Roger Odenthal
Unternehmensberatung

(EDV-) Revision und personenbezogener Datenschutz

Roger Odenthal

Ergänzungen von Rolf-Dieter Wand

Vorwort

Die nachfolgenden Ausführungen richten sich an Mitarbeiter der in- und externen Revision, die häufig durch betriebliche Datenschutzbeauftragte gebeten werden, bestimmte Aspekte der Einhaltung von Datenschutz und -sicherheit zu prüfen. Die Vorgaben für die Prüfung sollten in einer Datenschutzrichtlinie des Unternehmens verankert sein.

Die Ausführungen sollen in aller Kürze einen ersten Überblick über Aufbau und Systematik des Bundesdatenschutzgesetzes sowie ableitbarer Prüfungsansätze vermitteln. Hierbei stehen die Anforderungen an die Privatwirtschaft im Vordergrund.

Keinesfalls ersetzt sie eine fundierte - juristische - Betrachtung des komplexen Themas oder beschäftigen sich mit „Zweifelsfragen“ des Datenschutzes. Derartige Betrachtungen, wie sie z.B. für einen betrieblichen Datenschutzbeauftragten notwendig sind, werden in einer Reihe guter, detaillierter Handbücher beschrieben, auf die an dieser Stelle verwiesen wird.

Roger Odenthal

Inhaltsverzeichnis

I Einführung

Diskussionen um den Schutz personenbezogener Daten folgen einer langen Tradition. Bereits der erstmalige großflächige Einsatz von EDV-Systemen zur Unterstützung der amerikanischen Volkszählung im Jahre 1928 auf der Basis der sogenannten Hollerith-Technik, führte zu Befürchtungen über die möglicherweise missbräuchliche Verwendung der erhobenen Informationen.

Mit der raschen Entwicklung der EDV-Technik bildeten sich hiernach auch gesetzliche Rahmenbedingungen für deren Einsatz heraus. Der Zusammenhang von EDV und Finanzbuchhaltung, wurde in Deutschland innerhalb des HGB sowie der Abgabenordnung geregelt. Für den Einsatz der EDV im öffentlichen Bereich, sind Vorschriften in den entsprechenden Haushaltsgesetzen sowie den Sozialgesetzbüchern vorhanden. Innerhalb des Strafgesetzbuches werden Verletzungen der Vertraulichkeit von EDV-aufbereiteten Daten sowie deren Verfälschung sanktioniert. Hierbei sind immer auch personenbezogene Daten, z.B. zu Kunden, Lieferanten, Personal, Patienten, etc. angesprochen. Ergänzt werden diese Regelungen durch ein Informationsschutzsystem in Form von rechtlich geschützten Geheimnissen wie z.B. die ärztliche Schweigepflicht, das Brief- Post- und Fernmeldegeheimnis, das Bankgeheimnis etc.

Eine zusammenfassende Regelung, die die Rechte des Einzelnen - über die beschriebenen Vorschriften hinaus - an seinen originären, personenbezogenen Daten formuliert, wurde zum 1. Februar 1977 als „Gesetz zum Schutz vor Missbrauch personenbezogener Daten bei der Datenverarbeitung (Bundesdatenschutzgesetz - BDSG)“ in Kraft gesetzt. Nachrangig sollte dieses Gesetz Tatbestände für den Umgang mit personenbezogenen Daten regeln, für die nicht bereits detailliertere Schutz- und Umgangsvorschriften existierten. Am 20.Dezember 1990 trat eine weitgehend überarbeitete Fassung dieses Gesetzes in Kraft. Diese wurde maßgeblich durch das Volkszählungsurteil vom 15. Dezember 1983 geprägt, in dem die informationelle Selbstbestimmung festgeschrieben wurde. Im Oktober 1995 wurde die sog. EU-Datenschutzrichtlinie von den Mitgliedsstaaten verabschiedet, die gemäß der Übereinkunft binnen drei Jahre in nationales Recht umgesetzt werden sollte. Es dauerte dann jedoch bis zum 18.05.2001 ehe die erneute Novellierung rechtskräftig wurde.

Der Wirkungsbereich des Bundesdatenschutzgesetzes (BDSG bezieht sich auf Unternehmen der Privatwirtschaft und auf bundeseigene Unternehmen sowie öffentlich-rechtliche Körperschaften, soweit sie dem Bund zuzuordnen sind.

Vorschriften für Landes- und Kommunalverwaltungen, landeseigene und kommunale Unternehmen sowie öffentlich-rechtlicher Körperschaften auf dieser Ebene, finden sich in den jeweiligen Landesdatenschutzgesetzen. Diese orientieren sich häufig am Wortlaut des BDSG, im Einzelfall gehen sie auch über dessen Regelung hinaus.

Die nachfolgenden weiteren Ausführungen beziehen sich -mit den Ergänzungen von Herrn Wand- auf das Bundesdatenschutzgesetz in der Fassung vom Mai 2001.

II Zweck- und Regelungsraum des BDSG

1 Ziel und Zweck des BDSG

Das Bundesdatenschutzgesetz

- ❏ *schützt* den Einzelnen *vor Verletzungen des Persönlichkeitsrechts durch die missbräuchliche Verwendung personenbezogener Daten*. Dieses umfasst im einzelnen das
  - Erheben, Speichern, Verändern, Übermitteln, Nutzen,

  solcher Daten,
- ❏ *regelt* die *Rechte der Betroffenen* auf
  - Auskunft sowie auf Berichtigung, Löschung, Sperrung und Schadenersatz bei (missbräuchlicher) Verwendung von zu seiner Person gespeicherter Daten,
- ❏ *regelt* die *Pflichten der verantwortlichen Stelle* im Hinblick
  - auf *Transparenz und Übersicht* der gespeicherten Informationen,
  - die vollständige *Benachrichtigung* der betroffenen Personen,
  - die *Sicherung* rechtmäßig gespeicherter und verarbeiteter Daten *vor unbefugtem Zugriff und unbefugter Nutzung*
- ❏ *legt* die notwendigen *Kontrollinstanzen* beim Einsatz personenbezogener Datenverarbeitung fest und gibt *Handlungsanweisungen zu Kontrollmaßnahmen*,
- ❏ *beschreibt* die *Folgen von Gesetzesverstößen* beim fahrlässigen oder missbräuchlichem Umgang mit personenbezogenen Daten.

Das BDSG ist ein sog. Auffanggesetz, d.h. es gelten die Vorschriften des Bundesdatenschutzgesetzes ausschließlich dann, wenn nicht vorrangige Rechtsvorschriften, z.B. zur Polizeiarbeit, zum Steuergeheimnis, zur Fernmeldeübermittlung, zur Buchführung o.ä. Bestimmungen enthalten, die Art und den Umfang der Verarbeitung personenbezogener Daten vorschreiben.

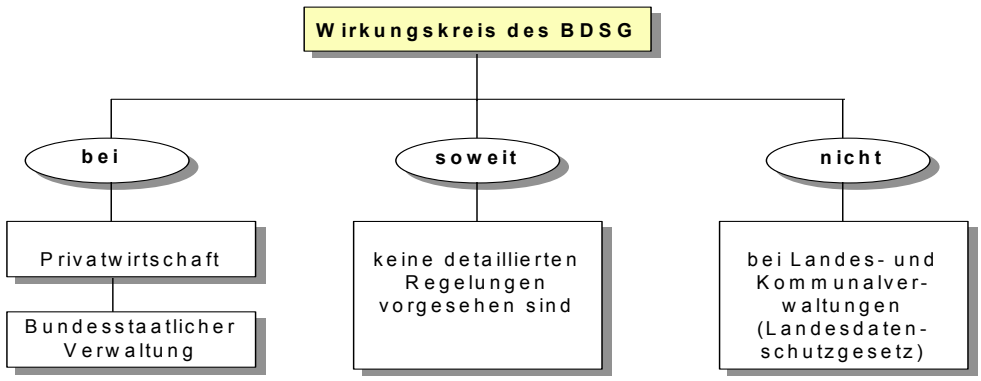

Bild 1 Wirkungskreis des BDSG

2 Navigation durch das Bundesdatenschutzgesetz

Das Bundesdatenschutzgesetz berücksichtigt die Unterschiede zwischen öffentlichen und nicht-öffentlichen Stellen und regelt Einzelheiten in jeweils gesonderten Gesetzesbereichen. Daneben werden grundlegende Dinge in einem allgemeinen Bereich geregelt und von dieser Systematik abweichende Vorgänge in Sondervorschriften behandelt. Dieses erschwert die Beantwortung von Fragen an den Datenschutz mit Bezug auf die jeweilige rechtliche Regelung. Die nachstehende - unvollständige - Übersicht soll die grundlegende Navigation innerhalb des Gesetzestextes erleichtern.

Regelungen / Fragen an das Gesetz	Allgemeiner Teil	Öffentliche Stellen	Nicht-öffentliche Stellen
1. Wann und für wen gelten die Regelungen des BDSG?	§§ 1, 2 BDSG	§ 12 BDSG	§ 27 BDSG
2. Was sind Daten im Sinne des BDSG?	§ 3 BDSG		
3. Wann ist die Verarbeitung, Nutzung, Speicherung und Übermittlung von Daten zulässig?	§ 4 BDSG	§ 13 - 16 BDSG	§ 28 - 31 BDSG
4. Datengeheimnis und Verpflichtung der Mitarbeiter	§ 5 BDSG		
5. Meldepflichten/Unterrichtungspflichten Abruf und Übermittlung von Daten	§ 10 BDSG	§ 16 BDSG	§ 28 Abs. 3 BDSG
6. Verarbeitung von Daten durch Externe im Auftrag	§ 11 BDSG		
7. Automatisierte Einzelentscheidung	§ 6a BDSG		
8. Videoüberwachung	§ 6b BDSG		
9. Mobile personenbezogene Speichermedien	§ 3 Abs.10 § 6c BDSG		
10. Vorabkontrolle bei der Verarbeitung kritischer Daten	§3 Abs. 9 BDSG § 4 d Abs. 5 BDSG		
11. Übermiitlung personenbezogener Daten ins Ausland	§ 4 b BDSG		
12. Rechte des Betroffenen			
❑ Auskunft	§ 6 BDSG	§ 19 BDSG	§ 34 BDSG
❑ Benachrichtigung	§ 6 BDSG	§ 16 Abs. 3 BDSG	§ 33 BDSG
❑ Berichtigung, Löschung, Sperrung von Daten	§ 6 BDSG	§ 20 BDSG	§ 35 BDSG

Regelungen / Fragen an das Gesetz	Allgemeiner Teil	Öffentliche Stellen	Nicht-öffentliche Stellen
❑ Einschaltung des Bundesdatenschutz-beauftragten		§ 21 BDSG	
13. Folgen bei Verstößen			
❑ Schadensersatz	§§ 7, 8 BDSG		
❑ Bußgeld	§ 43 BDSG		
❑ Strafen	§ 44 BDSG		
14. Technische und organi-satorische Maßnahmen zum Datenschutz	§ 9 BDSG und Anhang zu § 9 (8 Gebote)		
15. Dokumentationspflichten			
❑ Dateien	§ 9 BDSG Anhang 1	§ 18 Abs. 2 BDSG	§ 32 Abs. 2 Ziff. 6 BDSG § 38 Abs. 2 BDSG
❑ Verantwortlichkeiten	§ 9 BDSG Anhang 1	§ 18 Abs. 2 BDSG	§ 32 Abs. 2 BDSG
❑ Übermittlung	§ 9 BDSG Anhang 1		§ 29 Abs. 2 Ziff. 2 BDSG
❑ Eingabe/Änderung	§ 9 BDSG Anhang 1		
16. Überwachungsstellen			
❑ Bundesdatenschutz-beauftragter			
• Organisatorische Stellung		§§ 22, 23 BDSG	
• Betriebsmittel		§ 23 BDSG	
• Befugnisse		§§ 24, 25 BDSG	
• Meldepflichten, Verzeichnisse		§ 26 Abs. 5 BDSG	
❑ Betrieblicher Daten-schutzbeauftragter			
• Organisatorische Stellung		§ 18 Abs. 1, 2 BDSG	§ 4 f BDSG
• Betriebsmittel			§ 4 fAbs. 5 BDSG
• Befugnisse			§ 4 g BDSG
• Meldepflichten, Verzeichnisse			§ 4 g Abs. 2 BDSG
❑ Aufsichtsbehörden			
• Organisatorische Stellung			§ 38 Abs. 1 BDSG
• Befugnisse			§ 38 Abs. 4 BDSG
• Meldepflichten, Verzeichnisse			§ 38 Abs. 2 BDSG

Bild 2 Regelungsumfang des BDSG

3 Grundlagen des BDSG

3.1 Verarbeitung personenbezogener Daten

Die Vorschriften des Datenschutzgesetzes sind zweckgebunden. Sie beschäftigen sich nicht mit jeder Art von Daten, sondern nur mit der Verarbeitung „personenbezogener" Daten.

