



## Datenschutz-Prüfung von Rechenzentren

# **Datenschutz-Prüfung von Rechenzentren**

2015

## **GDD-Ratgeber Datenschutz-Prüfung von Rechenzentren**

**1. Auflage, 2015**

**Herausgeber:**

**Axel Moritz (CISA, CISM), Dipl.-Ing. Doris Wolf und die Gesellschaft für Datenschutz und Datensicherheit e.V.**

**Verfasser:**

**GDD-Erfa-Nord-Arbeitskreis „Prüfung von Rechenzentren“**

Dipl.-Ing. Holger Brand, Axel Moritz (CISA, CISM), Volker Nehrhoff, Dipl.-Math. Birgit Pauls, Marcus Pump, Dipl.-Inform. Peer Reymann B.Sc. (CISA), Dipl.-Inform. Curt-Jürgen Schädlich, Eric Schreiber, Uwe Steen, Carmen Ullrich, Dipl.-Ing. Berthold Weghaus (CISA), Dipl.-Ing. Doris Wolf

- Alle Rechte vorbehalten -

© 2015 Gesellschaft für Datenschutz und Datensicherheit e.V. (GDD)  
Heinrich-Böll-Ring 10 • 53119 Bonn

Telefon: (0228) 96 96 75-00

Telefax: (0228) 96 96 75-25

E-Mail: [info@gdd.de](mailto:info@gdd.de)

Internet: [www.gdd.de](http://www.gdd.de)

Nachdruck und Vervielfältigung jeder Art sind nur mit ausdrücklicher Genehmigung der GDD gestattet.

## Vorwort

Die Auslagerung von Datenbeständen und die Auslagerung von komplexen Datenverarbeitungen (IT-Outsourcing) an externe Rechenzentrumsanbieter haben sich zu einem gängigen Schritt in der Wirtschaft und in der Verwaltung entwickelt. Dabei sind Datenschutz und Datensicherheit für den Auftraggeber die Qualitätsmerkmale und für den Anbieter Wettbewerbsfaktoren.

Nun unterliegen Datenschutz, Datensicherheit und ordnungsgemäße Datenverarbeitung gesetzlichen Pflichten, die alle Unternehmen und Verwaltungseinheiten treffen, gleich welcher Größe und Branche. Das bedeutet für den Datenschutzbeauftragten eine große Herausforderung, da das Datenschutzmanagement der Datenauslagerung bzw. externen Datenverarbeitung lückenlos und vollständig abgearbeitet werden muss.

Es beginnt mit der Bestimmung des Schutzniveaus der Daten, der Bestimmung der Anforderungskriterien und mit der Freigabe eines ausgewählten Rechenzentrums. Wenn die Datenauslagerung bzw. die externe Datenverarbeitung begonnen hat, erfolgt die erste Kontrolle als Dokumentensichtung und/oder als Datenschutzaudit im Rechenzentrum vor Ort. Es folgen ausführliche Dokumentationen nicht nur an die verantwortliche Stelle, sondern auch Dokumentationen im Rahmen eines guten Anforderungsmanagements für spätere Kontrollen. Die Prüf- und Kontrollfragen sollen über den gesamten ausgelagerten Bereich sinnvoll und angemessen verteilt sein. Das Anforderungsmanagement mit den Kontrollen soll das anfänglich, vertraglich definierte und vereinbarte Schutzniveau widerspiegeln und zeigen, dass es für die Dauer des IT-Outsourcings aufrechterhalten wird.

Die 12 Autoren dieses Leitfadens haben diese Hilfestellung für sich und ihre Kolleginnen und Kollegen in ehrenamtlicher Arbeit als Arbeitskreis „Rechenzentrum“ des GDD-Erfa-Kreises Nord erarbeitet. Es ist die erste Zusammenstellung in dieser Qualität mit gut erklärten und tiefgreifenden Fragestellungen in den Checklisten.

Bonn, im Juli 2014

Der Vorstand der GDD

**Vorstand:** Prof. Dr. Rolf Schwartmann (Vorsitzender), Dr. Astrid Breinlinger, Prof. Dr. Rainer W. Gerling, Thomas Muthlein, Harald Eul, Heiko Kern, Gabriela Krader, Prof. Dr. Gregor Thüsing, Dr. Martin Zilkens, Gerhard Stampe, Prof. Peter Gola (Ehrenvorsitzender)



# Inhaltsverzeichnis

<b>Vorwort</b>	<b>3</b>
<b>Inhaltsverzeichnis</b>	<b>5</b>
<b>Einleitung</b>	<b>9</b>
<b>1. Grundlagen und Normen</b>	<b>11</b>
1.1 Rechtliche Vorgaben	12
1.1.1 Bundesdatenschutzgesetz (BDSG)	12
1.1.2 Landesdatenschutzgesetze (LDSG)	14
1.1.3 Strafgesetzbuch (StGB)	14
1.1.4 Sozialgesetzbuch (SGB)	15
1.1.5 Telekommunikations-Überwachungsverordnung (TKÜV)	16
1.1.6 Telekommunikationsgesetz (TKG)	17
1.1.7 Telemediengesetz (TMG)	17
1.1.8 Abgabenordnung (AO)	18
1.1.9 Betriebsverfassungsgesetz (BetrVG)	19
1.1.10 Handelsgesetzbuch (HGB)	19
1.1.11 Personalausweisgesetz (PersAuswG)	20
1.1.12 Grundsätze ordnungsmäßiger Buchführung (GoB)	21
1.1.13 Grundsätze ordnungsmäßiger DV-gestützter Buchführungssysteme (GoBS)	21
1.1.14 Grundsätze zum Datenzugriff und zur Prüfbarkeit digitaler Unterlagen (GDPdU)	21
1.1.15 Datenerfassungs- und -übermittlungsverordnung (DEÜV)	21
1.1.16 Kreditwesengesetz (KWG)	22
1.1.17 Steuerdaten-Übermittlungsverordnung (StDÜV)	22
1.1.18 Strafprozessordnung (StPO)	23

1.1.19	Versicherungsvertragsgesetz (VVG)	23
1.1.20	Zugangskontrolldiensteschutzgesetz (ZKDSG)	23
1.2	Technische und organisatorische Vorgaben	24
1.3	Einschlägige Normen für RZ-Sicherheit	24
1.3.1	Normierung der physischen IT-Sicherheit	25
1.3.2	Normierung der informationstechnischen Sicherheit	26
1.3.3	Normierung der organisatorischen Sicherheit	26
1.4	Selbstregulierung	27
<b>2.</b>	<b>Arten von Rechenzentren</b>	<b>30</b>
2.1	Definition Rechenzentrum	30
2.2	Ausstattungsmerkmale von Rechenzentren	32
2.3	Risikobehandlung in Rechenzentren	36
2.4	Betriebsorganisation von Rechenzentren	40
2.4.1	Prozesse in Rechenzentren	41
2.4.2	Unterstützende Systeme/datenhaltende Systeme eines RZ-Betreibers	43
2.5	Rechenzentrumsausprägungen - Eigenbetrieb/ Fremdbetrieb	44
2.5.1	Beschreibung Rechenzentrum, Eigenbetrieb	45
2.5.2	Beschreibung Rechenzentrum, Fremdbetrieb	46
2.5.3	Betriebsarten von Clouds	50
2.5.4	Beschreibung Rechenzentrum, Fremdbetrieb Cloud Computing	52
<b>3.</b>	<b>Anforderungsmanagement</b>	<b>55</b>
3.1	Definition der Begriffe „Anforderung“ und „Anforderungsmanagement“	55
3.2	Kriterien für Anforderungen	56
3.3	Themenbereiche des Anforderungsmanagements	59

3.3.1	Schutzbedarf	59
3.3.2	Schutzklassen	61
3.3.3	Die 8 Gebote (TOMs)	62
3.3.4	K.-o.-Kriterien	63
3.3.5	Personal	64
3.4	Typischer Schutzbedarf	66
3.5	Änderungsmanagement	68
3.6	Berücksichtigung der Anforderungen	69
<b>4.</b>	<b>Allgemeine Prüfpraxis</b>	<b>71</b>
4.1	Warum prüfen?	71
4.2	Was ist angemessen?	73
4.3	Prüfungen planen	74
4.4	Prüfungsablauf	75
4.4.1	Die Prüfungsvorbereitung	76
4.4.2	Die Durchführung	77
4.4.3	Dokumentenprüfung	78
4.4.4	Vor-Ort-Prüfung	80
4.4.5	Die Nachbereitung	81
4.4.6	Nachverfolgung und Maßnahmenkontrolle	82
4.4.7	Aufbau einer Prüfungsdokumentation	83
<b>5.</b>	<b>Anlagen</b>	<b>84</b>
	Tierklassifizierung gemäß Uptime Institut	84
	RZ-Organisation (Beispiel)	85
	Einschlägige Normen für RZ-Sicherheit	86
	Zertifizierungskriterien	97
	Begriffserläuterungen	101
	Abkürzungsverzeichnis	105



Quellen	111
Die Checklisten	113
Checkliste Organisation	115
Checkliste Zutrittskontrolle	125
Checkliste Zugangskontrolle	130
Checkliste Zugriffkontrolle	140
Checkliste Weitergabekontrolle	148
Checkliste Eingabekontrolle	153
Checkliste Auftragskontrolle	157
Checkliste Verfügbarkeitskontrolle	163
Checkliste Trennungskontrolle	168
Die Autoren	169
Satzung der GDD e.V.	176

Ausschließlich aus Gründen der Lesbarkeit haben wir in vielen Fällen auf eine Unterscheidung zwischen femininen und maskulinen Personenbezeichnungen verzichtet.

## Einleitung

Das Bundesdatenschutzgesetz fordert, dass sich Unternehmen, die personenbezogene Daten durch einen Auftragnehmer verarbeiten lassen, vor Beginn der Datenverarbeitung und sodann regelmäßig von der Einhaltung der beim Auftragnehmer getroffenen technischen und organisatorischen Maßnahmen überzeugen müssen (§ 11 Abs. 2 Satz 4 BDSG). Wenn es dann zu einer Auslagerung einer Datenverarbeitung kommt, wird die Prüfung des Rechenzentrums und der umgesetzten Maßnahmen zu einer nicht zu unterschätzenden Herausforderung für den Datenschutzbeauftragten.

Wie wird ein Rechenzentrum landläufig definiert? Als Rechenzentren bezeichnet man sowohl das Gebäude bzw. die Räumlichkeiten, in denen zentrale Rechentechnik einer oder mehrerer Unternehmen bzw. Organisationen untergebracht sind, als auch die Organisation selbst, die sich um diese Computer kümmern.<sup>1</sup>

Was sagt das Bundesamt für Sicherheit in der Informationstechnik (BSI) im IT-Grundschutzkatalog dazu? Als Rechenzentrum werden die für den Betrieb von komplexen IT-Infrastrukturen (Server- und Speichersysteme, Systeme zur Datensicherung, aktive Netzkomponenten und TK-Systeme, zentrale Drucksysteme usw.) erforderlichen Einrichtungen (Klimatechnik, Elektroversorgung, überwachende und alarmierende Technik) und Räumlichkeiten (z.B. Rechnersaal, Räume für die aktiven Netzkomponenten, Technikräume, Archiv, Lager, Aufenthaltsraum usw.) bezeichnet.<sup>2</sup>

Die Anwendungen werden immer komplexer und vernetzter. Moderne Technologien erfordern einen stark steigenden Betreuungsaufwand der Datenverarbeitungssysteme. Die gegenwärtige Entwicklung verlangt zunehmend größere Rechnerkapazitäten und damit größere Speichermöglichkeiten, die von Unternehmen nicht unbedingt selbst geleistet werden können oder auch nicht wollen. Die Folge ist, dass sehr oft auf

---

<sup>1</sup> <http://de.wikipedia.org/Rechenzentrum>.

<sup>2</sup> [https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/\\_content/baust/b02/b02009.html](https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/baust/b02/b02009.html).

externes Know-how sowie auf externe Ressourcen zurückgegriffen wird und immer mehr Datenbestände zu kompetenten Anbietern von Rechenzentren ausgelagert werden. In diesen Fällen den Datenschutz und die Datensicherheit zu bewerten, ist ein weites Feld. Datenschutzbeauftragte der Auftraggeber benötigen dazu eine Menge Erfahrung und ein umfassendes Fachwissen. Der vorliegende Leitfaden soll dabei unterstützen, das entsprechende Fachwissen aufzubauen oder zu erweitern.

Die Arbeitsgruppe Rechenzentrum des Erfa-Kreises Nord der GDD hat diesen Leitfaden „Datenschutz-Prüfung von Rechenzentren“ als Hilfestellung für die Kolleginnen und Kollegen, die ein Rechenzentrum prüfen müssen, entworfen. Wenn man anfängt, das Thema Datenschutzprüfung eines Rechenzentrums systematisch zu zerlegen, entstehen viele Blickwinkel und Themenbereiche. Die Umweltfreundlichkeit, die Arbeitsbedingungen und die Sicherheit für Beschäftigte eines Rechenzentrums werden in diesem Leitfaden nicht angesprochen. In diesem Leitfaden fokussieren wir uns auf eine Prüfung nach dem Bundesdatenschutzgesetz und hoffen damit, Datenschutzbeauftragten bei der Prüfung von Rechenzentren eine fundierte Arbeitshilfe zu geben. Die Prüfung eines Rechenzentrums, mit dessen Hilfe personenbezogene Daten erhoben, verarbeitet und genutzt werden, steht im Fokus der vorliegenden Arbeitshilfe. Der Leitfaden ist nicht abschließend und erhebt keinen Anspruch auf Vollständigkeit. Er dient als Orientierungshilfe, die im Einzelfall in Abhängigkeit der konkreten Beauftragung und der Kritikalität der zu verarbeitenden Daten noch angepasst werden kann.

Axel Moritz

Doris Wolf

## 1. Grundlagen und Normen

Die Einführung der elektronischen Speicherung von personenbezogenen Daten durch eine immer größer werdende Zahl von Unternehmen, Behörden oder Institutionen führte dazu, dass der Bürger nicht mehr erkennen konnte, was, wo und in welchem Umfang über ihn an Informationen bei wem vorhanden sind. Über das Volkszählungsurteil des Bundesverfassungsgerichtes (BVerfG) von 1983 trat dann das Recht auf informationelle Selbstbestimmung in den Vordergrund. Damit gewann auch das Datenschutzrecht an Gewicht und trat verstärkt in den Fokus der Öffentlichkeit. Der Grundsatz des „Verbots mit Erlaubnisvorbehalt“<sup>3</sup> manifestierte sich und sollte die Persönlichkeitsrechte der Bürger verbessern.

Grundsätzlich ist die Erhebung, Verarbeitung und Nutzung personenbezogener Daten also verboten. Erlaubt ist sie nur in Ausnahmefällen, wenn Rechtsvorschriften sie legitimieren oder wenn die Einwilligung des Betroffenen zur Erhebung, Verarbeitung oder Nutzung vorliegt.

Aus beiden Erlaubnistatbeständen leitet sich regelhaft auch eine konsequente Zweckbindung der Datenverwendung ab.

Insbesondere vor dem Hintergrund des in diesem Leitfaden thematisierten Prüffeldes sind die Berichtigungs-, Sperr- und Lösungsverpflichtungen als wichtige Pfeiler der Einhaltung der Datenschutzgesetzgebung anzusehen. Zu treffende technische und organisatorische Maßnahmen sollen zur Sicherheit der Verfahren beitragen und sind in vielen datenschutzrechtlichen Regelungen zu finden - insbesondere im § 9 BDSG und der Anlage dazu.

Mit den datenschutzrechtlichen Regelungen verbunden sind auch andere Ausprägungen des Persönlichkeitsrechts, wie z.B. das Fernmeldegeheimnis. Auch hier sollen sowohl die Inhalte einer Kommunikation als auch die zugehörigen Verbindungsdaten vor unbefugter Einsichtnahme geschützt werden. Ergänzend zum spezifischen Fernmeldeschutz greifen hier auch datenschutzrechtliche Vorschriften, da mit

---

<sup>3</sup> Vgl. etwa § 4 Abs. 1 BDSG, § 67b Abs. 1 Satz 1 SGB X.

dem Kommunikationsvorgang auch personenbezogene Daten erhoben, verarbeitet oder genutzt werden.

Zu nennen wäre noch das Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme (kurz: IT-Grundrecht). Dieser Schutz betrifft jedoch nur IT-Systeme, über die eine natürliche Person selbstbestimmt verfügt und erstreckt sich auf IT-Systeme anderer, über die das selbstbestimmt nutzbare IT-System verbunden ist.

Für spezifische Berufsgruppen oder Tätigkeiten bestehen überdies Geheimhaltungsverpflichtungen (z.B. im § 203 StGB), die neben dem für den Fall einer automatisierten Verarbeitung mit personenbezogenen Daten geltenden Datengeheimnis zu beachten sind.

## 1.1 Rechtliche Vorgaben

### 1.1.1 Bundesdatenschutzgesetz (BDSG)

Das Bundesdatenschutzgesetz (BDSG) setzt die Europäische Datenschutzrichtlinie 95/46/EG vom 24.10.1995 um. Der Zweck des BDSG ist es, den Einzelnen davor zu schützen, dass er durch den Umgang mit seinen personenbezogenen Daten in seinem Persönlichkeitsrecht beeinträchtigt wird.

Das BDSG unterliegt dem Subsidiaritätsgrundsatz - es handelt sich somit um ein Auffanggesetz. Es kommt zum Tragen, wenn keine anderen Gesetze oder bereichsspezifische Bestimmungen zum Datenschutz anzuwenden sind.

Das BDSG gilt für die Erhebung, Verarbeitung und Nutzung personenbezogener Daten durch

- öffentliche Stellen des Bundes,
- öffentliche Stellen der Länder, soweit der Datenschutz nicht durch Landesgesetz geregelt ist und soweit sie
  - Bundesrecht ausführen oder

- als Organe der Rechtspflege tätig werden und es sich nicht um Verwaltungsangelegenheiten handelt,
- nicht öffentliche Stellen, soweit sie die Daten unter Einsatz von Datenverarbeitungsanlagen verarbeiten, nutzen oder dafür erheben oder die Daten in oder aus nicht automatisierten Dateien verarbeiten, nutzen oder dafür erheben, es sei denn, die Erhebung, Verarbeitung oder Nutzung der Daten erfolgt ausschließlich für persönliche oder familiäre Tätigkeiten.

Zur Prüfung eines nach § 11 BDSG beauftragten Rechenzentrums sind insbesondere folgende Paragraphen des BDSG zu berücksichtigen (für die Prüfung eines selbstbetriebenen Rechenzentrums gilt § 11 BDSG nicht):

Datenverarbeitung nicht öffentlicher Stellen und öffentlich rechtlicher Wettbewerbsunternehmen	Datenverarbeitung der öffentlichen Stellen
§ 4f Beauftragter für den Datenschutz	§ 4f Beauftragter für den Datenschutz
§ 4g Aufgaben des Beauftragten für den Datenschutz	§ 4g Aufgaben des Beauftragten für den Datenschutz
§ 5 Datengeheimnis	§ 5 Datengeheimnis
§ 6 Rechte des Betroffenen	§ 6 Rechte des Betroffenen
§ 7 Schadensersatz	§ 7 Schadensersatz
§ 8 Schadensersatz bei automatisierter Datenverarbeitung durch öffentliche Stellen	§ 8 Schadensersatz bei automatisierter Datenverarbeitung durch öffentliche Stellen
§ 9 Technische und organisatorische Maßnahmen (und Anlage zu § 9 BDSG)	§ 9 Technische und organisatorische Maßnahmen (und Anlage zu § 9 BDSG)
§ 11 Erhebung, Verarbeitung oder Nutzung personenbezogener Daten im Auftrag	§ 11 Erhebung, Verarbeitung oder Nutzung personenbezogener Daten im Auftrag

## 1. Grundlagen und Normen

---

	§ 18 Durchführung des Datenschutzes in der Bundesverwaltung
§ 34 Auskunft an den Betroffenen	§ 19 Auskunft an den Betroffenen
§ 35 Berichtigung, Löschung und Sperrung von Daten	§ 20 Berichtigung, Löschung und Sperrung von Daten; Widerspruchsrecht
§ 38 Aufsichtsbehörde	§ 24 Kontrolle durch den Bundesbeauftragten für den Datenschutz und die Informationsfreiheit
	§ 25 Beanstandungen durch den Bundesbeauftragten für den Datenschutz und die Informationsfreiheit
	§ 26 Weitere Aufgaben des Bundesbeauftragten für den Datenschutz und die Informationsfreiheit
§ 43 Abs. 1 Nr. 2, 10, 11 Bußgeldvorschriften	§ 43 Abs. 1 Nr. 2, 10, 11 Bußgeldvorschriften
§ 43 Abs. 2 Nr. 1, 2, 3 Bußgeldvorschriften	§ 43 Abs. 2 Nr. 1, 2, 3 Bußgeldvorschriften
§ 44 Strafvorschriften	§ 44 Strafvorschriften

### 1.1.2 Landesdatenschutzgesetze (LDSG)

Die Bundesländer haben jeweils Landesdatenschutzgesetze, die den Umgang der Landesbehörden mit personenbezogenen Daten und die Rechtsstellung des jeweiligen Landesbeauftragten für Datenschutz regeln.

### 1.1.3 Strafgesetzbuch (StGB)

Das Strafgesetzbuch regelt im fünfzehnten Abschnitt die Verletzung des persönlichen Lebens- und Geheimbereichs. Hier sind für die Prüfung eines Rechenzentrums insbesondere §§ 202a bis 202c StGB (Ausspähen und Abfangen von Daten sowie die Vorbereitung) dazu zu beachten.

Besondere Beachtung für die Prüfung eines Rechenzentrums bedarf § 203 StGB Verletzung von Privatgeheimnissen. Die dort geregelte Schweigepflicht der in § 203 StGB genannten Berufsgruppen umfasst die rechtliche Verpflichtung dieser Berufsgruppen, ihnen anvertraute Geheimnisse nicht an Dritte weiterzugeben. Hierunter fallen z.B. Ärzte, Anwälte, Wirtschaftsprüfer, Angehörige der privaten Kranken-, Unfall- oder Lebensversicherung sowie der Datenschutzbeauftragte dieser Unternehmen.

Die Wahrung der ärztlichen Schweigepflicht wird in Bezug auf Ärzte über den Straftatbestand des § 203 StGB hinaus noch unter den Schutz der ärztlichen Berufsordnungen der Ärztekammern in den Bundesländern gestellt. Jeder Arzt, der gegen die Berufsordnung verstößt, kann vom Berufsgericht zu einer Warnung, einem Verweis, einer Geldbuße sowie der Aberkennung der Mitgliedschaft und des aktiven und passiven Wahlrechts in die Organe der Ärztekammer verurteilt werden.

Im siebenundzwanzigsten Abschnitt des StGB werden die Sachbeschädigungsdelikte geregelt. Hierunter fallen u.a. § 303a StGB (Datenveränderung) und § 303b StGB (Computersabotage), die für die Prüfung eines Rechenzentrums von Bedeutung sein können.

### **1.1.4 Sozialgesetzbuch (SGB)**

Durch Datenverarbeitung im Zusammenhang mit den Gesetzbüchern des SGB entstehen Sozialdaten. Solche Daten sind gemäß § 35 SGB I in Verbindung mit dem 2. Kapitel des SGB X besonders schützenswert, auch innerhalb der genannten Institutionen. Häufig enthalten Sozialdaten auch Daten zur Gesundheit von Versicherten oder deren Angehörigen. Solche Informationen gehören dann zur Gruppe der besonderen Arten personenbezogener Daten (§ 67 Abs. 12 SGB X). Daher sind die mit der Erhebung, Verarbeitung oder Nutzung beschäftigten Personen nicht nur auf das Datengeheimnis zu verpflichten, sondern auch auf das Sozialgeheimnis.



Ein Verstoß gegen die jeweils entsprechenden Datenschutzvorschriften kann eine Ordnungswidrigkeit nach § 85 Abs. 2 SGB X darstellen.

Für einzelne Bereiche wurden im Sozialdatenschutz zudem erweiterte Anforderungen erlassen. So ist vor allem das Erfordernis der zu ergreifenden technischen und organisatorischen Maßnahmen mit einer Beweislastumkehr versehen worden: Während nach § 9 BDSG technische und organisatorische Maßnahmen nur erforderlich sind, wenn ihr Aufwand in einem angemessenen Verhältnis zum angestrebten Schutzzweck steht, sind nach § 78a SGB X Maßnahmen nur dann nicht erforderlich, wenn ihr Aufwand in keinem angemessenen Verhältnis zu dem angestrebten Schutzzweck steht. Auf Grund des Begründungszwanges für die Nichteinführung von möglichen technischen und organisatorischen Maßnahmen ist die verantwortliche Stelle dazu verpflichtet, in einem Sicherheitskonzept zu beschreiben, wie die besonderen sozialdatenschutzrechtlichen und sicherheitstechnischen Anforderungen erfüllt werden.

Die darin dargestellten technischen und organisatorischen Maßnahmen müssen für den Schutzzweck geeignet und präzise bestimmt sein und dem Stand der Technik entsprechen. Das bedeutet, dass sie dem Entwicklungsstand technischer Systeme (Stand der Technik) entsprechen müssen, der zur präventiven Abwehr bestehender Gefahren geeignet und von der verantwortlichen Stelle nicht nachweislich zu Recht als unzumutbar angesehen werden kann.

### **1.1.5 Telekommunikations-Überwachungsverordnung (TKÜV)**

Diese Verordnung gilt für die Betreiber von Telekommunikationsanlagen, mittels derer Telekommunikationsdienstleistungen für die Öffentlichkeit (§ 3 Nr. 17 TKG) angeboten werden. Dies bedeutet, dass grundsätzlich alle Betreiber von Telekommunikationsanlagen, die ihre Dienste der Öffentlichkeit anbieten, zur Aufzeichnung und Weiterleitung der Kommunikationsdaten an die Strafverfolgungsorgane verpflichtet sind - unabhängig davon, ob es sich dabei um Sprache oder Daten handelt.

### **1.1.6 Telekommunikationsgesetz (TKG)**

Das Telekommunikationsgesetz (TKG) regelt den Wettbewerb im Telekommunikationsmarkt und hat dabei u.a. den Datenschutz in der Telekommunikation (Internet- und E-Mail-Zugang, Telefon u.a.) im Fokus.

Das TKG legt die Beziehungen zwischen dem Endkunden und den Telekommunikationsunternehmen fest, um den Kunden- und Verbraucherschutz zu stärken.

In § 88 TKG ist das Fernmeldegeheimnis geregelt. Hierin wird aufgeführt, welche Inhalte der Telekommunikation dem Fernmeldegeheimnis unterliegen.

Für Diensteanbieter ist der zweite Abschnitt des TKG zur Prüfung eines Rechenzentrums ebenfalls heranzuziehen. Hier werden neben dem Datenschutz weitere prüfungsrelevante Bereiche wie Einwilligung im elektronischen Verfahren, Vertragsverhältnisse, Verkehrsdaten, Entgeltmittlung und -abrechnung, Standortdaten, Einzelverbindungs nachweis, Störungen von Telekommunikationsanlagen und Missbrauch von Telekommunikationsdiensten, Mitteilen ankommender Verbindungen, Rufnummernanzeige und -unterdrückung, automatische Anrufweiterleitung, Teilnehmerverzeichnisse, Auskunftserteilung, Nachrichtenübermittlungssysteme mit Zwischenspeicherung geregelt.

### **1.1.7 Telemediengesetz (TMG)**

Das Telemediengesetz (TMG) regelt die rechtlichen Rahmenbedingungen für sogenannte Telemedien (elektronische Informations- und Kommunikationsdienste). Beispiele: Informationsdienste (z.B. Nachrichten, Wetter, Verkehr), Portale (z.B. mit Auktionen, Dating), Web-Maildienste, Webshops, Suchmaschinen, Chatrooms, Blogs (auch private Blogs). Es regelt ferner als zentrale Vorschrift des Internetrechts u.a. die Vorschriften zum Datenschutz beim Betrieb von Telemediendiensten und zur Herausgabe von Daten.

Der vierte Abschnitt des TMG enthält die Vorschriften zum Datenschutz, wie das Anbieter-Nutzer-Verhältnis, Grundsätze, Pflichten des

Diensteanbieters, Bestandsdaten, Nutzungsdaten, Informationspflicht bei unrechtmäßiger Kenntniserlangung von Daten.

### 1.1.8 Abgabenordnung (AO)

Die Abgabenordnung (AO) wird auch als „Steuergrundgesetz“ bezeichnet. Sie enthält grundlegende, für alle Steuerarten geltende Regelungen zum Besteuerungsverfahren, zur Ermittlung von Besteuerungsgrundlagen, Festsetzung, Erhebung und Vollstreckung von Steuern, Vorschriften über außergerichtliche Rechtsbehelfe und zum steuerlichen Straf- und Ordnungswidrigkeitenrecht.

Das Steuergeheimnis ist in § 30 der AO, die elektronische Kommunikation ist in § 87a AO geregelt. Hierbei sind bei der Übermittlung elektronischer Dokumente insbesondere die Verschlüsselung und Signatur zu beachten.

Gemäß §§ 93, 93b AO i. V. m. § 24c Kreditwesengesetz (KWG) haben Kreditinstitute eine Datei mit allen von ihnen in Deutschland geführten Konten und Depots zum automatisierten Abruf bereitzuhalten. In der AO sind ebenfalls die Zugriffsmöglichkeiten des Bundeszentralamts für Steuern (BZSt) auf diese Datei geregelt.

§ 147 AO regelt die Aufbewahrung von Unterlagen. Ein großer Teil der Unterlagen kann auch als Wiedergabe auf einem Bildträger oder auf anderen Datenträgern aufbewahrt werden, wenn dies den Grundsätzen ordnungsmäßiger Buchführung entspricht. Und sichergestellt ist, dass die Wiedergabe oder die Daten mit den Originalen bildlich und mit den anderen Unterlagen inhaltlich übereinstimmen, wenn sie lesbar gemacht werden können und während der Dauer der Aufbewahrungsfrist jederzeit verfügbar sind, und nach den Vorgaben der Finanzbehörde maschinell ausgewertet werden können.

Die Aufbewahrungsfristen liegen i.d.R. bei sechs bzw. zehn Jahren, sofern nicht in anderen Steuergesetzen kürzere Aufbewahrungsfristen zugelassen sind. Am Ende der Aufbewahrungsfrist besteht die Pflicht zur Löschung.

Wichtig zur Prüfung eines Speicherortes (z.B. bei Verwendung in der Cloud) ist der § 146 Abs. 2 (2), denn Bücher und die sonst erforderlichen Aufzeichnungen sind im Geltungsbereich des Gesetzes zu führen und aufzubewahren.

### 1.1.9 Betriebsverfassungsgesetz (BetrVG)

Die Betriebsverfassung ist die grundlegende Ordnung der Zusammenarbeit von Arbeitgeber und der von den Arbeitnehmern gewählten betrieblichen Interessenvertretung. Ihre Grundlage ist in Deutschland das Betriebsverfassungsgesetz (BetrVG).

In § 83 BetrVG ist das Akteneinsichtsrecht der Arbeitnehmer geregelt. Der Arbeitnehmer hat das Recht, in die über ihn geführten Personalakten Einsicht zu nehmen. Werden Angaben kodiert oder mittels elektronischer Datenverarbeitung gespeichert, so sind sie entschlüsselt und in allgemein verständlicher Form zu erläutern.

§ 87 BetrVG regelt die Mitbestimmung des Betriebsrates zu der Einführung technischer Einrichtungen, die dazu bestimmt sind, das Verhalten oder die Leistung der Arbeitnehmer zu überwachen.

