf die Einhaltung der Datenschutzbestimmungen hin. Aus dieser Hinwirkungspflicht ergeben sich zahlreiche Detailfragen, was im Einzelnen wie durch den Datenschutzbeauftragten zu tun ist. Die folgenden Ausführungen beschreiben die Aufgaben, die ein fachkundiger und zuverlässiger Datenschutzbeauftragter auszuführen hat. Der Datenschutzbeauftragte ist verpflichtet, die Aufgaben gewissenhaft und sachgerecht umzusetzen.

1.1. Organisation der Arbeit des Datenschutzbeauftragten

1.1.1. Planung

Der Datenschutzbeauftragte organisiert eigenverantwortlich seine Tätigkeit. Hierzu erstellt er eine Planung hinsichtlich der Durchführung der Tätigkeiten.

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 seine Aufgaben, Maßnahmen, Audits und Termine eigenverantwortlich. Der Plan gibt Auskunft über Ziele und Vorgehensweise sowie den Erledigungsstand der Aktivitäten zum Datenschutz in der verantwortlichen Stelle.

Darin sind die Prüfungs- sowie Tätigkeitsschwerpunkte darzustellen. Diese sind so weit wie möglich zu priorisieren und zu terminieren, ferner sind die geplanten personellen und sachlichen Aufwände sowohl für den Datenschutzbeauftragten als auch für andere in der verantwortlichen Stelle Beteiligte zu benennen.

Bei der Aktivitätenplanung sind ausreichende Reserven für aktuelle Entwicklungen zu berücksichtigen.

Insbesondere stellt der Datenschutzbeauftragte im Rahmen der Aktivitätenplanung jährlich eine Prüfungsplanung mit Angaben über die durchzuführenden Prüfungen auf. Darüber hinaus beinhaltet die Aktivitätenplanung Angaben über die erforderlichen Schulungen inklusive Schulungsthemen und Zielgruppen.

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

1.1.2. Dokumentationsaufgaben

Der Datenschutzbeauftragte dokumentiert seine Tätigkeiten.

Gegenstand der Dokumentation sind insbesondere die folgenden Tätigkeiten:

1. Aktivitätenplan
2. Schulungen, Sensibilisierungsmaßnahmen
3. Prüfungen
4. Tätigkeitsbericht
5. Beratungen
6. Stellungnahmen, Vorabkontrollen
7. Vorfälle und Beschwerden
8. Mitwirkung bei Richtlinien oder Betriebs- bzw. Dienstvereinbarungen
9. Gespräche und Schriftverkehr mit der Aufsichtsbehörde
10. sonstige Gesprächsergebnisse.

Ziel der Dokumentation ist die Nachvollziehbarkeit seiner Tätigkeit, insbesondere auch für eine etwaige Amtsübergabe an einen Nachfolger.

Bei der Dokumentation der Planung (1.) und von Schulungen (2.) muss erkennbar sein, ob der geplante Ressourceneinsatz bereits von der Unternehmens- bzw. Behördenleitung (Behördenleitung) getragen wird. So ist erkennbar, ob die Planungen der Unternehmens- bzw. Behördenleitung mit den Planungen des Datenschutzbeauftragten übereinstimmen oder voneinander abweichen. Der Aktivitätsplan dient als Grundlage der Dokumentation auch gegenüber der Aufsichtsbehörde.

Bei Schulungen (2.) werden diejenigen Schulungsinhalte dokumentiert, die über das Basiswissen hinausgehen. Außerdem werden die Teilnehmer namentlich festgehalten. Es wird festgelegt, wann eine Auffrischung voraussichtlich erforderlich wird. Bei Sensibilisierungsmaßnahmen kann die namentliche Dokumentation der Teilnehmer entfallen, wenn die Art der Veranstaltung dies so nicht zulässt (z.B. Mitarbeiterversammlung).

Soweit das Arbeitsergebnis seiner Tätigkeit bereits ein Dokument beinhaltet (4., 6., 8. und teilweise 3. und 9.) genügt es, dass dies in einer Dokumentenübersicht verzeichnet ist.

Gespräche sind in Protokollnotizen festzuhalten, (5., 7. und 10.; teilweise 3. und 9.). Prüfungen (3.) sind in einem Prüfungsbericht zu dokumentieren, der auch den Prüfungsanlass benennt.