> *„... Zweck des Gesetzes ist es, den einzelnen davor zu schützen, daß er durch den Umgang mit seinen personenbezogenen Daten in seinem Persönlichkeitsrecht beeinträchtigt wird."*
>
> *Auszug aus § 1 Abs. 1 BDSG*
>
> *„...(1) Personenbezogene Daten sind Einzelangaben über persönliche oder sachliche Verhältnisse einer bestimmten oder bestimmbaren natürlichen Person (Betroffener)..."*
>
> *Auszug aus § 3 Abs. 1 BDSG*

Das Bundesdatenschutzgesetz betrachtet ausschließlich Daten über persönliche oder sachliche Verhältnisse einer bestimmten, bzw. bestimmbaren natürlichen Person.

Innerhalb dieses Rahmens ist der Datenkranz sehr weit gefasst. Er bezieht sich sowohl auf alle Merkmale zur Identifikation von Personen, wie z.B. Namen, Alter, Größe, Gewicht, Familienstand, als auch zu Merkmalen über seine persönlichen und geschäftlichen Verhältnisse, wie z.B. Vermögen, Grundbesitz, Mitgliedschaften, Automarken, aber auch Umsätze, Kosten, Wohnsitze u.ä. Dinge.

Wichtig ist in diesem Zusammenhang, daß es sich um eine natürliche und bestimmbare, also konkrete Person handeln muss.

Fügt man beide Komponenten, die Beschreibung über die personenbezogenen Daten sowie die Vorschrift über die natürliche Person zusammen, so ist sehr schnell erkennbar, daß in einem Unternehmen mit komplexer EDV-Landschaft eine Vielzahl von Daten zu den unterschiedlichsten Personenkreisen betroffen sein können.

Zunächst trifft dies sicherlich für das in einem Unternehmen beschäftigte *Personal* zu. Gleiches gilt allerdings auch für eine größere Anzahl von *Lieferanten und Kunden*. Betroffen sein können ferner Angehörige, Personen über die man schreibt oder Dossiers sammelt. Gleiches gilt für Informationen über *externe Zuarbeiter*, soweit deren Daten für Abrechnungs- oder Kostenrechnungszwecke benötigt werden.

Allein in dieser kleinen Zusammenstellung sind unterschiedlichste EDV-Applikationen, aus dem Personal- und Lohnbereich, der Auftragsabwicklung, Finanzbuchhaltung, Produktionsplanung und -steuerung, dem Vertrieb, Einkauf sowie dem Marketing involviert.

3.2 Einschränkungen bei der Verarbeitung personenbezogener Daten

Das Bundesdatenschutzgesetz soll den Einzelnen vor der unzulässigen Verarbeitung seiner personenbezogenen Daten schützen. Hierzu vermittelt das BDSG einige Grundsätze, die Diesem Sachverhalt Rechnung tragen:

- Datenvermeidung und Datensparsamkeit, § 3a BDSG.
- Pseudonymisieren und anonymisieren von personenbezogenen Daten (wenn möglich), § 3 Abs., 6 und 6a BDSG.
- Verbot der ausschließlichen automatisierten Einzelentscheidung, wenn für den Betroffenen daraus Nachteile entstehen können, § 6a BDSG.
- Erhebung von Daten nur im Rahmen der Zweckbindung, § 28 BDSG.

3.3 Verwendung personenbezogener Daten für geschäftliche Zwecke

Das Bundesdatenschutzgesetz begrenzt seinen Zuständigkeitsbereich auf die Verwendung personenbezogener Daten für berufliche, geschäftliche bzw. amtliche oder dienstliche Zwecke:

> *„... Soweit sie die Daten unter Einsatz von Datenverarbeitungsanlagen... es sei denn, ausschließlich für private oder familiäre Zwecke verarbeiten..."*
>
> *Auszug aus § 1 Abs. 2 Ziff. 3 BDSG*

Soweit jemand (auch innerhalb eines Unternehmens, wenn es gestattet ist) in einer von ihm genutzten Datei personenbezogene Daten (z.B. von Freunden und Angehörigen) ausschließlich zur privaten Verwendung (z.B. Geburtstagslisten) erfasst, greift das Bundesdatenschutzgesetz nicht. Ebenso gilt das Bundesdatenschutzgesetz nicht für Vereine, sofern sie kein Gewinnstreben verfolgen.

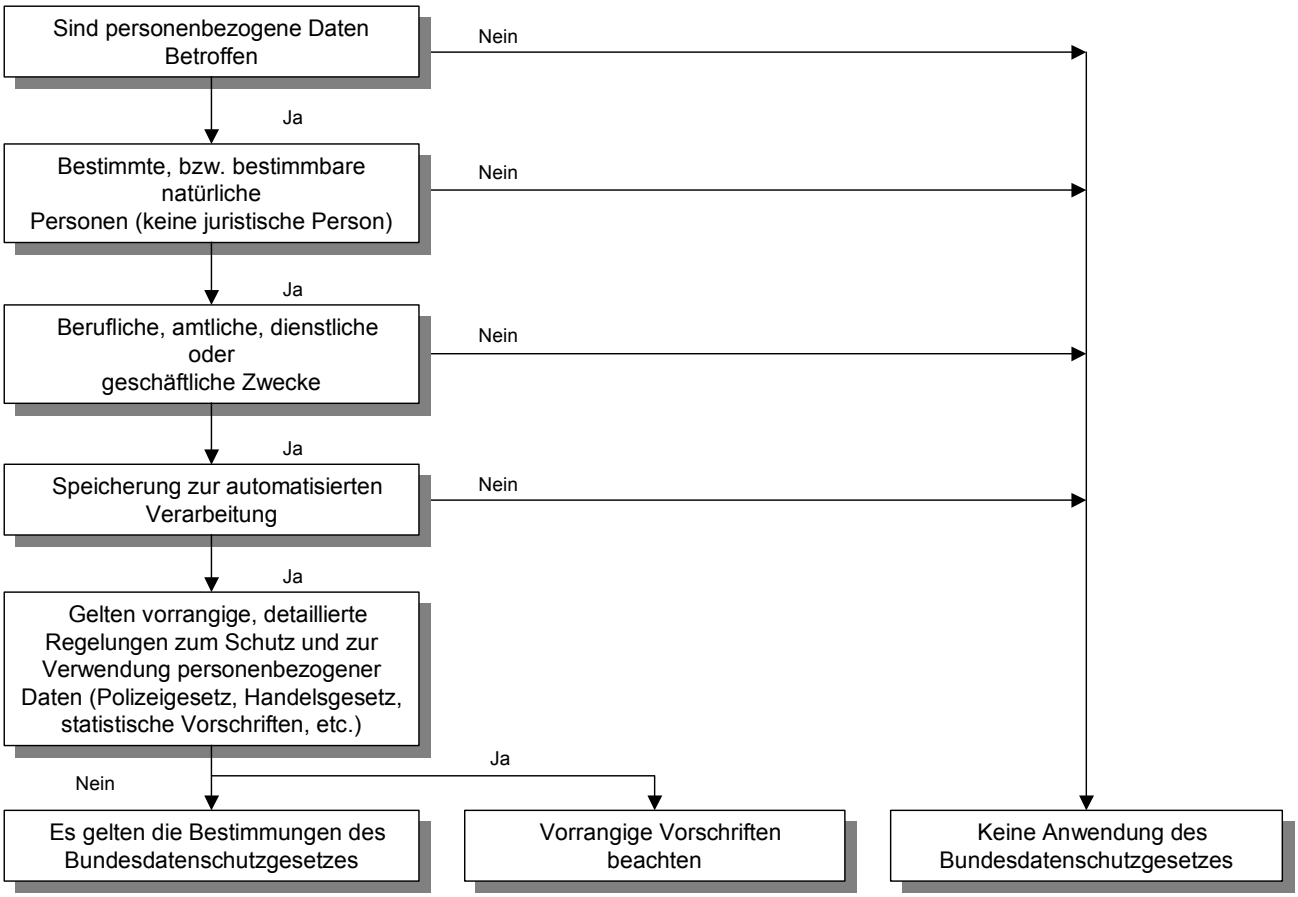

Bild 3 Voraussetzungen für die Anwendung des BDSG

Die Zulässigkeit personenbezogener Daten von nicht-öffentlichen Stellen ist – abweichend von der vorherigen Darstellung – gesondert zu prüfen.

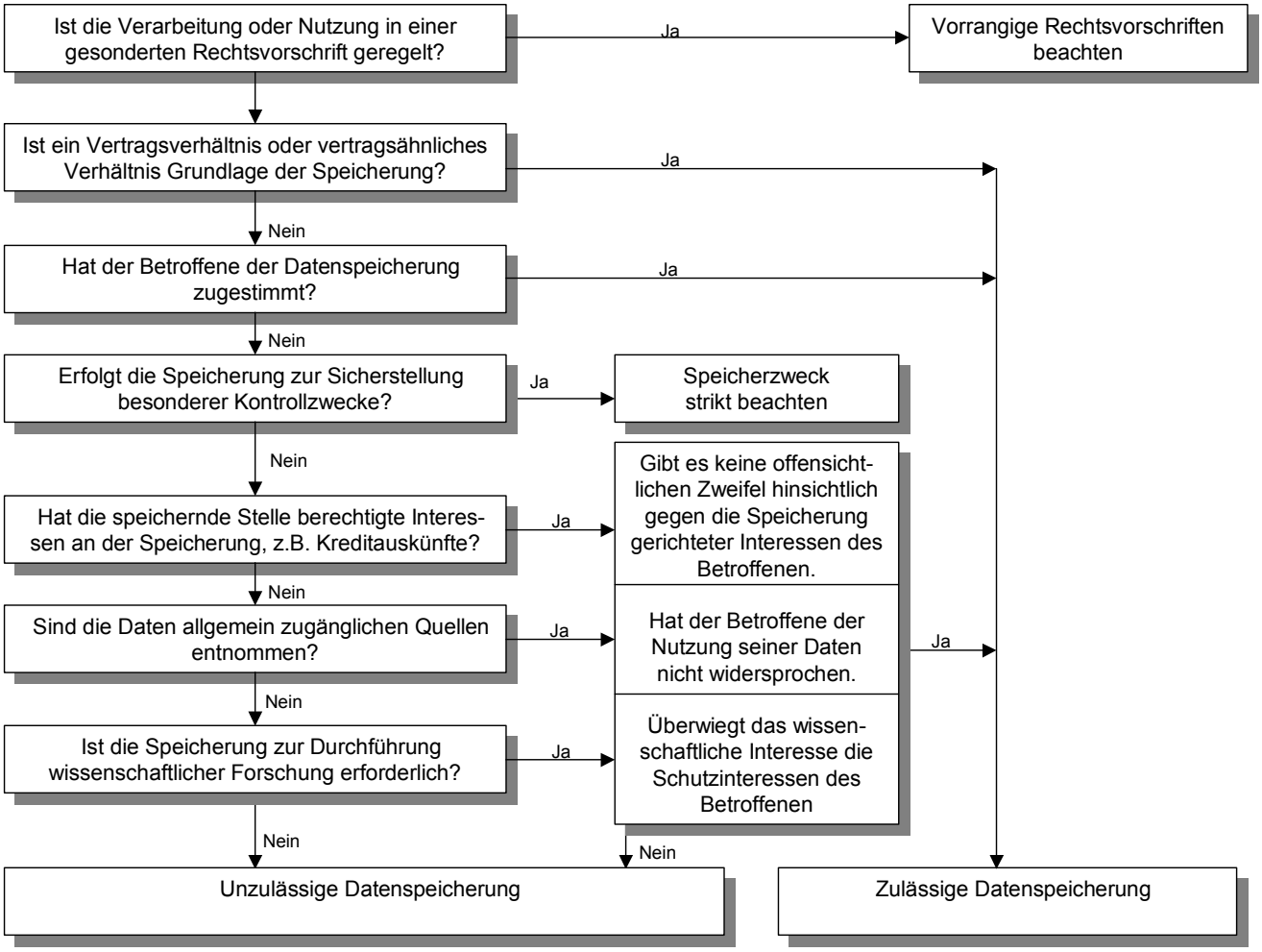

Bild 4 Zulässigkeit der Datenspeicherung nicht-öffentlicher Stellen

III Aufsichts- und Prüfungsorgane

1 Einführung

Das Bundesdatenschutzgesetz gibt verbindliche Regelungen für den Umgang mit personenbezogenen Daten vor und droht mit strafrechtlichen Konsequenzen bei deren Nichteinhaltung.