### 1.1.10 Handelsgesetzbuch (HGB)

Im Handelsgesetzbuch in den §§ 238, 239 wird die Pflicht zur und die Art der Buchführung geregelt. Das gilt insbesondere für die Führung von Handelsbüchern und sonstigen Aufzeichnungen. Daten müssen während der Aufbewahrungsfrist verfügbar sein.

Es muss sichergestellt werden, dass der Kaufmann eine Urschrift der Handelsbriefe zurückbehält. Dies kann auch auf einem Schrift-, Bild- oder anderen Datenträger erfolgen, wenn dies den Grundsätzen ordnungsmäßiger Buchführung entspricht und sichergestellt ist, dass die Wiedergabe oder die Daten mit den Originalen bildlich und mit den anderen Unterlagen inhaltlich übereinstimmen, wenn sie lesbar ge-

macht werden können und während der Dauer der Aufbewahrungsfrist jederzeit verfügbar sind.

§ 257 HGB regelt die Aufbewahrung von Unterlagen und deren Aufbewahrungsfristen.

### 1.1.11 Personalausweisgesetz (PersAuswG)

In § 18 Personalausweisgesetz ist die Verwendung des Personalausweises als elektronischer Identitätsnachweis gegenüber öffentlichen und nicht öffentlichen Stellen geregelt.

Der elektronische Identitätsnachweis erfolgt durch Übermittlung von Daten aus dem elektronischen Speicher- und Verarbeitungsmedium des Personalausweises. Dabei sind dem jeweiligen Stand der Technik entsprechende Maßnahmen zur Sicherstellung von Datenschutz und Datensicherheit zu treffen, die insbesondere die Vertraulichkeit und Unversehrtheit der Daten gewährleisten. Im Falle der Nutzung allgemein zugänglicher Netze sind Verschlüsselungsverfahren anzuwenden.

Das Sperrmerkmal und die Gültigkeit sind zur Überprüfung immer zu übermitteln. Weiter können Daten, wie z.B. Namen, Titel, Geburtstag und -ort, Anschrift, Dokumentenart, dienste- und kartenspezifische Kennzeichen, Über- oder Unterschreitung eines bestimmten Alters, Angabe oder ob ein Wohnort dem abgefragten Wohnort entspricht, übermittelt werden.

Die Daten werden nur übermittelt, wenn der Diensteanbieter ein gültiges Berechtigungszertifikat und der Personalausweisinhaber seine Geheimnummer besitzt. Folgende Angaben sind vor Eingabe der Geheimnummer aus dem Berechtigungszertifikat zur Anzeige zu übermitteln:

1. Name, Anschrift und E-Mail-Adresse des Diensteanbieters,
2. Kategorien der zu übermittelnden Daten,
3. Zweck der Übermittlung,
4. Hinweis auf die für den Diensteanbieter zuständigen Stellen, die die Einhaltung der Vorschriften zum Datenschutz kontrollieren,
5. letzter Tag der Gültigkeitsdauer des Berechtigungszertifikats.

### **1.1.12 Grundsätze ordnungsmäßiger Buchführung (GoB)**

Die Grundsätze ordnungsmäßiger Buchführung sind Regeln zur Buchführung und Bilanzierung, die sich vor allem aus Wissenschaft und Praxis, der Rechtsprechung sowie Empfehlungen von Wirtschaftsverbänden ergeben. Ihre Aufgabe ist es, möglichst Gläubiger und Unternehmen vor unkorrekten Daten, Informationen und möglichen Verlusten zu schützen.

### **1.1.13 Grundsätze ordnungsmäßiger DV-gestützter Buchführungssysteme (GoBS)**

Die Grundsätze ordnungsmäßiger DV-gestützter Buchführungssysteme präzisieren die GoB für den Bereich der DV-gestützten Buchführung. Sie regeln die aufbewahrungspflichtigen Daten und Belege in elektronischen Buchführungssystemen und datensicheren Dokumentenmanagement- und revisionssicheren Archivsystemen. Bestandteil sind hierbei auch das Scannen und die Datenübernahme.

### **1.1.14 Grundsätze zum Datenzugriff und zur Prüfbarkeit digitaler Unterlagen (GDPdU)**

Die Grundsätze zum Datenzugriff und zur Prüfbarkeit digitaler Unterlagen konkretisieren bestimmte Rechtsnormen aus der Abgabenordnung und dem Umsatzsteuergesetz zur digitalen Aufbewahrung von Buchhaltungen, Buchungsbelegen und Rechnungen. Sie enthalten Regelungen zur Aufbewahrung digitaler Unterlagen und zur Mitwirkungspflicht der Steuerpflichtigen bei Betriebsprüfungen.

### **1.1.15 Datenerfassungs- und -übermittlungsverordnung (DEÜV)**

Die Vorschriften dieser Verordnung gelten für die Meldungen auf Grund des § 28a SGB IV, des § 200 Abs. 1 SGB V, der §§ 190 bis 194 und

281c SGB VI und des § 27 Abs. 2 des Zweiten Gesetzes über die Krankenversicherung der Landwirte sowie für den Beitragsnachweis nach § 28f Abs. 3 Satz 1 SGB IV. Die Meldungen und Beitragsnachweise für die jeweils beteiligten Träger der Sozialversicherung sind gemeinsam zu erstatten.

Die Meldungen erfolgen durch Datenübertragung. Hierfür sind geeignete Maßnahmen zur Sicherstellung von Datenschutz und Datensicherheit nach dem jeweiligen Stand der Technik vorzusehen. Bei der Nutzung allgemein zugänglicher Netze sind Verschlüsselungsverfahren anzuwenden.

### **1.1.16 Kreditwesengesetz (KWG)**

§ 24c KWG verpflichtet Kreditinstitute, eine aktuelle Datei mit allen von ihnen in Deutschland geführten Konten und Depots zum Abruf durch verschiedene öffentliche Einrichtungen bereitzuhalten. Strafverfolgungsbehörden, Strafgerichte, Finanzämter, Sozialämter, Sozialversicherungsträger (gesetzliche Krankenversicherer, Rentenversicherungsträger, etc.), Ämter, die die soziale Wohnraumförderung, Wohngeld, Erziehungsgeld und Unterhaltssicherung verwalten, BAföG-Ämter und die Bundesanstalt für Finanzdienstleistungsaufsicht dürfen Informationen in einem automatisierten Verfahren abfragen.

Enthaltene Daten sind Konto-/ Depotnummer, der Tag der Errichtung und Auflösung, die Namen und Geburtsdaten der jeweiligen Inhaber und Verfügungsberechtigten sowie die Namen und die Anschriften der abweichend wirtschaftlich Berechtigten. Die Kreditinstitute sind verpflichtet, die Daten in einer gesonderten Datenbank bereitzuhalten und dürfen nicht erfahren, auf welche Daten die Behörden zugreifen.

### **1.1.17 Steuerdaten-Übermittlungsverordnung (StDÜV)**

Diese Verordnung gilt für die Übermittlung von für das Besteuerungsverfahren erforderlichen Daten (Ausnahme: Daten, die für die Festset-

zung von Verbrauchsteuern bestimmt sind) durch elektronische Übermittlung an die Finanzverwaltung.

Bei der elektronischen Übermittlung sind dem jeweiligen Stand der Technik entsprechende Verfahren einzusetzen, die die Authentizität, Vertraulichkeit und Integrität der Daten gewährleisten. Im Falle der Nutzung allgemein zugänglicher Netze sind Verschlüsselungsverfahren anzuwenden.

### **1.1.18 Strafprozessordnung (StPO)**

In den §§ 94 ff. StPO werden die Durchsuchung von Räumlichkeiten und die Beschlagnahme von Unterlagen zu gerichtlichen Untersuchungszwecken geregelt.

### **1.1.19 Versicherungsvertragsgesetz (VVG)**

Die private Versicherungswirtschaft verwendet personenbezogene Daten in großem Umfang. Hierbei handelt es sich oftmals um besondere Arten personenbezogener Daten. Die Zulässigkeit der Datenverarbeitung ist im Versicherungsvertragsgesetz geregelt.

### **1.1.20 Zugangskontrolldiensteschutzgesetz (ZKDSG)**

Das Zugangskontrolldiensteschutzgesetz regelt das Verbot von gewerbmäßigen Eingriffen zur Umgehung von Zugangskontrolldiensten. Ein Zugangskontrolldienst ist ein technisches Verfahren oder eine Vorrichtung, die die erlaubte Nutzung eines zugangskontrollierten Dienstes ermöglicht. Bei einem passwortgeschützten Web- oder FTP-Server (Download- oder auch Datenaustauschserver) handelt es sich um einen zugangskontrollierten Dienst.

Im Rahmen eines Penetrationstests wird versucht, einen vorhandenen Schutzmechanismus zu umgehen. I.d.R. wird der Penetrationstest mit Hilfe von Tools (Umgehungsvorrichtungen) durchgeführt. Ferner erfüllt ein Penetrationstest die Voraussetzung, Hacker- und Sicherheitstools



zu gewerblichen Zwecken einzusetzen. Somit liegt ein ordnungswidriger Verstoß gegen das ZKDSG vor.

### 1.2 Technische und organisatorische Vorgaben

Ausfälle von Informationstechnologien bedeuten für Unternehmen finanzielle Schäden. Daher erwarten Betreiber von IT-Infrastrukturen und Rechenzentren, dass sich Sicherheitsrisiken objektiv identifizieren und professionell bewerten lassen. Dies leisten unterschiedlichste Dienstleister, wie spezialisierte Unternehmen, technische Überwachungsvereine oder Wirtschaftsprüfungsgesellschaften aber auch Interessenverbände, Vereine und sonstige Institutionen mit der Prüfung, Auditierung und Zertifizierung nach einschlägigen Standards. Diese standardisierten Anforderungskataloge beruhen auf anerkannten Normen und nachvollziehbaren Bewertungsmaßstäben.

Unternehmen, die nach einem bestimmten Regelwerk zertifiziert wurden, zeigen i.d.R. damit, dass sie den Stand der Technik nutzen, um die Verfügbarkeit der Systeme sicherzustellen. Dies kann sich positiv auf Ratings von Unternehmen und bei der Verhandlung von Versicherungskonditionen auswirken. Das Zertifikat dient zudem der Vertrauenssicherung gegenüber überwachenden Institutionen und als Nachweis für Innenrevisionen oder betrieblichen Datenschutzbeauftragten. Es hilft Risiken zu minimieren und nachzuweisen, dass das Rechenzentrum zuverlässig und verantwortungsvoll betrieben wird.

Nach den verbindlich festgelegten Kriterien werden dann die eingereichten Unterlagen analysiert und überprüft. Anschließend wird die Infrastruktur vor Ort in Augenschein genommen und der Betreiber der IT-Infrastruktur auditiert.

### 1.3 Einschlägige Normen für RZ-Sicherheit

Die im vorliegenden Leitfaden aufgeführten Normierungsunterlagen lassen sich in drei Ebenen aufteilen:

- Normierung der physischen IT-Sicherheit

- Normierung der informationstechnischen Sicherheit
- Normierung der organisatorischen Sicherheit

### **1.3.1 Normierung der physischen IT-Sicherheit**

Mit physischen Schutzmaßnahmen werden Rechenzentren gegen alle mechanischen Einwirkungen sowie die Einflüsse von Wasser, Feuer, elektromagnetischer Strahlung und Erschütterung gesichert. Die physische Sicherung muss zwischen den EDV-Systemen selbst und der sie umgebenden Infrastruktur, vor allem Stromversorgung und Klimatisierung, unterscheiden. Im Wesentlichen wird in den Standards der physischen Sicherheit die Widerstandsfähigkeit oder die Einhaltung zugesicherter Eigenschaften für einzelne Module oder Produkte wie Wände, Türen oder Baustoffe beschrieben. Die Evaluierung kompletter Systeme wie IT-Sicherheitsräume, Brandschutzracks oder Datensafes ist in der Regel weitaus schwieriger. Je nach IT-System oder Einzelmodul kann jedoch ein einschlägiger Standard für die Prüfung herangezogen werden. Neben diesen vielen allgemeinen Produktnormen und Vorgaben für Gebäude- bzw. Gebäudeteile, Datenverarbeitungsanlagen und IT-Systeme gibt es bisher nur wenige Standards, die sich direkt auf ein Rechenzentrum und dessen Umfeld beziehen. Deshalb vermitteln die hier gelisteten Normen ausschließlich eine Grundidee über die Prüfungsvielfalt und mögliche Zertifizierungsschemata. Da die Aussage eines Zertifikats deutlich von der Erwartungshaltung abweichen kann, sind sowohl die Einschlägigkeit der zugrunde gelegten Norm - wie z.B. die EN-50175-Serie, die EN-50174-Serie, die EN-50310-Serie und zukünftig auch die EN-50600-Serie - als auch die Abgrenzung des Prüfobjektes und der Inhalt der Prüfungen zu validieren. Darüber hinaus unterliegen Unternehmen auch branchenspezifischen Anforderungen, die durchaus Auswirkungen auf die zu überprüfende Datenschutzorganisation eines Unternehmens haben könnten. Ferner gibt es Vorgaben von privaten Organisationen, Bundesämtern, Verbänden oder Prüf- und Standardisierungsunternehmen. Damit sind ein Vergleich untereinander und damit eine qualitativ hochwertige und sichere technische Be-

wertung kaum möglich. Dieses Manko soll zumindest innerhalb von Europa künftig die neue Normenreihe EN-50600 beheben.<sup>4</sup>

### 1.3.2 Normierung der informationstechnischen Sicherheit

Die Sicherheit von IT-Produkten oder IT-Systemen kann nach Common Criteria (CC) zertifiziert werden. Für den Nutzer von solch einem zertifizierten Produkt/System stellt sich die Frage, ob das Produkt/System die Sicherheitsfunktionalität hat, die der Nutzer zurzeit benötigt. Durch die Definition von Schutzprofilen kann der Nutzer die benötigten Sicherheitseigenschaften festlegen. D.h. der Nutzer erstellt ein Sicherheitskonzept für das Produkt/System, das auch Erläuterungen beinhaltet. Die Korrektheit von Schutzprofilen wird in einem eigenständigen Evaluierungsprozess nachgewiesen und zertifiziert. Neben einem Katalog vordefinierter Funktionalitäten legt das Kriterienwerk Anforderungen an die Vertrauenswürdigkeit gemäß einer Vertrauenswürdigkeitsstufe fest. Die CC bieten die Möglichkeit, Sicherheitsanforderungen in vor-evaluierten Schutzprofilen zusammenzufassen<sup>5</sup>.

### 1.3.3 Normierung der organisatorischen Sicherheit

Um die Umsetzung von Informationssicherheit zu unterstützen, wurden in der Vergangenheit unterschiedliche Standards und Rahmenwerke - wie z.B. ISO/IEC 20000, ISO/IEC 27000 ff. und ISO 22301 -, aber auch Prüfstandards wie COBIT oder diverse Standards vom Institut der Wirtschaftsprüfer in Deutschland e.V. (IDW-Standards) - entwickelt. Durch die Anwendung dieser Sicherheitsstandards ist sichergestellt, dass allgemein anerkannte, einheitliche Methoden und Best Practices in die Realisierung von Informationssicherheit einfließen. Die standardkonforme Umsetzung ist i.d.R. auditierbar und je nach gewähltem

---

<sup>4</sup> LANline Events, Uwe von Thienen; Stand der Normierung beim RZ-Bau und Betrieb, [www.lanline.de](http://www.lanline.de)

<sup>5</sup> Hasso Plattner Institut, Studie zur Messbarkeit von Sicherheit in SOA, beauftragt durch das BSI, durchgeführt im Zeitraum 2010/2011; [www.hpi.uni-potsdam.de](http://www.hpi.uni-potsdam.de)

Standard auch zertifizierbar. Diese Zertifizierung kann als Nachweis die Standardkonformität für Kunden, Lieferanten oder Partnerinstitutionen dokumentieren.

Es existieren darüber hinaus Standards, in denen Informationssicherheit als Teilaspekt oder aus einer bestimmten fachlichen Perspektive betrachtet wird. Dadurch bestehen inhaltliche Überschneidungen zu den Standards und Rahmenwerken, die Informationssicherheit als Hauptaspekt betrachten. Weitere nützliche Informationen lassen sich aus der Tabelle „Einschlägige Normen für RZ-Sicherheit“ in der Anlage entnehmen. Es sei aber darauf hingewiesen, dass diese Ausführungen keine grundlegende technische wie auch juristische Beratung im Einzelfall ersetzen können.

## **1.4 Selbstregulierung**

Viele Unternehmen fragen sich nach dem Warum für eine Rechenzentrumsqualifizierung. Es geht bei einer solchen Qualifizierungsmaßnahme um einen Nachweis (Zertifikat). Das Rechenzentrum muss nach dem Stand der Technik geplant und gebaut sein. Nun bedeutet der Terminus „Stand der Technik“ auch, dass eine dynamische Komponente mit ins Spiel kommt - die Technik entwickelt sich weiter. Daher sollte eine Erstzertifizierung erfolgen und nach einem Zeitraum von etwa zwei Jahren ist die Prüfung zu aktualisieren. Dazu gilt ein Katalog mit Fragestellungen, der von einer neutralen Zertifizierungsstelle aktuell gehalten wird und der den momentanen Stand der Technik widerspiegelt, als notwendig. Generell ist eine Zertifizierung sinnvoll, wenn ein RZ-Betreiber Vertrauen für seine Kunden aufbauen oder halten will.



Auch eine Selbsteinschätzung auf Basis etablierter Gesetze, Standards und Normen kann als Einstieg in ein Qualifizierungsschema für kleine und mittelständige Unternehmen zielführend sein.

---

Eine große Anzahl von Sicherheitsstandards kommt bei der Planung und Gestaltung von Rechenzentren zur Anwendung. Sie stellen einerseits eine Hilfestellung für den Verantwortlichen dar, definieren andererseits aber auch Anforderungen hinsichtlich einer möglichen Selbstregulierung. Das Konzept der Selbstregulierung bedeutet, dass sich ein Unternehmen bestimmte Regeln, Standards oder Normen selbst setzt und diese nach dem Prinzip der Freiwilligkeit durchsetzt. Selbstregulierung ist insbesondere dort sinnvoll, wo gesetzliche Standards oder allgemeine Normierungsvorgaben branchenspezifisch konkretisiert werden sollen. Dadurch wird ein gemeinsames Verständnis von der Auslegung des geltenden Rechts in Bezug auf bestimmte Dienste geschaffen. Vollzugsdefizite können überwunden werden.

Die einschlägigen IT-Standards füllen unbestimmte Rechtsbegriffe aus: Technische Standards wie beispielsweise die BSI Grundschriftkataloge (ehemals Grundschrifthandbuch) und andere IT-Standards geben Lösungsansätze für Umsetzungsmaßnahmen. Prüfstandards (z.B. ITIL, COBIT, COSO) geben verschiedene Normierungen und Metriken für branchentypische Prüfungshandlungen vor. Standards legen Methoden zur Ermittlung des aktuellen Stands der Technik für IT-Sicherheitsmaßnahmen und Prüfungshandlungen fest. Empfehlungen in den IT-Grundschriftkatalogen für Standard-Sicherheitsmaßnahmen bei typischen IT-Systemen zeigen den Gestaltungsspielraum auf.



Ziel: Geeignete Anwendung von organisatorischen, personellen, infrastrukturellen und technischen Standard-Sicherheitsmaßnahmen, um ein angemessenes und ausreichendes Sicherheitsniveau für IT-Systeme zu erreichen.

---

Prüfstandards normieren die Prüfungshandlungen und geben eine Nachvollziehbarkeit hinsichtlich Feststellungen und Maßnahmenempfehlungen, die wiederum durch die technischen Standards ausgestaltet werden können. Die Einhaltung dieser Standards kann zumindest als Auslegungshilfe herangezogen werden und damit einen Maßstab für Sorgfalt/Pflichterfüllung bilden („Sorgfalt eines ordentlichen Kaufmanns“). IT-Standards werden häufig zu Vertragsbestandteilen gemacht, bei Nichteinhaltung drohen Vertragsstrafen.

Mit einer Qualifizierungsmaßnahme bzw. Zertifizierung des Rechenzentrums kann u.a. die hohe physikalische Sicherheit und Versorgungssicherheit eines Rechenzentrums nachgewiesen werden. Ausfallwahrscheinlichkeiten und Störanfälligkeiten lassen sich reduzieren und die Effizienz durch Reduzierung der Betriebskosten verbessern. Ein wichtiger Beitrag zum Business Continuity Managements oder des Informationssicherheits-Managementsystems kann dadurch geleistet werden. Letztendlich schafft man als IT-Verantwortlicher Sicherheit gegenüber der eigenen Geschäftsführung und seinen Kunden.

Um den Zertifizierungskriterien angemessen zu genügen, ist in der Anlage das einschlägige Regelwerk ohne Anspruch auf Vollständigkeit aufgelistet. Sicherlich lassen sich noch branchentypische Normierungen oder vertragstypischen Regelungen identifizieren. Diese notwendige Vollständigkeitsprüfung sei aber dem jeweils verantwortlichen IT-Sicherheitsbeauftragten des zu qualifizierenden Unternehmens überlassen.

Richtlinien und Standards haben keinen Gesetzescharakter, sind somit nicht unmittelbar durchsetzbar. Im IT-Bereich besteht i.d.R. keine „technische Gesetzgebung“ i.d.S., dass bestimmte Verfahren und Einrichtungen konkret beschrieben und vorgeschrieben sind, anders z.B. im Bereich der Normung oder Bauordnungsrecht/Baurecht. Die Beachtung von Standards kann in Streitfällen als Interpretationshilfe herangezogen werden (z.B. „marktübliches Format“). Sie liefern wichtige Hinweise für die praktische Umsetzung von IT-Compliance Anforderungen. Zertifizierungen können den Nachweis eigener Sorgfalt/Pflichterfüllung erleichtern

- z.B. „Sorgfalt eines ordentlichen Kaufmanns“ (§ 347 Abs. 1 HGB)
- z.B. „Sorgfalt eines ordentlichen und gewissenhaften Geschäftsleiters“ (§ 93 Abs. 1 AktG)

## 2. Arten von Rechenzentren

### 2.1 Definition Rechenzentrum

Nachfolgend werden typische verwendete Begriffe in der Informationstechnik (IT) und im Rechenzentrum (RZ) sowie Begriffsalternativen definiert. Gängige in der IT verwendete Abkürzungen oder Begriffe werden in englischer Sprache dargestellt.

#### Rechenzentrum

Als Rechenzentrum werden die für den Betrieb von IT-Systemen und IT-Infrastrukturen erforderlichen Gebäude, die Infrastruktur und die Organisation bezeichnet:

- die Gebäude bzw. Räumlichkeiten, in denen die Rechner-systeme untergebracht sind,
- die technische Infrastruktur zum Betrieb der Rechnersysteme (z.B. Stromversorgung, Klimatisierung, Netzwerkanbindung, Gebäudeleittechnik) und
- die Organisation zum Betrieb der Systeme (z.B. Operating, Backup).

#### IT-Systeme und IT-Infrastrukturen

In einem Rechenzentrum werden IT-Systeme und IT-Infrastrukturen betrieben.

Unter IT-Systemen und IT-Infrastrukturen werden folgende IT-Komponenten verstanden:

- Serversysteme (dediziert oder virtuell inkl. Applikation)
- Speichersysteme (z.B. SAN, NAS)
- Aktive Netzwerkkomponenten (z.B. Router, Firewalls, Switches)
- Telekommunikationssysteme (TK-Systeme)
- teilweise auch zentrale Drucksysteme

### Technische Einrichtungen eines Rechenzentrums

Die wesentlichen technischen Einrichtungen eines Rechenzentrums bestehen aus:

- der Elektroversorgung (z.B. Mittelspannungseinspeisung, Trafos, Überspannungsschutz, Unterbrechungsfreie Stromversorgung (USV) und Notstromgenerator),
- der Kälte- und Klimatechnik (z.B. Kältemaschinen, Rückkühlanlagen),
- den Brandschutzanlagen (z.B. Brandmeldeanlage, Brandfrühsterkennung, Löschanlage),
- der Sicherheitstechnik (z.B. Bewegungsmelder, Einbruchmeldeanlage, Videoüberwachung, Zutrittskontrollsystem, Vereinzelungssysteme) und
- der Gebäudeleittechnik (z.B. Temperatur, Luftfeuchtigkeit, Wassermelder).

### Sicherheitsbereiche in einem Rechenzentrum

Ein Rechenzentrum wird aus technischen, logistischen und sicherheitsrelevanten Gründen in mehrere Sicherheitsbereiche gegliedert. Dabei wird mindestens die Trennung in die organisatorisch und physisch getrennten Sicherheitsbereiche Technische Gebäudeausstattung (TGA), Server- und Systemräume (IT, zentrale IT-Räume zur Unterbringung der IT-Systemtechnik für den gesicherten Betrieb) und Infrastruktur eingehalten.

Die Sicherheitsbereiche werden in der Regel in Sicherheitszonen gegliedert, für die definierte Zutrittsregelungen bestehen (Business Need für den Zutritt zu den Räumen muss vorhanden sein).

- Technische Gebäudeausstattung (TGA)
  - Carrier-Raum (z.B. WAN-Einspeisung)
  - Klimasysteme
  - Spannungsversorgung (Trafo, Überspannungsschutz, Generatoren, USV (Batterieraum, Wechselrichter))
  - Feuerlöschsysteme (z.B. Räume für Flaschen mit Löschgas)



- Sicherheitszentrale (z.B. Videoüberwachung, Zutrittskontrolle)
- Server- und Systemräume (IT)
  - Systemräume (ggf. mit Suiten, Cages, Racks)
  - Vorbereitungsräume
  - Operating
- Zutritts- und Logistikbereiche
  - Zugangsschleuse/Anlieferungszone
  - Lager

### Raumstruktur eines Rechenzentrums

Aus den Sicherheitszonen und den Zutrittsregelungen ergeben sich die typischen Räumlichkeiten eines Rechenzentrums:

- Technikräume, (Elektroversorgung, Kältetechnik, Löschanlage, USV, Notstrom)
- IT-Räume (Server- oder Systemräume, Netzwerkräume, Carrierräume)
- Nebenräume (Lager, Aufenthaltsräume)
- Sicherheitszentrale
- Zutrittsschleusen

### Organisation eines Rechenzentrums

Je nach Art, Größe und Möglichkeiten eines Rechenzentrums ist es entweder ständig personell besetzt (Schichtdienst) oder es existiert in bedienerlosen Zeiten eine Rufbereitschaft („Dark Room“ mit oder ohne Fernadministrationsmöglichkeit). Für die Sicherung des Rechenzentrums und Gewährung des Zutritts ist in der Regel eine ständig besetzte Sicherheitszentrale mit Wachpersonal vorhanden.

## 2.2 Ausstattungsmerkmale von Rechenzentren

Nachfolgend wird grob dargestellt, wie die technische Infrastruktur eines Rechenzentrums aufgebaut ist, um einen möglichst stabilen und unterbrechungsfreien technischen Betrieb zu gewährleisten.

Die jeweilige Ausprägung des Rechenzentrums sowie der Systeme hängt in der Regel von Größe und Art des Rechenzentrums ab und ist jeweils im Kontext der Einzelprüfung auf die Angemessenheit zu bewerten.

### **Gebäude**

Rechenzentren können entweder als gesondertes technisches Funktionsgebäude hergestellt werden oder auch innerhalb eines anderweitig genutzten Gebäudes errichtet werden, z.B. innerhalb oder angrenzend an ein Bürogebäude.

Die Herstellung eines Rechenzentrums kann über- oder unterirdisch erfolgen.

Die Bauweise entspricht in der Regel einem Massivbau aus Stahlbeton mit einer Einzäunung und gesicherter Zufahrt.

Im Auswahlprozess eines RZ-Dienstleisters ist auf die Standortrisiken zu achten, die auf das RZ wirken und Einfluss auf die Verfügbarkeit haben können (z.B. Hochwasser, Sturm, Einflugschneisen in Flughafennähe, Katastrophen durch Industrieanlagen).

### **Sicherheitssysteme**

Unter Sicherheitssystemen im RZ sind im Allgemeinen folgende Systeme/Anlagen zu verstehen:

- Systeme und Anlagen für den Zutrittsschutz
- Überwachungs- und Alarmierungssysteme zur Meldung von unautorisiertem Zutritt
- Überwachungs- und Alarmierungssysteme zur Branderkennung und -meldung
- Überwachungs- und Alarmierungssysteme für Technische Anlagen (z.B. Lufttemperatur und -feuchtigkeit, Energieversorgung, Netzanbindung)

### **Systeme und Anlagen für Zutrittsschutz**

Auch bei Rechenzentren, die innerhalb eines anderweitig genutzten Gebäudes sind, bzw. direkt angrenzen, kann davon ausgegangen wer-

den, dass ein Zutrittsschutz sowie entsprechende Überwachungssysteme, wie z.B. Einbruchmeldeanlage vorhanden sind.

Bei Einzelgebäuden ist von einer Umzäunung sowie einem Anfahrtschutz und stabilen Pforten, Toren für Anlieferung und Personenzugang auszugehen.

Die Zutrittssicherung erfolgt in der Regel durch stabile Türen mit Einbruchschutz oder Personenvereinzelungsanlagen und gesicherten Materialschleusen.

Innerhalb des Gebäudes erfolgt der Zutritt zu den Bereichen in der Regel mittels Tokens, Key Cards oder Transpondern, selten mit Schlüsseln (Ausnahme: Serverracks), teilweise auch unter Nutzung biometrischer Systeme.

Zusammengefasst ist davon auszugehen, dass folgende Systeme und Anlagen für den Zutrittsschutz in Abhängigkeit zum Schutzbedarf der Daten in einem Rechenzentrum vorhanden sein sollten:

- Einzäunung mit stabilen Pforten und Toren
- Schleusen und/oder Personenvereinzelungsanlagen
- einbruchhemmende Gebäudetüren mit der Klassifizierung RC 4 nach DIN EC 1627-1630 oder vergleichbar (RC 4: Türen können einem erfahrenen Einbrecher mit Säge- und Schlagwerkzeugen 10 Minuten widerstehen)
- ein Zutrittskontrollsystem für die Vergabe von Zutrittsberechtigungen und Protokollierung der erfolgten Zutritte

### **Überwachungs- und Alarmierungssysteme - Einbruch**

Neben dem Primärschutz zur Sicherung des physischen Zutritts sind in der Regel umfassende Überwachungs- und Alarmierungseinrichtungen in einem Rechenzentrum implementiert. Hier kann von folgenden Systemen ausgegangen werden:

- Videoüberwachung des Außenbereichs (i.d.R. mit Bewegungsmeldern und Infrarot-Scheinwerfern für die Nacht-ausleuchtung)

- Videoüberwachung des Innenbereichs (mindestens alle IT-Zugänge, i.d.R. auch in Systemräumen)
- Einbruchmeldeanlage
- Aufschaltung auf Sicherheitszentrale eines Sicherheitsdienstes

### **Überwachungs- und Alarmierungssysteme - Feuer**

Zur Sicherung des Rechenzentrums gegen Brandschäden sind in der Regel umfangreiche Überwachungs- und Alarmierungssysteme installiert.

Üblicherweise sind folgende Systeme implementiert:

- Brandfrühsterkennungsanlage in IT und TGA Bereichen
- Löschanlage in IT und TGA Bereichen
- Aufschaltung der Brandmeldeanlage auf die Feuerwehr

### **Überwachungs- und Alarmierungssysteme - Technische Anlagen**

Zur Überwachung der technischen Anlagen eines Rechenzentrums ist in der Regel eine umfassende Gebäudeleittechnik (GLT) installiert. Über Sensoren und Meldepunkte oder Zähler werden Zustände über Funktion und Last der einzelnen Systeme/Anlagenteile in der Gebäudeleittechnikzentrale (häufig auch in der Sicherheitszentrale untergebracht) dargestellt.