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

1.1.3. Personelle und sachliche Unterstützung

Die vom Datenschutzbeauftragten benötigte sachliche und personelle Unterstützung fordert er von der Unternehmens- bzw. Behördenleitung ein. Er steuert das ihm zugeordnete Personal fachlich.

1.1.4. Zusammenarbeiten mit anderen internen Stellen

Durch die gemeinsame Abstimmung von Prozessen, Aktivitäten und Terminen mit anderen internen Stellen werden Synergien genutzt, die auch der Unternehmens- bzw. Behördenleitung dargestellt werden können; der Datenschutzbeauftragte nutzt und unterstützt solche Abstimmungsprozesse. 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.

Neben dem Datenschutzbeauftragten gibt es 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.

1.1.5. 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.

Stellt der Datenschutzbeauftragte fest, dass ihm wichtige Informationen fehlen und die Beschaffung von der Unternehmens- bzw. Behördenleitung nicht weiter unterstützt wird, so statuiert er einen Zweifelsfall.

1.1.6. Einbeziehung von Aufsichtsbehörden

Die Aufsichtsbehörde wird zur Beratung, in Zweifelsfällen oder zur Klärung von Sachfragen durch den Datenschutzbeauftragten einbezogen.

Zur Einholung von fachlichem Rat kann sich der Datenschutzbeauftragte jederzeit nach freiem Ermessen an die Aufsichtsbehörde wenden. Bei der Ratsuche hat er darauf zu achten, keine Einzelheiten über vertrauliche Vorgänge in der verantwortlichen Stelle kundzutun.

In Zweifelsfällen kann sich der Datenschutzbeauftragte an die Aufsichtsbehörde wenden, wenn die Möglichkeiten zur Klärung in der verantwortlichen Stelle nicht zum Erfolg geführt haben. Beziehen sich die Zweifel auf die Vorabkontrolle, muss die Aufsichtsbehörde einbezogen werden.

1.2. Prüfungsaufgaben

Der Datenschutzbeauftragte prüft die Verfahren und Geschäftsprozesse, die internen Regelungen und Verträge sowie die IT-Systeme (Prüfobjekte). Ein wichtiges Hilfsmittel der Prüfung ist die interne Verarbeitungsübersicht.

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

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

1.2.1. Prüfungsmaßstäbe und -methoden

Prüfungsmaßstäbe sind insbesondere:

- a. die Rechtskonformität,
- b. die anwendbaren IT-Sicherheitsnormen entsprechend dem Stand der Technik,
- c. Aktualität, Vollständigkeit und Richtigkeit,
- d. die internen 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 Sicherheitsnormen gehören u.a.:

- Regelungen des BSI IT-Grundschutz ("IT-Grundschutzhandbuch", seit 2005: "IT-Grundschutz-Kataloge"),
- Security Management nach ITIL (IT Infrastructure Library) und BS15000,
- ISO 27001
- Grundsätze ordnungsgemäßer DV-gestützter Buchführungssysteme (GoBS)
- weitere bereichsspezifische Normen, z.B. Basel II, S-OX

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.

1.2.2. Prüfung von Geschäftsprozessen und Regelungen

Der Datenschutzbeauftragte prüft die Datenschutzkonformität der Geschäftsprozesse sowie die Qualität, die praktische Umsetzung und den Umsetzungsgrad interner Regelungen. Ein wichtiges Hilfsmittel ist dabei die Dokumentation der Geschäftsprozesse und der angewendeten IT-Verfahren. Ein besonderer 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 (siehe Beteiligungen 1.4.1), so kann er eigene Prüfprozesse integrieren.

1.2.3. 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.

Prüfungsobjekte sind insbesondere:

- a. die Systemumgebung (wie die Netzwerke und die Datenübertragung),
- b. die eingesetzte Hardware und die Systemsoftware,
- c. Hard- oder Softwareschnittstellen, bei denen Daten übergeben werden
- d. Datenbanksysteme,
- e. Archivsysteme,
- f. Backupsysteme,
- g. Anwendersoftware (Standard- und Branchen-Software sowie eigen entwickelte Systeme)

- h. Telekommunikationssysteme und -netze,
- i. mobile IT- und Kommunikationsgeräte,
- j. Überwachungssysteme.