Die Verantwortung für die Einhaltung der formulierten Regelungen liegt bei den jeweiligen gesetzlichen Vertretern, also der Geschäftsführung bei privaten Unternehmen bzw. den Behördenleitern bei der öffentlichen Verwaltung. Für die Letzteren ist dies im Gesetz ausdrücklich festgehalten:

> *"...(1) Die obersten Bundesbehörden, der Präsident des Bundeseisenbahnvermögens sowie die bundesunmittelbaren Körperschaften, Anstalten und Stiftungen des Öffentlichen Rechts, über die von der Bundesregierung oder einer obersten Bundesbehörde lediglich die Rechtsaufsicht ausgeübt wird, haben für ihren Geschäftsbereich die Ausführung dieses Gesetzes sowie anderer Schutzvorschriften über den Datenschutz sicherzustellen. Das Gleiche gilt für die Vorstände der aus dem Sondervermögen Deutsche Bundespost durch Gesetz hervorgegangenen Unternehmen, ..."*
>
> *Auszug aus § 18 Abs. 1 BDSG*
>
> *"... Sie haben ferner dafür zu sorgen, daß die ordnungsgemäße Anwendung der Datenverarbeitungsprogramme, mit deren Hilfe personenbezogene Daten verarbeitet werden sollen, überwacht wird..."*
>
> *Auszug aus § 18 Abs. 2 BDSG*

Der Gesetzgeber stellt also zunächst - wie bei jedem anderen Gesetz auch - auf die mit einer Führungsfunktion verbundenen Eigenkontrolle sowohl in den Unternehmen, als auch in der Verwaltung ab. Daneben wurden mit dem Bundes- und den Länderbeauftragten für den Datenschutz, den betrieblichen Datenschutzbeauftragten und zusätzliche Aufsichtsstellen eine Reihe von Institutionen geschaffen, die über umfassende Kontroll- und Prüfungsberechtigungen verfügen.

2 Spezielle Aufsichts- und Prüfungsorgane

2.1 Verwaltung und öffentlich-rechtliche Unternehmen

2.1.1 Bundesverwaltung

Unabhängige Aufsichts- und Kontrollstelle für Fragen des Datenschutzes bei der Bundesverwaltung und für öffentlich-rechtliche Körperschaften bzw. Unternehmen, die hoheitliche Aufgaben des Bundes wahrnehmen, ist der Bundesbeauftragte für den Datenschutz.

> *"...(1) Der Bundesbeauftragte für den Datenschutz kontrolliert bei den öffentlichen Stellen des Bundes die Einhaltung der Vorschriften dieses Gesetzes und anderer Vorschriften für den Datenschutz..."*
>
> *"...(4) Die öffentlichen Stellen des Bundes sind verpflichtet, den Bundesbeauftragten und seine Beauftragten bei der Erfüllung ihrer Aufgaben zu unterstützen. Ihnen ist dabei insbesondere*
>
> *1. Auskunft zu ihren Fragen sowie Einsicht in allen Unterlagen und Akten, insbesondere in die gespeicherten Daten und in die Datenverarbeitungsprogramme zu gewähren, die im Zusammenhang mit der Kontrolle nach Absatz 1 stehen,*
>
> *2. jederzeit Zutritt in alle Diensträume zu gewähren...*
>
> *Auszug aus § 24 Abs. 1 BDSG (Öffentliche Stellen)*

Er kann Prüfungen vornehmen, wenn ihm Anhaltspunkte dafür vorliegen, daß Bestimmungen des Bundesdatenschutzgesetzes nicht eingehalten und von betroffenen Bürgern angerufen werden, die ihre Rechte bei der Verarbeitung personenbezogener Daten verletzt sehen.

2.1.2 Landes- und Kommunalverwaltung

Die Länder regeln, wie bereits ausgeführt, den Schutz personenbezogener Daten in eigenen gesetzlichen Bestimmungen. Dementsprechend gibt es,

- ausschließlich für die Verwaltung der Länder,
- für öffentlich-rechtliche Unternehmen, die der Länderebene zuzuordnen sind
- sowie Körperschaften und private Unternehmen, die hoheitliche Aufgaben der Länder und Kommunen ausführen,

mit den Länderbeauftragten für den Datenschutz gesonderte Kontroll- und Aufsichtsstellen.

> *„...(2) Dieses Gesetz gilt für die Erhebung, Verarbeitung und Nutzung personenbezogener Daten durch...*
>
> *2. Öffentliche Stellen der Länder, soweit der Datenschutz nicht durch Landesgesetz geregelt ist..."*
>
> *Auszug aus § 1 Abs. 2 Ziff. 2 BDSG*

2.2 Private Unternehmen

Bei *privaten Unternehmen steht die Eigenkontrolle im Vordergrund*. Die Verantwortung für die Einhaltung der Datenschutzbestimmungen liegt bei der Geschäftsführung. Darüber hinaus ist - sofern mindestens fünf Personen in die automatisierte Verarbeitung personenbezogener Daten involviert sind - ein betrieblicher Datenschutzbeauftragter zu bestellen.

> *„...(1) Die nicht-öffentlichen Stellen, die personenbezogene Daten automatisiert verarbeiten und damit i.d.R. mindestens fünf Arbeitnehmer ständig beschäftigen, haben spätestens innerhalb eines Monats nach Aufnahme ihrer Tätigkeit einen Beauftragten für den Datenschutz schriftlich zu bestellen...“*
>
> *Auszug aus § 4 Abs. 1 BDSG (Nicht-öffentliche Stellen)*

Zu den fünf aufgeführten Personen gehören hierbei sowohl beispielsweise die Mitarbeiter der Personalabteilung, die ständig Erfassungen vornehmen, als auch die zuständigen Mitarbeiter aus dem EDV-Bereich. Im Falle einer nicht-automatisierten Verarbeitung personenbezogener Daten ist ein betrieblicher Datenschutzbeauftragter dann zu bestellen, wenn sich mehr als zwanzig Mitarbeiter mit entsprechenden Arbeiten beschäftigen.

An Ausbildung, Erfahrung, organisatorische Zuordnung und Hilfsmittel werden darüber hinaus besondere Anforderungen gestellt, die ausdrücklich im Gesetz aufgeführt sind:

> *„...(2) Zum Beauftragten für den Datenschutz darf nur bestellt werden, wer die zur Erfüllung seiner Aufgaben erforderliche Fachkunde und Zuverlässigkeit besitzt....*
>
> *...(3) Der Beauftragte für den Datenschutz ist dem Leiter der nicht öffentlichen Stelle, unmittelbar zu unterstellen. Er ist bei Anwendung seiner Fachkunde auf dem Gebiet des Datenschutzes weisungsfrei...*
>
> *...(5) Die nicht-öffentliche Stelle hat den Beauftragten für den Datenschutz bei der Erfüllung seiner Aufgaben zu unterstützen und ihm insbesondere, soweit dies zur Erfüllung seiner Aufgaben erforderlich ist, Hilfspersonal sowie Räume, Einrichtungen, Geräte und Hilfsmittel zur Verfügung zu stellen...“*
>
> *Auszug aus § 4 f Abs. 2,3 und 5 BDSG*

Bei der Beurteilung der Fachkunde ist insbesondere darauf zu achten, daß er EDV-technische Sachverhalte unter juristischem Blickwinkel interpretiert und den jeweiligen gesetzlichen Tatbeständen zuordnen kann. Nützlich ist daher eine juristische Vorbildung bzw. die Erarbeitung entsprechender Kenntnisse in hierzu von zahlreichen Stellen angebotenen Seminaren.

Die organisatorische Zuordnung muss - soweit Datenschutzbelange betroffen sind - direkt unterhalb der Unternehmensleitung erfolgen. Darüber hinaus sollten Interessenskonflikte vermieden werden. So schließen sich z.B. die Rollen eines Leiters der EDV und die des Datenschutzbeauftragten aus, da sich hier häufig Interessenkonflikte ergeben.

Es ist nicht ausreichend, einen Datenschutzbeauftragten zu benennen, ihm müssen darüber hinaus seitens des Unternehmens die notwendigen Arbeitsmittel zur Verfügung gestellt werden. Benötigt er z.B Zugang zu den EDV-Applikationen mit denen personenbezogene Daten verarbeitet werden, so ist ihm dieser zu gewähren.

Er sollte über die notwendigen Zugriffsberechtigungen verfügen, um die Absicherung des Systems sowie die Zugriffsmöglichkeiten der einzelnen Anwender beurteilen zu können. Er muss darüber hinaus sowohl zeitlich als auch personell in der Lage sein, die für seinen Aufgabenbereich notwendigen Prüfungen selbst durchzuführen oder zu veranlassen.

Der Gesetzgeber ergänzt die Eigenkontrolle durch den betrieblichen Datenschutzbeauftragten durch eine zusätzliche Aufsichtsbehörde:

> *„...(1) Die Aufsichtsbehörde überprüft im Einzelfall die Ausführung des Gesetzes sowie anderer Vorschriften über den Datenschutz,...*
>
> *...(6) Die Landesregierung oder die von Ihnen ermächtigten Stellen bestimmen die für die Überwachung der Durchführung des Datenschutzes im Anwendungsbereich dieses Abschnittes zuständigen Aufsichtsbehörden...“*
>
> *Auszug aus § 38 Abs. 1 BDSG*

Die Benennung der Aufsichtsbehörde ist Ländersache. Dementsprechend sind recht unterschiedliche Institutionen mit der Aufsicht beauftragt. Häufig sind es die Landesbeauftragten für den Datenschutz sowie die Innenministerien oder regional nachgeordnete Verwaltungseinheiten, wie z.B. die Regierungspräsidenten.

Die Aufsichtsbehörde hat gemäß § 38 BDSG ein umfassendes Auskunfts- und Prüfungsrecht welches sie anlaßunabhängig wahrnehmen kann.. Ihr sind alle zur Erfüllung ihrer Aufgaben notwendigen Angaben zu machen. Sie kann zu den üblichen Betriebs- und Geschäftszeiten Überprüfungen in den Geschäftsräumen vornehmen und sich dort Aufzeichnungen relevanter Dateien und Programme zeigen lassen. Darüber hinaus ist sie - bei festgestellten Mängeln - berechtigt, technische und organisatorische Maßnahmen zur Beseitigung dieser Mängel anzuordnen oder, im ungünstigsten Fall, die Speicherung und Verarbeitung der personenbezogenen Daten zu untersagen.

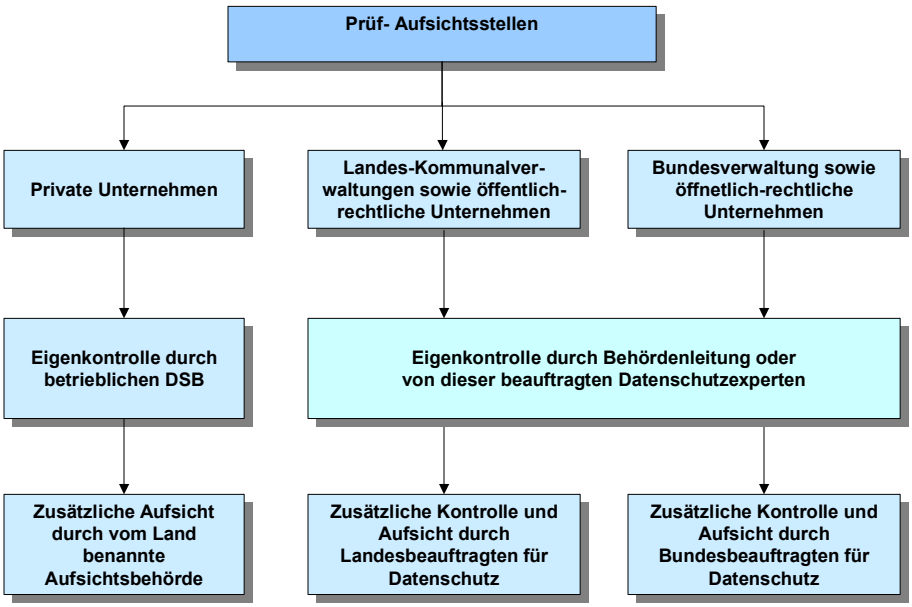

Bild 5 Zuständigkeiten der Prüf- und Aufsichtsbehörden

3 Sonstige Prüfungsstellen

Über die ausdrücklich im Gesetz aufgeführten Stellen hinaus gibt es weitere Institutionen, die sich - unter jeweils speziellem Blickwinkel - mit der Kontrolle von EDV-Verfahren beschäftigen.