Neben der reinen Überwachung ist die GLT in der Regel auch in der Lage Parametrierungen an den technischen Anlagen vorzunehmen und wird durch das TGA Operation Team eines Rechenzentrums genutzt.

### **Technische Anlagen**

Zum Betrieb des Rechenzentrums sind folgende technische Anlagen notwendig bzw. sinnvoll.

Diese untergliedern sich in die Bereiche:

- Energieversorgung und
- Kälte- & Klimatechnik

### Energieversorgung

Zur Sicherstellung einer unterbrechungsfreien Energieversorgung eines Rechenzentrums sind folgende technische Anlagen notwendig:

- Mittelspannungseinspeisung/Transformatoren
- USV Anlagen zur Überbrückung von Spannungsschwankungen und kurzen Ausfällen
- Dieselaggregat zur Notstromversorgung (ggf. mit Verträgen zur gesicherten Diesel-Versorgung)
- Überspannungsschutz

### Kälte- und Klimatechnik

Zur Sicherstellung der Raumtemperatur in Systemräumen sind folgende technische Anlagenelemente der Kälte- und Klimatechnik notwendig:

- Wasseraufbereitung
- Kältemaschinen
- Rückkühlanlagen im Außenbereich
- Pumpenanlagen

Der Umfang der Redundanz ist im Kontext der Verfügbarkeitsanforderungen individuell zu bewerten.

## 2.3 Risikobehandlung in Rechenzentren

Durch eine Risikoanalyse zur Datenverarbeitung bzw. Datenspeicherung leitet sich der Umfang und die Qualität der Anforderungen an ein Rechenzentrum ab. Ermittelte Bedrohungen, regulatorische Anforderungen aus der Datenschutzgesetzgebung und die Bewertung der Kritikalität für die Existenz des Unternehmens fließen in eine Risikoanalyse ein. Daraus ergeben sich die unterschiedlichsten Maßnahmen zur Risikobehandlung in einem Rechenzentrum (Arten der Risikobehandlung: Reduktion, Transfer, Vermeidung/Eliminierung oder Akzeptanz von Risiken).

### Lage und Gebäudesicherheit

Bereits die Auswahl des Standorts für ein Rechenzentrum sowie die Ausprägung des Gebäudes oder der Außenanlagen können Risiken mit sich bringen und sind zu bewerten. Dies betrifft insbesondere folgende Aspekte:

- Lage des Rechenzentrumsgebäudes (Überschwemmungsgebiete, Erdbebengefahr, Erdbeben, Einflugschneisen, Nähe zu Industrieanlagen, Tankstellen, mögliche Großveranstaltungen/Stadien, Trümmerkegel z.B. von Hochhäusern, etc.)
- Ausprägung der Gebäudesicherheit (massive Wände, Absicherung der Türen durch RC 4, Schutz, Fenster, etc.)
- Schutz des Gebäudes vor unbefugten Zutritt (Einzäunung, sichere Anfahrt, Videoüberwachung, Einbruchmeldeanlagen, etc.)
- Belastungen im Bereich elektromagnetischer Verträglichkeit (EMV) bzw. Berücksichtigung magnetischer Störfelder
- Energieversorgung sowie Kommunikationswege (getrennte Wegeführungen, mehrere Versorger, etc.)

### Betriebsorganisation

Die Qualität der Betriebsorganisation ist nicht zu unterschätzen und sollte gewissenhaft insbesondere unter folgenden Aspekten betrachtet und bewertet werden.

- Abschluss von Wartungsverträgen
- Qualifikation des eingesetzten Personals
- Verfügbarkeit von Personal im Störfall
- Ausfall/Fluktuation von Personal
- Reifegrad der Prozesse

### Technische Redundanz/Ausfallsicherheit

Für die Beschreibung von Redundanzen und Ausfallsicherheiten von Rechenzentren gibt es unterschiedlichste Normen und Klassifizierungen z.B. TÜVIT Trusted Site, Uptime Institute. Grundsätzlich wird die Höhe

und Qualität der Redundanz und der Ausfallsicherheit in einem Rechenzentrum an den Anforderungen ausgelegt. In der Regel wird für die verlässliche Aufrechterhaltung eines RZ-Betriebes die Ausfallsicherheit und Redundanz in folgenden Komponenten bzw. Teilbereichen benötigt. Keine Redundanz liegt vor, wenn Zuleitungen, Systeme oder Elemente nur einmal vorliegen. Im Folgenden werden mögliche Redundanzen in einem Rechenzentrum aufgezählt:

- Redundanz in der Versorgung
  - Anzahl der Einspeisungen zur Energieversorgung - mehr als eine Zuleitung (z.B. eine Versorgung über unterschiedliche Trafo-Stationen und einer zusätzlichen Notstromversorgung)
  - Anzahl der Systeme (Trafo, Generator, USV) - jeweils mindestens 2 Systeme
- Redundanz der wesentlichen technischen Anlagenelemente
  - N+1 Redundanz
  - Die Anlage besteht jeweils aus mehreren Einzelkomponenten. Es wird eine Einzelkomponente mehr als zum Erreichen der Nennkapazität der Gesamtanlage notwendig vorgehalten (z.B. ein USV Wechsel-/ Gleichrichter mehr als benötigt).
  - N+N oder 2N  
  
Es wird die Gesamtanlage jeweils zweimal vorgehalten.
- Räumliche Trennung
  - Die Anlagenelemente werden in unterschiedlichen Räumen untergebracht (z.B. Aufteilung der Batterien der USV Anlage auf zwei Räume). Bei einer räumlichen Trennung ist darauf zu achten, dass auf die Räumlichkeiten nicht die gleichen Risiken wirken (z.B. unterschiedliche Brandabschnitte).

### Beispiele für die Ausgestaltung von N+1 versus N+N Redundanz

Am Beispiel der technischen Realisierung einer USV-Anlage (Unterbrechungsfreie Stromversorgung) wird der Unterschied zwischen N+1 und N+N Redundanz kurz erläutert:

#### Annahme

In einem Rechenzentrum wird eine USV Leistung von 800 KW benötigt.

#### N+1

- Mögliche Ausprägung 2 USV Blöcke à 400 KW Leistung für die Nennkapazität von 800 KW
- Einbau eines weiteren Blocks von 400 KW für die N+1 Redundanz
- Hier wird ein Anlagenteil mehr vorgehalten als benötigt, d.h. in der Praxis darf ein 400 KW Block ausfallen

#### N+N oder 2N

- Mögliche Ausprägung zwei USV Blöcke à 400 KW Leistung für die Nennkapazität von 800 KW
- Aufbau von zwei weiteren USV Blöcken mit 2 x 400 KW
- Hier wird die komplette USV Anlage zweimal vorgehalten, d.h. in der Praxis darf eine gesamte Anlage mit 800 KW ausfallen

Je nach Ausgestaltung der Redundanzen ergeben sich folgende Vorteile für den Betrieb:

- Fehlertoleranz gegenüber Einzelfehlern
- Durch ein 2N Konzept kann auch bei Ausfall einer kompletten Anlage der Betrieb aufrechterhalten werden.
- Sicherstellung der Wartung im Betrieb
- Bei einem 2N Konzept oder sehr gut umgesetzten N+1 Konzeptes kann auch im Betrieb eine Wartung/Teilwartung ohne Betriebsunterbrechung durchgeführt werden.
- Verfügbarkeit



Die Verfügbarkeit des Rechenzentrums ist umso höher, je besser die technische Ausstattung ist und umso besser die Betriebsorganisation funktioniert.

### 2.4 Betriebsorganisation von Rechenzentren

Betriebsorganisationen von Rechenzentren arbeiten heute in der Regel arbeitsteilig und prozessorientiert. Die Betriebsorganisation eines Rechenzentrums gliedert sich in der Regel in den Technischen und den IT-Betrieb (siehe auch Anlage RZ-Organisation).

#### Technischer Betrieb

Der technische Rechenzentrumsbetrieb ist in der Regel eine vom IT-Betrieb organisatorisch getrennte Einheit, die sich in folgende Einheiten gliedert:

- TGA Betrieb  
(Betrieb der Elektro- und Kältetechnik sowie GLT)
- Facility Management  
(Hausmeister Services, Reinigungsdienste)
- Werkschutz/Sicherheitsdienst  
(Zutrittskontrolle, Warenannahme, Sicherheit)

#### IT-Betrieb

Die IT-Betriebsorganisation ist für den Betrieb der im Rechenzentrum zu betreibenden IT-Systeme (konzerninterne oder Kundensysteme) verantwortlich. In der Regel gibt es hier folgende Einheiten:

- Service Desk  
(Call Center zur Störungsannahme)
- Network Operation Center  
(Betriebssteuerung, Durchführung von Regeltätigkeiten)
- Operations  
(Störungsbearbeitung, Wartung)
- Transition Team  
(Projektteam zur Integration neuer Kundensysteme)

### 2.4.1 Prozesse in Rechenzentren

In Dienstleistungsrechenzentren, zunehmend aber auch bei firmen-/konzerninternen Rechenzentren wird im IT-Betrieb in der Regel nach den ITIL Best Practices gearbeitet.

ITIL beschreibt in fünf Kernbänden sowie einem Zusammenfassungsband Komponenten und Abläufe des Lebenszyklus von IT-Services.

Die konkrete Ausgestaltung der Prozesse nach ITIL obliegt jedem RZ-Betreiber selbst, ITIL bietet hier Erfahrungswerte, die aber auf den individuellen Betreiber (firmenintern oder Dienstleister) und sein Geschäftsmodell bzw. seine Anforderungen anzupassen und konkret auszugestalten sind. Dies bedeutet in der Praxis, dass die Ausgestaltung der Prozesse, wie auch der Implementierungsgrad im Unternehmen zu hinterfragen ist.

In Bezug auf IT-Sicherheit ist in Rechenzentren die Ausrichtung nach BSI IT-Grundschutz oder der ISO 27001 vorzufinden.

### Übersicht der ITIL Publikationen und Prozesse

Publikation ITIL V3	Prozess / Funktionen
<b>Band I - Service Strategy</b>	Strategy Generation Financial Management Service Portfolio Management Demand Management
<b>Band II - Service Design</b>	Service Level Management Service Catalogue Management Information Security Management Supplier Management IT Service Continuity Management Availability Management Capacity Management
<b>Band III - Service Transition</b>	Knowledge Management Change Management Service Asset and Configuration Management Transition Planning and Support Release and Deployment Management Service Validation and Testing Evaluation
<b>Band IV - Service Operation</b>	Function: Service Desk Function: Technical Management Function: IT-Operations Management Function: Application Management Incident Management Request Fulfilment Event Management Access Management Problem Management
<b>Band V - Continual Service Improvement</b>	The 7-Step Improvement Process Service Reporting Measurement Business Questions for CSI Return on Investment for CSI

Abbildung 1: Übersicht der fünf ITIL Bücher und Prozesse

### **2.4.2 Unterstützende Systeme/datenhaltende Systeme eines RZ-Betreibers**

Zur Sicherstellung des Betriebes sind in Rechenzentren häufig diverse datenhaltende Systeme vorhanden.

Es kann davon ausgegangen werden, dass in der Regel folgende datenhaltende Systeme bei einem RZ-Betreiber eingesetzt werden:

- Zutrittskontrollsystem  
(Speicherung von Zutrittsprofilen der zutrittsberechtigten Personen und Aufzeichnungen über erfolgte Zutritte)
- Ticketsystem  
(Speicherung von Anwenderdaten und Auftragsdaten)
- Configuration Management System  
(Speicherung von Geräte- und Konfigurationsdaten zu den Systemen, dies können auch Anwenderinformationen sein)

Weiterhin können folgende unterstützende Systeme im Einsatz sein:

- Serviceportale  
(Veröffentlichung von Service Informationen, Statistiken (z.B. Überwachung von Service Level Agreements, SLAs), Dokumentationen etc.)
- Order Management System  
(Workflowbasierte Verarbeitung von Kundenaufträgen)
- Technical Change Management System  
(Verarbeitung von technischen Änderungsanträgen, Speicherung von Informationen zum jeweiligen Änderungsauftrag)

Die Systeme tauschen untereinander Daten aus oder greifen auf zentrale Datenquellen wie ein Configuration Management System oder Configuration Management Database als zentralen Informationsspeicher zu. Weitere individuelle datenhaltende Systeme können im Einsatz sein. Art und Umfang der gespeicherten bzw. verarbeiteten Kundendaten sind im Kontext des jeweiligen Auftragsverhältnisses zu prüfen und zu bewerten.

### 2.5 Rechenzentrumsausprägungen - Eigenbetrieb/ Fremdbetrieb

Gemäß der Anlage von § 9 BDSG („Technische und organisatorische Maßnahmen“) muss eine öffentliche oder nicht-öffentliche Stelle, die personenbezogene Daten erhebt, verarbeitet oder nutzt, die erforderlichen technischen oder organisatorischen Maßnahmen zum Schutz der Daten in einem angemessenen Umfang umsetzen.

Diese Anforderung ist unabhängig davon, ob die Stelle die Daten in einem eigenen RZ verarbeitet (Eigenbetrieb) oder einen Dienstleister (Fremdbetrieb) beauftragt.

Es obliegt grundsätzlich dem betrieblichen Datenschutzbeauftragten, die ordnungsgemäße Anwendung der Datenverarbeitungsprogramme unabhängig vom Eigen- oder Fremdbetrieb zu überwachen (§ 4g BDSG, Aufgaben des Beauftragten für den Datenschutz).

Werden die personenbezogenen Daten nicht in einem eigenen RZ verarbeitet, sondern erfolgt die Verarbeitung durch einen Dienstleister, ist zusätzlich eine Vereinbarung zur Auftragsdatenverarbeitung (ADV) abzuschließen (gemäß § 11 BDSG, Erhebung, Verarbeitung oder Nutzung personenbezogener Daten im Auftrag). In dieser Vereinbarung sind die technischen und organisatorischen Maßnahmen zu beschreiben, die der Auftragnehmer umsetzen muss. Darüber hinaus sind die Kontrollrechte des Auftraggebers in die ADV aufzunehmen (z.B. Besuch, Kontrolle und Auditierung des RZ). Der Auftraggeber hat vor der Beauftragung des Auftragnehmers und sodann regelmäßig die Einhaltung der getroffenen technischen und organisatorischen Maßnahmen beim Auftragnehmer zu kontrollieren.

### 2.5.1 Beschreibung Rechenzentrum, Eigenbetrieb

Bezeichnung	Eigenbetrieb
Begriffsbestimmung	Betrieb der IT-Infrastruktur in den eigenen Räumlichkeiten
Merkmale	Umgesetzte Maßnahmen auf Basis der eigenen Risikoanalyse
Systemzugriff	ja
Direkter Datenzugriff	ja
Anwendungszugriff	ja
Leistung des Dienstleisters	kein DL (interne DV)
Leistungen Kunde	Betrieb des eigenen IT-Systems inkl. aller Infrastruktureinrichtungen und Servicezeiten und Leistungen
Schnittstellen in der Zusammenarbeit	Keine externen Schnittstellen
Beispiele	Betrieb von produktiven Systemen aller Art in Eigenregie (z.B. Web-Präsenz, E-Mail, SAP, File-Server, Archiv-Systeme, etc.) Notfallvorsorge (Cold-/Hotstandby)
Datenverarbeitung durch den Dienstleister	keine
Ist eine ADV notwendig?	nein
Wer ist noch zu involvieren?	Intern: DSB, BR, Fachabteilungen, IT-Sicherheitsbeauftragte Extern: Telekommunikationsanbieter

### 2.5.2 Beschreibung Rechenzentrum, Fremdbetrieb

Bezeichnung	Colocation	Housing	Hosting
Begriffsbestimmung	Bereitstellung von Rechenzentrumsfläche und Netzanbindung zum Betrieb von Kundensystemen. Die Systeme werden in der Regel in einem abgegrenzten Bereich installiert (z.B. durch Gitterwände abgetrennte Cages, Suites)	Bereitstellung von Rechenzentrumsfläche und Netzanbindung zum Betrieb von Kundensystemen. Die Systeme werden in der Regel in abgeschlossenen Serverschränken (Rack) betrieben.	Kompletter Betrieb der Kundensysteme durch den Hostinganbieter (im RZ des Anbieters)
Merkmale	<p>Bereitstellung:</p> <ul style="list-style-type: none"> <li>– Abgetrennte Fläche (Suite, Cage)</li> <li>– Unterbrechungsfreie Stromversorgung</li> <li>– Redundante Klimatisierung</li> <li>– ggf. Netzwerkanbindung (Internet, dedizierte Leitungen z.B. MPLS)</li> <li>– Zutrittskontrolle (z.B. Vereinzelungsschleuse, PIN, RFID, Logging der Zutritte)</li> <li>– Videoüberwachung</li> <li>– Alarmsicherung</li> <li>– Branderkennung</li> <li>– Löscheinrichtung</li> </ul>	<p>Bereitstellung:</p> <ul style="list-style-type: none"> <li>– Abgetrennte Fläche (abgeschlossene Serverschränke)</li> <li>– Unterbrechungsfreie Stromversorgung</li> <li>– Redundante Klimatisierung</li> <li>– ggf. Netzwerkanbindung (Internet, dedizierte Leitungen z.B. MPLS)</li> <li>– Zutrittskontrolle (z.B. Vereinzelungsschleuse, PIN, RFID, Logging der Zutritte)</li> <li>– Videoüberwachung</li> <li>– Alarmsicherung</li> <li>– Branderkennung</li> <li>– Löscheinrichtung</li> </ul>	<p>Bereitstellung:</p> <ul style="list-style-type: none"> <li>– Rackspace</li> <li>– Unterbrechungsfreie Stromversorgung</li> <li>– Redundante Klimatisierung</li> <li>– Netzwerkanbindung (Internet, dedizierte Leitungen z.B. MPLS)</li> <li>– Zutrittskontrolle z.B. Vereinzelungsschleuse, PIN, RFID, Logging der Zutritte)</li> <li>– Videoüberwachung</li> <li>– Alarmsicherung</li> <li>– Branderkennung</li> <li>– Löscheinrichtung</li> </ul> <p><b>Zusätzlich:</b></p> <ul style="list-style-type: none"> <li>– Betrieb der Systeme (z.B. Kontrolle/Überwachung),</li> <li>– Wartung der Systeme (z.B. Patchmanagement)</li> <li>– qualifiziertes Personal (24x7)</li> </ul>
Systemzugriff	nein	nein	ja

## 2. Arten von Rechenzentren

Bezeichnung	Colocation	Housing	Hosting
Direkter Datenzugriff	Nein	Nein	ggf. (nicht wenn die Anwend.daten verschlüsselt sind und der DL keinen Zugang zum verwendeten Key hat)
Anwendungszugriff	nein	nein	Abhängig von der konkreten Beauftragung
Leistung des Dienstleisters	Technischer RZ Betrieb (siehe Merkmale) ggf. Helping Hands durch den Dienstleister	Technischer RZ Betrieb (siehe Merkmale) ggf. Helping Hands durch den Dienstleister	Technischer RZ Betrieb (siehe Merkmale) Betrieb von dedizierten und virtuellen IT-Systemen: <ul style="list-style-type: none"> <li>– Installation neuer Komponenten</li> <li>– Pflege des Betriebssystems</li> <li>– ggfs. Pflege der Applikation</li> <li>– Monitoring des Systems,</li> <li>– Datensicherung</li> <li>– Management der Protokolldaten (z.B. Aufzeichnung, Auswertung, Archivierung)</li> <li>– Entstörung von Systemen (auch Fehleranalyse)</li> <li>– Reparatur / Austausch der Komponenten</li> <li>– Vulnerability Management (z.B. identifizieren von Schwachstellen, regelm. Vulnerability Scan)</li> <li>– User Verwaltung</li> <li>– Konfigurationsmanagement</li> <li>– Überwachung der System-Compliance</li> <li>– Dokumentation</li> </ul>



## 2. Arten von Rechenzentren

Bezeichnung	Colocation	Housing	Hosting
Leistungen Kunde	Kunde stellt sein IT-Equipment bereit und betreibt die IT inkl. Applikationen weitestgehend selbstständig. Ggfs. Nutzung von Helping Hand Leistungen im Betrieb.	Kunde stellt sein IT-Equipment bereit und betreibt die IT inkl. Applikationen weitestgehend selbstständig. Ggfs. Nutzung von Helping Hand Leistungen im Betrieb.	Bereitstellung sämtlicher IT-Komponenten Bereitstellung der Applikation/Lizenzen ggfs. Applikationsbetrieb (möglicherweise erfolgt die Systempflege nur bis zur „Oberkante“ des Betriebssystems durch den DL)
Schnittstellen in der Zusammenarbeit	Qualifiziertes Personal vor Ort bei Komplikationen (Helping Hands)	Qualifiziertes Personal vor Ort bei Komplikationen (Helping Hands)	Qualifiziertes Personal vor Ort (Administratoren für Komponenten, Betriebssystem, Applikation, Datenbanken, etc.) Ticket-/Change Management-System (Beauftragung von Changes) Eskalation von Störungen SLA-Reporting
Beispiele	Notfallvorsorge (Cold-/Hotstandby) Betrieb von Produktivsystemen aller Art in Eigenregie (z.B. Web-Präsenz, E-Mail, SAP, File-Server, Archiv-Systeme, etc.)	Notfallvorsorge (Cold-/Hotstandby) Betrieb von Produktivsystemen aller Art in Eigenregie (z.B. Web-Präsenz, E-Mail, SAP, File-Server, Archiv-Systeme, etc.)	Notfallsystemen (Cold-/Hotstandby) Betrieb von Produktivsystemen aller Art durch einen Dienstleister (z.B. Web-Präsenz, E-Mail, SAP, File-Server, Archiv-Systeme, etc.)

## 2. Arten von Rechenzentren

Bezeichnung	Colocation	Housing	Hosting
Datenverarbeitung durch den Dienstleister	Der Dienstleister ist nicht in die DV eingebunden. Ein Dienstleistungsvertrag mit SLAs sowie einer Vertraulichkeitsvereinbarung ist ausreichend.	Der Dienstleister ist nicht in die DV eingebunden. Ein Dienstleistungsvertrag mit SLAs sowie einer Vertraulichkeitsvereinbarung ist ausreichend.	Der Dienstleister ist in die DV eingebunden. ADV notwendig.
	Der DL hat Zugang zu folgenden, für die Erbringung der DL notwendigen Informationen: <ol style="list-style-type: none"> <li>1. Liste von Zutrittsberechtigten</li> <li>2. Vertragsverwaltung</li> <li>3. Kommunikationsliste/Ansprechpartner für Betrieb, Eskalation &amp; Service</li> <li>4. ggfs. Helping Hands</li> <li>5. Aufzeichnungen von Zutritten zum Cabinnett, Cage bzw. zur Suite</li> <li>6. Aufzeichnungen der Videoüberwachung</li> </ol>	Der DL hat Zugang zu folgenden, für die Erbringung der DL notwendigen Informationen: <ol style="list-style-type: none"> <li>1. Liste von Zutrittsberechtigten</li> <li>2. Vertragsverwaltung</li> <li>3. Kommunikationsliste/Ansprechpartner für Betrieb, Eskalation &amp; Service</li> <li>4. ggfs. Helping Hands</li> <li>5. Aufzeichnungen von Zutritten zum Cabinett, Cage bzw. zur Suite</li> <li>6. Aufzeichnungen der Videoüberwachung</li> </ol>	Der DL hat Zugang zu folgenden, für die Erbringung der DL notwendigen Informationen: <ol style="list-style-type: none"> <li>1. Liste von Zutrittsberechtigten</li> <li>2. Vertragsverwaltung</li> <li>3. Kommunikationsliste/Ansprechpartner für Betrieb, Eskalation &amp; Service</li> <li>4. Assetdaten mit Systemownern</li> <li>5. Userdaten / Berechtigungsinformationen</li> <li>6. Aufzeichnungen von Zutritten zum Cabinett, Cage bzw. zur Suite</li> <li>7. Aufzeichnungen der Videoüberwachung</li> </ol>
Ist eine ADV notwendig?	In der Regel keine ADV notwendig.	In der Regel verein-fachte ADV sinnvoll.	ja
Wer ist noch zu involvieren?	Intern: DSB, BR, Fachabteilungen Extern: Telekommunikationsanbieter	Intern: DSB, BR, Fachabteilungen Extern: Telekommunikationsanbieter	Intern: DSB, BR, Fachabteilungen Extern: Telekommunikationsanbieter

### 2.5.3 Betriebsarten von Clouds

Im Betrieb von Clouds haben sich drei Formen herausgebildet:

- Private Cloud
- Public Cloud
- Hybrid Cloud

Die Cloud-Betriebsarten unterscheiden sich jedoch lediglich von den Zugangs- und Zugriffsmöglichkeiten auf die Daten bzw. Anwendungen, nicht jedoch in der technischen Umsetzung oder dem Systembetrieb.

#### Merkmale der Private Cloud

- Kundeneigene, dedizierte Cloud (Zugang zu Daten/Anwendungen für einen eingeschränkten Kreis von Anwendern Beispiele: Mitarbeiter, Kunden, Geschäftspartner und Lieferanten einer Organisation)
- Die in der Cloud befindlichen Daten und Anwendungen sind für unberechtigte Anwender aus dem öffentlichen Internet nicht erreichbar.
- Die Cloud-Systeme können im Eigen- oder Fremdbetrieb betrieben werden.
- Der Kunde kann auf den Standort der Server Einfluss nehmen, woraus sich eine einfachere Realisierbarkeit unter Datenschutzaspekten ergibt:
  - Der Speicherort der Daten ist (räumlich) bekannt (z.B. Betrieb der Cloud in D oder EU).
  - Eine Übermittlung von personenbezogenen Daten in ein Drittland kann ausgeschlossen werden. Daraus ergibt sich eine einfachere Gestaltung der notwendigen Verträge mit dem Anbieter der Cloud (EU-Standardvertragsklauseln vs. Vereinbarung zur Auftragsdatenverarbeitung).
  - Der Kunde kann durch den Betrieb einer eigenen Cloud bei einem höheren Schutzbedarf der Daten zusätzliche technische oder organisatorische Maßnah-

men umsetzen (z.B. eine starke Authentifikation oder die Verschlüsselung der Daten).

### **Merkmale der Public Cloud**

- Die Public Cloud ist die Cloud eines Anbieters von standardisierten Diensten.
- Die in der Cloud befindlichen Daten und Anwendungen sind i.d.R. für die registrierten Anwender erreichbar (Steuerung der Zugriffe über ein Berechtigungskonzept).
- Die Cloud-Systeme können im Eigen- oder Fremdbetrieb betrieben werden.
- Der Anwender kann auf den Standort der Server keinen Einfluss nehmen, woraus sich eine aufwendige Realisierung unter Datenschutzaspekten ergeben kann:
  - Der Speicherort der Daten ist nicht immer bekannt oder kann räumlich nicht eingeschränkt werden (Betrieb der Cloud in einem Drittland?).
  - Eine Übermittlung von personenbezogenen Daten in ein Drittland kann ggf. nicht ausgeschlossen werden. Daraus ergibt sich die Notwendigkeit der Nutzung der EU Standardvertragsklauseln. Nicht immer ist es jedoch möglich, auf die vertragliche Gestaltung der Verträge Einfluss zu nehmen.
  - Der Kunde kann durch die Nutzung von standardisierten Diensten bei Daten mit einem höheren Schutzbedarf keinen Einfluss auf die technischen oder organisatorischen Maßnahmen zum Schutz der Daten nehmen (z.B. durch höhere Datenschutz- oder Compliance-Anforderungen).

### **Merkmale Hybrid Cloud**

- Die Hybrid Cloud ist eine Mischform aus Private- und Public Cloud (Beispiel: Nutzung einer Private Cloud mit einer Schnittstelle zu einer Public Cloud, um (verschlüsselte) Daten für die Notfall-Vorsorge auszulagern)

### 2.5.4 Beschreibung Rechenzentrum, Fremdbetrieb Cloud Computing

Cloud Computing (abstrahierte IT-Infrastrukturen)			
Bezeichnung	Infrastruktur (IaaS)	Plattform (PaaS)	Anwendung (SaaS)
Begriffsbestimmung	Bereitstellung von virtuellen, dynamisch anpassbaren Ressourcen (z.B. Speicher)	Bereitstellung von virtuellen, dynamisch anpassbaren IT-Systemen (z.B. Rechen- und Speicherkapazitäten)	Bereitstellung einer virtuellen, mandantenfähigen Softwarelösung.
Merkmale	Speicher	Bereitstellung von Rechen- und Speicherkapazität	Bereitstellung einer Anwendung
Systemzugriff	ja	ja	ja
Direkter Datenzugriff	ggf. (nicht wenn die Anwendungsdaten verschlüsselt sind und der DL kein Zugang zum verwendeten Key hat)	ggf. (nicht wenn die Anwendungsdaten verschlüsselt sind und der DL kein Zugang zum verwendeten Key hat)	ggf. (nicht wenn die Anwendungsdaten verschlüsselt sind und der DL kein Zugang zum verwendeten Key hat)
Anwendungszugriff	ja	nein	ja
Leistung des Dienstleisters	Technischer RZ Betrieb (siehe Merkmale)	Technischer RZ Betrieb (siehe Merkmale) Bereitstellung der Infrastruktur	Technischer RZ Betrieb (siehe Merkmale) Bereitstellung der Anwendung

## 2. Arten von Rechenzentren

Cloud Computing (abstrahierte IT-Infrastrukturen)			
Bezeichnung	Infrastruktur (IaaS)	Plattform (PaaS)	Anwendung (SaaS)
Leistungen Kunde	Nutzung der bereitgestellten Dienste	Nutzung der bereitgestellten Systeme	Nutzung der bereitgestellten Anwendung
Schnittstellen in der Zusammenarbeit	keine	keine	Qualifiziertes Personal für die Unterstützung der Anwender
Beispiele	Storage Services (z.B. Dropbox, Google Drive)	Microsoft Azure, Salesforce.com	Livemeeting, SAP, Office Communications
Datenverarbeitung durch den Dienstleister	Der DL hat Zugang zu folgenden, für die Erbringung der DL notwendigen Informationen: 1. Vertragsverwaltung 2. Kommunikationsliste / Ansprechpartner für Betrieb, Eskalation & Service 3. Userdaten / Berechtigungsinformationen 4. Speichern der Daten	Der DL hat Zugang zu folgenden, für die Erbringung der DL notwendigen Informationen: 1. Vertragsverwaltung 2. Kommunikationsliste / Ansprechpartner für Betrieb, Eskalation & Service 3. Userdaten / Berechtigungsinformationen 4. Speichern der Daten	Der DL hat Zugang zu folgenden, für die Erbringung der DL notwendigen Informationen: 1. Vertragsverwaltung 2. Kommunikationsliste / Ansprechpartner für Betrieb, Eskalation & Service 3. Userdaten / Berechtigungsinformationen 4. Speichern der Daten 5. Betrieb der Applikation
Ist eine ADV notwendig?	ja	ja	ja
Wer ist noch zu involvieren?	Intern: DSB, BR, Fachabteilungen	Intern: DSB, BR, Fachabteilungen	Intern: DSB, BR, Fachabteilungen



### 3. Anforderungsmanagement

#### 3.1 Definition der Begriffe „Anforderung“ und „Anforderungsmanagement“

Die Anforderung wird nach DIN EN ISO 9000:2005 definiert als „ein Erfordernis oder eine Erwartung, das oder die festgelegt, üblicherweise vorausgesetzt oder verpflichtend ist“. Der Begriff „üblicherweise“ beinhaltet, dass Merkmale implizit vorhanden sind und nicht explizit genannt werden müssen.