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

1.2.4. Verträge

Verträge sind an den Erfordernissen des Datenschutzes zu prüfen.

Diese Prüfung umfasst insbesondere die Prüfung von Verbraucher- und Kundenverträgen einschließlich der AGB's, von Mitarbeiter- und Beschäftigtenverträgen sowie Verträgen mit Dienstleistern.

Dabei sind bereits abgeschlossene Verträge und noch zu erstellende Verträge in die Betrachtung mit einzubeziehen.

Insbesondere bei Datenverarbeitung im Auftrag (z.B. § 11 BDSG) und bei Übermittlung (z.B. konzerninterne Weitergabe, „Einkauf“ und „Verkauf“) von personenbezogenen Daten sind die Verträge zu prüfen.

1.2.5. Prüfung technischer und organisatorischer Maßnahmen

Der Datenschutzbeauftragte prüft die Vollständigkeit, die Qualität sowie die Wirksamkeit der technischen und organisatorischen Maßnahmen zum Schutz der personenbezogenen Daten.

Er schlägt gegebenenfalls neue oder geänderte Maßnahmen vor. Der Umfang der Prüfung hängt dabei von der Komplexität der Organisation und deren Datenverarbeitung ab. Die zu überprüfenden Maßnahmen beziehen sich dabei im Wesentlichen auf die folgenden Kontrollbereiche:

- Organisationskontrolle
- Zutrittskontrolle
- Zugangskontrolle
- Zugriffskontrolle
- Weitergabekontrolle
- Eingabekontrolle
- Auftragskontrolle
- Verfügbarkeitskontrolle
- Zweckbindung und Trennungsgebot.

1.2.6. Prüfungen vor Einführung („Vorabkontrolle“)

Der Datenschutzbeauftragte prüft vor Einführung von Geschäftsprozessen oder IT-Systemen sowie bei Verfahren im Falle der Vorabkontrolle, ob insbesondere:

- a. die Zweckbestimmung und die Rechtsgrundlage der vorgesehenen automatisierten Verarbeitung folgende Punkte abdecken: ,
 - die Art der gespeicherten Daten- oder Datenkategorien,
 - die geplanten Übermittlungen oder Übertragungen,
 - die Zugriffsberechtigungen und
 - die Regelfristen zur Löschung
- b. die materiellen Datenschutzbestimmungen – auch unter dem Gesichtspunkt der Datenvermeidung und Datensparsamkeit - eingehalten werden,
- c. die Rechte der Betroffenen in der geplanten Verarbeitung gewahrt werden und auch technisch umsetzbar sind und
- d. die geplanten technischen und organisatorischen Maßnahmen zum Schutz der personenbezogenen Daten ausreichend und der jeweiligen Sensibilität der Daten angemessen sind.

1.2.7. 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 ist er verpflichtet, den Beschwerden ohne Verzögerung nachzugehen. Hierzu hat er den Sachverhalt umfassend aufzuklären und zu überprüfen. Am Ende der Prüfung hat er eine schriftliche Bewertung des Sachverhaltes zu erstellen. Sie ist dem Betroffenen umgehend mitzuteilen. Zuvor ist der verantwortlichen Stelle Gelegenheit zur Stellungnahme einzuräumen.

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.

1.3. Gestaltungsaufgaben

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

1.3.1. Erstellung datenschutzrelevanter Unterlagen

Der Datenschutzbeauftragte unterstützt die verantwortliche Stelle bei der Erstellung von Unterlagen, 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 Datenschutz Gesichtspunkten und erstellt bei Bedarf Verbesserungsvorschläge.

c.) Öffentliches Verzeichnisse („Verfahrensregister“)

Der Datenschutzbeauftragte unterstützt die verantwortliche Stelle bei der Erstellung des öffentlichen Verzeichnisses; hierbei holt er die notwendigen Angaben des IT-Bereichs bzw. des jeweiligen Fachbereiches ein.