❑ **Interne Revision**

Die Interne Revision hat eine umfassende Überwachungsaufgabe in den Unternehmen. Sie kontrolliert Funktionalität und Qualität des internen Kontrollsystems. Die hierfür zur Verfügung stehenden Werkzeuge, wie z.B. Funktionstrennung und Vier-Augen-Prinzip lassen sich, insbesondere bei komplexen, prozessorientierten EDV-Verfahren durch geeignete Einstellungen und Berechtigungen im EDV-System sicherstellen.

Im Rahmen ihrer Arbeit (EDV-Revision) beschäftigt sich die Interne Revision zwangsläufig auch mit Fragen des Daten- und Zugriffschutzes sowie der Einhaltung datenschutzrechtlicher Regelungen. Eine enge Abstimmung mit dem Datenschutzbeauftragten und eine Unterrichtung über die für ihn interessanten Prüfungsfeststellungen ist deshalb unerlässlich.

❑ **Wirtschaftsprüfer**

Die Wirtschaftsprüfung interessiert sich für das System der Bilanzerstellung sowie der hierzu führenden Finanzbuchhaltung. Erfolgt diese EDV-unterstützt, so sind die gesetzlichen Bestimmungen des Handelsgesetzbuches, der Abgabenordnung sowie die eindeutigen fachlichen Verlautbarungen der Berufsorganisation der Wirtschaftsprüfer (RS FAIT 1) und der Finanzverwaltung (GoBS) zu beachten. In diesem Zusammenhang interessiert sich der Wirtschaftsprüfer dafür, ob ein System ganz generell vor unberechtigtem Zugriff geschützt ist, ob die Daten ausreichend sicher und in guter Qualität gesichert und aufbewahrt werden, ob das vorhandene EDV-System vor Manipulationen schützt und ob es - z.B. aufgrund der vorliegenden Dokumentation - ausreichend prüfbar ist.

Eine Reihe der aufgezeigten Prüfungsinteressen und -ziele stimmen mit denen des Datenschutzbeauftragten überein. Insoweit sollte sich der Datenschutzbeauftragte über die Prüfungen und Feststellungen der Wirtschaftsprüfer informieren.

❑ **Rechnungsprüfer**

Für den Einsatz der Informationstechnik im Bereich öffentlich-rechtlicher Unternehmen sowie der Verwaltung wurden „Mindestanforderungen der Rechnungshöfe des Bundes und der Länder zum Einsatz der Informationstechnik - IT-Mindestanforderungen 1991 -“ formuliert. Mit deren Hilfe soll auch beim EDV-Einsatz ein funktionierendes internes Kontrollsystem sichergestellt werden. Die in den Mindestanforderungen formulierten Grundsätze zu den Bereichen Datenschutz und -sicherheit, Funktionstrennung, Prüfbarkeit u.ä. stimmen in Teilen mit den Prüfungszielen und -inhalten des Datenschutzbeauftragten überein. Daher ist ein enger Informationsaustausch sowie eine Abstimmung sinnvoll.

Es gibt weitere, hier nicht näher aufgeführte Prüfungsstellen, die sich mit der EDV unter Revisionsaspekten beschäftigen. Gleichlautende Forderungen an ein Prüfobjekt, die EDV, können sich somit aus den unterschiedlichsten gesetzlichen Bestimmungen ergeben.

Beispiel:	**Prüfungsanforderung nach einer organisatorischen Übersicht für den EDV-Bereich**
BDSG	*„...“die innerbehördliche oder innerbetriebliche Organisation so zu gestalten, daß sie den besonderen Anforderungen des Datenschutzes gerecht wird* *Auszug Anlage zu § 9 Satz 1 BDSG*
IT-Mindestanforderungen	*„...4.2.3 Die Abgrenzung und Zuweisung der Funktionen und Verantwortungsbereiche ist im einzelnen schriftlich festzulegen...“* *Auszug Ziff. 4.2.3 der IT-Mindestanforderungen der Rechnungshöfe*
RS FAIT 1	*„4.1. IT-Umfeld und IT-Organisation...“* *„... müssen Aufgaben, Kompetenzen und Verantwortlichkeiten der IT- Mitarbeiter klar definiert sein. Übliche Instrumente hierfür sind Prozess- und Funktionsbeschreibungen oder Organisationshandbücher ...“* *Auszug RS FAIT 1, Ziffer 4.1*
GoBS	*„...b) Die Zuständigkeit/Verantwortung für betriebliche Funktionen muss eindeutig geregelt sein...“* *Auszug aus Ziff. 4.4 Teil b GoBS*
Allg. Verwaltungsschrift über das Rechnungswesen in der Sozialversicherung SRVwV	*„...7. Die zur Sicherheit des Verfahrens zu erlassende Datenanweisung (§ 13 SVRwV) muss insbesondere Bestimmungen erhalten über die Abgrenzung von Verantwortungsbereichen im Bereich der automatischen Datenverarbeitung...“* *Auszug aus den SRVwV, sechster Abschnitt, § 37 Ziff. 7*

Bild 6 Zusammenwirken verschiedener Prüfungsanforderungen

IV Datenschutz und Anforderungen an die Unternehmen

1 Einführung

Die an die Unternehmen zu stellenden (und später zu prüfenden) datenschutzrechtlichen Anforderungen ergeben sich u.a. aus:

- ❑ **den Auskunftsrechten der Betroffenen**

  nach Art und Umfang der gespeicherten personenbezogenen Informationen, deren Herkunft und Weitergabe an Dritte,

- ❑ **der Pflicht speichernder Unternehmen**

  - auf Benachrichtigung der Betroffenen bei Datenspeicherung und -verarbeitung,
  - auf Auskunftserteilung sowie auf Meldung der gespeicherten Dateien an öffentliche Register,

- ❑ **den Rechten der Datenschutzbeauftragten sowie sonstiger Aufsichtsstellen**

  - nach umfassender und vorausschauender Unterrichtung geplanter EDV-Maßnahmen,
  - auf umfassende Prüfbarkeit und Dokumentation der personenbezogenen EDV-Verfahren,

- ❑ **Sorgfaltspflichten der speichernden Unternehmen**

  z.B. bei der Datenschutzverpflichtung von Mitarbeitern bei der Verarbeitung personenbezogener Daten

Darüber hinaus legt das Gesetz durch nachfolgende Forderung Unternehmen und der Verwaltung ausdrücklich auf,

> *„...öffentliche und nicht-öffentliche Stellen, die selbst oder im Auftrag personenbezogene Daten verarbeiten, haben die technischen und organisatorischen Maßnahmen zu treffen, die erforderlich sind, um die Ausführungen der Vorschriften dieses Gesetzes, insbesondere die in der Anlage zu diesem Gesetz genannten Anforderungen, zu gewährleisten...“*
>
> *Auszug aus § 9 BDSG*

dass alle notwendigen technischen und organisatorischen Maßnahmen zu treffen sind, um den angestrebten Schutzzweck zu erfüllen.

2 Einzelheiten zur Herleitung der Anforderungen an die Unternehmen

2.1 Aus den Auskunftsrechten hergeleitete Anforderungen

Dem von einer Speicherung personenbezogener Daten Betroffenen steht, unabhängig ob diese Speicherung von der öffentlichen Verwaltung oder privaten Unternehmen vorgenommen wird, ein umfassendes Auskunftsrecht zu.

„...(1) Dem Betroffenen ist auf Antrag Auskunft zu erteilen über

1. *die zu seiner Person gespeicherten Daten, auch soweit sie sich auf Herkunft oder Empfänger dieser Daten beziehen, und*
2. *den Zweck der Speicherung....“*

Auszug aus § 19 Abs. 1 BDSG (Öffentliche Stelle)

„...(1) Der Betroffene kann Auskunft verlangen über

1. *die zu seiner Person gespeicherten Daten, auch soweit sie sich auf Herkunft und Empfänger beziehen,*
2. *den Zweck der Speicherung und*
3. *Personen und Stellen, an die seine Daten regelmäßig übermittelt werden, wenn seine Daten automatisiert verarbeitet werden.*

Auszug aus § 34 Abs. 1 BDSG (Nicht-öffentliche Stellen)

Damit die speichernden Stellen dem Auskunftsbegehren nachkommen können, muss bekannt sein, welche personenbezogenen Daten in welchen Dateien vorhanden sind und an wen diese Daten übermittelt werden. Zumindest für den Bereich der personenbezogenen Daten ergibt sich daher an die speichernden Unternehmen die Anforderung, daß ein vollständiges und aktuelles Datenverzeichnis vorliegen muss, aus dem Art und Umfang der gespeicherten Informationen entnommen werden können.

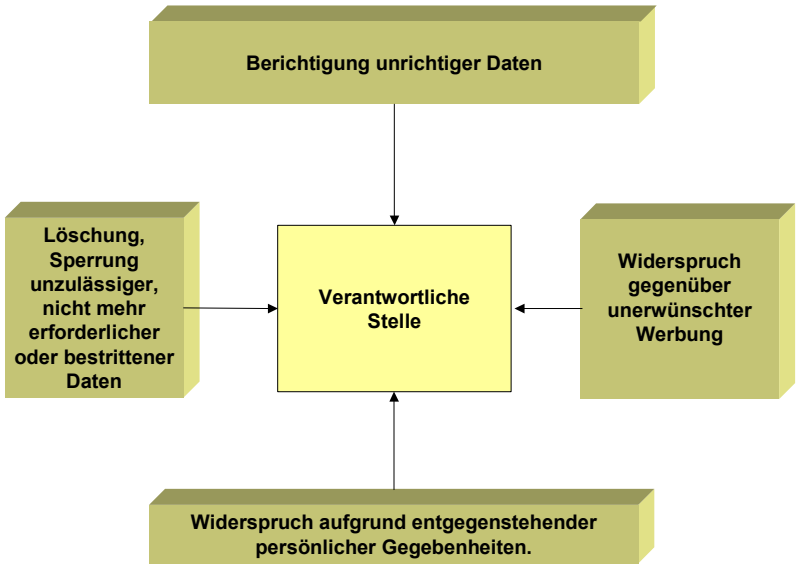

Bild 7 Übersicht über Rechte von einer Datenspeicherung Betroffener

2.2 Anforderungen aus Benachrichtigungs- und Auskunftserteilungspflichten

Die verantwortliche Stelle trifft nach den gesetzlichen Bestimmungen die Pflicht, den von der Speicherung personenbezogener Daten Betroffenen über die Datenspeicherung, -verarbeitung und -übermittlung zu unterrichten.

> *„...(1) Die Erhebung, Verarbeitung und Nutzung personenbezogener Daten ist nur zulässig, wenn dieses Gesetz oder eine andere Rechtsvorschrift sie erlaubt oder anordnet oder soweit der Betroffene eingewilligt hat...“*
>
> *Auszug aus § 4 Abs. 1 BDSG (Allgemeiner Teil)*
>
> *„...(1) Werden erstmals personenbezogene Daten für eigene Zwecke ohne Kenntnis der Betroffenen gespeichert, ist der Betroffene von der Speicherung und der Art der Daten zu benachrichtigen. Werden personenbezogene Daten geschäftsmäßig zum Zwecke der Übermittlung gespeichert, ist der Betroffene von der erstmaligen Übermittlung und der Art der übermittelten Daten zu benachrichtigen....“*
>
> *Auszug aus § 33 Abs. 1 BDSG (Nicht-öffentliche Stellen)*
>
> *„...(1) Die Übermittlung personenbezogener Daten an nicht-öffentliche Stellen ist zulässig, wenn ...*
>
> *....(2) der Empfänger ein berechtigtes Interesse an der Kenntnis der zu übermittelnden Daten glaubhaft darlegt und der Betroffene kein schutzwürdiges Interesse an dem Ausschluss der Übermittlung hat...*
>
> *....(3) In den Fällen der Übermittlung nach Abs. 1 Nr. 2 unterrichtet die übermittelnde Stelle den Betroffenen von der Übermittlung seiner Daten....“*
>
> *Auszüge aus § 16 Abs. 1 bis 3 BDSG (Öffentliche Stellen)*

Aus den Gesetzesbestimmungen geht hervor, daß, um der Benachrichtigungspflicht zu entsprechen, bekannt sein muss, an welchen Stellen und in welchen Dateien personenbezogene Daten gespeichert werden und an welche Stelle diese - auch innerhalb eines Konzerns - weitergegeben werden.