So wird zum Beispiel bei einem Rechenzentrum erwartet, dass eine Zutrittskontrolle stattfindet und man nicht einfach wie bei einem Kaufhaus hineingehen kann, auch wenn es nicht explizit formuliert wurde.



Das Anforderungsmanagement beschreibt die Methodik des Vorgehens und Leitens von Anforderungen.

---

Das Anforderungsmanagement basiert auf der Definition der Anforderungen, der Erhebung und Abfolgenbestimmung der zu untersuchenden Prüfungskriterien und der anschließenden Dokumentation. Das Ziel ist, die Ergebnisse aus einer beschriebenen Vorgehensweise unter definierten Bedingungen reproduzierbar zu machen.

Das Management von Anforderungen beinhaltet, dass die zu bearbeitenden Prozesse nicht nur definiert und implementiert werden, es erfordert auch, dass die Anforderungsdokumentation während des gesamten Projektverlaufs aktualisiert wird und diese als Grundlage für die Durchführung von Prüfungen (Erstellung und Auswahl von Prüffragen) verwendet werden kann.

Die definierten Anforderungen sollen im Rahmen des Anforderungsmanagement nicht nur Aussagen über gewünschte Eigenschaften machen, sondern sie müssen parallel dazu die Kriterien beschreiben, wie sie überprüft werden können.

Das Ziel des Anforderungsmanagement ist es, ein gemeinsames Verständnis über die zu erfüllenden Aufgaben herzustellen.



## 3.2 Kriterien für Anforderungen

Anforderungen sollen in Bezug auf den Schutzbedarf der Daten und die erforderliche Verfügbarkeit und die Mindestanforderungen an Datenschutz und Datensicherheit möglichst konkret und messbar sein. In Bezug auf die technischen und organisatorischen Maßnahmen sollten die Anforderungen allerdings vor Vertragsabschluss nicht zu konkret werden, um dem Dienstleister mehrere Optionen zur Erreichung des gewünschten Schutzniveaus offen zu lassen. Die Beschreibung der gemeinsam abgestimmten tatsächlichen technischen und organisatorischen Maßnahmen wird dann in der Auftragsbeschreibung konkretisiert.

Bei der Beschreibung der Anforderungen soll immer angegeben werden, ob die Erfüllung zwingend erforderlich ist (muss, shall) oder wünschenswert ist (sollte, should). Sofern schon bekannt, sollte bei der Definition der Anforderungen schon auf zukünftige Anforderungen (wird, will) späterer Ausbaustufen, z.B. in Bezug auf Performance, größere Datenmengen, höhere Verfügbarkeit durch geplante Ausdehnung der Geschäftszeiten oder zusätzliche geografische Standorte des Unternehmens in anderen Zeitzonen, eingegangen werden, um sicherzustellen, dass der gewählte Dienstleister die Anforderungen auch in einigen Jahren noch erfüllen kann.

Ausnahmen vom Normalverhalten sind zu definieren, z.B. was ist bei besonderen Vorkommnissen zu tun?

### **Gute Anforderungen sind:**

- **Vollständig**  
Die gewünschten Merkmale sind vollständig beschrieben.
- **Korrekt**  
Die Anforderung gibt genau das wieder, was der Auftraggeber möchte und der Dienstleister machen soll.
- **Abgestimmt**  
Alle Beteiligten akzeptieren die Anforderungen.
- **Klassifiziert**  
Die vertragliche Verbindlichkeit ist festgelegt. Für jede An-

forderung ist das entsprechende Kriterium anzugeben (muss, kann, spätere Ausbaustufe).

- **Konsistent**  
Es gibt keine Widersprüche innerhalb einer Anforderung und zwischen den Anforderungen untereinander.
- **Testbar**  
Die Erfüllung der Anforderungen ist nachweisbar. Dies ist wichtig im Hinblick auf die Prüfung des Auftragnehmers. Hierzu gehört insbesondere auch die Messbarkeit der verlangten Eigenschaften in Bezug auf Mengengerüst, Verfügbarkeitszeiten und Performance.
- **Eindeutig**  
Es gibt keinen Interpretationsspielraum.
- **Verständlich**  
Die Anforderung wird von allen Beteiligten verstanden.
- **Gültig und aktuell**  
Es macht keinen Sinn, Anforderungen an ein Rechenzentrum zu stellen, die veraltet sind.
- **Realisierbar**  
Die Anforderungen müssen erfüllbar sein.
- **Notwendig**  
Unnötige Anforderungen führen häufig zu Fehlern und erhöhen die Kosten.
- **Verfolgbar**  
Die Anforderungen müssen über ihren gesamten Lebenszyklus eindeutig identifizierbar sein, damit bei der Prüfung auf die Anforderung referenziert werden kann. Zur Identifizierung von Anforderungen eignen sich laufende Nummern oder kurze, eindeutige Überschriften. Wichtig: Wenn eine Anforderung wegfällt, darf der Identifizierungscode für die Anforderung später nicht für einige andere Anforderung verwendet werden. Dies führt zu Verwirrung und verhindert die Revisionssicherheit.

- Bewertet  
Die Anforderungen sind priorisiert bezüglich des Umsetzungszeitpunktes.

Die Anforderungen sollten kurz, frei von Floskeln, unnötigen Füllworten und redundanzfrei beschrieben werden. Abbildungen können das Verständnis erleichtern. Sie sollten dann mit einer eindeutigen Bezeichnung versehen werden, auf die im Text verwiesen wird. Wichtig ist, dass die Anforderungen keine impliziten Annahmen auf Basis branchenspezifischer Eigenheiten enthalten, die der Vertragspartner nicht kennen kann.

Besondere Begriffe sollten in einem Glossar erläutert werden, damit alle Beteiligten ein gleiches Verständnis haben. Auch Abkürzungen sollten ins Glossar aufgenommen werden, damit es nicht zu Fehlinterpretationen kommt.

Anforderungen sollten in regelmäßigen Abständen überprüft werden, damit sichergestellt ist, dass der ausgewählte Dienstleister die Bedürfnisse des Auftraggebers auch weiterhin erfüllt. Es reicht nicht aus, nur den Fragenkatalog für die regelmäßige Überprüfung des Dienstleisters an die geänderten Erfordernisse anzupassen.

Bei der Definition von Anforderungen empfiehlt es sich, auch die Herkunft der Anforderungen (z.B. gesetzliche Anforderungen aus einer branchenspezifischen Norm, besonderer Prozess für einen Kunden usw.) zu dokumentieren, damit allen Beteiligten nachträglich klar ist, warum die Anforderung aufgenommen wurde und die Anforderung nicht versehentlich wegdefiniert wird.

Außerdem sollte das Datum, an dem die Anforderung aufgenommen wurde, und der Verantwortliche für die Anforderung (z.B. IT, Fachabteilung, DSB) vermerkt werden.

## 3.3 Themenbereiche des Anforderungsmanagements

### 3.3.1 Schutzbedarf

In der Regel wird der betriebliche Datenschutzbeauftragte nicht derjenige sein, der eine umfangreiche Bedrohungs- und Schwachstellenanalyse oder eine vollständige Risikoanalyse aller Komponenten der Informationsverarbeitung für sein Unternehmen durchführt. Der Datenschutzbeauftragte kann leider auch nicht davon ausgehen, dass eine entsprechende Analyse vorliegt. Gerade bei kleinen und auch mittleren Unternehmen wird eine Risikoanalyse häufig nicht vorliegen. Es ist aber unabdingbar, sich im Rahmen der Definition der Anforderungen darüber im Klaren zu sein, welche Schutzbedarfe für die eigenen Anwendungen, IT-Systeme, Infrastrukturkomponenten und letztlich für die Räumlichkeiten, in denen die Informationsverarbeitung stattfindet, bestehen (die ISO 27001 spricht hier von „Assets“, die es zu betrachten gilt).

#### **Schutzbedarfskategorien BSI-Standard**

Das BSI hat hier eine einfache Methode (vgl. BSI-Standard 100-2 und 100-3) definiert, die sich grob in folgende Schritte gliedert:

- Definition der Schutzbedarfskategorien (Schutzbedarfsklassen) unter Berücksichtigung der Schutzziele Vertraulichkeit, Integrität und Verfügbarkeit, mit den drei Kategorien „normal“, „hoch“ und „sehr hoch“.
- Feststellung des Schutzbedarfs der Anwendungen der IT-Systeme, der Kommunikationsverbindungen und Räume mit Hilfe der definierten Kategorien.
- Dokumentation und Auswertung der vorgenommenen Einschätzungen.

Der Schutzbedarf ergibt sich in der Regel aus Bedrohungen die auf den IT-Betrieb wirken, Schwachstellen, die es ermöglichen den IT-Betrieb hinsichtlich der Schutzziele zu kompromittieren und der potenziellen Schadenshöhe, die bei einem eintretenden Sicherheitsvorfall zu erwarten ist. Bewährt haben sich in der Praxis Einteilungen in drei bis fünf Stufen.

Der Schutzbedarf ist relativ, da vertretbare Ausfallzeiten, finanzielle Schäden, verlangsamte Abläufe usw. sehr unternehmensspezifisch sind.

**Beispiel:**

**Schutzbedarfsdefinition zu Ausfallzeiten und finanzielle Auswirkungen (aus BSI-Standard 100-2 IT-Grundschutz)**

normal:

Ausfallzeiten von mehr als 24 Stunden können hingenommen werden.

Der finanzielle Schaden bleibt für die Institution tolerabel.

hoch:

Die maximale Ausfallzeit liegt zwischen einer und 24 Stunden.

Der Schaden bewirkt beachtliche finanzielle Verluste, ist jedoch nicht existenzbedrohend.

sehr hoch:

Die maximale tolerierbare Ausfallzeit ist kleiner als eine Stunde.

Der finanzielle Schaden ist für die Institution existenzbedrohend.

#### **Schutzbedarf vererbt sich weiter**

Beispiel: Die Anwendung Online-Shop ist bei Verfügbarkeit als „hoch“ eingestuft, dann gilt das automatisch auch für

- den Server,
- das Netzwerk,
- den Raum,
- den IT-Verbund.

Für den Schutzbedarf „hoch“ und „sehr hoch“ ist IT-Grundschutz normalerweise nicht mehr ausreichend!

#### **Kumulationseffekt**

Beispiel: Alle zehn Anwendungen sind als Verfügbarkeit „normal“ eingestuft.

Da aber alle zehn Anwendungen auf dem gleichen Server (Virtualisierung) laufen, sollte der Server insgesamt höher eingestuft werden.

Ein einzelner Ausfall einer Normal-Anwendung ist vielleicht akzeptabel, aber nicht wenn alle gleichzeitig ausfallen.

### **3.3.2 Schutzklassen**

Häufig werden Schutzklasse und Schutzbedarf synonym verwendet. Dies ist aber nicht immer richtig, da erst nach Feststellung des Schutzbedarfs einer Komponente die Einordnung in eine Schutzklasse erfolgen kann.

Im Bereich der Elektrotechnik gibt es eine Reihe von Schutzklassen wie z.B.

- USV-Schutzklassen (vgl. DIN-EN 5009-6, IEC 62040-3, IEC 61002-2 und VDE 0558). Hier sind Normen definiert wie sich unterbrechungsfreie Stromversorgungen gegenüber den verschiedenen Störungen (z.B. Netzausfälle, Spannungsschwankungen, Spannungsspitzen, Unter- und Über-

spannungen, Blitzeinwirkung und Spannungsstöße usw.) verhalten.

- IP-Schutzklassen (IP = International Protection), nach DIN 40050 bzw. IEC 529, zum Fremdkörper- und Wasserschutz.

Weitere Schutzklassen im Bereich der Gebäude sind z.B.:

- Resistance Class (RC) bzw. früher Widerstandsklasse (WK) von Bauelementen zum Einbruchschutz nach DIN-EN 1627 (vorherige Norm DIN V ENV 1627).
- Feuerwiderstandsklassen und Baustoffklassen (vgl. DIN 4102)

Beispielsweise sind mit der **DIN Norm 66399 zur Datenträgervernichtung** folgende drei Schutzklassen für Daten definiert:

- Schutzklasse 1  
normaler Bedarf für interne Daten
- Schutzklasse 2  
hoher Bedarf für vertrauliche Daten
- Schutzklasse 3  
sehr hoher Bedarf für besonders vertrauliche und geheime Daten

Bei der Definition der Anforderungen kann es natürlich sehr hilfreich sein, von dem RZ-Betreiber für bestimmte Bereiche den Nachweis zu fordern, dass die verbauten Komponenten oder die eingesetzten Verfahren allgemeinen Schutzklassen entsprechen.

#### 3.3.3 Die 8 Gebote (TOMs)

Bei der Formulierung und der Überprüfung von Anforderungen an die Sicherheit von Rechenzentren muss der Datenschutzbeauftragte sich an den technisch-organisatorischen Maßnahmen nach § 9 BDSG bzw. der Anlage zu § 9 BDSG.

Die **Anlage zum § 9 BDSG** fordert die Umsetzung von Schutzmaßnahmen in folgenden Kategorien:

1. Zutrittskontrolle
2. Zugangskontrolle
3. Zugriffskontrolle
4. Weitergabekontrolle
5. Eingabekontrolle
6. Auftragskontrolle
7. Verfügbarkeitskontrolle
8. Trennungsgebot

In Abhängigkeit vom Schutzbedarf, der für die eigenen Anwendungen und Systeme erforderlich ist, sind angemessene Maßnahmen zu definieren. Der Begriff „Angemessenheit“ beinhaltet vor allem auch die Frage nach der Wirtschaftlichkeit von Maßnahmen zum Erreichen des angestrebten Schutzzwecks.

Bei der Formulierung der Anforderungen ist vor allem zu klären, an wen diese Anforderungen zu stellen sind. Nicht alle erforderlichen Maßnahmen aus den o.g. Kategorien sind automatisch Anforderungen an den Betreiber des Rechenzentrums. Typischerweise sind Maßnahmen aus den Kategorien Zutrittskontrolle und Verfügbarkeitskontrolle überwiegend Anforderungen an den Betreiber des RZ (vgl. Abschnitt 1, Kapitel 1.5 Rechenzentrumsausprägungen), andere aber nur dann, wenn auch Kundensysteme vom RZ-Anbieter (im Rahmen von „hosting“) betrieben werden.

#### 3.3.4 K.-o.-Kriterien

Nach Formulierung aller Anforderungen an den Betrieb ist es erforderlich, die Anforderungen bezüglich ihrer Relevanz zu priorisieren. Dies bedeutet auch die Definition von „K.-o.-Kriterien“, also Anforderungen ohne deren Erfüllung ein sicherer Betrieb nicht gewährleistet werden kann bzw. gar nicht aufgenommen werden sollte.



„K.-o.-Kriterien“ können vielfältig sein:

- mangelnde Zutrittskontrolle (z.B. fehlende Regelungen zu Schlüsseln, Schließsystemen usw.)
- Datenverarbeitung außerhalb sicherer Länder
- fehlende Schutzmaßnahmen zum Brandschutz, Stromausfall, Wasser etc.

Letztendlich hängt die Einstufung, was ein „K.-o.-Kriterium“ ist, von dem festgestellten Schutzbedarf ab: Ein Online-Händler dessen System im Internet nicht erreichbar ist, hat da sicherlich andere Kriterien als ein Unternehmen, das lediglich eine einfache (informierende) Internetpräsenz betreibt.

#### 3.3.5 Personal

Bei der Definition von Anforderungen sollte berücksichtigt werden, dass auch gewisse Mindestanforderungen an das eingesetzte Personal vorhanden sein können.

Es sollte selbstverständlich sein, dass das beim Dienstleister eingesetzte Personal auf das Datengeheimnis verpflichtet ist, regelmäßig geschult wird und dass ein fachkundiger Datenschutzbeauftragter wirksam bestellt ist. Trotzdem ist es sinnvoll, auch diese Anforderungen in den Anforderungskatalog aufzunehmen, um aus vollständigen Anforderungen einen geeigneten Umfang aus Prüfungsfragen abzuleiten.

Weitere Anforderungen an die Qualifikation des Personals können sich auch aus Gesetzen und Verordnungen zum Datenschutz ergeben. So fordert das Datenschutzgesetz Nordrhein-Westfalen z.B. in § 11 Abs. 4: „Externe Personen und Stellen, die mit der Wartung und Systembetreuung von Einrichtungen zur automatisierten Datenverarbeitung beauftragt sind, unterliegen den Regelungen der Datenverarbeitung im Auftrag. Sie müssen die notwendige fachliche Qualifikation und Zuverlässigkeit aufweisen...“. Was notwendig ist, muss der Auftraggeber an dieser Stelle selbst entscheiden.

Auch aus der Art der beauftragten Dienstleistung können sich insbesondere bei ASP/SaaS und Hosting besondere Anforderungen an die Qualifikation der Mitarbeiter ergeben, damit die Applikationen bestmöglich betrieben werden und die User ggf. bei Fragen kompetente Ansprechpartner haben. Hier sollte vertraglich sichergestellt werden, dass die Mitarbeiter im Rechenzentrum, die z.B. eine Firewall administrieren und überwachen, Mindestkenntnisse über das System haben. Wenn Mitarbeiter nicht über ausreichende Kenntnisse verfügen und bei der Auswertung von Protokollen nur Standardlisten abarbeiten, kann es sein, dass kritische Vorkommnisse nicht erkannt werden, während ein erfahrener Mitarbeiter diese Besonderheiten erkennen würde.

Weitere Anforderungen an das Personal können das Vorliegen polizeilicher Führungszeugnisse oder gar eine Sicherheitsüberprüfung sein.

Zugriffe auf das Rechenzentrum aus dem Home-Office der Mitarbeiter des Dienstleisters oder Nutzung von privater Hard- und Software (BYOD - Bring your own device<sup>6</sup>) bergen zusätzliche Risiken für die Datensicherheit, werden in den nächsten Jahren aber wahrscheinlich zunehmen.

Daher sollte bei den Anforderungen an den Dienstleister explizit aufgenommen werden, ob und in welcher Form der Zugriff auf die Daten des Auftraggebers bei Telearbeit und über private Geräte möglich sein darf. Insbesondere sollte sich der Auftraggeber bei Nutzung bei Telearbeit vertraglich das Recht vorbehalten, bei der Prüfung des Dienstleisters auch der Telearbeitsplatz (z.B. Privatwohnung) ggf. auch zusammen mit Mitarbeitern einer Aufsichtsbehörde prüfen zu dürfen, besonders dann, wenn er selbst einer Prüfung der Aufsichtsbehörde unterliegt oder ein Verdachtsfall auf ein Datenschutzproblem eine kritische Prüfung aller technischen und organisatorischen Maßnahmen erfordert.

---

<sup>6</sup> Hierzu näher Franck, Bring your own device – Rechtliche und tatsächliche Aspekte, RDV 2013, 185 ff., online unter <http://bit.ly/14scJCD>.

## 3.4 Typischer Schutzbedarf

Der Schutzbedarf eines Gegenstandes richtet sich nach dem Ausmaß an Schäden, die entstehen können, wenn die Arbeits- und Einsatzweise in ihrer Funktion beeinträchtigt sind. Weil die Schadenshöhe oftmals nicht exakt definiert werden kann, sollten an Hand von entsprechenden Datenkategorien der Schutzbedarf<sup>7</sup> bestimmt werden.

**Schutzbedarf normal:** Die Schadensauswirkungen sind begrenzt und überschaubar.

**Schutzbedarf hoch:** Die Schadensauswirkungen können beträchtlich sein.

**Schutzbedarf sehr hoch:** Die Schadensauswirkungen können ein existenziell bedrohliches, katastrophales Ausmaß erreichen.

Um eine Bedarfsfeststellung durchzuführen, kann man die datenschutzrelevanten Werte Vertraulichkeit, Integrität und Verfügbarkeit als Basis heranziehen:

- wenn vertrauliche Informationen nicht ordnungsgemäß zur Kenntnis gelangen oder unberechtigt weitergeleitet werden (**Vertraulichkeit**),
- wenn die Richtigkeit von Informationen und die Einsatzweise von Systemen/Methoden verletzt sind (**Integrität**)
- wenn User bei der **Verfügbarkeit** von Informationen eingeschränkt und behindert werden.

Durch Eintritt einer oder mehrfacher Verletzung der o.g. Werte ergeben sich diverse Schädigungen, die unterschiedliche Auswirkungen haben können:

- Verstöße gegen Gesetze, Vorschriften, Normen, Verträge
- Minderung der informationellen Selbstbestimmung
- Behinderung der Aufgabenerfüllung und -ausführung
- Imageschädigung in der Außendarstellung

---

<sup>7</sup> BSI-Standard 100-2 IT-Grundschutz.

- Vertrauensverlust der Kunden/Lieferanten
- finanzielle Auswirkungen

Als Beispiel für den Verlust der Datenbank von Bestellungen für einen Onlineshop oder Versandhandel, kann man für das Unternehmen folgende Schädigungen ableiten:

- Vertragsverstoß, weil keine Informationen über die Bestellungen vorliegen
- Aufgabenerfüllung ist nicht durchführbar
- das Image leidet stark, das führt zu Vertrauensverlust bei den Kunden
- derzeitige und zukünftige Einnahmeverluste

#### **Bei den Datenkategorien mit hohem oder sehr hohem Schutzbedarf gilt in jedem Fall:**

Für einen hohen und sehr hohen Schutzbedarf gilt es, die Risiken genau zu identifizieren, zu analysieren und zu bewerten. Es reicht nicht aus, sich auf Standard-Einschätzungen zu verlassen. Darauf aufbauend ist die Erstellung eines ganzheitlichen Sicherheitskonzeptes nötig. Ein solches Sicherheitskonzept hat festzulegen und zu beschreiben, wie die Organisationsmaßnahmen auszusehen haben, wie Zuständigkeiten und Berechtigungen definiert und welche Kontrollmechanismen etabliert sind. Dazu zählt auch die Bestimmung von Mindestanforderungen für Sicherheitsmerkmale.

#### **Kann der RZ-Betreiber die Anforderung erfüllen?**

Dies ist letztendlich die elementare Frage, um die es bei der Auswahl und Prüfung eines RZ-Betreibers geht. Wie schon unter Punkt „Kriterien für Anforderungen“ beschrieben, soll bei den Anforderungen immer angegeben werden, ob die Erfüllung zwingend erforderlich ist (muss, shall) oder wünschenswert ist (sollte, should).

Zwingend erforderliche Anforderungen stellen damit für die Auswahl des RZ-Dienstleisters ein „K.-o.-Kriterium“ da. Der Nachweis ob die Erfüllung dieser Anforderungen überhaupt möglich ist, muss also bereits im Rahmen des Auswahlverfahrens erfolgen. Geeignete Nachwei-

se können hier Zertifizierungen (IT-Grundschutz, ISO 27001 etc.) und vor allem entsprechende Datenschutz- bzw. Sicherheitskonzepte sein.

Wünschenswerte Anforderungen können unter Umständen durch andere Anforderungen kompensiert werden. Hier sollte ggf. bereits bei der Formulierung der Anforderungen auf mögliche Alternativen hingewiesen werden. Beispielhaft sei hier die Kompensation von längerfristiger Videoaufzeichnung durch entsprechend dokumentierte Zugangskontrollen genannt (vgl. „Payment Card Industrie Data Security Standard Abschnitt 9.1.1“).

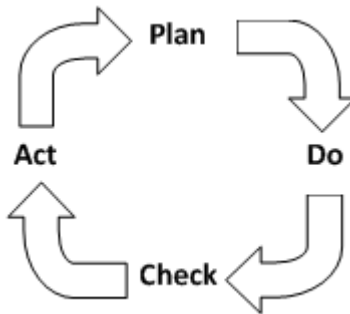
## 3.5 Änderungsmanagement

Anforderungen an die Sicherheit von Rechenzentren ändern sich. Anforderungen müssen nicht statisch sein, sondern sind häufig dynamisch. Die Ursachen für veränderte Anforderungen sind vielfältig, z.B.:

- gesetzliche Änderungen
- Veränderungen in zugrunde gelegten Normen und Standards
- Veränderungen in den eigenen Datenverarbeitungsprozessen
- Veränderungen durch Geschäftswachstum und dadurch Anforderungen an Speicherbedarf und Performance
- Veränderte Risikoeinschätzungen und veränderte Bedrohungsszenarien
- Budgetveränderungen

Um ein erreichtes Sicherheitsniveau zu erhalten, ist es erforderlich, Anforderungen und deren Umsetzung im Rahmen eines sog. „kontinuierlichen Verbesserungsprozesses“ (KVP) regelmäßig zu überprüfen. Der KVP ist elementarer Bestandteil der Normen ISO 9000, ISO 27001 und des BSI-Standards 100-1. Der kontinuierliche Verbesserungsprozess erfolgt mit Hilfe des sog. „PDCA-Zyklus“, der auch unter der Bezeichnung Deming-Kreis bekannt ist. „PDCA“ steht für die englischen Begriffe:

Plan	Planung, d.h. Festlegung der Anforderungen
Do	Umsetzung der Planung bzw. Umsetzung der Anforderungen im Betrieb
Check	Erfolgskontrolle bzw. Überwachung, ob die Anforderungen umgesetzt wurden und eingehalten werden
Act	Erkannte Defizite oder Mängel abstellen, durch Änderungen oder Anpassungen Prozesse optimieren



Der PDCA-Zyklus beschreibt einen iterativen und inkrementellen Entwicklungsprozess mit dem nach jedem Durchlauf ein verbesserter Status des Gesamtsystems erreicht wird. Mit jedem Durchlauf werden neue und veränderte Anforderungen berücksichtigt, sowie Fehler und Schwachstellen reduziert.

Nach jedem Durchgang des Zyklus beginnt dieser erneut mit der Phase „Plan“, in der auf neue und veränderte Anforderungen zu prüfen ist.

### 3.6 Berücksichtigung der Anforderungen

#### Ausschreibungen

Die vorweg aufgeführten Kriterien für die Anforderungen sind in der Projektphase zwingend zu formulieren und in der Ausschreibung aufzuführen, damit sie bei der Auswahl des Dienstleisters berücksichtigt werden. Dazu ist die ständige Einbindung des Datenschutzbeauftragten

in der Projektphase zu gewährleisten und schon hier sind nicht nur die K.-o.-Kriterien explizit zu benennen sondern eine Gewichtung aller Anforderungen vorzunehmen.

#### **Implementierung**

In der Implementierungsphase werden häufig Änderungen an Inhalten und Abläufen vorgenommen. In dieser Phase ist insbesondere darauf zu achten, dass die in der Ausschreibung formulierten Anforderungen weiterhin beachtet werden. Hier ist es zu gewährleisten, dass der Datenschutzbeauftragte eingebunden ist. Die Änderungen sind entsprechend der Anforderungen zu überprüfen und ggf. ist zu entscheiden, ob die Änderungen oder die Anforderungen anzupassen sind und wie eine Fortschreibung zu gewährleisten ist.

#### **Betrieb**

Auch im Betrieb ist eine regelmäßige Überprüfung der zu Grunde gelegten Anforderungen vorzunehmen und dazu sind auch regelmäßige Kontrollen sowohl der Dokumente als auch vor Ort vorzunehmen. Während bei Softwareänderungen schriftliche Änderungsdienste mitgeliefert werden, werden Änderungen beim Rechenzentrumsdienstleister nicht immer vorweg mitgeteilt bzw. abgestimmt. Dies sollte deshalb auf jeden Fall vertraglich abgesichert werden ebenso wie auch Lösungswege bei Dissensen.

## 4. Allgemeine Prüfpraxis

Das Bundesdatenschutzgesetz regelt in § 11 die formalen Anforderungen an die Auftragsdatenverarbeitung. Bestandteil der Regelung ist, dass der Auftraggeber die ordnungsgemäße Datenverarbeitung prüfen muss. Die Ausprägung dieser Prüfung wird allerdings nicht näher spezifiziert. Es ist naheliegend, dass neben den ausgegliederten IT-Verfahren auch die im Unternehmen vorliegende Verarbeitung personenbezogener Daten geprüft werden muss. Der Auftraggeber als verantwortliche Stelle muss auch hier der Prüfpflicht nachkommen. Eine Prüfung geschieht an Hand der IT-Verfahren, die die Prüfobjekte bilden.

### 4.1 Warum prüfen?

Die Überprüfung der Ordnungsmäßigkeit eines IT-Verfahrens ist eine Forderung aus dem Bundesdatenschutzgesetz. Die Kontrollpflicht ergibt sich aus §§ 4g und 11 BDSG, die in Abbildung 2: Auszug Prüfpflicht BDSG mit den entsprechenden Gesetzestexten dargestellt werden. Neben diesen Anforderungen kann die Prüfpflicht auch aus anderen Gesetzen wie SGB etc. resultieren. Ein entsprechender Verweis auf die Rechtsprechung oder branchenspezifische Standards ist in Kapitel 2 zu finden.

Neben der Vorabkontrolle bei einem IT-Verfahren ergibt sich demnach auch die Pflicht des Datenschutzbeauftragten, regelmäßige Überprüfungen der IT-Verfahren mit Verarbeitung personenbezogener Daten durchzuführen. Aus der oben stehenden Formulierung des BDSG resultiert, dass diese Prüfpflicht sowohl bei einer Auftragsdatenverarbeitung als auch bei intern betriebenen Verfahren vorliegt. Als Nachweis, dass der Datenschutzbeauftragte diesen Bestimmungen nachgeht, sind alle Prüfungen angemessen zu dokumentieren.



##### § 4g Abs. 1 Satz 4 Nr.1 BDSG

•Der DSB hat insbesondere (...), 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.

##### § 11 Abs. 2 Sätze 4 + 5 BDSG

•Der Auftraggeber hat sich vor Beginn der Datenverarbeitung und sodann **regelmäßig** von der Einhaltung der beim Auftragnehmer getroffenen technischen und organisatorischen Maßnahmen zu **überzeugen**. Das Ergebnis ist zu dokumentieren.

Abbildung 2: Auszug Prüfpflicht BDSG

Bei Kontrollen muss die Angemessenheit der inhaltlichen Prüfung vorliegen. Bei einer IT-Dienstleistung wie IT-Housing mag eine Überprüfung auf Basis der Dokumentation ausreichend sein, bei einer Überprüfung einer ausgegliederten Personaldatenverarbeitung sind in der Regel weiterführende Prüfungen vor Ort durchzuführen. Die Abwägung der Vorgehensweise sowie der konkreten Prüfungshandlung obliegt dem Auftraggeber.

Der nächste Abschnitt gibt mit Hilfe eines risikoorientierten Ansatzes die Möglichkeit, Prüfungen zielgerichtet zu planen.

## 4.2 Was ist angemessen?

Unternehmen unterhalten die vielfältigsten Lieferantenbeziehungen und unterliegen firmeninternen Verpflichtungen. Eine Überprüfung aller Lieferanten auf die ordnungsgemäße IT-Produktion ist im Regelfall nicht mit den bestehenden Ressourcen möglich. Aus diesem Grund ist es notwendig, die jährlichen Überprüfungen zu priorisieren.

Bei Überprüfung des Verfahrensverzeichnisses erkennt man schnell, in welchen Verfahren besonders schutzbedürftige Daten verarbeitet werden. Außerdem wird hier ersichtlich, ob eine Ausgliederung stattgefunden hat. Es empfiehlt sich eine Priorisierung der IT-Verfahren festzulegen, um die Risikoreichsten einer Überprüfung zu unterziehen. In Tabelle 1: Priorisierung von Verfahren wird ein Beispiel für eine solche Priorisierung gegeben.