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

Auf Antrag macht er die Angaben des 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).

d.) Interne Verarbeitungsübersicht

Der Datenschutzbeauftragte erstellt für seine Arbeit und für die verantwortliche Stelle eine interne Übersicht über alle Prozesse und Verwendungen mit personenbezogenen Daten. Dabei sind die Angaben eines Verzeichnisses sowie weitere Informationen über den Datenfluss, das Systemumfeld sowie über die Organisation und den Schutz der Datenverwendung zu dokumentieren.

e.) 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 im bzw. 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.

1.3.2. Datenschutzkonzept

Über die einzelnen Maßnahmenvorschläge hinaus erstellt der Datenschutzbeauftragte eine strukturierte Gesamtschau aller Maßnahmen unter Berücksichtigung der unternehmens- bzw. behörden-spezifischen 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.

1.3.3. 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 koordiniert und überwacht der Datenschutzbeauftragte die ordnungsgemäße Abwicklung.

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

1.3.4. Aufklärungspflichten

Der Datenschutzbeauftragte ist verpflichtet, auf eine umfassende Transparenz der Datenverarbeitung in der verantwortlichen Stelle und eine weit reichende Aufklärung über die Erhebung und Verarbeitung personenbezogener Daten hinzuwirken. Hierzu entwickelt er 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.

1.4. Mitwirkung in Prozessen und Projekten der verantwortlichen Stelle

Der Datenschutzbeauftragte wirkt bei der datenschutzgerechten Gestaltung von Betriebs- bzw. Behördenprozessen in unterschiedlicher Weise mit. Bei der Mitwirkung des Datenschutzbeauftragten werden zwei Arten von datenschutzrelevanten Prozessen unterschieden. Er sorgt für:

- die Initiierung der Prozesse zur Umsetzung des gesetzlichen Datenschutzes (z.B. Mitarbeiterverpflichtung, Mitarbeiterschulung, Datenschutzkontrollen).
- die Berücksichtigung der Datenschutzerfordernungen in Prozessen, die mittelbar den Datenschutz beeinflussen (z.B. Prozess Einführung neuer IT-Systeme, IT-Einkaufsprozess, Sicherheitsmanagement, Marketing).

1.4.1. Beteiligungen

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

- a. den Verhandlungen zwischen Unternehmens- bzw. Behördenleitung und Mitarbeitervertretung als Sachverständiger,
- b. der Festlegung von Kriterien bei der Investitionsplanung,
- c. der Gestaltung von IT Sicherheitsprozessen,
- d. IT Revisionsprozessen zur Wahrnehmung der Datenschutzkontrollaufgaben,
- e. der Einführung neuer IT-Systeme mittels Vorabkontrolle und Beratung
- f. 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 ein Prozess beratend oder prüfend begleiten, darf jedoch keine tragende Säule des Projektes werden.

1.4.2. 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 soll 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), soll die Stellungnahme zugleich Lösungsansätze (Maßnahmenvorschläge § 9 BDSG) enthalten.

Der Datenschutzbeauftragte trägt die Verantwortung für die Richtigkeit seiner Bewertung.

1.4.3. Projektmitarbeit

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

1.5. Berichts- und Informationspflichten

Der Datenschutzbeauftragte informiert und berichtet gegenüber internen Stellen. Dies geschieht regelmäßig oder anlassbezogen. Darüber hinaus informiert und berichtet er gegenüber externen Stellen anlassbezogen.

Adressaten sind insbesondere Unternehmens- bzw. Behördenleitung, Mitarbeitervertretungen, Aufsichtsbehörden, Betroffene und Dritte.

1.5.1. Umfang und Grenzen

Die Weisungsfreiheit des Datenschutzbeauftragten entbindet ihn nicht von der Berichtspflicht.

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.

1.5.2. 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. sowie über seine durchgeführten und geplanten Tätigkeiten als Datenschutzbeauftragter.