Neben diesen allgemeinen Vorschriften, aus denen bereits hergeleitet werden kann, daß zumindest bei einer Übermittlung eine Übersicht über Dateien mit personenbezogenen Inhalten sowie deren Empfänger vorhanden sein muss, gibt es Melde- und Dokumentationspflichten, die Art und Umfang solcher Verzeichnisse noch genauer darlegen:

> *„...(2) Die öffentlichen Stellen führen ein Verzeichnis der eingesetzten Verarbeitungsanlagen. Für Ihre automatisierte Verarbeitung haben sie die Angaben nach § 4e sowie den Zweck festzulegen.*
>
> *Auszug aus § 18 Abs. 2 BDSG (Öffentliche Stellen)*

Diese Vorschrift für die öffentlichen Stellen wird ergänzt durch eine Regelung für die privaten Unternehmen, die über einen Datenschutzbeauftragten verfügen:

> *„...(2) Dem Beauftragten ist von der verantwortlichen Stelle eine Übersicht zur Verfügung zu stellen die den Angaben in § 4 e entspricht..*

Um bei automatischer Übermittlung personenbezogener Daten Herkunft und Empfänger zu erkennen und die Sicherheit der Übertragung beurteilen zu können, bedarf es transparenter Schnittstellen. Damit zugriffsberechtigte Personengruppen oder allein zugriffsberechtigte Personen erkennbar werden, sollte ein Organigramm mit der Beschreibung von Verantwortlichkeiten zumindest für den EDV- und Personalbereich vorhanden sein.

2.3 Anforderungen aus den Rechten der Datenschutzbeauftragten sowie sonstiger Aufsichtsstellen

Die in der Verwaltung und in den Unternehmen für den Datenschutz zuständigen Personen haben ein Recht auf angemessene Unterstützung bei der Durchführung ihrer Aufgaben. Hierauf wurde an anderer Stelle bereits hingewiesen. Sie haben darüber hinaus einen gesetzlich festgelegten Anspruch, daß die EDV-Verfahren zur Verarbeitung und Übermittlung personenbezogener Daten ausreichend dokumentiert und prüfbar sind. Die Datenverarbeitungsprogramme mit deren Hilfe personenbezogene Daten verarbeitet werden, sind zu überwachen.

Um die Eigenkontrolle durch den betrieblichen Beauftragten für den Datenschutz in den nicht-öffentlichen Unternehmen zu stärken sind dessen Rechte noch umfassender und detaillierter formuliert. Auf das ihm zur Verfügung zu stellende Dateienregister wurde bereits eingegangen.

> *„...Er hat insbesondere*
>
> *1. die ordnungsgemäße Anwendung der Datenverarbeitungsprogramme, mit deren Hilfe personenbezogene Daten verarbeitet werden sollen zu überwachen; zu diesem Zweck ist er über Vorhaben der automatisierten Verarbeitung personenbezogener Daten rechtzeitig zu unterrichten,...“*
>
> *Auszug aus § 4 g Abs. 1 Satz 1 BDSG*

Aus den Prüfungsrechten des Datenschutzbeauftragten sowie sonstiger Aufsichtsstellen läßt sich ableiten, daß die EDV-Landschaft zur Verarbeitung personenbezogener Daten transparent und prüfbar sein muss und der Datenschutzbeauftragte bereits bei der Gestaltung entsprechender EDV-Verfahren einzubeziehen ist.

2.4 Anforderungen aus den Sorgfaltspflichten der speichernden Unternehmen

Sowohl die Verwaltung als auch private Unternehmen müssen sicherstellen, daß personenbezogene Daten nicht zweckentfremdet verarbeitet oder deren Inhalt unbefugt an Dritte weitergeben werden.

> *„...Den bei der Datenverarbeitung beschäftigten Personen ist untersagt, personenbezogene Daten unbefugt zu verarbeiten oder zu nutzen (Datengeheimnis). Diese Personen sind, soweit sie bei nicht-öffentlichen Stellen beschäftigt werden, bei der Aufnahme ihrer Tätigkeit auf das Datengeheimnis zu verpflichten. Das Datengeheimnis gilt auch nach Beendigung ihrer Tätigkeit fort....“*
>
> *Auszug aus § 5 BDSG (Öffentliche und Nicht-öffentliche Stellen)*

Dies wird ergänzt, durch eine Schulungs- und Informationsverpflichtung

„...(1) Der Beauftragte für den Datenschutz hat insbesondere ...

2. die bei der Verarbeitung personenbezogener Daten tätigen Personen durch geeignete Maßnahmen mit den Vorschriften dieses Gesetzes sowie anderer Vorschriften über den Datenschutz, bezogen auf die besonderen Verhältnisse in diesem Geschäftsbereich und die sich daraus ergebenden besonderen Erfordernisse für den Datenschutz vertraut zu machen,

Auszug aus § 4 g Abs. 1 Satz 2. 2 BDSG

Mitarbeiter, die sich mit personenbezogenen Daten beschäftigen, sind über deren besondere Schutzbedürftigkeit sowie über die Anforderung dieses Gesetzes zu unterrichten. Dies kann im Rahmen von Seminaren erfolgen. Zusätzlich ist anzuraten, im nicht-öffentlichen Bereich sogar vorgeschrieben, die Mitarbeiter schriftlich in Form einer abzuzeichnenden Verpflichtungserklärung von den Vorschriften des BDSG in Kenntnis zu setzen.

2.5 Technisch/Organisatorische Maßnahmen zur Einhaltung der Bestimmungen der Anlage des § 9 BDSG

Datenschutz hat zur Aufgabe, die personenbezogenen Daten einer natürlichen Person vor missbräuchlicher Verwendung zu schützen.

Datensicherheit dagegen ist der Schutz von Daten jeder Art, Hard- und Software vor Verlust, Zerstörung oder Missbrauch durch Unbefugte.

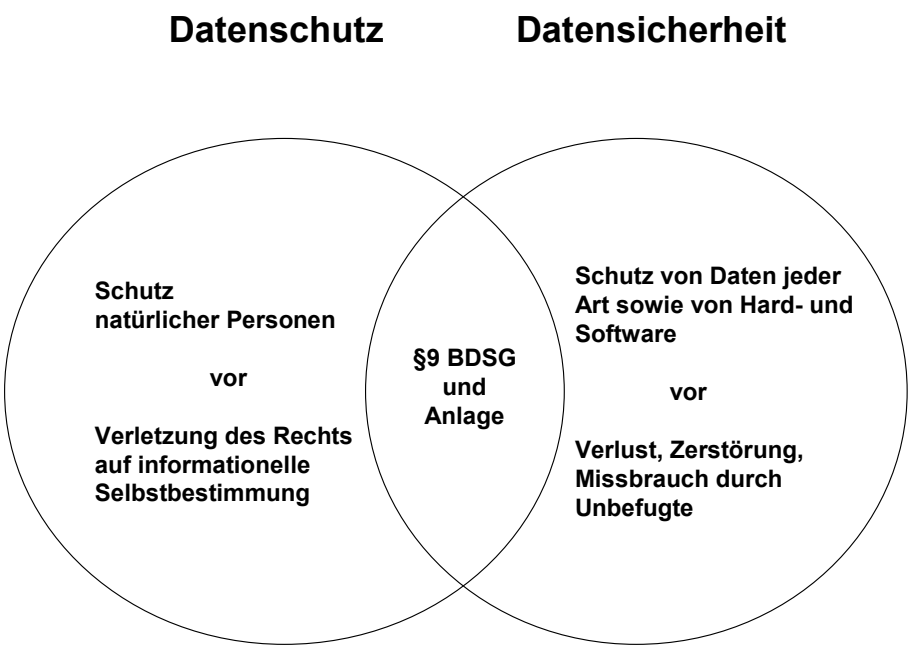

Bild 8 Beziehungszusammensetzung von Datenschutz- und Richtwert

Die Schnittmenge zwischen Datenschutz und Datensicherheit sind die Maßnahmen zur Sicherstellung der datenschutzrechtlichen Bestimmungen, die in der Anlage zum § 9 BDSG beschrieben sind.

Diese Anlage umfasst acht Unterpunkte, die im Folgenden erläutert werden.

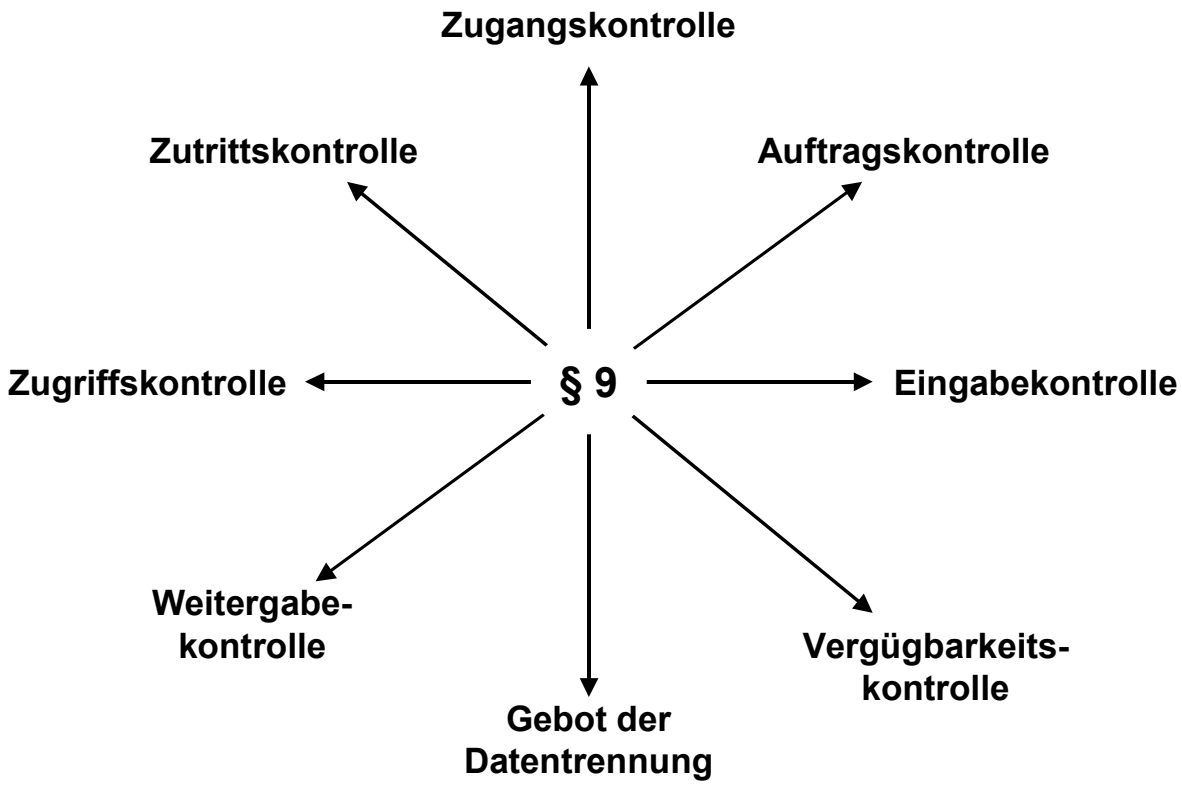

Bild 9 Übersicht über Anforderungen des BDSG

❏ **Zutrittskontrolle**

Die Zutrittskontrolle soll mit Hilfe geeigneter Maßnahmen sicherstellen, dass Unbefugten der Zutritt zu Gebäuden und Räumlichkeiten, in welchen personenbezogene Daten computergestützt verarbeitet werden, erschwert wird.

Besonderes Augenmerk ist hier auf den Zutritt zu Server- und Archivräumen sowie zu Administrationsarbeitsplätzen zu legen. Dies gilt ebenso für Räume, in denen zu vernichtendes Datenmaterial (Drucklisten, CDs, Mikrofilme, Festplatten etc.) zwischengelagert werden.