<b>Verarbeitung von</b>	<b>personenbezogenen Daten</b>	<b>besonders schützenswerte „personenbezogene“ Daten</b>
<b>Verfahren wird im Haus bereitgestellt</b>	Priorität 1	Priorität 2
<b>Teilweise Ausgliederung (Housing) des Verfahrens</b>	Priorität 2	Priorität 2
<b>Ausgliederung des Verfahrens</b>	Priorität 3	Priorität 3

Tabelle 1: Priorisierung von Verfahren

In Tabelle 2 wird die Bedeutung der Prioritäten erläutert. In diesem Beispiel weist die Kategorie 3 die höchste Kritikalität aus. Diese Einordnung sollte auf das betroffene Unternehmen angepasst werden.

Kategorie	Bedeutung	Prüfintervall
<b>Priorität 1</b>	Es besteht ein geringer Prüfungsbedarf. Eine Überprüfung könnte zurückgestellt werden.	alle 3 Jahre
<b>Priorität 2</b>	Es besteht ein mittlerer Prüfungsbedarf. Es sollte mindestens eine Überprüfung auf Dokumentenbasis stattfinden. Ausgehend von dieser sind weitere Schritte zu planen.	alle 2 Jahre
<b>Priorität 3</b>	Es besteht ein hoher Prüfungsbedarf. Es muss eine Überprüfung auf Basis der Dokumentation sowie vor Ort stattfinden.	jährlich

Tabelle 2: Bedeutung der Prioritäten

Diese Priorisierung sollte ins Verfahrensverzeichnis aufgenommen werden, sodass bei Änderungen eine Anpassung sichergestellt ist.

### 4.3 Prüfungen planen

Nachdem den Verfahren eine Kritikalität zugewiesen wurde, ist ein Prüfprogramm aufzustellen. Die Aufstellung des Programms kann mit Hilfe einer tabellarischen Auflistung geschehen. Bei größeren Organisationen oder bei steigender Verfahrenszahl empfiehlt es sich, unterstützende Programme einzusetzen.

In jedem Fall sollte bereits in der Jahresplanung des Datenschutzbeauftragten dieses Prüfprogramm enthalten sein. Ggf. werden für spezielle Verfahren auch spezielle Experten benötigt, die budgetiert werden

müssen. Ein Prüfprogramm ist die Obermenge der im Jahr durchgeführten Prüfungen und Prüfpläne.



Stimmen Sie sich als Datenschutzbeauftragter mit den internen Stellen ab. IT-Sicherheitsbeauftragte oder die IT-Revision führen ebenfalls Kontrollen durch, an die Sie sich anschließen können. Es bietet sich in jedem Fall an, einen erfahrenen IT-Auditor hinzuzuziehen, da IT-Risiken betrachtet werden müssen.

---

## **4.4 Prüfungsablauf**

Der Prüfungsablauf gliedert sich in mehrere Phasen. Ziel der Prüfung ist es, die Konformität der Leistungserbringung mit den Prüfkriterien festzustellen und angemessen zu dokumentieren (siehe hierzu § 11 Abs. 2 BDSG).



Die Prüfkriterien bilden dabei ein Soll-Konzept, welches mit dem IST-Zustand abzugleichen ist. Letztendlich ist das Ziel, die Konformität zum BDSG nachweisbar zu erreichen. Je nach Datenschutzorganisation, Aufbau der Dokumentation und Prüfungsobjekt, können die Prüfkriterien in Phase 1 und 2 unterschiedlich sein.

Während in Phase 1 der Fokus auf der Vertragslage und Funktionstüchtigkeit des Anforderungsmanagements liegt, ist in Phase 2 die Vertragserfüllung gemäß Vertrag zur Auftragsdatenverarbeitung zu prüfen. Prüfkriterium ist demnach die ADV nach § 11 BDSG, ohne die eine Kontrolle nicht möglich ist.

### 4.4.1 Die Prüfungsvorbereitung

Prüfungen sind rechtzeitig zu planen und zu kommunizieren. Es sollte der Termin mit ausreichendem Vorlauf angemeldet werden, so dass die geprüften Bereiche die nötigen Ressourcen zur Verfügung stellen können. Während der Planung sollte ein Ansprechpartner benannt werden, der seitens des geprüften Bereichs die Prüfung koordiniert. Sofern Sie einen Dienstleister überprüfen, sollten Sie den entsprechenden Ansprechpartner aus Ihrem Haus einbinden. Dieser kennt die Organisation und gibt Ihnen die notwendigen Informationen.

Der Prüfer bespricht die anstehende Prüfung mit dem Ansprechpartner und bestimmt mit diesem einen Termin. Der Prüfer legt den Prüfungsumfang fest und sollte die Prüfungsthemen und Erwartungshaltung klar formulieren, so dass während der Prüfung alle Betroffenen zur Verfügung stehen und der Aufwand gering gehalten wird. Bei der Vorbereitung auf eine Überprüfung sind relevante Dokumente anzufordern, die die betrieblichen Standards und damit den Rahmen der Leistungserbringung widerspiegeln.

Für eine Strukturierung des Prüfplans empfiehlt es sich, die Maßnahme aus der Anlage zu § 9 BDSG zu listen und zu jedem Maßnahmenbereich passende Fragen zu formulieren. Auf diese Weise wird sichergestellt, dass alle relevanten Bereiche in der Überprüfung einbezogen werden. Die Tiefe der Überprüfung obliegt dem Prüfer und kann in jeder Prüfung variieren. Die Dauer der Prüfung hängt maßgeblich von der Komplexität der Prozesse, von dem Schutzbedarf der Daten und damit von dem geplanten Umfang und der Tiefe der Prüfung ab. Der Zeitrahmen sollte überschaubar bleiben. In der Erstprüfung steht meist die physische Sicherheit der Daten verarbeitenden Systeme im Vordergrund, während es im Folgeprüfungszyklus die logische Sicherheit im Vordergrund ist. Es können die Checklisten aus den Anlagen genutzt werden.

Aufgaben während der Prüfungsvorbereitung:

- Machen Sie sich Gedanken über den Inhalt der Prüfung und erstellen Sie einen Prüfplan
- Stimmen Sie die Inhalte mit dem zu prüfenden Bereich ab

- Überprüfen Sie alte Prüfberichte, Bewertung offener Maßnahmen
- Fordern Sie relevante Verträge inklusive Leistungsscheine, die ADV nach § 11 BDSG, die technisch-organisatorischen Vorgaben nach § 9 BDSG, sowie die Datenschutzrichtlinie an
- Fordern Sie Prozessbeschreibungen und Betriebsvorgaben an



Bei einer Auftragsdatenverarbeitung ist es bereits während der Auswahl eines Dienstleisters notwendig, dessen Eignung festzustellen. Auf Basis des Datenschutzkonzepts wird dann festgestellt, ob der Dienstleister fähig ist, die Maßnahmen geeignet umzusetzen.

---

#### **4.4.2 Die Durchführung**

Die Durchführung der Überprüfung geschieht in zwei Phasen, die Dokumentensichtung und die Vor-Ort-Überprüfung. Wie in Abschnitt „4.3 Prüfungen planen“ dargelegt, kann eine Überprüfung auch ausschließlich auf Dokumentationsbasis erfolgen. Auf Basis der Ergebnisse der Dokumentenprüfung kann entschieden werden, ob eine Vor-Ort-Prüfung notwendig ist.

Während der Vorbereitung wurde ein Prüfplan erstellt, der sich aus den Fragen der Checkliste zu den technisch/organisatorischen Maßnahmen zusammenstellt. Der Prüfplan dient als Gedankenstütze und sorgt für den roten Faden in der Prüfung. Es empfiehlt sich, einen Teil der Fragestellung dem Geprüften zur Verfügung zu stellen, so dass dieser den Umfang der Prüfung absehen kann.

Aufgaben während der Durchführung der Prüfung:

- Alle Prüfer, ob extern oder intern sind der Geheimhaltung verpflichtet, weshalb firmeninterne Informationen vorgelegt werden können.

- Der Prüfer hat keinen Anspruch auf Aushändigung von internen, sensiblen Dokumenten. Machen Sie sich einen Prüfungsvermerk mit Angabe der Quelle.
- Wenn der Prüfer Abweichungen zu bestehenden und allgemein gültigen Regularien erkennt, werden diese im Prüfbericht dokumentiert.

### 4.4.3 Dokumentenprüfung

Die Dokumentenprüfung überschneidet sich mit der Vorbereitungsphase. Je nach Verfahren ist die relevante Dokumentation anzufordern oder vor Ort einzusehen. Folgende Dokumente sollten Sie dabei prüfen:

- Verträge  
Bei einer Auftragsdatenverarbeitung sind die vertraglichen Verpflichtungen des Auftragnehmers zu prüfen. Dabei sind die Vollständigkeit des Vertragswerks und die inhaltliche Ausgestaltung zu prüfen. Demnach muss eine ADV gemäß § 11 BDSG vorliegen, in der auch die Kontrollrechte des Auftraggebers formuliert sind. Prüfen Sie, ob Subunternehmer eingesetzt werden und wenn ja, ob die Vorgaben der ADV auch für diesen gelten. Prüfen Sie, ob die Daten im Ausland verarbeitet werden.
- Testate  
Einsichtnahme und Bewertung von Testaten, Berichten oder Berichtsauszügen unabhängiger Instanzen. Beispiele:
  - Wirtschaftsprüfer
  - Revision
  - Datenschutzbeauftragte
  - IT-Sicherheitsabteilung
  - Datenschutzauditoren
  - Qualitätsauditoren
- Datenschutzrichtlinie  
Prüfen Sie die Datenschutzrichtlinie des Unternehmens. Werden die für die Auftragsdatenverarbeitung relevanten

Punkte angesprochen? Sofern branchenspezifische gesetzliche Anforderungen Anwendung finden, sind diese zu überprüfen.

- Betriebliche und organisatorische Vorgaben

Gibt es ein Betriebshandbuch oder Konzept für das IT-Verfahren? Grundlage eines ordnungsgemäßen IT-Betriebs sind SOLL-Vorgaben. Das SOLL definiert dabei die Maßnahmen (Regelwerk), wie das Verfahren zu betreiben ist und welche organisatorischen Vorgaben darauf einwirken. Diese Vorgaben sind mit dem internen Verfahrensverzeichnis und dem Vertrag abzugleichen. Dabei ist festzustellen, ob die inhaltliche Ausgestaltung der Maßnahmen zum Schutz der Daten ausreicht.

Bei der Überprüfung der Dokumentation ist darauf zu achten, ob die Dokumentation einen einheitlichen und strukturierten Aufbau besitzt. Achten Sie bei der Prüfung der Dokumentation darauf, Angaben über folgenden Informationen zu finden:

- Version/Datum
- Freigabestatus (z.B. Entwurf, freigegebene Version)
- Verantwortliche Personen (Autor, Prüfer, Freigebender usw.)
- Änderungshistorie
- Zielgruppe und Anwendungsbereich

Diese Informationen geben einen Aufschluss darüber, inwieweit Dokumentationsprozesse bei der entsprechenden Abteilung umgesetzt werden.

Die IT-Dokumentation oder ein IT-Handbuch gibt Ihnen einen ersten Eindruck über die IT-Organisation. Eine schlechte Dokumentation bedeutet allerdings nicht, dass die IT-Systeme besonders unsicher betrieben werden, vielmehr sollte hier eine Vor-Ort-Prüfung vorgenommen werden. Eine gleichermaßen gute Dokumentation bedeutet nicht, dass die Vorgaben genauso umgesetzt werden. Für den Fall sollten Nachweise angefordert werden, die das belegen. Aus der Dokumentation



sollte bereits hervorgehen, welche qualitätssichernden Maßnahmen umgesetzt werden.

Sollten Zertifizierungen bei dem Auftragnehmer vorliegen, so sind folgende Punkte sicherzustellen.

- Die Zertifizierung basiert auf einer anerkannten Norm (ISO oder Wirtschaftsprüfer).
- Die Zertifizierung wurde von einem anerkannten und unabhängigen Unternehmen durchgeführt.
- Die durch den Auftraggeber beauftragte Dienstleistung wird im Anwendungsbereich der Zertifizierung erbracht (Einsichtnahme in den dokumentierten Anwendungsbereich der Zertifizierung).
- Das „Statement of Applicability“ (Erklärung der Anwendbarkeit i.S.d. ISO/IEC 27001) kann eingesehen werden (Bewertung der Frage, welche Maßnahmen umgesetzt bzw. noch offen sind).
- Die Zertifikate sind aktuell (die Zertifizierung wird aufrechterhalten).

Ausgehend von der Dokumentenprüfung muss der Prüfplan weiter ausformuliert werden. Es sind Fragen zu notieren, die ggf. vor Ort geklärt werden müssen. Ist die Dokumentenprüfung ausreichend, ist diese im Prüfbericht zu vermerken und dieser abzuschließen.



Da die Durchführung einer Kontrolle Aufwand beim Auftragnehmer hervorruft, ist festzustellen, inwieweit diese Kosten getragen werden.

---

#### 4.4.4 Vor-Ort-Prüfung

Die Maßnahmen, durch die sich ein Auftragnehmer von der Einhaltung der getroffenen technischen und organisatorischen Maßnahmen bei dem Auftragnehmer zu überzeugen hat, sind durch den Gesetzgeber

nicht näher definiert. Eine zwingende Vor-Ort-Prüfung kann aus dem BDSG nicht abgeleitet werden.

Die Vor-Ort-Prüfung sollte mit einem zeitlichen Vorlauf von ca. 2 Wochen geplant werden. Bei begründetem Zweifel sind Vor-Ort-Prüfungen -auch unangemeldet oder mit weniger zeitlichem Vorlauf möglich.

Die Prüfung beginnt mit einem kurzen Einführungsgespräch, bei dem der Ansprechpartner des geprüften Bereiches seinen Verantwortungsbereich vorstellt und entsprechende Sicherheitsmaßnahmen darstellt. Der Prüfer wird auf Grundlage der zugrunde liegenden Konformitätskriterien und des Prüfplans die Einhaltung prüfen.

Als Prüfungsgrundlage dienen die vertraglich vereinbarten technisch-organisatorischen Maßnahmen. Diese sind Grundlage für das Sicherheitsniveau, welches auch durch den Dienstleister erfüllt sein muss. Fragen Sie nach einem Sicherheitskonzept für das entsprechende Verfahren. Im Regelfall sind solche Sicherheitskonzepte für IT-Unternehmen vertrauliche Dokumente, weshalb diese nur Vor-Ort eingesehen werden können. Das Sicherheitskonzept geht über die in Anlage zu § 9 BDSG benannten Maßnahmen hinaus und wird deutlich konkreter.

Da eine vollumfängliche Prüfung im Regelfall nicht möglich sein wird, ist eine risikoorientierte Vorgehensweise an Hand aussagekräftiger Stichproben durchzuführen. Dies ist mittels objektiver Nachweise zu belegen. Bei Stichprobenprüfungen können Mängel ggf. auch unbemerkt bleiben.

Es wird empfohlen im Rahmen eines Abschlussgespräches das Prüfungsergebnis der geprüften Stellen vorzustellen und zu verifizieren.

### 4.4.5 Die Nachbereitung

Nach der Prüfung wird der Prüfer seine Ergebnisse in einem Prüfbericht zusammenfassen. Er beschreibt die gefundenen Abweichungen und sendet sie an die verantwortliche Stelle. Eine Abweichung kann darin bestehen, dass eine vertraglich geschuldete Leistung nicht oder unzureichend erfüllt bzw. geregelt wurde.

Die verantwortliche Stelle hat nun die Möglichkeit die Abweichungen zu prüfen und ggf. zu kommentieren. Jede gefundene Abweichung ist mit einer passenden Maßnahme und einer Frist für deren Umsetzung zu versehen. Dieser Termin steht im Kontext des durch die Abweichung entstandenen Risikos. Schwerwiegende Mängel mit Auswirkung auf die Vertraulichkeit von personenbezogenen Daten sind unverzüglich abzustellen.

Es muss eine konkrete Handlungsanweisung formuliert werden, die die Möglichkeit bietet, festzustellen, dass die Maßnahme auch wirksam ist. Sofern der Prüfer die benannten Gegenmaßnahmen als angemessen empfindet, wird der Prüfbericht abgeschlossen. Legen Sie fest, ob eine Nachprüfung notwendig wird oder die verantwortliche Stelle die Abstellung der Maßnahme melden kann. Diese Entscheidung hängt von der Tragweite der Abweichung ab. Setzen Sie ggf. einen Termin zur Nachprüfung fest.

Bei einem Dienstleister ist hierbei zu beachten, dass ggf. vertraglich geregelte Vereinbarungen angepasst werden müssen (siehe PDCA-Zyklus im Kapitel Anforderungsmanagement). Dies hat Auswirkungen auf kaufmännische Aspekte, weshalb neben der verantwortlichen Stelle auch das Anforderungsmanagement einzubeziehen ist.

Aufgaben während der Nachbereitung:

- Der Prüfbericht ist innerhalb weniger Tage der verantwortlichen Stelle zur Verfügung zu stellen.
- Bei festgestellten Abweichungen sind passende Maßnahmen zu formulieren und nachzuverfolgen.

#### 4.4.6 Nachverfolgung und Maßnahmenkontrolle

Zur Nachverfolgung von Maßnahmen empfiehlt es sich, die Abweichungen, Maßnahmen und deren Umsetzungsdatum tabellarisch zu listen. Je nach Größe der Organisation ist die für die Umsetzung verantwortliche Stelle zu benennen.

### 4.4.7 Aufbau einer Prüfungsdokumentation

Die Erstellung einer Prüfungsdokumentation obliegt dem Datenschutzbeauftragten. Die in folgender Abbildung vorgeschlagenen Inhalte sollte jeder Bericht enthalten.

#### Einleitung

(für verantwortliche Stelle)

- Enthält Angaben zur Prüfung (Prüfer, Geprüfter, Datum, Prüfungsobjekt)
- Enthält Angaben zum Grund der Überprüfung

#### Prüfbericht

(für verantwortliche Stelle)

- Der Bericht ist eine Zusammenfassung aus dem Prüfprotokoll
- Enthält die gefundenen Abweichung mit einer Beschreibung, worin die Abweichung besteht und das resultierende Risiko, sowie das Datum zur Umsetzung

#### Prüfplan

(für Datenschutzbeauftragten als Anlage)

- Enthält die Agenda der Prüfung
- Enthält die Fragen, die während der Überprüfung gestellt werden

#### Prüfprotokoll

(für Datenschutzbeauftragten als Anlage)

- Enthält die Mitschriften während der Prüfung, eventuelle Vermerke werden hier für die Folgeprüfung gesetzt
- Hier werden alle objektiven Nachweise mit vollständigem Namen und Datum der Erstellung gelistet
- Das Prüfprotokoll sollte ausschließlich den Prüfern zugänglich sein

Abbildung: Aufbau einer Dokumentation

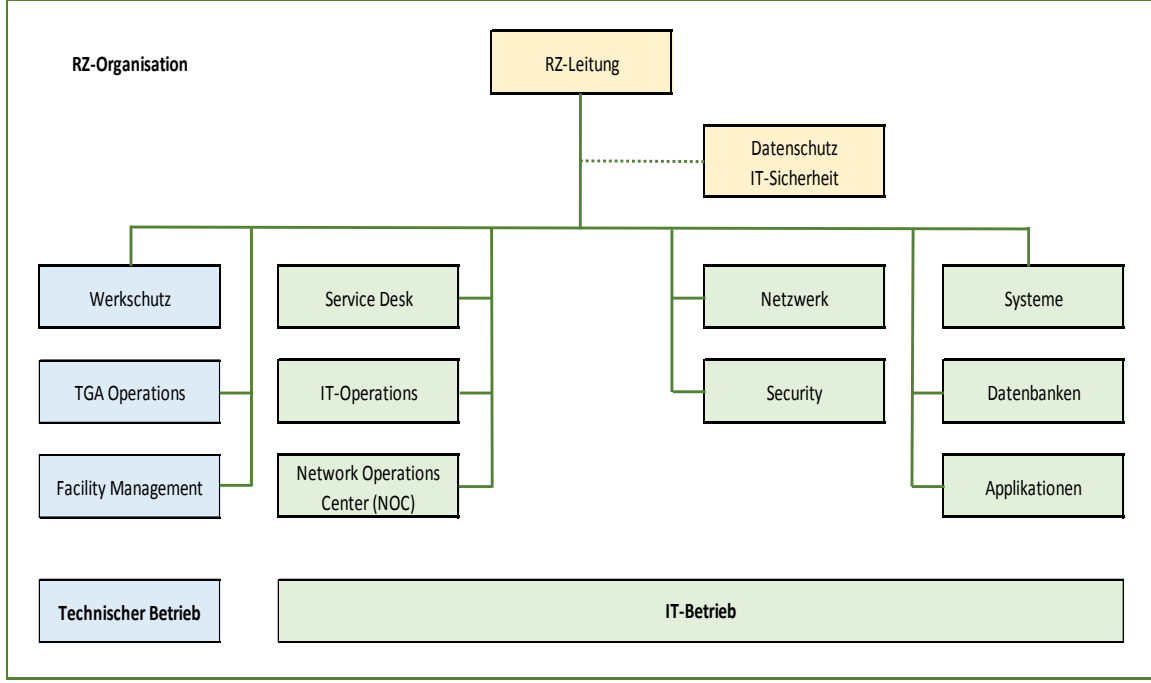
## 5. Anlagen

### Tierklassifizierung gemäß Uptime Institut

Tier Klassifizierung für Rechenzentren und deren Verfügbarkeitseinstufung

Merkmal / Tierklasse	Tier I	Tier II	Tier III	Tier IV
<b>Versorgung</b>	1 System	1 System	1 System	2 Systeme
<b>Versorgungspfade</b>	1	1	1 x normal 1 x alternativ	2 x gleichzeitig aktiv
<b>Redundanzen (der technischen Anlagen)</b>	1	N+1	N+1	Minimum N+1
<b>Räumliche Trennung</b> (d.h. gesondertes RZ Gebäude)	Nein	Nein	Ja	Ja
<b>Abwechselnde Wartung möglich</b> (d.h. ohne Unterbrechung für den Betrieb)	Nein	Nein	Ja	Ja
<b>Fehlertoleranz</b> (gegenüber Einzelfehlern)	Nein	Nein	Nein	Ja
<b>"Single Point of Failures"</b> (Konzeptbedingte SPoFs)	Viele + menschliche Fehler	Viele + menschliche Fehler	Wenige + menschliche Fehler	Keine / nur Feuer und EPO
<b>Verfügbarkeit des RZ</b> (bezogen auf die technischen Anlagen)	99,67%	99,75%	99,98%	99,99%

## RZ-Organisation (Beispiel)



## Einschlägige Normen für RZ-Sicherheit

### **ISAE 3402**

**(<http://isae3402.com/>)**

Der International Standard on Assurance Engagements (ISAE) 3402 ist ein Audit-Standard des International Auditing and Assurance Standards Board (IAASB). Die weltweit einheitlichen Prüfberichte beurteilen die internen Kontrollen und deren Durchführung. ISAE 3402 hat das Ziel, das interne Kontrollsystem einer Organisation umfassend zu testen und eine detaillierte Bewertung seiner Effektivität zu ermöglichen.

### **SSAE 16**

**([http://ssae16.com/SSAE16\\_overview.html](http://ssae16.com/SSAE16_overview.html))**

SSAE 16 steht für Statement on Standards for Attestation Engagements (SSAE) No. 16, Reporting on Controls at a Service Organization. SSAE 16 wurde durch das Auditing Standards Board der American Institute of Certified Public Accountants (AICPA) im Januar 2010 verabschiedet. SSAE 16 ersetzt SAS 70 – Sarbanes Oxley Act (Quelle: <http://www.soxlaw.com/>) und SAS 70 (Quelle: <http://sas70.com/>) – und ist als Prüfstandard für alle Berichtsperioden anzuwenden, die am oder nach dem 15.06.2011 enden.

### **ISO 9001**

**(<http://www.iso9001.qmb.info/>)**

Die ISO 9001 ist ein weltweit anerkannter Standard zur Implementierung und Betrieb eines Qualitätsmanagementsystems und gilt als Grundlage für die Implementierung eines Managementsystems. Die in der Norm geregelten Prozesse und Verfahren finden in allen zertifizierungsfähigen ISO-Standards zur Implementierung eines Managementsystems erneut Anwendung. Die Norm stellt keine direkten bzw. konkreten Anforderungen an die implementierten Prozesse hinsichtlich des Datenschutzes bzw. der IT-Sicherheit. In dem Managementsystem hat der Kunde eine Schlüsselrolle, in der er als Emp-

fänger eines Produktes bzw. einer Dienstleistung gewisse Erwartungen an das Produkt oder die Dienstleistungen hat.

### **IT-GS Katalog**

**([https://www.bsi.bund.de/DE/Themen/ITGrundschutz/IT-GrundschutzKataloge/itgrundschutzkataloge\\_node.html](https://www.bsi.bund.de/DE/Themen/ITGrundschutz/IT-GrundschutzKataloge/itgrundschutzkataloge_node.html))**

Als IT-Grundschutz bezeichnet man eine Vorgehensweise zum Identifizieren und Umsetzen von Sicherheitsmaßnahmen der unternehmenseigenen Informationstechnik (IT). Das Ziel des Grundschutzes ist das Erreichen eines mittleren, angemessenen und ausreichenden Schutzniveaus für IT-Systeme. Zur Erreichung des Ziels empfiehlt der Grundschutz technische, infrastrukturelle, organisatorische und personelle Maßnahmen.

### **ISO/IEC 15408 (CC)**

**(<https://www.commoncriteriportal.org/>)**

Die Norm definiert ein Kriterienwerk für die Sicherheitsevaluierung von IT-Produkten und IT-Systemen. Teil 1 stellt das allgemeine Konzept der Evaluationskriterien vor. Grundlegende Begriffe wie Sicherheitsanforderungen, Sicherheitsziele, Schutzprofile und Evaluationsgegenstand (Target of Evaluation, TOE) werden eingeführt. Teil 2 enthält einen Katalog vordefinierter Funktionalitäten. Die Sicherheitsanforderungen an die Funktionalität sind nach Klassen strukturiert und innerhalb einer Klasse weiter in Familien aufgeteilt. Jede Familie besitzt zumindest eine Komponente, in der die Sicherheitsanforderungen an die konkrete Funktionalität beschrieben werden. Darüber hinaus können eigene Sicherheitsvorgaben als Grundlage für die Evaluierung/Zertifizierung definiert werden. Teil 3 spezifiziert Kriterien für die Evaluierung von Schutzprofilen und Sicherheitsvorgaben. Die Sicherheitsvorgaben werden vor Beginn der eigentlichen Evaluierung eines TOE separat evaluiert.



## **ISO/IEC 21827**

**([http://www.iso.org/iso/catalogue\\_detail.htm?csnumber=4471](http://www.iso.org/iso/catalogue_detail.htm?csnumber=4471))**

Ziel des Dokumentes ist es, Informationssicherheit mittels eines Prozess-Referenz-Modells darzustellen. Der Standard wurde Mitte der Neunziger Jahre in den USA von staatlichen Behörden und einigen Großunternehmen aus dem allgemeinen Reifegradmodell dem sog. Capability maturity model (CMM), das besonders in der Softwareentwicklung verbreitet ist, weiterentwickelt und an die speziellen Anforderungen des Sicherheitsmanagements angepasst. Es dient dem Managen von Sicherheit in einer Organisation, indem es die einzelnen Aktivitäten - also das „Wie“ - beschreibt. Der organisatorische Reifegrad in Bezug auf das Sicherheitsmanagement wird betrachtet. Das Dokument richtet sich an den IT-Sicherheitsbeauftragten einer Organisation.

## **ISO 20000**

**([http://www.iso.org/iso/catalogue\\_detail?csnumber=51986](http://www.iso.org/iso/catalogue_detail?csnumber=51986))**

Die ISO 20000 ist ein verbreiteter Standard, der sich mit dem IT Service Management beschäftigt. Der Standard rührt aus den umfangreichen Büchern der Information Technology Information Library (ITIL) her. Sie wurden aufgrund einer Auswertung der Ereignisse beim Versagen von militärischen IT-Systemen zusammengestellt. Der Standard betrifft im Wesentlichen die Organisation der IT-Abteilungen. Er sorgt für eine klare Aufgabenabgrenzung und für die Definition eindeutiger Ansprechstellen bei IT-Problemen sowie geeignete Eskalationsstufen.

Der auf ISO 20000 bzw. ITIL abgestimmte Standard zur Informationssicherheit ist ISO 27001. Hier finden sich im Detail vielfältige Überschneidungen. Bei gleichzeitiger Einführung von IT-Grundschutz ist das Bedürfnis der Integration mit ITIL ein erfolgskritischer Faktor. Bei Anwendung von ISO 20000 ist eine sehr genaue Interpretation und Anwendung der Normerfordernisse auf die Organisation notwendig.

## **ISO 22301**

**(<http://www.bsigroup.com/en-GB/iso-22301-business-continuity/>)**

Die ISO 22301:2012 stellt die neue, zentrale Richtlinie für ein Business Continuity Management dar. Im November 2006 wurde vom British Standards Institute der British Standard 25999-1 „Business Continuity Management – Part 1: Code of Practice“ als erster offizieller Standard für den Aufbau eines Managementsystems für das betriebliche Kontinuitätsmanagement veröffentlicht. Dieser enthält unter anderem Anforderungen für den Aufbau einer Organisationsstruktur, die Umsetzung eines Business Continuity Management-Prozesses auf Basis von Good Practice Vorgaben und die Konzeption organisatorischer Maßnahmen.

## **ISO/IEC 27000-Reihe**

**(<http://www.27000.org/>)**

Die ISO/IEC 27000-Reihe ist eine Reihe von Standards der IT-Sicherheit. Herausgegeben werden die über 20 Normen (Stand: Juni 2013) von der International Organization for Standardization (ISO) und der International Electrotechnical Commission (IEC).

Die Normenreihe dient dem Schutz von Informationen als Geschäftswerten vor Bedrohungen. Sie gewinnt an Bedeutung, da sie Unternehmen in die Lage versetzt, Anforderungen dritter Instanzen zu genügen. Das sind beispielsweise gesetzliche Anforderungen (wie KonTraG, HGB sowie GoB, GoBS, GDPdU, BDSG, TMG, TKG, StGB), vertragliche Anforderungen (z.B. von Kunden) oder sonstige Anforderungen.

## **ISO 27001 mit Anlehnung an den IT-Grundschutz**

**(<https://www.bsi.bund.de>)**

Eine weitere Grundlage für den sicheren Betrieb von Rechenzentren sind die Maßgaben des IT-Grundschutz-Kataloges des Bundesamtes für Sicherheit in der Informationstechnik (BSI) für Anlagen mit erhöhtem Schutzbedarf. Neben den Rechenzentrumssystemen und den darauf betriebenen Anwendungen und Diensten für die genannten Aufgaben sind die Administrationsarbeitsplätze und Netzzugänge vom Geltungsbereich umfasst. Das ISO 27001-Zertifikat auf der Basis von IT-

Grundschatz bestätigt, dass der Informationsverbund des Dienstleistungsunternehmens durch die Anwendung des IT-Grundschatzes abgesichert wird. Das eingesetzte Informationssicherheitsmanagementsystem erfüllt die Anforderungen nach ISO 27001. Zudem bestätigt das Zertifikat, dass die technischen und organisatorischen Anforderungen der IT-Grundschatz-Methodik erfolgreich umgesetzt worden sind.

### **IT-Grundschatz, BSI Standard 100-1 bis 4 (<https://www.bsi.bund.de>.)**

Das Gesamtwerk, das in einem engeren Sinne die IT-Sicherheit einschließlich Datenschutzes behandelt, hatte eine maßnahmen-orientierte Sichtweise und stellte Standard-Maßnahmen vorwiegend für den normalen Schutbedarf vor. Diese detaillierten Maßnahmen sind von einer Organisation grundsätzlich umzusetzen, wenn eine Konformität zum IT-Grundschatzhandbuch hergestellt werden soll. Inzwischen hat sich der IT-Grundschatz insofern gewandelt, als die Ausführungen zum Sicherheitsmanagement an ISO 27001 ausgerichtet und die Methodik insgesamt der ISO 27001 angenähert wurde.