1.5.3. 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 zu den folgenden Bereichen entstehen:

- a. IT Abteilung
- b. IT-Revision
- c. Personalabteilung

- d. Qualitätsmanagement
- e. Vertrieb, Marketing
- f. branchenspezifische operative Bereiche

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

1.5.4. Mitarbeitervertretung

Im Bereich des Arbeitnehmerdatenschutzes informiert der Datenschutzbeauftragte unmittelbar die Mitarbeitervertretung über:

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

Die Informationspflicht gegenüber der Mitarbeitervertretung besteht nur dann nicht, wenn dadurch seine Arbeit erheblich beeinträchtigt wird. Die Mitarbeitervertretung hat gegenüber der Unternehmens- bzw. Behördenleitung ein Informationsrecht zum Arbeitnehmerdatenschutz in der verantwortlichen Stelle sowie über die diesbezüglichen Aktivitäten des Datenschutzbeauftragten.

1.5.5. 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 er verpflichtet, die Aufsichtsbehörde in Kenntnis zu setzen. Besonders schwerwiegend sind Verstöße, wenn

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

Darüber hinaus sollte er regelmäßig mit der Aufsichtsbehörde kommunizieren

- a. über bereits aktenkundige, die verantwortliche Stelle betreffende Vorgänge,
- b. wenn dies aus seiner Sicht für die Umsetzung des Datenschutzes in der verantwortlichen Stelle förderlich erscheint.

1.5.6. Tätigkeitsbericht

Unabhängig von den vorstehenden Kommunikationspflichten berichtet der Datenschutzbeauftragte durch einen regelmäßigen Tätigkeitsbericht gegenüber der Unternehmens- und Behördenleitung.

Der Tätigkeitsbericht dient

- a. der Information der Unternehmens- bzw. Behördenleitung,
- b. der revisionssicheren Dokumentation,
- c. als Aktivitätennachweis des Datenschutzbeauftragten,
- d. der Gewährleistung der ordnungsgemäßen Amtsübergabe beim Wechsel des Datenschutzbeauftragten,
- e. als Nachweis gegenüber der Aufsichtsbehörde,
- f. der Nachvollziehbarkeit und Messbarkeit der Datenschutzentwicklung in der verantwortlichen Stelle.

Der Bericht soll folgende Punkte enthalten:

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

Der Bericht sollte mindestens einmal im Jahr abgegeben werden, wenn nicht die Anforderungen in der verantwortlichen Stelle ein anderes Berichtsintervall verlangen.

1.6. 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.

Der Datenschutzbeauftragte überwacht 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.

1.6.1. Schulungsinhalte

Der Datenschutzbeauftragte vermittelt grundlegendes Basiswissen und Vertiefungswissen.

Zum Basiswissen gehören insbesondere:

- a. Begrifflichkeiten im Datenschutz
- b. Hintergründe und Entstehung
- c. Was ist Datenschutz, Prinzipien im Datenschutz
- d. Stellung und Aufgaben des Datenschutzbeauftragten
- e. Datenschutzorganisation des Unternehmens bzw. der Behörde
- f. Grundlagen der IT-Sicherheit

Das zu vermittelnde Vertiefungswissen umfasst insbesondere:

- a. Unternehmens- bzw. behördenspezifische Kenntnisse

- b. Zielgruppenspezifische Kenntnisse (z.B. Vertrieb, Marketing, aber auch Beauftragtenwesen wie Betriebsarzt)
- c. Beschäftigten-/Arbeitnehmerdatenschutz
- d. Kundendatenschutz
- e. Technische und organisatorische Maßnahmen zum Datenschutz

1.6.2. 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 ist 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.

1.6.3. Sensibilisierungsmaßnahmen

Neben der reinen Datenschutzeschulung bzw. über diese Schulung hinaus, ist der Datenschutzbeauftragte für die angemessene Sensibilisierung der Beschäftigte 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.



1.7. Beratung

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. Die Beratungspflicht gehört zur allgemeinen Hinwirkungspflicht.

1.7.1. Beratungsmaßstab

Der Datenschutzbeauftragte berät bei der Erstellung und Implementierung von technischen und organisatorischen Maßnahmen zum Datenschutz. Die Maßstäbe dafür sind:

- a. Wirksamkeit
- b. Wirtschaftlichkeit
- c. Praktikabilität
- d. Angemessenheit
- e. 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.

1.7.2. 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.

1.7.3. 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.

1.7.4. Betroffene

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.

1.7.5. 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.



1.8. Qualitätssicherung der Aufgaben

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 1.5).

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 Amtsübergabe.

Im Falle des Amtswechsels 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.