Einzelanforderungen:

- Festlegung der berechtigten Personen,
- Zutrittsregelungen für betriebsfremde Personen,
- Schaffung von Sicherheitszonen,
- Protokollierung der Zu- und Abgänge,
- Kontrolle der ausgegebenen Zugangsmittel,
- Revisionsfähigkeit der Vergabe und des Entzugs der Zutrittsberechtigungen.

❏ **Zugangskontrolle**

Eine wirksame Zugangskontrolle soll mit Hilfe geeigneter Maßnahmen verhindern, dass Unbefugte Datenverarbeitungssysteme, mit denen personenbezogene Daten verarbeitet werden, nutzen können.

Ziel ist eine sicherere Identifikation mit anschließender Authentifikation (Verifikation) des Nutzers. Die Zugangskontrollen erstrecken auf das Einschalten des informationstechnischen Gerätes und reichen bis zum Hochfahren des Betriebssystems. Sie umfassen nicht den Zugriff auf Applikationen, Daten oder periphere Geräte.

Einzelanforderungen:

- regelmäßige Kontrolle der Gültigkeit von Berechtigungen,
- Identifikation der Zugangsberechtigten durch geeignete Maßnahmen,
- Sicherung der Bildschirmarbeitsplätze bei Abwesenheit und laufendem System,
- sichere Verwahrung der personenbezogenen Identifikationsmedien,
- Abschottung interner Netze gegen Zugriffe von außen,
- Absicherung der Übertragungsleitungen und des Datenstroms.

❏ **Zugriffskontrolle**

Aufbauend auf die Zugangskontrolle (unbedingte Voraussetzung) wirkt die Zugriffskontrolle, bei der Mitarbeiter Rechte zum Zugriff auf Daten, Applikationen und Schnittstellen zugewiesen bekommen. Die Zugriffskontrolle soll verhindern, dass Unberechtigte Daten lesen, kopieren, verändern (incl. löschen) oder vom Datenträger entfernen können.

Einzelanforderungen:

- Absicherung der Bereiche, in denen Datenträger aufbewahrt werden,
- Verwendung von Benutzerkennungen,
- Identifikation und Authentifizierung der Benutzer,
- maschinelle Überprüfung der Berechtigungen,
- zeitliche Begrenzung der Zugriffsmöglichkeiten,
- Protokollierung der Benutzer und ihrer Aktivitäten,
- Protokollierung des Zugriffs auf bestimmte Dateien,
- Kontrolle der Aktivitäten der Systemadministration,
- Einsatz von Verschlüsselungsverfahren,
- Trennung von Test und Produktionsbetrieb,
- Abschottung interner Netze,
- datenschutzgerechte Entsorgung nicht mehr benötigter Datenträger.

❏ **Weitergabekontrolle**

Ziel der Weitergabekontrolle ist es, zu gewährleisten, dass personenbezogene Daten bei der elektronischen Übertragung oder während des Transports oder ihrer Speicherung auf Datenträgern nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können, und dass überprüft und festgestellt werden kann, an welcher Stelle eine Übermittlung personenbezogener Daten durch Einrichtungen zur Datenübertragung vorgesehen ist.

Einzelanforderungen:

- Festlegen der Übermittlungswege und der Datenempfänger,
- Dokumentation der Abruf- und Übermittlungsprogramme,
- Prüfung der Zulässigkeit einer Übermittlung,
- Protokollierung der Datenübermittlung und der Empfänger,
- Auswertungsmöglichkeiten der Übermittlungsprotokolle,
- Beauftragung zuverlässiger Transportunternehmen,
- Dokumentation des Transportweges,
- Verwendung verschließbarer Transportbehälter,
- Sicherung des Übertragungs- oder Transportweges,
- digitale Signatur,
- Einsatz kryptographischer Verfahren.

❏ **Eingabekontrolle**

Die Eingabekontrolle soll gewährleisten das nachvollzogen werden kann, wer, wann, welche personenbezogenen Daten in Datenverarbeitungssystemen eingegeben, verändert oder entfernt hat.

Einzelanforderungen:

- Führung revisionssicherer Zugriffsberechtigungen,
- Protokollierung von Eingabe, Veränderungen oder Löschungen personenbezogener Daten,
- Speicherung des Veranlassers und des Grundes einer Eingabe, Veränderung oder Löschung von personenbezogenen Daten,
- elektronische Signatur,
- lückenlose Vorgangsprotokollierung für jeden Einzelfall.

❏ **Auftragskontrolle**

Ziel der Auftragskontrolle ist es, zu gewährleisten, dass personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen des Auftraggebers verarbeitet werden können.

Einzelanforderungen:

- schriftlicher Vertrag,
- klare Abgrenzung der Kompetenzen zwischen Auftraggeber und Auftragnehmer,
- Definition von Sicherheitsmaßnahmen,
- gelegentliche Kontrolle der ordnungsgemäßen Vertragsausführung,
- Sanktionen bei Vertragverletzungen.

❏ **Verfügbarkeitskontrolle**

Die Verfügbarkeitskontrolle soll sicherstellen, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind.

Im Mittelpunkt steht ein vernünftiges Datensicherungskonzept, ergänzt um technische Vorkehrungen zur Verfügbarkeit, wie z.B. der Einsatz einer USV.

Einzelanforderungen:

- Durchführung einer Risiko- und Schwachstellenanalyse für den gesamten DV-Bereich,
- zentrale und einheitliche Beschaffung von Hard- und Software,
- formalisierte Freigabeverfahren für neue DV-Verfahren und bei wesentlichen Änderungen in Altverfahren,
- Einsatz geprüfter Fremdsoftware,

- Einsatz der Fernwartung,
- Erstellen eines Notfallhandbuches,
- Vorhandensein ausreichender Personalressourcen in der DV,
- Erlass von Sicherheitsrichtlinien.

❑ **Trennungskontrolle**

Besonderes Augenmerk sollte darauf gelegt werden, dass gewährleistet ist, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden können. Unter den Bedingungen moderner Datenbanktechnik ist dieses Gebot über Zugriffskontrollmechanismen umzusetzen.

Einzelanforderungen:

- klare innerbetriebliche Vorgaben für Datenerhebung und Verarbeitung,
- Verzicht auf integrierte Datenspeicherung,
- Dokumentation der verwendeten Datenbanken,
- Einrichtung logischer Datenbanken,
- eventuell physikalische Trennung von sensiblen Daten.

3 Zusammenfassung

Das Bundesdatenschutzgesetz stellt eine Reihe detaillierter Anforderungen an die Unternehmen, die durch geeignete organisatorische und technische Maßnahmen umzusetzen sind. Den speichernden Stellen stehen für deren Umsetzung eine Reihe von Alternativen zur Verfügung, die im Einzelfall zu prüfen sind. Erst eine *Gesamtschau und eine Würdigung aller getroffenen Einzelmaßnahmen* lassen einen zuverlässigen Schluss dahingehend zu, ob sie den Anforderungen dieses Gesetzes gerecht werden.

V Prüfungsansätze

1 Prüfungsfragen Zutrittskontrolle

Forderung	Ja	Nein	Teilweise
Festlegung der berechtigten Personen			
Zutrittsregelungen für betriebsfremde Personen			
Schaffung von Sicherheitszonen			
Protokollierung der Zu- und Abgänge			
Kontrolle der ausgegebenen Zugangsmittel			
Revisionsfähigkeit der Vergabe und des Entzugs der Zutrittsberechtigungen			

2 Prüfungsfragen Zugangskontrolle

Forderung	Ja	Nein	Teilweise
Regelmäßige Kontrolle der Gültigkeit von Berechtigungen			
Identifikation der Zugangsberechtigten durch geeignete Maßnahmen			
Sicherung der Bildschirmarbeitsplätze bei Abwesenheit und laufendem System			
Sichere Verwahrung der personenbezogenen Identifikationsmedien			
Abschottung interner Netze gegen Zugriffe von außen			
Absicherung der Übertragungsleitungen und des Datenstroms			

3 Prüfungsfragen Zugriffskontrolle

Forderung	Ja	Nein	Teilweise
Absicherung der Bereiche, in denen Datenträger aufbewahrt werden			
Verwendung von Benutzerkennungen			
Identifikation und Authentifizierung der Benutzer			
Maschinelle Überprüfung der Berechtigungen			
Zeitliche Begrenzung der Zugriffsmöglichkeiten			
Protokollierung der Benutzer und ihrer Aktivitäten			
Protokollierung des Zugriffs auf bestimmte Dateien			
Kontrolle der Aktivitäten der Systemadministration			
Einsatz von Verschlüsselungsverfahren			
Trennung von Test und Produktionsbetrieb			
Abschottung interner Netze			
Datenschutzgerechte Entsorgung nicht mehr benötigter Datenträger			

4 Prüfungsfragen Weitergabekontrolle

Forderung	Ja	Nein	Teilweise
Festlegen der Übermittlungswege und der Datenempfänger			
Dokumentation der Abruf- und Übermittlungsprogramme			
Prüfung der Zulässigkeit einer Übermittlung			
Protokollierung der Datenübermittlung und der Empfänger			
Auswertungsmöglichkeiten der Übermittlungsprotokolle			
Beauftragung zuverlässiger Transportunternehmen			

Forderung	Ja	Nein	Teilweise
Dokumentation des Transportweges			
Verwendung verschließbarer Transportbehälter			
Sicherung des Übertragungs- oder Transportwe-ges			
Digitale Signatur			
Einsatz kryptographischer Verfahren			

5 Prüfungsfragen Eingabekontrolle

Forderung	Ja	Nein	Teilweise
Führung revisionssicherer Zugriffs-berechtigungen			
Protokollierung von Eingabe, Veränderungen o-der Löschungen personenbezogener Daten			
Speicherung des Veranlassers und des Grundes einer Eingabe, Veränderung oder Löschung von personenbezogenen Daten			
Elektronische Signatur			
Lückenlose Vorgangsprotokollierung für jeden Einzelfall			

6 Prüfungsfragen Auftragskontrolle

Forderung	Ja	Nein	Teilweise
Schriftlicher Vertrag			
Klare Abgrenzung der Kompetenzen zwischen Auftraggeber und Auftragnehmer			
Definition von Sicherheitsmaßnahmen			
Gelegentliche Kontrolle der ordnungsgemäßen Vertragsausführung			
Sanktionen bei Vertragverletzungen			

7 Prüfungsfragen Verfügbarkeitskontrolle

Forderung	Ja	Nein	Teilweise
Durchführung einer Risiko- und Schwachstellen-analyse für den gesamten DV-Bereich			
Funktionstrennung zwischen Fachabteilung und DV			
Zentrale und einheitliche Beschaffung von Hard- und Software			
Formalisierte Freigabeverfahren für neue DV-Verfahren und bei wesentlichen Änderungen in Altverfahren			
Einsatz geprüfter Fremdsoftware			
Einsatz der Fernwartung			
Erstellen eines Notfallhandbuches			
Vorhandensein ausreichender Personal-ressourcen in der DV			
Erlass von Sicherheitsrichtlinien			
Systemüberwachung			

8 Prüfungsfragen Trennungskontrolle

Forderung	Ja	Nein	Teilweise
Klare innerbetriebliche Vorgaben für Datenerhebung und Verarbeitung			
Verzicht auf integrierte Datenspeicherung			
Dokumentation der verwendeten Datenbanken			
Einrichtung logischer Datenbanken			
Eventuell physikalische Trennung von sensiblen Daten			

VI Anlagen

Anlage 1	Muster Verpflichtungserklärung gemäß § 5 BDSG	
Anlage 2	Erhebungs- Meldungsbogen für die Verarbeitung personenbezogener Daten	
Anlage 3	Fallstudien:	Vorgaben bei der Implementierung eines gesetzeskonformen Datenschutzkonzeptes

Anlage 1 (1)

Muster Verpflichtungserklärung, Vorderseite

Verpflichtung gemäß § 5 BDSG

Sehr geehrte/r _____

Nach den Vorschriften des Bundesdatenschutzgesetzes (BDSG) gilt für Sie aufgrund Ihrer Aufgabenstellung § 5 des Gesetzes. Danach ist es Ihnen untersagt, geschützte personenbezogene Daten unbefugt zu erheben, zu verarbeiten oder zu nutzen.

Gemäß § 5 BDSG sind Sie verpflichtet, das Datengeheimnis zu wahren. Diese Verpflichtung besteht über das Ende der Tätigkeit in unserem Unternehmen hinaus.