Bei der Maßnahmen-Auswahl im technischen, organisatorischen und infrastrukturellen Bereich sind weiterhin die Baustein- und Maßnahmenkataloge anzuwenden. Für die Gefährdungsanalysen existieren umfangreiche Gefährdungskataloge.

Beschreibungen der Methodik sind von diesen Katalogen getrennt und in so genannte BSI-Standards aufgenommen worden:

- 100-1: Managementsysteme für Informationssicherheit,
- 100-2: IT-Grundschatz-Vorgehensweise,
- 100-3: Risikoanalyse auf der Basis von IT-Grundschatz.

Diese Synthese von ISO-Standard und IT-Grundschatz ist für viele Anwender ein wichtiges Kriterium. Die Möglichkeiten individueller Anpassungen sind beim IT-Grundschatz natürlich geringer als bei einer Vorgehensweise nach ISO 27001. Zudem ist der Anwendungsbereich des IT-Grundschatzes stark auf Aspekte der klassischen IT-Sicherheit eingeschränkt.

### **IDW PS 330 - Abschlussprüfung beim Einsatz von Informationstechnologie**

(<http://www.idw.de/idw/portal/n281334/n281114/n302246/index.jsp>)

Dieser Standard wird bei Abschlussprüfungen eingesetzt, wenn die Rechnungslegung durch den Einsatz von Informationstechnologie umgesetzt wird. Der PS 330 beschreibt die Ziele, den Umfang, die Durchführung, Überwachungsmaßnahmen sowie die Dokumentation von rechnungslegungsrelevanten IT-Systemen. In diesem Zusammenhang spielen außerdem noch einige andere Prüfungsstandards wie der PS 340 und PS 321 eine Rolle.

### **IDW PS 951 - Die Prüfung des internen Kontrollsystems bei Dienstleistungsunternehmen**

(<http://www.idw.de/idw/portal/n281334/n281114/n302246/index.jsp>)

Der Prüfungsstandard IDW PS 951 „Prüfung des internen Kontrollsystems beim Dienstleistungsunternehmen für auf das Dienstleistungsunternehmen ausgelagerte Funktionen“ gibt vor, wie das Interne Kontrollsystem (IKS) geprüft und wie die Ergebnisse dokumentiert werden müssen. IDW PS 951 basiert auf den Anforderungen des Statement on Auditing Standards No. 70 (SAS 70) des American Institute of Certified Public Accountants (AICPA). Im Gegensatz zum SAS 70 berücksichtigt der IDW PS 951 Standard deutsche Besonderheiten. Der PS 951 bietet Dienstleistungsunternehmen die Möglichkeit über eine gesonderte Prüfung einen Nachweis für die Angemessenheit und ggf. Wirksamkeit ihres dienstleistungsbezogenen, internen Kontrollsystems zu erhalten. Eine Prüfung nach IDW PS 951 kann daher für einen Dienstleister sinnvoll sein, damit er hierüber seinen Kunden Angemessenheit und Wirksamkeit seines Kontrollsystems nachweisen kann und nicht jeder Auftraggeber dieses einzeln überprüfen muss.

## **IDW PS 980 - Grundsätze ordnungsmäßiger Prüfung von Compliance Management Systemen**

(<http://www.idw.de/idw/portal/n281334/n281114/n302246/index.jsp>)

Das Institut der Wirtschaftsprüfer in Deutschland e.V. (IDW) verdeutlicht in diesem IDW Prüfungsstandard den Inhalt freiwilliger Prüfungen von Compliance Management Systemen (CMS) und legt die Berufsauffassung dar, nach der Wirtschaftsprüfer unbeschadet ihrer Eigenverantwortlichkeit derartige Aufträge durchführen. Als integraler Bestandteil der Corporate Governance des Unternehmens ist das Compliance Management System auf die Einhaltung von Regeln im Unternehmen ausgerichtet. Die Einrichtung, Ausgestaltung und Überwachung des CMS ist eine im Organisationsermessen der gesetzlichen Vertreter stehende unternehmerische Entscheidung, durch die die gesetzlichen Vertreter vor dem Hintergrund der unternehmensindividuellen Gegebenheiten ihrer Leitungspflicht zur präventiven Sicherstellung der Gesetzeskonformität des Unternehmens nachkommen.

## **IDW RS FAIT 1 - Grundsätze ordnungsgemäßer Buchführung bei Einsatz von Informationstechnologie**

(<http://www.idw.de/idw/portal/d302224>)

IDW FAIT 1 ist eine Stellungnahme, die die Anforderungen der §§ 238, 239 und 257 HGB für die IT-gestützte Führung der Handelsbücher konkretisiert. Sie stellt die grundlegenden Definitionen für die IT-spezifischen Prüfungsstandards des IDW (z.B. PS 330, PS 880) zusammen. Insbesondere wird hier der Geltungsbereich des Begriffs „IT-System“ definiert. Im Gegensatz zu anderen Standards ist „IT-System“ hier nicht als Hardware inklusive Betriebssystem, sondern als übergeordneter Begriff zu verstehen. Ein IT-System nach RS FAIT 1 beinhaltet die rechnungslegungsrelevanten IT-gestützten Geschäftsprozesse, IT-Anwendungen, IT-Infrastruktur wie bauliche Einrichtungen, Hardware und den IT-Betrieb. Das Zusammenwirken der Elemente des IT-Systems wird durch das IT-Kontrollsystem definiert. In diesem werden die Risiken des IT-Einsatzes behandelt. Neben den Sicherheitsanforderungen werden in der RS FAIT 1 die gesetzlichen Anforderungen ordnungsgemäßer Buchführung auf die IT abgebildet. Der Standard legt hier die im

HGB verlangten Werte Vollständigkeit, Richtigkeit, Zeitgerecht, Ordnung, Nachvollziehbarkeit und Unveränderlichkeit für die IT aus.

### **IDW RS FAIT 2 - Grundsätze ordnungsgemäßer Buchführung bei Einsatz von Electronic Commerce**

**(<http://www.idw.de/idw/portal/d302224>)**

Diese IDW Stellungnahme zur Rechnungslegung konkretisiert die aus den §§ 238, 239 und 257 HGB resultierenden Anforderungen an die Führung der Handelsbücher mittels IT gestützter Systeme. Sie verdeutlicht damit die im IDW RS FAIT 1 dargestellten Ordnungsmäßigkeits- und Sicherheitsanforderungen im Bereich von E-Commerce und stellt ergänzende, über den IDW RS FAIT 1 hinausgehende Anforderungen auf, um den mit dem Einsatz von E-Commerce-Systemen zusammenhängenden besonderen IT-Risiken zu begegnen.

### **IDW RS FAIT 3 - Grundsätze ordnungsgemäßer Buchführung beim Einsatz elektronischer Archivierungssysteme**

**(<http://www.idw.de/idw/portal/d302224>)**

Die Überprüfung der Einhaltung der Vorgaben und die Zertifizierung von elektronischen Archivsystemen, bzw. in kaufmännische Anwendungen oder Dokumentenmanagement integrierte Archivkomponenten, erfolgt in der Regel durch Wirtschaftsprüfer beim Anwender vor Ort. Seitens des IDW, Institut der deutschen Wirtschaftsprüfer, gibt es hierfür mit den FAIT eigene Vorgaben. Die Einhaltung der Revisionssicherheit kann auf Grundlage einer Verfahrensdokumentation zertifiziert werden.

### **IDW RS FAIT 4 - Anforderungen an die Ordnungsmäßigkeit und Sicherheit IT-gestützter Konsolidierungsprozesse**

**(<http://www.idw.de/idw/portal/d302224>)**

Die IDW Stellungnahme zur Rechnungslegung Anforderungen an die Ordnungsmäßigkeit und Sicherheit IT-gestützter Konsolidierungsprozesse (IDW RS FAIT 4) wurde vom HFA am 08.08.2012 verabschiedet. IDW RS FAIT 4 konkretisiert die aus den §§ 290 bis 315 HGB resultie-

renden Anforderungen an IT-gestützte Konsolidierungsprozesse. Veranschaulicht werden die im IDW RS FAIT 1 (Grundsätze ordnungsmäßiger Buchführung bei Einsatz von Informationstechnologie) dargestellten Ordnungsmäßigkeits- und Sicherheitsanforderungen für die softwaregestützte Konzernabschlusserstellung.

### **COSO**

**(<http://www.coso.org>)**

Das COSO (Committee of Sponsoring Organizations of the Treadway Commission) ist eine freiwillige privatwirtschaftliche Organisation in den USA, die helfen soll, Finanzbericht-erstattungen durch ethisches Handeln, wirksame interne Kontrollen und gute Unternehmensführung qualitativ zu verbessern. COSO hat einen anerkannten Standard für interne Kontrollen, das COSO-Modell publiziert. Dieses Kontrollmodell dient der Dokumentation, Analyse und Gestaltung des internen Kontrollsystems, es gliedert sich in die drei Bereiche: Operationelle Risiken, Finanzberichterstattung und Compliance.

Die Bestandteile des internen Kontrollsystems nach dem COSO-Modell sind Kontrollumfeld, Risikobeurteilung, Kontrollaktivitäten, Information und Kommunikation, Überwachung.

### **COBIT = Control Objectives for Information and related Technologies**

**(<http://www.isaca.org/COBIT/Pages/default.aspx?cid=1003566&Appeal=PR>)**

COBIT ist ein Verfahren zur IT Governance und gliedert die Aufgaben der IT in Prozesse und Control Objectives (Regelziele). COBIT verfolgt ähnlich ISO 27001 einen Top-Down Ansatz, bei dem ausgehend von den Geschäftszielen IT-Ziele festgelegt werden, welche wiederum die IT-Architektur beeinflussen. COBIT nimmt für sich in Anspruch, ein integrierendes Modell zu sein, welches die Anforderungen sämtlicher verbreiteter Modelle für die IT-Organisation in einem Reifegradmodell integriert.

COBIT wurde 1993 vom internationalen Verband der IT-Prüfer und Auditoren ISACA entwickelt und steht seit 2000 unter Verantwortung des IT-Governance Institute, einer Schwesterorganisation der ISACA.

COBIT 4.1. definiert 34 Prozesse zur Verarbeitung von Informationen, Planung von IT-Ressourcen und Erbringung von Services. In jedem Prozess wird beschrieben, wie mit Hilfe von Control Objectives (Steuervorgaben) zuvor definierte Prozessziele erreicht werden können. COBIT 5.0 ist derzeit das aktuelle Regelwerk. COBIT 5 als ausgereiftes Modell zur Unterstützung bei der Implementierung der unternehmensweiten Governance und des Managements der Unternehmens-IT dar. COBIT 5 unterstützt die Implementierung eines Managementsystems nach ISO 27001 durch inhaltliche Überschneidungen und eine verbesserte Ausrichtung auf die Unterstützung der Business Prozesse und Unternehmensziele. Ausgeprägte Synergien ergeben sich bei der Implementierung eines IT-Service-Managementsystems nach ISO 20000.

**ITIL = Information Technology Infrastructure Library**  
**(<http://www.itil-officialsite.com/>)**

ITIL ist von britischen Regierungsbehörden entwickelt und in Büchern definiert, die vom Office of Government Commerce seit 1989 herausgegeben werden.

Beschrieben werden Modelle und Organisationsformen für IT-Servicemanagement nach „Best-Practice“ Ansätzen. In verschiedenen Büchern (+1 Ergänzungsbuch) werden Aufgabenstellungen definiert, die beim Betrieb der IT-Infrastruktur anfallen

ITIL beschreibt nicht, wie etwas getan werden muss, sondern nur was getan werden sollte. Es ist keine Zertifizierung als „ITIL konform“ möglich, aber eine Zertifizierung nach zugehöriger Norm ISO 20000.





# Zertifizierungskriterien

Zertifizierungskriterien können sein:	
Sicherheitsmanagement beim Anbieter	Einhaltung der Sicherheitsrichtlinien nach deutschen Datenschutzbestimmungen durch den Serverstandort Deutschland
	Prozessmanagement nach ITIL-Standards
	Zertifizierung nach ISO 27001
	Zertifizierung Trusted Cloud
	benannter Datenschutzbeauftragter nach BDSG & etabliertes Security Management
Rechenzentrumssicherheit	Redundante Auslegung aller Versorgungskomponenten (Backbone, Klimatisierung, Strom)
	Zutrittskontrollsysteme inkl. Videoüberwachung & Alarmsystem
	Brandschutzsysteme, Brandmeldeanlage, Brandfrüherkennungssysteme und regelmäßige Brandschutzübungen
Serversicherheit	Sichere Grund-Konfiguration des Hosts durch Einsatz gehärteter Betriebssysteme: <ul style="list-style-type: none"> <li>• Systematisches Patchmanagement</li> <li>• Dienstverwaltung</li> <li>• Benutzerverwaltung</li> <li>• Rechteverwaltung auf Dateisystemebene</li> <li>• Gesicherter Zugang</li> </ul>
	Qualitätsgesicherte Images für virtuelle Maschinen

<b>Zertifizierungskriterien können sein:</b>	
Netzsicherheit	Netzsegmentierung
	Fernadministration durch verschlüsselten Remote-Zugang
Datensicherheit	Sichere Isolierung der Kundendaten durch virtuelle Speicherbereiche
	Vollständige und zuverlässige Löschung der Kundendaten nach Beendigung des Vertragsverhältnisses oder auf Wunsch des Kunden
Rechtemanagement	Rollenbasierte Zugriffskontrolle und regelmäßige Überprüfung der Rollen und Rechte
	Least Privilege Mode
	Vier-Augen-Prinzip für kritische Administrationstätigkeiten
Monitoring & Security Incident Management	24/7 umfassende Überwachung der Cloud-Infrastruktur sowie zeitnahe Reaktion
	Erfassung und Auswertung von Datenquellen, wie z.B. Systemlogs usw., sowie der Administratortätigkeiten
	24/7-erreichbares, handlungsfähiges Team für Security Incident Handling
	Bereitstellung relevanter Logdaten auf Kundenwunsch unter Berücksichtigung des Datenschutzes
Notfallmanagement	Notfallmanagementsystem
	Regelmäßige Wartungen und Tests sowie Notfallübungen

<b>Zertifizierungskriterien können sein:</b>	
Anforderungen an Personal	Regelmäßige Schulungen des Personals
	Sensibilisierung der Mitarbeiter für Informationssicherheit und Datenschutz
	Verpflichtung der Mitarbeiter auf Datenschutz sowie angemessenen Umgang mit Kundendaten
Transparenz	Offenlegung der Standorte, an denen Kundendaten gespeichert und verarbeitet werden
	Regelmäßige und anlassbezogene Unterrichtung über Änderungen



## Begriffserläuterungen

<b>Ausstattungsmerkmale</b>	<b>Technische Infrastruktur eines RZs</b>
Colocation	Bereitstellung von Rechenzentrumsfläche und Netzanbindung zum Betrieb von Kundensystemen.
Daten	Formalisierte Darstellung von Fakten, Konzepten oder Befehlen, geeignet für Kommunikation, Interpretation oder Verarbeitung durch Menschen oder automatisierte Abläufe.
Datenträger	Objekt oder Gegenstand, der Daten enthält
Datenverarbeitung im Auftrag	Erhebung, Verarbeitung und Nutzung von Daten durch beauftragte Dritte
dediziert, dedizierter Server	Server, der nur dafür da ist, ganz bestimmte Dienste und Daten anderen Rechnern zukommen zu lassen oder nur für ganz bestimmte Großkunden zu arbeiten
Einrichtung	Zusammenstellung von in räumlichem und funktionalem Zusammenhang stehenden Maschinen zum Zweck der Datenträgervernichtung
Fehlertoleranz	In der Technik, besonders in der Datenverarbeitung, bedeutet Fehlertoleranz die Eigenschaft eines technischen Systems, seine Funktionsweise auch aufrechtzuerhalten, wenn unvorhergesehene Eingaben oder Fehler in der Hard- oder Software auftreten.

Hosting	Kompletter Betrieb der Kundensysteme durch den Hostinganbieter (im RZ des Anbieters)
Housing	Bereitstellung von Rechenzentrumsfläche und Netzanbindung zum Betrieb von Kundensystemen
Hybrid Cloud	Die Hybrid Cloud ist eine Mischform aus Private- und Public Cloud
Infrastructure as a service, IaaS	Bereitstellung von virtuellen, dynamisch anpassbaren Ressourcen (z.B. Speicher)
Personenbezogene Daten	Einzelangaben über persönliche oder sachliche Verhältnisse einer bestimmten oder bestimmbarer natürlichen Person
Performance	Leistungsfähigkeit
Platform as a Service, PaaS	Bereitstellung von virtuellen, dynamisch anpassbaren IT-Systemen (z.B. Rechen- und Speicherkapazitäten)
Private Cloud	Eigene Cloud für einen eingeschränkten Kreis von Anwendern
Public Cloud	Public Cloud ist die Cloud eines Anbieters von standardisierten Diensten
Rechenzentrum Eigenbetrieb	Betrieb der IT-Infrastruktur in den eigenen Räumlichkeiten
Rechenzentrum Fremdbetrieb	Verarbeitung von Daten durch einen Dienstleister
Redundanz, Technik	mehrfaches Vorhandensein funktional gleicher oder vergleichbarer technischer Ressourcen, wenn diese für den störungsfreien Normalbetrieb nicht benötigt werden.

Schutzbedarf	Eigenschaft von Daten und Informationen, welche unter Berücksichtigung der bei einer Verletzung der Grundwerte Vertraulichkeit, Integrität oder Verfügbarkeit zu erwartenden Schäden die Notwendigkeit beschreibt, diese Daten und Informationen vor einer Verletzung dieser Grundwerte zu bewahren.
Schutzniveau	Definition nach BSI-Standard 100-2 : normal, hoch, sehr hoch  Nach der Bestimmung des zutreffenden Sicherheitsniveaus kann diese als Grundlage einer Schutzbedarfsfeststellung der Geschäftsprozesse dienen
Schutzzweck	Wahrung der Grundwerte der Informationssicherheit auf Vertraulichkeit, Integrität und Verfügbarkeit der Daten. Im Entsorgungsprozess ist die Vertraulichkeit (Kenntnisnahme von Unbefugten) ein Schutzzweck, dem ein ausreichendes Schutzniveau zugeordnet werden muss.
Sicherheitskonzept	Ein Sicherheitskonzept stellt im Allgemeinen eine Analyse möglicher Angriffs- und Schadensszenarien mit dem Ziel, ein definiertes Schutzniveau zu erreichen. Unterschieden werden muss dabei die Sicherheit gegenüber böswilligen Angriffen ( <i>Security</i> ) und die Sicherheit gegenüber menschlichem und technischem Versagen ( <i>Safety</i> ).
Sicherheitsstufe	Klassifizierung des Aufwands zur Wiederherstellung von Informationen



## Begriffserläuterungen

---

Sicherheitszone	Entsprechend der Schutzklasse geschützter Bereich
Software (Anwendung) as a Service, SaaS	Bereitstellung einer virtuellen , mandantenfähigen Softwarelösung
Verantwortliche Stelle	Jede Person oder Stelle, die Daten für sich selbst erhebt, verarbeitet oder nutzt oder dies durch andere im Auftrag vornehmen lässt
Verfügbarkeit	die Wahrscheinlichkeit oder das Maß, dass das System bestimmte Anforderungen innerhalb eines vereinbarten Zeitrahmens erfüllt
Vernichtung	Vorgang, bei dem Form oder Zustand von Datenträgern in der Regel durch Zerkleinern, Auflösen, Schmelzen, Erhitzen oder Verbrennen verändert werden

## Abkürzungsverzeichnis

AAA	American Accounting Association
ADV	Auftragsdatenverarbeitung gemäß § 11 BDSG
AICPA	American Institute of Certified Public Accountants
AktG	Aktiengesetz
AO	Abgabenordnung
BaFin	Bundesanstalt für Finanzdienstleistungsaufsicht
BDSG	Bundesdatenschutzgesetz
BR	Betriebsrat
BSI	Bundesamt für Sicherheit in der Informationstechnik
BSIG	Gesetz über die Errichtung des Bundesamtes für Sicherheit in der Informationstechnik
BVerfG	Bundesverfassungsgericht
CESR	Committee of European Securities Regulators
CIO	Chief Information Officer
COBIT	Control Objectives for Information and Related Technology
COSO	Committee of Sponsoring Organizations of the Treadway Commission
CTO	Chief Technology Officer/Chief Technical Officer
D	Deutschland
DCGK	Deutscher Corporate Governance Kodex
DL	Dienstleister

DS	Datenschutz
DSB	Datenschutzbeauftragter
DV	Datenverarbeitung
Ecofin-Rat	Rat der Europäischen Union in der Formation „Wirtschaft und Finanzen“
ECV	Emittenten-Compliance-Verordnung
EDPAA	Electronic Data Processing Auditors Association
EG	Europäische Gemeinschaft
EMV	elektromagnetische Verträglichkeit
ERFA	Erfahrungsaustauschkreis
EU	Europäische Gemeinschaft
FASB	Financial Accounting Standards Board
FC	Federal Criteria
FDIC	Federal Deposit Insurance Corporation
FEI	Financial Executives International
FESCO	Forum of European Securities Commissions
FFIEC	Federal Financial Institutions Examinations Council
FIPS	Federal Information Processing Standards
FISMA	Federal Information Security Management Act of 2002
FRB	Federal Reserve Bank / Federal Reserve System
FSAP	Financial Services Action Plan
GDD	Gesellschaft für Datenschutz und Datensicherheit e.V.

GDPdU	Grundsätze zum Datenzugriff und zur Prüfbarkeit digitaler Unterlagen
GLP	Good Laboratory Practice
GLT	Gebäudeleittechnik
GMP	Good Manufacturing Practice
GoB	Grundsätze ordnungsmäßiger Buchführung
GoBS	Grundsätze ordnungsmäßiger DV-gestützter Buchführungssysteme
HGB	Handelsgesetzbuch
HIPAA	Health Insurance and Accountability Act
IAM	Identity and Access Management
IAS	International Accounting Standards
IASB	International Accounting Standards Board
IASC	International Accounting Standards Committee
IDW	Institut der Wirtschaftsprüfer in Deutschland
IDW	PS 330 IDW-Prüfungsstandard 330
IDW	PS 880 IDW-Prüfungsstandard 880
IDW	RS FAIT 1 IDW-Stellungnahme zur Rechnungslegung Fachausschuss IT 1
IEC	International Electrotechnical Commission
IFRS	International Financial Reporting Standards
IIA	Institute of Internal Auditors
IMA	Institute of Management Accountants
ISA 401	International Standards on Auditing 401
ISACA	Information Systems Audit and Control Association

ISD	Investment Services Directive
ISMS	Information Security Management System
ISO	Internationale Organisation für Normung
IT	Informationstechnologie
ITCi IT	Compliance Institute
ITGI IT	Governance Institute
ITIL IT	IT Infrastructure Library
ITSEC	Information Technology Security Evaluation Criteria (Kriterien für die Bewertung der Sicherheit von Informationstechnologie)
ITSM	IT-Servicemanagement
itSMF	Information Technology Service Management Forum
ISMS	Information Security Management System Managementsystem für Informationssicherheit
JCB	Japan Credit Bureau
KonTraG	Kontroll- und Transparenzgesetz
KWG	Kreditwesengesetz
LDSG	Landesdatenschutzgesetz
MaRisk	Mindestanforderungen an das Risikomanagement
MiFID	Markets in Financial Instruments Directive
MLPS	multi-label protocolswitching
NAA	National Association of Accountants
NAS	Network Attached Storage, netzgebundener Speicher
NCUA	National Credit Union Administration

NIST	National Institute of Standards and Technology
OCC	Office of the Comptroller of the Currency
OECD	Organization for Economic Cooperation and Development
OGC	Office of Global Communications, US-amerik. Behörde
OTS	Office of Thrift Supervision
PCAOB	Public Company Accounting Oversight Board
PCI DSS	Payment Card Industry Data Security Standard
PIN	Persönliche Identifikationsnummer
PKI	Public Key Infrastructure
RC	Resistance Class (Widerstandsklasse; früher WK)
REACH	Registration, Evaluation and Authorization of Chemicals
RFID	radio-frequency identification
ROI	Return on Investment
RZ	Rechenzentrum
SAN	Storage-Area-Network bzw. Speichernetzwerk
SAS 70	Statment on Auditing Standards No. 70
SEC	United States Securities and Exchange Commission
SEM	Security Event Management
SigG	Signaturgesetz
SIEM	Security Information and Event Management
SIM	Security Information Management

SLA	Service-Level-Agreement, Dienstleistungsvereinbarung
SOX	Sarbanes-Oxley Act
TGA	Technische Grundausrüstung
TKG	Telekommunikationsgesetz
TMG	Telemediengesetz
TUG	Transparenzrichtlinie-Umsetzungsgesetz
TK	Telekommunikation
US-GAAP	United States Generally Accepted Accounting Principles
USV	Unterbrechungsfreie Stromversorgung
VDE	Verband der Elektrotechnik Elektronik Informationstechnik e.V.
VdS	Vertrauen durch Sicherheit (Anerkennungsverfahren DIN)
WAN	Wide Area Network
WK	Widerstandsklasse (heute RC)

## Quellen

BSI, Bundesamt für Sicherheit in der Informationstechnik, [www.bsi.de](http://www.bsi.de)

BITKOM, das Sprachrohr der IT-, Telekommunikations- und Neue-Medien-Branche, [www.bitkom.org](http://www.bitkom.org)

CEN, European Committee for Standardization, [www.cen.eu](http://www.cen.eu)

COSO, committee of Sponsoring Organizations, [www.coso.org](http://www.coso.org)

DIN, Deutsches Institut für Normung, [www.din.de](http://www.din.de)

Europäisches Parlament, [www.europarl.europa.de](http://www.europarl.europa.de)

GDD-Leitfaden Datenschutzgerechte Datenträgervernichtung, 2014

GDD, Gesellschaft für Datenschutz und Datensicherheit e. V.,  
[www.gdd.de](http://www.gdd.de)

Gesetze im Internet, [www.gesetze-im-internet.de](http://www.gesetze-im-internet.de)

ISACA, Information Systems Audit and Control Association,  
[www.isaca.de](http://www.isaca.de)

ISO, International Organization for Standardization, [www.iso.org](http://www.iso.org)

ITIL, Information Technology Infrastructure Library, [www.itil-officialsite.com](http://www.itil-officialsite.com)

Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein,  
[www.datenschutzzentrum.de](http://www.datenschutzzentrum.de)

Uptime Institute, The Global Data Center Authority,  
[www.uptimeinstitute.com](http://www.uptimeinstitute.com)

PCI DSS, Payment Card Industry Data Security Standard,  
[www.pcisecuritystandard.org](http://www.pcisecuritystandard.org)

WIKIPEDIA, Die freie Enzyklopädie, [www.wikipedia.de](http://www.wikipedia.de)

EuroPrise, Europäisches Datenschutz-Gütesiegel, [www.european-privacy-seal.eu](http://www.european-privacy-seal.eu)





# Die Checklisten

Ratgeber und Checklisten stehen zum Download zur Verfügung.

→ <https://www.gdd.de/gdd-arbeitshilfen/gdd-ratgeber>

Beispiel einer Checkliste:

Kontrolle von elektronischen Übertragungen										
1	Werden personenbezogene Daten des Auftraggebers an andere Stellen elektronisch übertragen? Wenn ja: + An welche Stellen werden Daten übertragen? + An welche Stellen ist die Übertragungsganglinie?	X	-	-	X	X	X	X	X	X
2	Welche personenbezogenen Daten werden übertragen? (bei Stand ermittelt) + Art der Daten + Zweck + Quelle, Absender, Verantwortlichkeit + Ziel, Empfänger	X	-	-	X	X	X	X	X	X
3	Welche Übertragungswege werden genutzt? Beispiele: + E-Mail + Internet (IP, SIP) + Festverbindung (z. B. MPLS) + SD-WAN + GPRS, GSM + Datenkabeltransporte	X	-	-	X	X	X	X	X	X
4	Wie werden die Daten während der Übertragung vor unberechtigten Zugriffen geschützt? Beispiele: + Verschlüsselter Übertragungsweg (z. B. IPSec, VPN, LAN, https/SFTP) + Datenverschlüsselung	X	-	-	X	X	X	X	X	X
5	Ist die Passwörterhandlung ausreichend sicher? + Werden ausreichend komplexe Passwörter verwendet? + Erfolgt die Übermittlung von Passwörtern auf einem getrennten Weg?	X	-	-	X	X	X	X	X	X
6	Muss das Einrichten von neuen Übertragungswegen genehmigt werden (z. B. durch die Geschäftsleitung)?	X	-	-	X	X	X	X	X	X
7	Erfolgt vor der Einrichtung einer neuen Datenübertragung oder der Durchführung eines Datenübertragungsvertrags die Prüfung der Legitimation des Genehmigers (bgl. die Berechtigung vor)?	X	-	-	X	X	X	X	X	X
8	Wer ist befugt, neuen Übertragungswege einzurichten?	X	-	-	X	X	X	X	X	X
9	Wird die Übertragung von personenbezogenen Daten protokolliert?	X	-	-	X	X	X	X	X	X
10	Wird die Integrität der empfangenen Daten vor der Weiterverarbeitung geprüft?	X	-	-	X	X	X	X	X	X
11	Legen entsprechende Verträge zu Datenübertragungen vor?	X	-	-	X	X	X	X	X	X
12	Sind alle Übertragungswege dokumentiert (z. B. in einem Netzwerkverzeichnis)?	X	-	-	X	X	X	X	X	X
13	Werden Angriffe auf die Netzwerksicherheit (Übertragungswege) zeitnah erkannt?	X	-	-	X	X	X	X	X	X
14	Werden regelmäßig Maßnahmen durchgeführt, um eine ausreichende Sicherheit für die Netzwerkausgänge sicherzustellen? Beispiele: + Schwachstellen-Scan (Vulnerability Scan) + Penetrationstests + Firewall-Updates	X	-	-	X	X	X	X	X	X
Kontrolle von Datentransportwegen										
15	Erfolgt Datentransporte? Wenn ja, welche Transportarten von Datenträgern gibt es? + Logistikdienstleister (z. B. Paketdienst, Kurierdienst, zweifelhafte Bots) + Begeleitete Transporte	X	-	-	X	X	X	X	X	X
16	Wurde der Schutzbedarf der Datenträger und die daraus resultierenden Maßnahmen zum Schutz während des Transports festgelegt?	X	-	-	X	X	X	X	X	X
17	Werden alle Datenträger versiegelt? Beispiele: + Kennzeichnung von Datenträgern (z. B. Datenträgerkennzeichnung) + Kennzeichnung des Datenträgers (Schlüsselwort) + Inventarisierung des Datenträgers (Sicherheitskopie) + Dokumentation von Auf- und Entnahmen von Datenträgern + Durchführung von Inventuren	X	-	-	X	X	X	X	X	X
18	Ist sichergestellt, dass nur berechnete Personen auf die Dokumenten zugreifen können?	X	-	-	X	X	X	X	X	X
19	Werden Lieferschein bzw. Datenträger-Begleitzettel erstellt (Dokumentation des Versands bzw. des Transports)? Beispiele: + Anzahl der Zeichnung der Datenträger + Hinweis zur Durchführung des Transports (z. B. Maßnahmen zum Schutz des Datenträgers) + Am Transport beteiligten Personen/Orten festgelegt (Ausgabe, Transport und Empfang der Datenträger) + Prüfung der Legitimation vor der Übergabe der Datenträger an den Empfänger + Bestätigung der ausgehenden Daten + Empfangsbestätigung durch den Empfänger (ggf. mit Rückmeldung)	X	-	-	X	X	X	X	X	X
20	Müssen Datenträger Transportwege genehmigt werden? Wenn ja, wer ist befugt, diese zu genehmigen?	X	-	-	X	X	X	X	X	X
21	Erfolgt vor der Durchführung eines Datenübertragungsvertrags die Prüfung der Legitimation des Genehmigers (bgl. die Berechtigung vor)?	X	-	-	X	X	X	X	X	X
22	Wie werden die Datenträger während des Transports vor unberechtigten Zugriffen geschützt? Beispiele: + Verschlüsselter Datenträger + Verschlüsselte Transportverpackung	X	-	-	X	X	X	X	X	X
23	Können unberechtigte Zugriffe während des Transports erkannt werden? Beispiel: + Sicherung der Transportverpackung durch Siegel + Überprüfung der Integrität der Daten (Vollständigkeitsprüfung)	X	-	-	X	X	X	X	X	X
24	Werden Maßnahmen zum Schutz der Datenträger vor Umweltklimaschwankungen (z. B. Störstrahlung, hohe Feuchtigkeit, Temperaturschwankungen, Luftfeuchtigkeit)?	X	-	-	X	X	X	X	X	X
25	Erfolgt der Transport auf dem besten Weg oder werden die Datenträger zweigeteilt? Bei einer Zweiteilung: Welche Maßnahmen werden zum Schutz der Datenträger umgesetzt?	X	-	-	X	X	X	X	X	X
26	Werden die Personen, die einen begleiteten Transport durchführen, speziell geschult (richtiges Verhalten während des Transports, Medien von Verboten, etc.)?	X	-	-	X	X	X	X	X	X
27	Werden Datenträger vor dem Empfangen der Daten auf das Vorhandensein von Mängeln geprüft?	X	-	-	X	X	X	X	X	X
Kontrolle von Wertungsdaten										
28	Kann während der Durchführung von Wertungsarbeiten auf personenbezogene Daten zugegriffen werden?	X	-	-	X	X	X	X	X	X
Kontrolle von privaten Datenträgern										
29	Ist der Einsatz nicht autorisierter Datenträger (z. B. private Datenträger) genehmigt?	X	-	-	X	X	X	X	X	X

## Zum Umgang mit den Checklisten

Die gesamten Checklisten können als Microsoft Excel™-File heruntergeladen und angepasst werden.