Wir weisen darauf hin, dass Verstöße gegen das Datengeheimnis nach § 43 BDSG mit einem Bußgeld bis zu 250.000 € und unter Umständen nach § 44 BDSG und anderen Strafvorschriften mit Freiheits- oder Geldstrafe geahndet werden können.

Abschriften der hier genannten Vorschriften des Bundesdatenschutzgesetzes (§§ 5, 43, 44) sind beigefügt (s. Rückseite).

Ihre sich aus Dienstvertrag und Arbeitsordnung ergebende Geheimhaltungsverpflichtung wird durch diese Verpflichtung nicht berührt. Geben Sie bitte die beigefügte Zweitschrift dieses Schreibens nach Vollzug Ihrer Unterschrift an die Personalabteilung zurück.

Meine Verpflichtung auf das Datengeheimnis gemäß. § 5 des Bundesdatenschutzgesetzes habe ich zur Kenntnis genommen.

Mit der für meine Tätigkeit geltenden Datenschutzunterlagen wurde ich in schriftlicher Form / und während einer Datenschutzschulung am _____ bekannt gemacht.

_____ _____
Ort Datum

_____
Unterschrift des Mitarbeiters

Datenschutzbeauftragter ist

_____ Tel.:_____

Anlage 1 (2)

Muster Verpflichtungserklärung, Rückseite

§ 5
Datengeheimnis

Den bei der Datenverarbeitung beschäftigten Personen ist untersagt, personenbezogene Daten unbefugt zu erheben, zu verarbeiten oder zu nutzen (Datengeheimnis). Diese Personen sind, soweit sie bei nicht öffentlichen Stellen beschäftigt werden, bei der Aufnahme ihrer Tätigkeit auf das Datengeheimnis zu verpflichten. Das Datengeheimnis besteht auch nach Beendigung ihrer Tätigkeit fort.

§ 43
Bußgeldvorschriften

(1) Ordnungswidrig handelt, wer vorsätzlich oder fahrlässig

1. entgegen § 4d Abs. 1, auch in Verbindung mit § 4e Satz 2, eine Meldung nicht, nicht richtig, nicht vollständig oder nicht rechtzeitig macht,

2. entgegen § 4f Abs. 1 Satz 1 oder 2, jeweils auch in Verbindung mit Satz 3 und 6, einen Beauftragten für den Datenschutz nicht, nicht in der vorgeschriebenen Weise oder nicht rechtzeitig bestellt,

3. entgegen § 28 Abs. 4 Satz 2 den Betroffenen nicht, nicht richtig oder nicht rechtzeitig unterrichtet oder nicht sicherstellt, dass der Betroffene Kenntnis erhalten kann,

4. entgegen § 28 Abs. 5 Satz 2 personenbezogene Daten übermittelt oder nutzt,

5. entgegen § 29 Abs. 2 Satz 3 oder 4 die dort bezeichneten Gründe oder die Art und Weise ihrer glaubhaften Darlegung nicht aufzeichnet,

6. entgegen § 29 Abs. 3 Satz 1 personenbezogene Daten in elektronische oder gedruckte Adress-, Rufnummern-, Branchen- oder vergleichbare Verzeichnisse aufnimmt,

7. entgegen § 29 Abs. 3 Satz 2 die Übernahme von Kennzeichnungen nicht sicherstellt,

8. entgegen § 33 Abs. 1 den Betroffenen nicht, nicht richtig oder nicht vollständig benachrichtigt,

9. entgegen § 35 Abs. 6 Satz 3 Daten ohne Gegendarstellung übermittelt,

11. einer vollziehbaren Anordnung nach § 38 Abs. 5 Satz 1 zuwiderhandelt.

(2) Ordnungswidrig handelt, wer vorsätzlich oder fahrlässig

1. unbefugt personenbezogene Daten, die nicht allgemein zugänglich sind, erhebt oder verarbeitet,

2. unbefugt personenbezogene Daten, die nicht allgemein zugänglich sind, zum Abruf mittels automatisierten Verfahrens bereithält,

3. unbefugt personenbezogene Daten, die nicht allgemein zugänglich sind, abruft oder sich oder einem anderen aus automatisierten Verarbeitungen oder nicht automatisierten Dateien verschafft,

4. die Übermittlung von personenbezogenen Daten, die nicht allgemein zugänglich sind, durch unrichtige Angaben erschleicht,

5. entgegen § 16 Abs. 4 Satz 1, § 28 Abs. 5 Satz 1, auch in Verbindung mit § 29 Abs. 4, § 39 Abs. 1 Satz 1 oder § 40 Abs. 1, die übermittelten Daten für andere Zwecke nutzt, indem er sie an Dritte weitergibt, oder

6. entgegen § 30 Abs. 1 Satz 2 die in § 30 Abs. 1 Satz 1 bezeichneten Merkmale oder entgegen § 40 Abs. 2 Satz 3 die in § 40 Abs. 2 Satz 2 bezeichneten Merkmale mit den Einzelangaben zusammenführt.

(3) Die Ordnungswidrigkeit kann im Falle des Absatzes 1 mit einer Geldbuße bis zu fünfundzwanzigtausend Euro, in den Fällen des Absatzes 2 mit einer Geldbuße bis zu zweihundertfünfzigtausend Euro geahndet werden.

§ 44
Strafvorschriften

(1) Wer eine in § 43 Abs. 2 bezeichnete vorsätzliche Handlung gegen Entgelt oder in der Absicht, sich oder einen anderen zu bereichern oder einen anderen zu schädigen, begeht, wird mit Freiheitsstrafe bis zu zwei Jahren oder mit Geldstrafe bestraft.

(2) Die Tat wird nur auf Antrag verfolgt. Antragsberechtigt sind der Betroffene, die verantwortliche Stelle, der Bundesbeauftragte für den Datenschutz und die Aufsichtsbehörde.

Anlage 2 (1)

Muster einer Ersterhebung zur eingesetzten DV und Meldung an den Datenschutzbeauftragten

Frage	Antwort
1. Bezeichnung der Verarbeitung	
2. Betroffene Personengruppe	
3. Verantwortlicher Fachbereich/ Abteilung	
4. Zweck der Verarbeitung	
5. Daten oder Datenkategorien	
6. Empfänger oder Empfänger katagorien, denen die Daten mitgeteilt werden können	
7. Zugriffsberechtigungen	
8. Eingesetzte Hard- und Software	
9. Ort/Stelle der Datenverarbeitung	
10. Datensicherheitsmaßnahmen	
11. Stadium der Verarbeitung	
12. Löschungs- Aufbewahrungs- fristen	
13. Angaben zur eventuell notwendigen Vorabkontrolle	
14. Neue Verarbeitung oder Änderung	

Erläuterungen zu den einzelnen Fragen:

1 Bezeichnung der Verarbeitung

Name, unter der die Anwendung im Unternehmen bekannt ist.

2 Betroffene Personengruppen

Die, von der Datenverarbeitung betroffenen Personengruppen leiten sich aus den einzelnen Verfahren (Kunden-, Personal, Lieferanten, Handelsvertreterverwaltung, Interessentenbetreuung) ab.

3 Verantwortlicher Fachbereich / Abteilung

Wenn gewährleistet ist, dass die Zuordnung zum jeweiligen Unternehmen eindeutig ist, können in der internen Verarbeitungsübersicht die Angaben zur verantwortlichen Stelle unterbleiben (§ 4 e Nr. 1 - 3). Dafür ist die verantwortliche Fachabteilung (meist Auftraggeber der Verarbeitung) zu nennen.

4 Zweck der Verarbeitung

§28 (1) 1 Vertragsverhältnis oder vertragsähnliches Vertrauensverhältnis

- Auswahl-, Beurteilungs-, Scoringsysteme
- Antragsbearbeitung- und -entscheidung
- Zahlung / Abrechnung / Verbuchung
- Informations- und Steuerungssysteme
- Nachvertragliche Bearbeitung / Betreuung

§28 (1) 2 berechtigte Interessen der verantwortlichen Stelle

- Veröffentlichungen (z. B. Konzerntelefonbuch)
- Datenweitergabe im Konzern

§28 (3) 3 Werbung, Markt-/Meinungsforschung

- Direktmarketingaktionen
- Abgleichprogramme (z. B. interne Robinsonliste)
- Adressweitergabe

5 Daten oder Datenkategorien

- Zum gewünschten Zweck erforderliche Identifikations- und Adressdaten
- Vertragsstammdaten (Vertragsbeziehung, Produkt- bzw. Vertragsinteresse)
- Vertragsabrechnungs- und Zahlungsdaten
- Planungs- und Steuerungsdaten
- Auskunftsangaben
- Freiwillige Angaben des Betroffenen
- IT-Nutzungsdaten

6 Empfänger oder Empfängerkategorien

Empfänger oder Kategorien von Empfängern, welchen die Daten mitgeteilt werden können (speziell auch Auftragsdatenverarbeiter und Drittstaatenübermittlung!)

Konkrete Angaben zu beispielsweise folgenden Empfängern:

- *öffentliche Stellen*: z.B. Krankenkasse, Rentenversicherungsträger etc.
- *interne Stellen:* z.B. Vertrieb, Rechnungswesen etc.
- *Dienstleister:* z.B. Service-Rechenzentrum der A-GmbH, Fernwartung, Call Center, Help-Desk in B-Stadt, C-Land
- *externe Stellen (Bearbeitung säumiger Kunden):* z.B. Inkassobüro, Rechtsanwaltspraxis
- *Konzernunternehmen:* Bei den Empfängern sollte auch der Sitz (Standort, Land) angegeben werden.

7 Zugriffsberechtigungen

In Abhängigkeit vom eingesetzten DV-System sollte hier angegeben werden, welche *Berechtigungsprofile (Rollen)* existieren und in welchen Abteilungen diese zum Einsatz kommen. Diese Angabe sollen den DSB in die Lage versetzen, erkennen zu können, ob überall nur solche Berechtigungsprofile eingesetzt werden, die den Aufgaben der jeweiligen Abteilung gerecht werden.

- *Handelskundenbetreuung* (in Abt. Vertriebsinnendienst, Außendienst, ...)
- *Lieferantenbetreuung* (in Abt. Einkauf)
- *Lieferanteninformation* (in Abt. Einkauf, Revision, ...)

8 Eingesetzte Hard- und Software

- Art der eingesetzten DV-Anlagen (Konfigurationsübersicht, Netzwerkstruktur)

  DV-Anlagen sind alle eingesetzten Rechner (Host, Client, Server) sowie alle sonstigen physikalischen Komponenten.
- Betriebssysteme und Anwendungssoftware, spezielle Sicherheitssoftware

  Welches Programm, welcher Stand, welches Release ist im Einsatz

  Welche spezielle Sicherheitssoftware im Einsatz

9 Ort / Stelle der Datenverarbeitung

Beispiele

- Intern, in der Hauptverwaltung,
- in den Niederlassungen oder
- extern an anderen Orten von Auftragnehmern

10 Datensicherheitsmaßnahmen

- *Zutrittskontrolle*
  - zu Gebäuden und Räumlichkeiten.
- *Zugangskontrolle*
  - das Eindringen unbefugter in die DV-Systeme zu verhindern.
- *Zugriffskontrolle*
  - die unerlaubte Tätigkeit in DV-Systemen außerhalb eingeräumter Berechtigungen ist zu verhindern.
- *Weitergabekontrolle*
  - sämtliche Aspekte der Weitergabe personenbezogener Daten: elektronische Übertragung, Datentransport, Übermittlungskontrolle.
- *Eingabekontrolle*
  - Nachvollziehbarkeit, Dokumentation der Datenverwaltung und Pflege.
- *Auftragskontrolle*
  - Gewährleistung einer weisungsgemäßen Auftragsdatenverarbeitung.
- *Verfügbarkeitskontrolle*
  - Daten sind gegen zufällige Zerstörung oder Verlust zu schützen.
- *Trennungskontrolle*
  - Daten die zu unterschiedlichen Zwecken erhoben wurden, auch getrennt zu verarbeiten.

11 Stadium der Verarbeitung

- Planungs-/Einführungsphase,
- Testbetrieb,
- Produktivbetrieb,
- außer Betrieb,
- überführt in/abgelöst durch

Der Datenschutzbeauftragte ist bereits im Planungsstadium der Einführung neuer Verarbeitungen einzubeziehen (§ 4 g Abs. 1 Satz 3 Nr. 1 BDSG).

12 Löschungs- Aufbewahrungsfristen

- Im Hinblick auf die konkrete Verarbeitung sollten hier die durch die verantwortliche Fachabteilung vorgesehenen Löschungsfristen angegeben werden.
- Grundsätzlich sind personenbezogene Daten dann zu löschen, wenn sie für den konkreten Zweck zu dem sie gespeichert wurden, nicht mehr benötigt werden.
- Im Rahmen der allgemeinen Beschreibung der Sicherheitsmaßnahmen (zu § 9 BDSG Organisationskontrolle) können auch die Verarbeitungsroutinen, die das Löschen und Sperren von Daten in Dateien zum Gegenstand haben, erwähnt werden.

13 Angaben zur eventuell notwendigen Vorabkontrolle

Der Datenschutzbeauftragte benötigt Angaben, um feststellen zu können, ob eine automatisierte Verarbeitung der Vorabkontrolle überhaupt unterliegt.

- Notwendige Informationen
  - Vorliegen einer gesetzlichen Verpflichtung zur Datenverarbeitung
  - Vorliegen einer wirksamen Einwilligung des Betroffenen
  - Vorliegen eines Vertragsverhältnisses
  - Vorliegen eines vertragsähnlichen Vertrauensverhältnisses

Wenn eine der vorgenannten Voraussetzungen gegeben ist, ist eine Vorabkontrolle entbehrlich.

14 Neue Verarbeitung oder Änderung

Aus den Angaben muss hervorgehen, ob es sich um eine neue Verarbeitung oder eine Änderung einer bereits bestehenden Verarbeitung handelt.

Änderungen bestehender Verarbeitungen sind besonders zu kennzeichnen, wenn damit die beschriebenen

- Zwecke, Datenkategorien, Empfänger oder Zugriffsberechtigte

verändert werden.

Fallstudie: Implementierung eines gesetzeskonformen Datenschutzes im Unternehmen, Bestellung eines externen Datenschutzbeauftragten.

Vorgehensweise:

Die Vorgehensweise gliedert sich in drei Phasen, die im nachfolgenden beschrieben werden:

Phase 1 „Erhebung der Grundlagen“

Ziel:

Mit der Erhebung der Grundlagen soll ein Überblick über die eingesetzte Datenverarbeitung gewonnen werden. Verwendet werden für die Erhebung Fragebögen, die einen ersten Überblick vermitteln. Je Anwendungssystem oder auch Teilsystem wird ein Bogen benutzt.

In einem Folgeschritt werden die Anwendungssysteme klassifiziert.

Dies dient

- zur Ermittlung des Zwecks der Datenverarbeitung,
- zur Feststellung der Art der Daten, die verarbeitet werden (besonders schutzbedürftig?),

um daraus den Schutzbedarf der Daten abzuleiten.

Darauf aufbauen werden die in der Anlage zum § 9 BDSG geforderten Maßnahmen zur Einhaltung der

- Zutrittskontrolle,
- Zugangskontrolle,
- Zugriffskontrolle,
- Weitergabekontrolle,
- Eingabekontrolle,
- Auftragskontrolle,
- Verfügbarkeitskontrolle und
- Trennungskontrolle

geprüft und eventuell Vorschläge zur Verbesserung der Einhaltung der Bestimmungen des BDSG bei der Verarbeitung personenbezogener Daten formuliert.

Ferner wird in der Phase geprüft, inwieweit weitergehende Vorschriften zur Einhaltung der Bestimmungen des BDSG bereits umgesetzt sind.

Dazu gehört im Einzelnen:

- Verpflichtung der Mitarbeiter gemäß § 5 BDSG,
- Auskunftsverfahren gemäß § 34 BDSG,
- Anweidungen zur Auftragsdatenverarbeitung gemäß § 11 BDSG,
- Implementierung der Privacy Policy gemäß TDS und TDDSG beim Internetauftritt.

Damit sind die grundlegenden Arbeitsschritte erledigt; der Handlungsbedarf ist festgestellt.

Phase 2 „Umsetzung des festgestellten Handlungsbedarfs“

Ziel:

Abgeleitet aus dem Handlungsbedarf erfolgt nun die Umsetzung in die Einbindung des Datenschutzes in die Ablauforganisation.

Der grundlegendste Schritt in dieser Phase ist die Erstellung einer Datenschutzrichtlinie, in der die Regelungen zur Einhaltung der Bestimmungen des BDSG festgelegt werden. Aus dieser Richtlinie heraus werden wiederum Arbeitsanweisungen generiert, um in der täglichen Arbeit dem Datenschutz gerecht zu werden.

Beispiel: In der Datenschutzrichtlinie steht, dass alle Mitarbeiter bei ihrer Einstellung auf das BDSG gemäß § 5 verpflichtet werden müssen. Die Arbeitsanweisung dazu ergänzt das Einstellungsverfahren um die Schritte die notwendig sind, um die Ausführungen der Richtlinie in die Tat umzusetzen.

Die Phase 2 endet mit der

- Bestellung des externen Datenschutzbeauftragten,
- der Ernennung eines Mitarbeiters zum Datenschutzkoordinator, der sozusagen als Auge, Ohr und Hand des Datenschutzbeauftragten vor Ort fungiert und
- der Schulung der Mitarbeiter, die Umgang mit personenbezogenen Daten haben.

Phase 3 „laufender Betrieb“

Ziel:

Im laufenden Betrieb ist die Einhaltung der Bestimmungen des BDSG sicherzustellen.

Im laufenden Betrieb nimmt der externe Datenschutzbeauftragte zwei Rollen wahr. Einerseits erfolgt bei Bedarf eine Beratung innerhalb des laufenden Betriebes zu den unterschiedlichsten Themen, wie z.B.:

- Maßnahmen zur Einhaltung der technisch/organisatorischen Vorgaben aus der Anlage zu § 9 BDSG,
- Durchführung einer eventuell notwendigen Vorabkontrolle bei der Einführung neuer Verfahren,
- Unterstützung bei der Erteilung von Weisungen zur Auftragsdatenverarbeitung.

Andererseits wird eine Kontrollfunktion wahrgenommen, die sich durch Prüfung

- auf Einhaltung der Arbeitsanweisungen und Richtlinien im Unternehmen mit Bezug auf die Einhaltung des BDSG sowie
- durch eine Prüfung der Weisungen der Auftragsdatenverarbeitung bei Auftragnehmer

ausdrückt.

Anlage 5

Unternehmen und Mitarbeiter

- **ODENTHAL Dienstleistungen**
- **Aufsätze, Veröffentlichungen und Prüfleitfäden**
- **Ansprechpartner**

Anlage 5

ODENTHAL-Dienstleistungen

Neben der computergestützten Revision beschäftigt sich unser Unternehmen mit *betriebswirtschaftlicher Beratung und Prüfung im EDV- Umfeld*, die in nachfolgenden Übersichten beschrieben sind. Wir senden Ihnen diese auf Wunsch gerne zu.

- ❑ **ODENTHAL-Partner für die Interne Revision und Wirtschaftsprüfung**
- ❑ **Dienstleistungen in der EDV-Revision**
- ❑ **Dienstleistungen im SAP R/3™-Umfeld**
- ❑ **Projektbegleitende Prüfung bei einer SAP R/3™-Einführung**
- ❑ **Softwaretestate für Anwendungssysteme**
- ❑ **Methoden und Techniken zur Risikobeurteilung im IT-Bereich**
- ❑ **Vorgehensmodell für die Datenmigration auf neue EDV-Systeme**
- ❑ **Wirtschaftliche und ordnungsgemäße Datenarchivierung**
- ❑ **Vorbereitung und Begleitung von Outsourcing-Projekten**
- ❑ **IT-Verträge und deren Prüfung**

Anlage 5

Aufsätze, Veröffentlichungen und Prüfleitfäden

Nachfolgende Aufsätze, Veröffentlichungen und Prüfleitfäden unserer Mitarbeiter stellen wir Ihnen auf Wunsch gerne zur Verfügung:

Revision und **Zahlenanalyse,** WIK, Zeitschrift für Sicherheit der Wirtschaft, Ausgabe 3, Juni 2001
EDV-Beweissicherung bei Computerkriminalität, KES, Zeitschrift für Kommunikations- und EDV-Sicherheit, NR. 3, Juli 2001
Mit **Digitaler Ziffernanalyse** gegen **Unterschlagungen:** Ein Beitrag zu IT-gestützten Möglichkeiten zur Enttarnung von Mitarbeitern, WIK, Zeitschrift für die Sicherheit der Wirtschaft, Nr. 3, Juni 2001
Beweissicherung bei Computerkriminalität**,** **KES, Zeitschrift für Kommunikations- und EDV-Sicherheit, Ausgabe 3, Juli 2001**
EDV-Revision im Bereich des Rechnungswesens bei Einsatz von EDI und EDIFACT, Die Wirtschaftsprüfung, Nr. 15, 1995
KonTraG und (EDV-)Verfahrensprüfung, ZIR, Zeitschrift Interne Revision, Ausgabe 6/2000
Vorgehensmodell zur **Prüfung des Berechtigungswesens** in einer SAP R/3™ Umgebung, ZIR, Zeitschrift Interne Revision, Juni 2000, Ausgabe 3/2000
Verfahren und Instrumente zur **Aufdeckung wirtschaftskrimineller Handlungen,** Teil 1 – 2, RWZ, Zeitschrift für Recht und Rechnungswesen, 10/1999
Notfallstrategie für den Umgang mit **Mitarbeiterkriminalität,** Audit Journal, Heft 4, Dezember 1999
Digitale Ziffernanalyse: Ein Beitrag zur computergestützten Deliktrevision, WPg, Die Wirtschaftsprüfung, Der Berater der Wirtschaft, Heft 16, August 1999
Grundschutzhandbuch: Ein Werkzeug für die wirkungsvolle EDV-Revision? KES, Zeitschrift für Kommunikations- und EDV-Sicherheit, Ausgabe 2, Mai 1999
Wege und Verfahren zur **Prüfung doloser Handlungen** Zeitschrift Interne Revision, Hefte 5 und 6, Oktober und Dezember 1997
Verfahren für die EDV-Revision KES, Zeitschrift für Kommunikations- und EDV-Sicherheit, Ausgabe 6, Dezember 1997
Mit Software gegen Unterschlagungen, WIK, Zeitschrift für Wirtschaft, Kriminalität und Sicherheit, Nr. 4, August 1997, Zeitschrift „Sicherheit Forum“, Zürich, Nr. 6, November 1997
In Eigenregie auswerten: **SAP™-Standardlisten** KES, Zeitschrift für Kommunikations- und EDV-Sicherheit, Ausgabe 5, Oktober 1996
EDV-Revision in einer PC-**Netzwerkumgebung** Zeitschrift Datensicherheits-Report, Ausgabe 7, Juli 1996
File interrogation in a **SAP™-Host** environment Zeitschrift audit, Issue 34, London, Mai 1996
Unterschlagungsprüfung und –prophylaxe mit Hilfe von EDV-Unterstützung Zeitschrift „Deutsche Steuerrecht“, Nr. 12, März 1996
Prüfsoftware im **Vergleich** (Ein Überblick) Zeitschrift Interne Revision, Ausgabe 1, Februar 1996
Unterschlagung, **Detektivarbeit** am Bildschirm KES, Zeitschrift für Kommunikations- und EDV-Sicherheit, Ausgabe 1, Februar 1996

Anlage 5

Windows-Prüfleitfäden

- ❑ **Die Anwendung math.-statistischer Prüfungsmethoden**
- ❑ **Der Einsatz des SAP R/3™-AIS-Systems im Bereich der EDV-Systemprüfung sowie der kaufmännischen Revision**
- ❑ **EDV-Checkliste zur Ermittlung unterschlagungsgefährdeter Bereiche im Unternehmen**
- ❑ **Prüfung von Netzwerksystemen**
- ❑ **SAP™-R/3 Grundlagenprüfung**
- ❑ **Unterschlagungsprüfung und PC-Prüfsoftware**
- ❑ **EDV-Übersicht, Software für die Revision**
- ❑ **Grundlagen und Arbeitstechniken der internen Revision**
- ❑ **Betriebsprozesse in SAP-R/3™ und deren Prüfung**
- ❑ **Die Übernahme druckaufbereiteter Dateien in gängige PC-Prüfsoftware IDEA und ACL**

Anlage 5

Ihr Ansprechpartner:

Roger Odenthal

ROGER ODENTHAL Unternehmensberatung
Windmühlenstr. 159-161
51063 Köln

Telefon 0221-4924403
Telefax 0221-4921404

eMail info@roger-odenthal.de

Home: www.roger-odenthal.de

Roger Odenthal