Im Leitfaden haben wir uns darauf beschränkt, nur die ersten zwei Spalten (Nummerierung und Fragen) abzudrucken. In einer Checkliste stehen Ihnen nach dem Download 11 weitere Spalten zur Verfügung.

In 10 Spalten ist durch Kreuze die Zugehörigkeit einer Frage zu den Rechenzentrumsausprägungen gesetzt. Außerdem wird in den Spalten 8, 9 und 10 auf den Schutzbedarf eingegangen.

In der 11. Spalte können sie eigene Bemerkungen eintragen.

Systematik der weiteren Spalten (Beispiel):

1	2	3	4	5	6	7	8	9	10
				Cloud			Schutzbedarf		
Eigenes RZ	Colocation	Housing	Hosting	Infrastruktur (IaaS)	Plattform (PaaS)	Anwendung (SaaS)	Normal	Hoch	Sehr hoch

## Checkliste Organisation

### Auftragsdatenverarbeitung i.S.d. § 11 BDSG

1	Werden im Rahmen der Beauftragung personenbezogene Daten des Auftraggebers (verantwortliche Stelle) durch den Auftragnehmer weisungsgebunden verarbeitet oder genutzt?
2	<p>Existiert ein schriftlicher Auftrag, in dem insbesondere folgende Punkte festgelegt wurden?</p> <ul style="list-style-type: none"> <li>• Gegenstand und Dauer des Auftrags</li> <li>• Umfang, Art und Zweck der vorgesehenen Erhebung, Verarbeitung oder Nutzung</li> <li>• Art der Daten und Kreis der Betroffenen</li> <li>• die nach § 9 BDSG und Anlage zu treffenden technischen und organisatorischen Maßnahmen</li> <li>• Berichtigung, Löschung und Sperrung von Daten</li> <li>• die bestehenden Pflichten des Auftragnehmers, insbesondere die von ihm vorzunehmenden Kontrollen</li> <li>• etwaige Berechtigung zur Begründung von Unterauftragsverhältnissen</li> <li>• Kontrollrechte des Auftraggebers und die entsprechenden Duldungs- und Mitwirkungspflichten des Auftragnehmers</li> <li>• mitzuteilende Verstöße des Auftragnehmers oder der bei ihm beschäftigten Personen</li> <li>• Umfang der Weisungsbefugnisse</li> <li>• Rückgabe überlassener Datenträger und die Löschung beim Auftragnehmer gespeicherter Daten nach Beendigung des Auftrags</li> </ul>
3	Sind die umgesetzten technischen und organisatorischen Maßnahmen dokumentiert?
4	Wann wurde die letzte Prüfung der technischen und organisatorischen Maßnahmen durchgeführt?

5	<p>Ist der Ort für die Vertragsausführung bzw. der Datenverarbeitung schriftlich vereinbart? Beispiele:</p> <ul style="list-style-type: none"><li>• Ort des Rechenzentrum bzw. des Backup-Rechenzentrum,</li><li>• Cloud-Dienstleistung: In welchem Land werden die Daten verarbeitet? (D, EU, USA etc.)</li></ul>
6	<p>Ist der Umgang mit Weisungen vertraglich eindeutig geregelt?</p> <p>Beispiele:</p> <ul style="list-style-type: none"><li>• Wer darf wem gegenüber Weisungen erteilen? Ist sichergestellt, dass Weisungen immer in schriftlicher Form erfolgen?</li><li>• Umfang der Weisungsbefugnisse</li><li>• Ist vertraglich vereinbart, dass der Auftragnehmer den Auftraggeber unverzüglich informiert wenn er der Meinung ist, eine Weisung verstoße gegen datenschutzrechtliche Vorschriften?</li></ul>
7	<p>Ist mit dem Auftragnehmer vertraglich vereinbart, dass das Speichern, Verändern oder Nutzen der Daten für andere Zwecke unzulässig ist?</p>
8	<p>Ist der zulässige Rahmen eines Remote-Zugangs vereinbart (z.B. Fernwartung aus Privatwohnungen [Telearbeit])?</p>
9	<p>Sind bei Telearbeit Zutritts- und Kontrollrechte für den Auftraggeber vereinbart?</p>
10	<p>Sind bei Telearbeit Vorgaben zu Sicherheitsmaßnahmen vereinbart, die der Telearbeiter beachten und einhalten muss?</p>
11	<p>Ist vertraglich vereinbart, wie die Entsorgung bzw. Vernichtung von Datenträgern (z.B. Bänder, Festplatten, Papier) zu erfolgen hat? Eine Rekonstruktion von entsorgten Datenträgern darf nicht möglich sein.</p>

12	Sind Nachweise über die sichere Entsorgung von Datenträgern verfügbar?
13	Ist die Einbeziehung von Unterauftragnehmern im Rahmen der Verarbeitung oder Nutzung der Daten des Auftraggebers Unterauftragnehmer vertraglich geregelt?
14	Wenn ja, ist sichergestellt, dass die vertraglich vereinbarten Regelungen auch für den Unterauftragnehmer gelten?
15	Welche Unterauftragnehmer werden derzeit durch den Auftragnehmer eingesetzt? Liegt für jede Unterbeauftragung eine schriftliche Genehmigung durch den Auftraggeber vor?
16	Beinhaltet der Vertrag mit dem Auftragnehmer, dass Auskünfte an Dritte oder den Betroffenen nur nach einer vorherigen schriftlicher Zustimmung durch den Auftraggeber erteilt werden dürfen?
17	Wann hat sich der Datenschutzbeauftragte des Auftragnehmers zuletzt von der Einhaltung der beim Unterauftragnehmer getroffenen technischen und organisatorischen Maßnahmen überzeugt? Liegen hierzu schriftliche Aufzeichnungen vor?
18	Ist vertraglich vereinbart, welche fachliche Qualifikation und Zuverlässigkeit die mit der Wartung und Systembetreuung beauftragten Beschäftigten des Auftragnehmers aufweisen müssen (z.B. aus § 11 Abs. 4 DSG NRW)? Wenn gefordert, liegen entsprechende Nachweise vor?
19	Werden die per E-Mail zwischen dem Auftraggeber und dem Auftragnehmer übertragenen Daten verschlüsselt übertragen?
20	Ist sichergestellt, dass neue gesetzliche Anforderungen rechtzeitig an den Auftragnehmer kommuniziert werden?

## Datenschutzbeauftragter i.S.d. § 4f BDSG

21	Wurde ein Datenschutzbeauftragter schriftlich bestellt (§ 4f BDSG)?
22	Ist der Datenschutzbeauftragte direkt der Geschäftsführung unterstellt (Organigramm einsehen)?
23	Welche Fachkunde hat der Datenschutzbeauftragte? Liegen Nachweise über die Fachkunde vor?
24	Wird sichergestellt, dass die Fachkunde aufrechterhalten und erweitert wird? Nimmt der Datenschutzbeauftragte an Fortbildungsmaßnahmen teil?
25	Wie wird die Zuverlässigkeit (einschließlich persönlicher Integrität und Unabhängigkeit) des DSB sichergestellt? Sind Interessenskonflikte im Unternehmen ausgeschlossen (z.B. welche weiteren Funktionen hat der Datenschutzbeauftragte)?
26	<p>Wie ist der Datenschutzbeauftragte in die Organisation eingebunden?</p> <ul style="list-style-type: none"><li>• Wurde der Datenschutzbeauftragte in das Organigramm aufgenommen?</li><li>• Hat der Datenschutzbeauftragte ein Vorspracherecht bei der Geschäftsführung?</li><li>• Stehen dem Datenschutzbeauftragten ausreichende Ressourcen zur Verfügung?</li><li>• Führt der Datenschutzbeauftragte interne Prüfungen durch und gibt es hierzu Berichte?</li></ul>
27	Gibt es beim Auftragnehmer Prozesse und Verfahren um sicherzustellen, dass die Vorgaben des Datenschutzes umgesetzt werden?
28	Wie überwacht der Datenschutzbeauftragte die ordnungsgemäße Anwendung der Datenverarbeitungsprogramme, mit deren Hilfe personenbezogene Daten verarbeitet werden sollen i.S.d. § 4g BDSG?

29	Wird der Datenschutzbeauftragte über Vorhaben der automatisierten Verarbeitung personenbezogener Daten rechtzeitig unterrichtet, um eine Vorabkontrolle durchführen zu können?
30	Existiert ein Verfahren zur Durchführung von Vorabkontrollen durch den Datenschutzbeauftragten?
31	Wie ist sichergestellt, dass geänderte Anforderungen (z.B. Gesetze, Standards oder SLAs) identifiziert, analysiert, bewertet und im Unternehmen angewendet werden?
32	Gibt es Aufzeichnungen zu Datenschutzvorfällen im Unternehmen?
33	Ist ein Verfahrensverzeichnis für die Verfahren, in denen Daten des Auftraggebers verarbeitet werden, vorhanden?
34	Ist eine Verfahrensübersicht „für jedermann“ i.S.d. § 4e Satz 1 Nr. 1 bis 8 BDSG vorhanden?

## Personalsicherheit

35	Gibt es einen Prozess, um alle Bewerber, insbesondere, wenn sie sensible Tätigkeiten ausführen sollen, vor der Anstellung angemessen zu überprüfen („Background-Check“)? Wie wird sichergestellt, dass im Rahmen der Einstellung von neuen Beschäftigten nur vertrauenswürdige Beschäftigte eingestellt werden?
36	Existieren formale Prozesse zur Einstellung oder zum Ausscheiden von Beschäftigten, die Folgendes abdecken? Beispiele: <ul style="list-style-type: none"> <li>• Einrichten, verändern oder entziehen von Berechtigungen,</li> <li>• Ausgabe und Rücknahme von Schlüsseln und Firmeneigentum.</li> </ul>



37	Ist sichergestellt, dass durch eine klare Trennung von Aufgaben und Funktionen Interessenskonflikte bzw. Unverträglichkeiten ausgeschlossen werden können?
38	Existiert eine Übersicht, die Interessenskonflikte bzw. Unverträglichkeiten darstellt?
39	<p>Wurde die Funktionstrennung schriftlich fixiert?</p> <p>Beispielsweise in:</p> <ul style="list-style-type: none"><li>• Stellenbeschreibungen</li><li>• Organisationsplänen</li><li>• Verfahrens-/Arbeitsanweisungen</li></ul>
40	<p>Werden die Funktionstrennungen durch technische Maßnahmen unterstützt?</p> <p>Beispiele:</p> <ul style="list-style-type: none"><li>• Workflows (u.a. Genehmigungsverfahren)</li><li>• Login-Prozeduren</li></ul>
41	Existiert eine dokumentierte Vorgabe über die benötigten Berechtigungen für jede Funktion im Unternehmen?
42	Sind die Berechtigungen im Unternehmen zweifelsfrei nachvollziehbar (auch über eine angemessene Zeitperiode in der Vergangenheit)?

## Schulung der Beschäftigten/Datengeheimnis (§§ 4g, 5 BDSG)

43	<p>Wurden alle Beschäftigten mit Zugriff auf personenbezogene Daten auf das Datengeheimnis verpflichtet?</p> <p>Wird darauf hingewiesen, dass das Datengeheimnis auch nach Beendigung der Tätigkeit im Unternehmen weiter besteht?</p>
44	Ist sichergestellt, dass auch Dienstleister, die der Auftragnehmer bei Dritten als Nebendienstleistung zur Unterstützung bei der Auftragsdurchführung in Anspruch nimmt

	(z.B. Service-Personal, Reinigungs-/Wartungspersonal etc.) auf das Datengeheimnis verpflichtet werden?
45	<p>Ggf. sind darüber hinaus weitergehende Verpflichtungen notwendig.</p> <p>Beispiele:</p> <ul style="list-style-type: none"> <li>• Fernmeldegeheimnis</li> <li>• Sozialgeheimnis</li> <li>• Amtsgeheimnis</li> </ul> <p>Werden die Verpflichtungen durchgeführt? Liegen entsprechende Nachweise vor?</p>
46	<p>Ist sichergestellt, dass alle Beschäftigten sowie Unterauftragnehmer an einer Datenschutz Basisschulung teilnehmen?</p> <p>Wird regelmäßig eine Auffrischung der relevanten Inhalte durchgeführt? (z.B. jährlich)</p> <p>Ist sichergestellt, dass alle Beschäftigten erfasst werden?</p> <p>Liegen entsprechende Nachweise vor?</p>
47	<p>Ist sichergestellt, dass die Schulungsinhalte regelmäßig bewertet und aktualisiert werden?</p> <p>Beispiele:</p> <ul style="list-style-type: none"> <li>• Novellierung von Gesetzen</li> <li>• Erlass neuer Gesetze und Vorschriften</li> <li>• geänderte Bedrohungslage (u.a. IT-Sicherheit)</li> <li>• Häufung von Fehlern (u.a. „Lernen aus Fehlern“)</li> </ul>

48	<p>Wird durch eine ständige Präsenz der Themen sichergestellt, dass die Schulungsinhalte nachhaltig im Gedächtnis bleiben? Z.B. durch die Nutzung unterschiedlicher Kommunikationskanäle.</p> <p>Beispiele:</p> <ul style="list-style-type: none"><li>• Präsenzschiung</li><li>• Informationen per E-Mail</li><li>• Intranet</li><li>• Aushänge am „Schwarzen Brett“</li></ul>
49	<p>Wird in regelmäßigen Abständen das Niveau der Awareness zu den Themen Datenschutz und Informationssicherheit bei den Beschäftigten erhoben, um Verbesserungspotentiale erkennen zu können?</p> <p>Beispiele:</p> <ul style="list-style-type: none"><li>• Gewinnspiel/Quiz</li><li>• Umfrage im Unternehmen</li><li>• persönliche Gespräche</li></ul>

### Schriftlich fixierte Ordnung (SFO)

50	Existiert im Unternehmen eine Richtlinie zum Datenschutz bzw. zur Informationssicherheit (= IT-Sicherheit)?
51	<p>Ist diese Richtlinie allen Beschäftigten zugänglich und bekannt? Z.B. durch</p> <ul style="list-style-type: none"><li>• die Übergabe eines persönlichen Exemplars im Rahmen der Einstellung oder der Datenschutzschulung</li><li>• die zentrale elektronische Ablage der Vorgaben (z.B. auf dem File-Server oder im Intranet)</li></ul>

52	<p>Existieren Dokumente, in denen die Vorgaben aus der Richtlinie konkretisiert sind?</p> <p>Beispiele:</p> <ul style="list-style-type: none"> <li>• Verfahrensanweisungen</li> <li>• Arbeitsanweisungen</li> <li>• Workflows</li> <li>• Checklisten</li> </ul>
----	---

## Zertifizierung/Auditierung

53	<p>Wie kann die Umsetzung der technischen und organisatorischen Maßnahmen gegenüber dem Auftraggeber durch eine geeignete Zertifizierung nachgewiesen werden?</p> <p>Beispiele:</p> <ul style="list-style-type: none"> <li>• ISO 27001</li> <li>• Datenschutzaudit (auch interne Audits)</li> <li>• PCI DSS</li> </ul>
54	<p>Ist eine ausreichende Qualifizierung des Gutachters/Auditors - auch bei internen Auditoren - vorhanden?</p>
55	<p>Umfasst der Anwendungsbereich der Zertifizierung (Scope) den Bereich, in dem die personenbezogenen Daten des Auftraggebers verarbeitet werden (Prüfungsberichte vorlegen lassen)?</p>
56	<p>Wird die vorhandene Zertifizierung aufrechterhalten? Ist die Zertifizierung noch gültig?</p>
57	<p>Existiert eine Erklärung zur Anwendbarkeit (Statement of Applicability; Forderung aus der ISO 27001), die die relevanten und anwendbaren Maßnahmenziele und Maßnahmen beschreibt? (Hilfestellung: Prüfen, ob alle Maßnahmen umgesetzt sind)</p>

## Checkliste Organisation

---

58	Ist ein Datenschutz-/Datensicherheitskonzept vorhanden und einsehbar?
59	Ist ein Notfallkonzept vorhanden und einsehbar?
60	Sind die vorgelegten Dokumente konsistent oder enthalten sie Widersprüche?
61	Existieren Berichte über externe Audits/Prüfungen? Sind diese einsehbar?
62	Wurden eventuell vorhandene Beanstandungen früherer Audits/Prüfungen beseitigt?

## Checkliste Zutrittskontrolle

### Umfeld des Gebäudes

1	<p>Ist sichergestellt, dass nur Berechtigte das Betriebsgelände betreten können?</p> <p>Beispiele:</p> <ul style="list-style-type: none"> <li>• Tor mit Klingel, System zur Authentifizierung von Zutrittsberechtigten (z.B. Magnet-/Chipkarte)</li> <li>• Zaunanlage</li> <li>• Pfortner, Werkschutz (24/7)</li> </ul>
2	<p>Sind die Zutrittsberechtigten schriftlich festgelegt (eine betriebliche Notwendigkeit für den Zutritt ist erforderlich)?</p> <p>Wird regelmäßig überprüft, ob die Zutrittsberechtigten die Zutrittsberechtigung noch benötigen?</p>
3	<p>Sind Maßnahmen vorhanden, um ein Eindringen von unberechtigten Kraftfahrzeugen auf das Betriebsgelände zu verhindern?</p> <p>Beispiele:</p> <ul style="list-style-type: none"> <li>• Tore</li> <li>• Schrankenanlage</li> <li>• Poller</li> </ul>
4	<p>Werden im Außenbereich Maßnahmen (Überwachungseinrichtungen) zur Erkennung von unberechtigten Zutritten zum Betriebsgelände umgesetzt?</p> <p>Beispiele:</p> <ul style="list-style-type: none"> <li>• Bewegungsmelder (Alarmanlage)</li> <li>• Videoüberwachung</li> <li>• Ausleuchtung der Außenbereiche</li> <li>• Werkschutz</li> </ul>

5	<p>Wird eine Videoüberwachung im Außenbereich eingesetzt?</p> <p>Zu prüfen sind u.a.</p> <ul style="list-style-type: none"><li>• die überwachten Bereiche,</li><li>• die Aufbewahrungsdauer der Aufzeichnungen,</li><li>• die Aufbewahrungsorte der Aufzeichnungen,</li><li>• die Zugriffsberechtigten.</li></ul>
---	---

### Zutritt zum Gebäude

6	<p>Wird der Zutritt zum Gebäude kontrolliert?</p> <p>Beispiele:</p> <ul style="list-style-type: none"><li>• Personenkontrolle durch Empfang, Werkschutz, etc.</li><li>• Automatische Zutrittskontrolle inkl. Protokollierung (Authentifizierung über biometrische Merkmale, RFID, PIN, Magnetkarte, Vereinzelungsschleuse)</li><li>• Berechtigungsausweise</li><li>• Schlüsselregelung (inkl. Prüfung der Berechtigung, Protokollierung, Regelung zum Schlüsselverlust)</li></ul>
7	<p>Sind die Zutrittsberechtigten schriftlich festgelegt (eine betriebliche Notwendigkeit für den Zutritt ist erforderlich)?</p> <p>Wird regelmäßig überprüft, ob die Zutrittsberechtigten die Zutrittsberechtigung noch benötigen?</p>
8	<p>Besteht eine Ausweispflicht für die Zutrittsberechtigten?</p>
9	<p>Existieren schriftlich Regelungen für den Zutritt betriebsfremder Personen (z.B. Reinigungspersonal, Wartungstechniker oder Besucher)?</p> <p>Beispiele:</p> <ul style="list-style-type: none"><li>• Tragen von Besucherausweisen</li><li>• Protokollierung des Zutritts: z.B. Datum, Uhrzeit des Zutritts, Name, Firma, Anlass</li><li>• Begleitung von betriebsfremden Personen im Gebäude</li></ul>

10	<p>Sind die Türen, Fenster und Lüftungsschächte ausreichend gesichert?</p> <p>Beispiele:</p> <ul style="list-style-type: none"> <li>• Türen mit einer ausreichenden Widerstandsklasse, Sicherheitsschlösser</li> <li>• Vergitterte Fenster</li> <li>• Einbruchhemmende Verglasung (ausreichende Widerstandsklasse)</li> <li>• Vergitterte Licht- und Lüftungsschächte</li> <li>• Einbruchhemmende Rollläden</li> <li>• Gesicherte Fluchttüren und Feuerleitern</li> </ul>
11	<p>Sind im Gebäude verschiedene Sicherheitsbereiche/-zonen vorhanden.</p> <p>Beispiele:</p> <ul style="list-style-type: none"> <li>• Versorgungseinrichtungen (z.B. Energie, Klimatisierung, Systeme zur Branderkennung/-bekämpfung)</li> <li>• Rechnerräume</li> <li>• Archiv für Datensicherungen</li> <li>• Logistik/Lager</li> </ul>

## Sicherung der RZ-Räume

12	<p>Sind die RZ-Räume ausreichend gesichert?</p> <p>Beispiele:</p> <ul style="list-style-type: none"> <li>• Türen mit einer ausreichenden Widerstandsklasse, Sicherheitsschlösser</li> <li>• Vergitterte Fenster</li> <li>• Einbruchhemmende Verglasung (ausreichende Widerstandsklasse)</li> <li>• Vergitterte Licht- und Lüftungsschächte</li> <li>• Einbruchhemmende Rollläden</li> <li>• Gesicherte Fluchttüren und Feuerleitern</li> </ul>
----	--



13	<p>Wird der Zutritt zu den RZ-Räumen kontrolliert?</p> <p>Beispiele:</p> <ul style="list-style-type: none"><li>• Berechtigungsausweise</li><li>• Automatische Zutrittskontrolle inkl. Protokollierung (Authentifizierung über biometrische Merkmale, RFID, PIN, Magnetkarte, Vereinzelungsschleuse)</li><li>• Schlüsselregelung (Schlüsselverzeichnis und Anweisung inkl. Prüfung der Empfangsberechtigung, Protokollierung, Regelung zum Schlüsselverlust)</li><li>• Videoüberwachung (z.B. Live-Überwachung der Zonen vor den RZ-Räumen)</li></ul>
14	<p>Wird der unberechtigte Zutritt zu RZ-Räumen erkannt und gemeldet (z.B. durch Bewegungsmelder)?</p>
15	<p>Sind die Zutrittsberechtigten schriftlich festgelegt (eine betriebliche Notwendigkeit für den Zutritt ist erforderlich)?</p> <p>Wird regelmäßig überprüft, ob die Zutrittsberechtigten die Zutrittsberechtigung noch benötigen?</p>
16	<p>Besteht eine Ausweispflicht für die Zutrittsberechtigten?</p>
17	<p>Existieren schriftliche Regelungen für den Zutritt betriebsfremder Personen (z.B. Reinigungspersonal, Wartungstechniker oder Besucher)?</p> <ul style="list-style-type: none"><li>• Tragen von Besucherausweisen</li><li>• Protokollierung des Zutritts: Datum, Uhrzeit des Zutritts, Name, Firma, Anlass (Beispiele)</li><li>• Begleitung von betriebsfremden Personen im Gebäude</li></ul>
18	<p>Werden bei der Protokollierung der Zutritte sowie bei der Videoaufzeichnung die Datenschutzvorgaben beachtet?</p>
19	<p>Wurde auf Hinweisschilder, die Aufschluss über die Nutzung geben, verzichtet (z.B. Firmenname)?</p>
20	<p>Befinden sich die Komponenten (Server, Firewall, Switch, Storage, etc.) in abgeschlossenen Racks?</p>

21	Ist sichergestellt, dass Unbefugte keinen Zugriff auf die Komponenten haben (keine gemeinsame Nutzung von Racks mit anderen Firmen)?
22	Ist sichergestellt, dass Unberechtigte keinen Zutritt zu Datensicherungsmedien (z.B. Bänder, Wechselplatten, CDs) haben?

## Checkliste Zugangskontrolle

### Passwortverfahren

1	<p>Sind Maßnahmen umgesetzt, um eine unbefugte Nutzung der Datenverarbeitungssysteme zu verhindern?</p> <p>Beispiele:</p> <ul style="list-style-type: none"><li>• Personalisierte Benutzerkonten (Accounts, User-Name, Passwort)</li><li>• Bildschirmschoner mit Passwortaktivierung (automatische Aktivierung bei Inaktivität)</li></ul>
2	<p>Ist ein dokumentiertes Berechtigungskonzept vorhanden, in dem folgende Punkte in der Umsetzung verbindlich geregelt sind (schriftlich fixierte Ordnung)?</p> <ul style="list-style-type: none"><li>• Beantragung von Berechtigungen für den Zugang für DV-Systeme</li><li>• Genehmigung von Berechtigungen</li><li>• Umsetzung von beantragten Berechtigungen</li><li>• Entzug von nicht mehr benötigten Berechtigungen Kann zweifelsfrei nachvollzogen werden, wer wann welche Zugangsberechtigungen hatte?</li></ul>
3	<p>Gibt es eine Richtlinie, in der das Benutzer- und Passwortmanagement verbindlich geregelt ist?</p> <p>Beispiele:</p> <ul style="list-style-type: none"><li>• Initialpasswörter</li><li>• Passwortlänge (x Zeichen), regelmäßiger Passwortwechsel, Passwortkomplexität, Passworthistorie</li><li>• Log-In Versuche (x Versuche) und Dauer der Kontosperrung bei Fehlversuchen (x Min.; bei Daten mit dem Schutzbedarf „Sehr hoch“ sollte ein Prozess zur Rücksetzung gesperrter Accounts vorhanden sein)</li><li>• Löschung von inaktiven Benutzern</li><li>• Sofortige Sperrung von ausgeschiedenen Beschäftigten</li><li>• Vertraulichkeit von Passwörtern</li><li>• Verschlüsselte Speicherung von Passwörtern</li></ul>

4	Erfolgt eine gesicherte Übertragung von Authentisierungsgeheimnissen (Credentials) im Netzwerk?
5	Werden Maßnahmen zur Steigerung der Awareness im richtigen Umgang mit Passwörtern durchgeführt?
6	Existiert ein Verbot zur lokalen Speicherung von Passwörtern und/oder Formulareingaben?
7	<p>Werden Zugänge zum Netzwerk durch eine Zwei-Faktor-Authentifizierung (starke Authentifizierung) geschützt?</p> <p>Beispiele:</p> <ul style="list-style-type: none"> <li>• OneTimePass Token</li> <li>• SmartCard</li> <li>• Biometrische Merkmale</li> </ul>
8	<p>Werden <u>externe</u> Zugänge (z.B. VPN-Zugang) zum Netzwerk durch eine Zwei-Faktor-Authentifizierung (starke Authentifizierung) geschützt?</p> <p>Beispiele:</p> <ul style="list-style-type: none"> <li>• OneTimePass Token</li> <li>• SmartCard</li> <li>• Biometrische Merkmale</li> </ul>
9	<p>Werden die eingerichteten Benutzerkonten (Accounts) sowie die Authentifizierungsmedien (z.B. Token, Chip-Karte) einem jährlichen Review unterzogen?</p> <p>Wenn ja,</p> <ul style="list-style-type: none"> <li>• werden nicht mehr benötigte Benutzerkonten gelöscht?</li> <li>• werden die Reviews nachvollziehbar dokumentiert?</li> </ul>
10	<p>Gibt es verbindliche Regelungen zum Umgang mit Notfallpasswörtern?</p> <p>Beispiele:</p> <ul style="list-style-type: none"> <li>• Ablage in einem versiegelten Umschlag</li> <li>• Aufbewahrung in einem Tresor</li> <li>• Dokumentation der Verwendung der Passwörter</li> </ul>

## Protokollierung und Protokollauswertung (siehe auch Zugriffs-, Eingabe- und Auftragskontrolle)

11	Existiert eine verbindliche Vorgabe, die den Umfang der Protokollierung definiert (unter Beachtung der Verhältnismäßigkeit/Angemessenheit)? Der Umfang der Protokollierung sollte sich am Schutzbedarf der Daten orientieren (unter Beachtung der Sensibilität der Daten und der Eintrittswahrscheinlichkeit einer Gefährdung).
12	<p>Erfolgt eine Protokollierung der administrativen Tätigkeiten (Protokollierung zum Nachweis einer korrekten Funktionsweise der Systeme/Applikationen sowie der Verwaltung von Berechtigungen = Systemüberwachung)?</p> <p>Beispiele:</p> <ul style="list-style-type: none"><li>• Installation, Modifikation und Konfiguration von Hard- und Software</li><li>• Einrichten von Benutzern, Verwalten von Berechtigungen</li><li>• Durchführen von Backup-, Restore- und sonstigen Datensicherungsmaßnahmen</li></ul>
13	<p>Erfolgt eine Protokollierung zum Nachweis einer korrekten und rechtskonformen Verarbeitung von Daten (Verfahrensüberwachung)?</p> <p>Beispiele:</p> <ul style="list-style-type: none"><li>• Versuche unbefugten Einloggens (Überschreitung von Befugnissen)</li><li>• Datenübertragungen</li><li>• Dateneingabe und -veränderung</li><li>• Dateneinsicht</li><li>• Datenlöschung</li></ul>
14	<p>Geben die Protokolldaten Auskunft über:</p> <ul style="list-style-type: none"><li>• Wann (Zeitpunkt der Aktivität oder des Ereignisses)</li><li>• Wer (die ausführende Person/Systemkomponente)</li></ul>

	<ul style="list-style-type: none"> <li>• Was (Bezeichnung des Ereignisses/der Tätigkeit)</li> <li>• Wie (Ergebnis der Tätigkeit (erfolgreich ausgeführt?))</li> <li>• Wieviel (Datenmenge/betroffene Daten)</li> </ul>
15	Ist sichergestellt, dass alle Systeme protokollieren?
16	Wenn eine zentrale Speicherung von Protokolldaten erfolgt: Ist sichergestellt, dass die Protokolldaten vollständig übertragen werden (TCP (verbindungsorientiertes Protokoll) statt UDP (verbindungsloses Protokoll))?
17	Ist sichergestellt, dass ein Ausfall der Protokollierung umgehend bemerkt wird?
18	<p>Ist bei der Übertragung der Protokolldaten auf zentrale Server (z.B. zur Auswertung oder Archivierung) sichergestellt, dass die Daten ausreichend geschützt werden?</p> <p>Maßnahmenziele:</p> <ul style="list-style-type: none"> <li>• Vertraulichkeit: Kann eine Einsichtnahme durch Unberechtigte ausgeschlossen werden?</li> <li>• Integrität: Können nicht autorisierte Änderungen ausgeschlossen werden?</li> <li>• Authentizität: Kommen die Daten von dem angegebenen System?</li> </ul>
19	<p>Ist der Umfang der Auswertungen festgelegt?</p> <ul style="list-style-type: none"> <li>• Auswertungszyklus (zeitnah, z.B. täglich; zeitnahe Auswertungen sollen ermöglichen, bei aufgedeckten Verstößen Schäden abzuwenden)</li> <li>• Auswertungsumfang (z.B. vollständig oder in Stichproben)</li> </ul>
20	Sind die Verantwortlichkeiten für die Auswertung der Protokolle festgelegt?
21	Wird der Zugriff auf Protokolldaten für Unberechtigte verhindert („need-to-know“-Prinzip)? Die Zugriffsbefugnisse sollten in einem Berechtigungskonzept geregelt werden.

22	Ist die Aufbewahrungsdauer für die Protokolle festgelegt und dokumentiert? Werden Protokolle nach Ablauf der Aufbewahrungsdauer gelöscht?
23	Erfolgt eine Überwachung der Integrität bei den Protokolldaten (Schutz vor dem Löschen und Verändern von Ereignissen)? Wenn ja, werden Integritätsverletzungen gemeldet?

## Maßnahmen zum Schutz der DV-Systeme

24	Existieren Richtlinien für eine sichere Konfiguration von Systemen?
25	<p>Werden Systeme gehärtet?</p> <p>Beispiele:</p> <ul style="list-style-type: none"><li>• Entfernen von nicht benötigten Diensten und Funktionalitäten</li><li>• Entfernen von nicht benötigten Applikationen</li><li>• Nutzung von sicheren Protokollen</li><li>• Minimalkonfiguration</li></ul>
26	<p>Wie werden Daten während der Übertragung vor unberechtigten Zugriffen geschützt?</p> <p>Beispiele:</p> <ul style="list-style-type: none"><li>• Verschlüsselter Übertragungsweg (z.B. IPSec, VPN, VLAN, https/SFTP)</li><li>• Datenverschlüsselung</li></ul>
27	Ist das Netzwerk nach außen durch Firewalls abgeschottet?
28	<p>Existiert eine angemessene Netzwerkarchitektur bestehend aus einem mehrstufigen Firewallkonzept (Netzwerksegmente mit einem unterschiedlichen Schutzbedarf)</p> <p>Beispiele:</p> <ul style="list-style-type: none"><li>• Demilitarisierte Zone (DMZ)</li><li>• interner Bereich</li></ul>

29	<p>Existieren verbindliche Vorgaben für die Konfiguration von Firewalls?</p> <p>Beispiele:</p> <ul style="list-style-type: none"> <li>• Regelungen für das Öffnen/Schließen von Ports</li> <li>• Nutzung einer „deny-all“-Regel</li> <li>• Nutzung von Stateful Inspection (zustandsgesteuerte Filterung von Datenpaketen)</li> <li>• Nutzung von NAT oder einer anderen Masquerading-Technologie (Verbesserung der NW-Sicherheit durch das Verbergen von IP-Adressen)</li> </ul>
30	Erfolgt eine regelmäßige Überprüfung der Firewall-Konfigurationen (Identifikation von fehlerhaften und ineffizienten Regelsätzen)?
31	Werden angemessene Filter zur Identifikation und Abwehr von Spam genutzt (ggf. mehrstufige Filter)?
32	Wird ein System zur Erkennung und zur Abwehr von Angriffen umgesetzt (Intrusion Detection System/Intrusion Prevention System)?
33	Gibt es eine Richtlinie zur Behandlung fremder Speichermedien?
34	Ist sichergestellt, dass in öffentlichen Bereichen des Unternehmens (z.B. am Empfang oder in Besprechungsräumen) kein unbeaufsichtigter Zugang zum Netzwerk möglich ist?



35	<p>Sind Maßnahmen (Erkennung, Verhinderung, Beseitigung) zum Schutz vor Malware (u.a. Viren, Würmer, Cookies, Applets, CGI Skripte, Trojaner, ROOT Kits) umgesetzt?</p> <ul style="list-style-type: none"><li>• Ist eine regelmäßige Aktualisierung der Clients sichergestellt (Applikation, Scan-Pattern)?</li><li>• Gibt es Managementsysteme zur Alarmierung von Virenfunden?</li><li>• Wie werden Virenfunde behandelt (Löschen oder Quarantäne)?</li></ul> <p><b>Achtung:</b> Die Löschung eines Virus darf niemals undokumentiert erfolgen, ggf. werden relevante Informationen gelöscht!</p>
36	<p>Wie werden die Datenträger während des Transports vor unberechtigtem Zugang geschützt (z.B. verschlossener Transportbehälter)?</p>
37	<p>Werden personenbezogene Daten über öffentliche, unsichere Netze versendet?</p> <p>Beispiele:</p> <ul style="list-style-type: none"><li>• E-Mail</li><li>• Internet</li><li>• GPS/GPRS</li><li>• WLAN</li></ul>
38	<p>Wie werden die Daten während der Übertragung vor unberechtigten Zugriffen geschützt?</p> <p>Beispiele:</p> <ul style="list-style-type: none"><li>• Verschlüsselter Übertragungsweg (z.B. IPSec, VPN, VLAN, https/SFTP)</li><li>• Datenverschlüsselung</li></ul>

39	<p>Werden personenbezogene Daten mittels WLAN übertragen? Wenn ja,</p> <ul style="list-style-type: none"><li>• ist ein starker Verschlüsselungsmechanismus aktiviert (z.B. WPA2)?</li><li>• wurde der voreingestellte Schlüssel (Key) zum Zeitpunkt der Installation geändert?</li><li>• werden kryptographische Schlüssel geändert, wenn ein Beschäftigter, der die Schlüssel kennt, das Unternehmen oder die Position wechselt?</li><li>• wurde das Kennwort für den Zugang zum System geändert?</li><li>• wird die Firmware auf den Geräten regelmäßig aktualisiert?</li></ul>
40	<p>Ist sichergestellt, dass Unberechtigte keinen Zugang zu den DV-Systemen haben?</p> <p>Beispiele:</p> <ul style="list-style-type: none"><li>• Die Racks mit den aktiven Komponenten (z.B. Server, Storage, Firewall) sind abzuschließen</li><li>• Die Racks mit den Netzwerkverteilern sind abzuschließen</li></ul>
41	<p>Erfolgen Zugriffe auf die Systeme im Rahmen einer Fernwartung? Wenn ja, sind Festlegungen und Verfahren für die Zugriffe getroffen?</p>

42	<p>Ist der Umgang mit mobilen Datenträgern geregelt, auf denen personenbezogene Daten gespeichert werden?</p> <ul style="list-style-type: none"><li>• CD/DVD</li><li>• USB-Sticks</li><li>• Mobile Festplatten</li><li>• Multimediageräte mit Datenspeicher (MP3-Player, PDAs, Smartphones, etc.)</li></ul> <p>Werden die personenbezogenen Daten auf mobilen Endgeräten angemessen vor unberechtigten Zugriffen geschützt? (z.B. durch eine Verschlüsselung)</p>
43	<p>Existieren verbindliche Vorgaben zum Umgang mit Ausdrucken &amp; Faxen?</p>

## Sicherheitsmanagement

44	<p>Werden externe Quellen zur Erkennung von neuen Sicherheitslücken herangezogen?</p> <p>Beispiele:</p> <ul style="list-style-type: none"><li>• Mailingdienste von Herstellern</li><li>• Newsboards</li><li>• Cert-Dienste</li></ul> <p>Wurde ein Verantwortlicher benannt, der sich in regelmäßigen Abständen über neue Sicherheitslücken informiert und ggf. die notwendigen Maßnahmen veranlasst?</p>
45	<p>Werden regelmäßig sowie nach signifikanten Netzwerkänderungen Schwachstellen-Scans (Vulnerability Scans) zur Erkennung von Sicherheitslücken durchgeführt?</p>
46	<p>Werden regelmäßig sowie nach signifikanten Netzwerkänderungen Penetrationstests zur Überprüfung der Wirksamkeit der umgesetzten Maßnahmen gegen das Eindringen durch unbefugte Dritte durchgeführt?</p>

47	Ist sichergestellt, dass kritische Sicherheitspatche zeitnah installiert werden? (z.B. innerhalb von 30 Tagen nach ihrer Veröffentlichung)
48	<p>Werden Systeme zur Erkennung von erfolgten Angriffen eingesetzt?</p> <p>Beispiele:</p> <ul style="list-style-type: none"> <li>• IDS/IPS (Intrusion Detection System/Intrusion Prevention System)</li> <li>• WLAN IDS/IPS</li> </ul>
49	<p>Sind Richtlinien vorhanden, die Vorgehen und Methoden im Fall von Sicherheitsvorfällen beschreiben?</p> <p>Werden die Richtlinien und Verfahren in regelmäßigen Abständen getestet?</p>

## Checkliste Zugriffskontrolle

### Netzwerkarchitektur

1	<p>Ist ein aktuelles Netzwerkdiagramm für die Netzwerksegmente, in denen personenbezogene Daten verarbeitet werden (Server, Datenbanken, Router, Firewall, etc.) vorhanden? Werden die Netzwerkdiagramme regelmäßig aktualisiert?</p>
2	<p>Sind eine angemessene Netzwerkarchitektur sowie ein angemessenes Firewallkonzept vorhanden?</p> <p>Beispiele:</p> <ul style="list-style-type: none"><li>• Ist das Netzwerk angemessen segmentiert? (z.B. Demilitarisierte Zone [DMZ], sicherer Bereich)</li><li>• Ist ein ein- oder mehrstufiges Firewallkonzept vorhanden?</li><li>• Sind die Verantwortlichkeiten festgelegt?</li></ul>
3	<p>Werden Firewalls angemessen konfiguriert?</p> <p>Beispiele:</p> <ul style="list-style-type: none"><li>• Existieren Regeln für eine sichere Konfiguration („Systemhärtung“)?</li><li>• Erfolgt ein(e) regelmäßige(s) Prüfung/Review der Konfiguration bzw. der Regelwerke?</li><li>• Existieren Regelungen zum Management von Firewalls (Aktivierung von neuen Firewalls, Reviews, etc.)?</li><li>• Existieren Regelungen für das Öffnen/Schließen von Ports?</li><li>• Ist eine „deny-all“-Regel vorhanden (der nicht zwingend notwendige ein- und ausgehende Datenverkehr ist durch eine „deny-all“-Anweisung zu verhindern)?</li><li>• Werden die Systeme regelmäßig aktualisiert?</li><li>• Ist ein Änderungsmanagement vorhanden (Change-Control-Procedures)?</li></ul>

4	<p>Ist sichergestellt, dass neue Sicherheitslücken identifiziert werden?</p> <p>Beispiele:</p> <ul style="list-style-type: none"> <li>• Werden externe Mailingdienste, Newsboards, CERT, etc. genutzt?</li> <li>• Sind die Verantwortlichkeiten festgelegt?</li> </ul>
5	<p>Welche weitergehenden Maßnahmen werden zum Schutz des Netzwerkes und der Systeme sowie zur Angriffs- und Schwachstellenerkennung eingesetzt?</p> <ul style="list-style-type: none"> <li>• IDS/IPS</li> <li>• Schwachstellen-Scanner (in regelmäßigen Abständen sowie nach signifikanten Netzwerkänderungen)</li> <li>• WLAN IDS/IPS</li> <li>• WLAN Scans</li> <li>• Content-Filter</li> <li>• WAF</li> </ul>
6	<p>Ist sichergestellt, dass sicherheitskritische Patche zeitnah installiert werden (z.B. innerhalb von 30 Tagen nach ihrer Veröffentlichung)?</p>
7	<p>Sind Maßnahmen zum Schutz vor Schadsoftware umgesetzt?</p>
8	<p>Werden in Netzwerksegmenten, in denen personenbezogene Daten verarbeitet werden, drahtlose Technologien verwendet (z.B. WLAN)?</p>
9	<p>Werden Maßnahmen zum Schutz der personenbezogenen Daten während der Übertragung mittels drahtloser Technologien umgesetzt?</p> <ul style="list-style-type: none"> <li>• Implementierung starker Verschlüsselungsmechanismen? (z.B. WPA2)</li> <li>• Werden voreingestellte Schlüssel vor der Produktivnahme der Systeme geändert?</li> </ul>

	<ul style="list-style-type: none"><li>• Werden kryptographische Schlüssel geändert, wenn ein Beschäftigter, der die Schlüssel kennt, das Unternehmen verlässt oder die Position wechselt?</li><li>• Werden Standardkennwörter vor der Produktivnahme von Systemen und sodann regelmäßig geändert?</li><li>• Wird die Firmware auf den Systemen regelmäßig aktualisiert?</li></ul>
10	Ist sichergestellt, dass der Zugriff auf Daten nur für Beschäftigte mit einem Business-Need ermöglicht wird (der Zugriff muss für die Erledigung der Aufgaben zwingend notwendig sein)?
11	Sieht das Netzkonzept eine Trennung zwischen Test- und Produktionsumgebung vor?
12	Wird der Netzwerkverkehr in besonders sensiblen Netzwerksegmenten mit einem IDS/IPS-System überwacht?

## Berechtigungskonzept

13	<p>Ist ein dokumentiertes Berechtigungskonzept vorhanden, in dem folgende Punkte in der Umsetzung verbindlich geregelt sind (schriftlich fixierte Ordnung)?</p> <ul style="list-style-type: none"><li>• Beantragung von Berechtigungen</li><li>• Genehmigung von Berechtigungen</li><li>• Umsetzung von beantragten Berechtigungen</li><li>• Entzug von nicht mehr benötigten Berechtigungen</li><li>• Bedingungen zur Vergabe von Administrationsrechten</li></ul> <p>Kann zweifelsfrei nachvollzogen werden, wer wann welche Berechtigungen hatte (auch über eine angemessene Zeitperiode in der Vergangenheit)?</p>
14	Existieren abgestufte Berechtigungen für das Lesen, Löschen oder Ändern von Daten?

15	Existieren abgestufte Berechtigungen für Zugriffe auf <ul style="list-style-type: none"> <li>• Daten,</li> <li>• Anwendungen und</li> <li>• das Betriebssystem?</li> </ul>
16	Ist eine Trennung der Rollen zur Genehmigung und Einrichtung von Berechtigungen vorhanden (4-Augen-Prinzip)?
17	Ist sichergestellt, dass Zugriffe dem „need-to-know“-Prinzip (minimale Berechtigungen) entsprechen?
18	Ist sichergestellt, dass es nicht zu einer Konzentration von Funktionen kommen kann (hieraus resultierendes Problem: sehr umfangreiche Berechtigungen)?
19	Werden regelmäßig Reviews der eingerichteten Berechtigungen durchgeführt?
20	Erfolgt ein Monitoring bzw. eine regelmäßige Kontrolle der Aktivitäten von Administratoren?

### Protokollierung und Protokollauswertung (siehe Zugangs-, Eingabe- und Auftragskontrolle)

21	Existiert eine verbindliche Vorgabe, die den Umfang der Protokollierung definiert (unter Beachtung der Verhältnismäßigkeit/Angemessenheit)? Der Umfang der Protokollierung sollte sich am Schutzbedarf der Daten orientieren (unter Beachtung der Sensibilität der Daten und der Eintrittswahrscheinlichkeit einer Gefährdung).
22	Erfolgt eine Protokollierung der administrativen Tätigkeiten (Protokollierung zum Nachweis einer korrekten Funktionsweise der Systeme/Applikationen sowie der Verwaltung von Berechtigungen = Systemüberwachung)?



	<p>Beispiele:</p> <ul style="list-style-type: none"><li>• Installation, Modifikation und Konfiguration von Hard-/Software</li><li>• Einrichten von Benutzern, Verwalten von Berechtigungen</li><li>• Durchführen von Backup-, Restore- und sonstigen Datensicherungsmaßnahmen</li></ul>
23	<p>Erfolgt eine Protokollierung zum Nachweis einer korrekten und rechtskonformen Verarbeitung von Daten (Verfahrensüberwachung)?</p> <p>Beispiele:</p> <ul style="list-style-type: none"><li>• Versuche unbefugten Einloggens (Überschreitung von Befugnissen)</li><li>• Datenübertragungen</li><li>• Dateneingabe und -veränderung</li><li>• Dateneinsicht</li><li>• Datenlöschung</li></ul>
24	<p>Geben die Protokolldaten Auskunft über:</p> <ul style="list-style-type: none"><li>• Wann (Zeitpunkt der Aktivität oder des Ereignisses)</li><li>• Wer (die ausführende Person/Systemkomponente)</li><li>• Was (Bezeichnung des Ereignisses/der Tätigkeit)</li><li>• Wie (Ergebnis der Tätigkeit (erfolgreich ausgeführt?))</li><li>• Wieviel (Datenmenge/betroffene Daten)</li></ul>
25	<p>Ist sichergestellt, dass alle Systeme protokollieren?</p>
26	<p>Wenn eine zentrale Speicherung von Protokolldaten erfolgt: Ist sichergestellt, dass die Protokolldaten vollständig übertragen werden (TCP (verbindungsorientiertes Protokoll) statt UDP (verbindungsloses Protokoll))?</p>
27	<p>Ist sichergestellt, dass ein Ausfall der Protokollierung umgehend bemerkt wird?</p>

28	<p>Ist bei der Übertragung der Protokolldaten auf zentrale Server (z.B. zur Auswertung oder Archivierung) sichergestellt, dass die Daten ausreichend geschützt werden?</p> <p>Maßnahmenziele:</p> <ul style="list-style-type: none"> <li>• Vertraulichkeit: Kann eine Einsichtnahme durch Unberechtigte ausgeschlossen werden?</li> <li>• Integrität: Können nicht autorisierte Änderungen ausgeschlossen werden?</li> <li>• Authentizität: Kommen die Daten von dem angegebenen System?</li> </ul>
29	<p>Ist der Umfang der Auswertungen festgelegt?</p> <ul style="list-style-type: none"> <li>• Auswertungszyklus (zeitnah, z.B. täglich; zeitnahe Auswertungen sollen ermöglichen, bei aufgedeckten Verstößen Schäden abzuwenden)</li> <li>• Auswertungsumfang (z.B. vollständig oder in Stichproben)</li> </ul>
30	<p>Sind die Verantwortlichkeiten für die Auswertung der Protokolle festgelegt?</p>
31	<p>Wird der Zugriff auf Protokolldaten für Unberechtigte verhindert („need-to-know“-Prinzip)? Die Zugriffsbefugnisse sollten in einem Berechtigungskonzept geregelt werden.</p>
32	<p>Ist die Aufbewahrungsdauer für die Protokolle festgelegt und dokumentiert? Werden Protokolle nach Ablauf der Aufbewahrungsdauer gelöscht?</p>
33	<p>Erfolgt eine Überwachung der Integrität bei den Protokolldaten (Schutz vor dem Löschen und Verändern von Ereignissen)? Wenn ja, werden Integritätsverletzungen gemeldet?</p>

## Datenträger und Systemnutzung

34	Existiert eine Liste der im Unternehmen zugelassenen Hard- und Software? Existiert ein Verbot der Nutzung von privater Software?
35	Existieren ausreichende Richtlinien und Prozesse zur Nutzung der im Unternehmen eingesetzten Technologien (z.B. PC, Telekommunikation, E-Mail, Internet, Laptops, Smartphones etc.)?
36	Existiert eine verbindliche Vorgabe (z.B. Richtlinie, Verfahrensanweisung, etc.) für die Arbeit im Rahmen von Telearbeit (z.B. Home Office)?
37	Sind die Schnittstellen von Computern abgesichert, um einen nicht genehmigten Abfluss von Daten zu verhindern? Beispiele für Schnittstellen: <ul style="list-style-type: none"><li>• USB-Schnittstelle</li><li>• CD/DVD-Brenner</li></ul>
38	Existiert eine verbindliche Regelung (schriftlich fixierte Ordnung) zum Umgang mit Backup-Medien? <ul style="list-style-type: none"><li>• Ist eine dokumentierte Datenträgerverwaltung vorhanden?</li><li>• Wer hat Zugang zu Backup-Medien (kein Zugang durch Unberechtigte: Lagerung z.B. in einem Safe, einem verschlossenen Stahlschrank, im Archiv oder in einem abschließbaren Büro)?</li><li>• Wer darf ein Zurückspielen von Daten anfordern?</li><li>• Wer darf Backup-Daten einspielen?</li><li>• Sind die Archivierungszeiten von Backups festgelegt?</li><li>• Ist eine sichere Entsorgung von Datenträgern sichergestellt?</li></ul>
39	Werden Backup-Medien sicher aufbewahrt? Beispiele: <ul style="list-style-type: none"><li>• Anderer Brandabschnitt als Rechenzentrum</li><li>• Lagerung außerhalb des Rechenzentrums (z.B. Bankschließfach)</li></ul>

40	<p>Ist der Umgang mit mobilen Datenträgern geregelt? Beispiele:</p> <ul style="list-style-type: none"> <li>• CD/DVD</li> <li>• USB-Sticks</li> <li>• Mobile Festplatten</li> <li>• Multimediageräte mit Datenspeicher (MP3-Player, PDAs, Smartphones, etc.)</li> </ul>
41	<p>Ist eine Richtlinie zum Umgang mit Ausdrucken und Faxen vorhanden?</p>
42	<p>Werden personenbezogene Daten bei Speicherung auf Datenträgern durch Verschlüsselungstechnologien vor einem unbefugtem Zugriff geschützt? Wenn ja, wie ist das Key-Management verbindlich geregelt?</p>

## Softwareentwicklung

43	<p>Erfolgt die Entwicklung von Software auf Basis formaler Richtlinien und Prozesse, die sich an Best Practices orientieren?</p>
44	<p>Werden im Rahmen des Softwareentwicklungsprozesses (vor der Produktivnahme von Applikationen) Code Reviews durchgeführt? Existiert eine formale Richtlinie für die Durchführung von Code-Reviews? Beispiele:</p> <ul style="list-style-type: none"> <li>• Zu prüfende Aspekte</li> <li>• Verantwortlichkeiten (4-Augen-Prinzip)</li> <li>• Nachweise, Dokumentation</li> </ul>
45	<p>Werden Webanwendungen auf der Basis sicherer Codierungsrichtlinien erstellt (z.B. Open Web Application Security Guide)?</p>

## Checkliste Weitergabekontrolle

### Kontrolle von elektronischen Übertragungen

1	<p>Werden personenbezogene Daten des Auftraggebers an andere Stellen elektronisch übertragen?</p> <p>Wenn ja:</p> <ul style="list-style-type: none"><li>• An welche Stellen werden Daten übertragen?</li><li>• An welche Stellen ist die Übertragung geplant?</li></ul>
2	<p>Welche personenbezogenen Daten werden übertragen? (Ist-Stand ermitteln)</p> <ul style="list-style-type: none"><li>• Art der Daten</li><li>• Zweck</li><li>• Quelle, Absender, Verantwortlichkeit</li><li>• Ziel, Empfänger</li></ul>
3	<p>Welche Übertragungswege werden genutzt?</p> <p>Beispiele:</p> <ul style="list-style-type: none"><li>• E-Mail</li><li>• Internet (FTP, SFTP)</li><li>• Festverbindung (z.B. MPLS)</li><li>• ISDN</li><li>• GPRS, GSM</li><li>• Datenträgertransporte</li></ul>
4	<p>Wie werden die Daten während der Übertragung vor unberechtigten Zugriffen geschützt?</p> <p>Beispiele:</p> <ul style="list-style-type: none"><li>• Verschlüsselter Übertragungsweg (z.B. IPSec, VPN, VLAN, HTTPS, SFTP)</li><li>• Datenverschlüsselung</li></ul>

5	<p>Ist das Passworthandling ausreichend sicher?</p> <ul style="list-style-type: none"> <li>• Werden ausreichend komplexe Passworte verwendet?</li> <li>• Erfolgt die Übermittlung von Passworten auf einem getrennten Weg?</li> </ul>
6	<p>Muss das Einrichten von neuen Übertragungswegen genehmigt werden (z.B. durch die Geschäftsführung)?</p>
7	<p>Erfolgt vor der Einrichtung einer neuen Datenübertragung oder der Durchführung eines Datenträgersversands die Prüfung der Legitimation des Genehmigers (liegt die Berechtigung vor)?</p>
8	<p>Wer ist befugt, neue Übertragungswege einzurichten?</p>
9	<p>Wird die Übertragung von personenbezogenen Daten protokolliert?</p>
10	<p>Wird die Integrität der empfangenen Daten vor der Weiterverarbeitung geprüft?</p>
11	<p>Liegen entsprechende Verträge zu Datenübertragungen vor?</p>
12	<p>Sind alle Übertragungswege dokumentiert (z.B. in einem Netzwerkdiagramm)?</p>
13	<p>Werden Angriffe auf die Netzwerkzugänge (Übertragungswege) zeitnah erkannt?</p>
14	<p>Werden regelmäßig Maßnahmen durchgeführt, um eine ausreichende Sicherheit für die Netzwerkzugänge sicherzustellen?</p> <p>Beispiele:</p> <ul style="list-style-type: none"> <li>• Schwachstellen-Scan (Vulnerability Scan)</li> <li>• Penetrationstest</li> <li>• Firewall-Review</li> </ul>

## Kontrolle von Datenträgertransporten

15	<p>Erfolgen Datenträgertransporte? Wenn ja, welche Transportarten von Datenträgern gibt es?</p> <ul style="list-style-type: none"> <li>• Logistikdienstleister (z.B. Paketdienst, Kurierdienst, zuverlässiger Bote)</li> <li>• Begleitete Transporte</li> </ul>
16	<p>Wurde der Schutzbedarf der Datenträger und die daraus resultierenden Maßnahmen zum Schutz während des Transports festgelegt?</p>
17	<p>Werden alle Datenträger verwaltet? Beispiele:</p> <ul style="list-style-type: none"> <li>• Kennzeichnung von Datenträgern (z.B. Datenträgername)</li> <li>• Klassifizierung des Datenträgers (Schutzklasse)</li> <li>• Inventarisierung des Datenträgers (Bestandsliste)</li> <li>• Dokumentation von Auf- und Entnahmen von Datenträgern</li> <li>• Durchführung von Inventuren</li> </ul>
18	<p>Ist sichergestellt, dass nur berechtigte Personen auf die Dokumentation zugreifen können?</p>
19	<p>Werden Lieferscheine bzw. Datenträger-Begleitzettel erstellt (Dokumentation des Versands bzw. des Transports)? Beispiele:</p> <ul style="list-style-type: none"> <li>• Anzahl/Bezeichnung der Datenträger</li> <li>• Hinweise zur Durchführung des Transports (z.B. Maßnahmen zum Schutz des Datenträgers)</li> <li>• Am Transport beteiligten Personen/Stellen festgelegt (Ausgabe, Transport und Empfang der Datenträger)</li> <li>• Prüfung der Legitimation vor der Übergabe der Datenträger an den Empfänger</li> <li>• Bestätigung der ausgebenden Stelle</li> <li>• Empfangsbestätigung durch den Boten</li> <li>• Empfangsbestätigung des Empfängers (ggf. mit Rückmeldung)</li> </ul>

20	Müssen Datenträgertransporte vorab genehmigt werden? Wenn ja, wer ist befugt, diese zu genehmigen?
21	Erfolgt vor der Durchführung eines Datenträgerversands die Prüfung der Legitimation des Genehmigers (liegt die Berechtigung vor)?
22	Wie werden die Datenträger während des Transports vor unberechtigten Zugriffen geschützt?  Beispiele: <ul style="list-style-type: none"> <li>• Verschlüsselte Datenträger</li> <li>• Verschlussene Transportbehälter</li> </ul>
23	Können unberechtigte Zugriffe während des Transportes erkannt werden?  Beispiel: <ul style="list-style-type: none"> <li>• Sicherung der Transportbehälter durch Siegel</li> <li>• Überprüfung der Integrität der Daten (Vollständig-/Richtigkeit)</li> </ul>
24	Werden Maßnahmen zum Schutz der Datenträger vor Umwelteinflüssen umgesetzt (z.B. Störstrahlung, hohe/niedrige Temperaturen, Luftfeuchtigkeit)?
25	Erfolgt der Transport auf dem direkten Weg oder werden die Datenträger zwischengelagert? Bei einer Zwischenlagerung: Welche Maßnahmen werden zum Schutz der Datenträger umgesetzt?
26	Werden die Personen, die einen begleiteten Transport durchführen, speziell geschult (richtiges Verhalten während des Transportes, Melden von Verlusten, etc.)?
27	Werden Datenträger vor dem Einspielen der Daten auf das Vorhandensein von Malware geprüft?



### Kontrolle von Wartungsarbeiten

28	Kann während der Durchführung von Wartungsarbeiten auf personenbezogene Daten zugegriffen werden?
----	---

### Kontrolle von privaten Datenträgern

29	Ist der Einsatz nicht autorisierter Datenträger (z.B. private Datenträger) geregelt?
----	--

### Kontrolle von Datenträgerentsorgungen

30	Existiert ein Prozess zum Sammeln von Datenträgern mit personenbezogenen Daten, die entsorgt werden sollen? Ist der Prozess allen relevanten Personen bekannt?
31	Erfolgt die Vernichtung der Datenträger so, dass eine Rekonstruktion der Daten ausgeschlossen ist?
32	Wird die Vernichtung von Datenträgern nachvollziehbar dokumentiert (z.B. Löschprotokolle)?

## Checkliste Eingabekontrolle

### Berechtigungen

1	<p>Ist ein dokumentiertes Berechtigungskonzept vorhanden, in dem folgende Punkte in der Umsetzung verbindlich geregelt sind (schriftlich fixierte Ordnung)?</p> <ul style="list-style-type: none"> <li>• Beantragung von Berechtigungen</li> <li>• Umsetzung von beantragten Berechtigungen</li> <li>• Genehmigung von Berechtigungen</li> <li>• Entzug von nicht mehr benötigten Berechtigungen</li> </ul> <p>Kann zweifelsfrei nachvollzogen werden, wer wann welche Berechtigungen hatte?</p>
2	Existieren abgestufte Berechtigungen z.B. für das Lesen, Löschen oder Verändern von Daten?
3	<p>Existieren abgestufte Berechtigungen für Zugriffe auf</p> <ul style="list-style-type: none"> <li>• Daten,</li> <li>• Anwendungen und</li> <li>• das Betriebssystem?</li> </ul>
4	Ist eine Trennung der Rollen zur Genehmigung und Einrichtung von Berechtigungen vorhanden (4-Augen-Prinzip)?
5	Ist sichergestellt, dass Zugriffe dem „need-to-know“-Prinzip (minimale Berechtigungen) entsprechen?
6	Werden regelmäßig Reviews der eingerichteten Berechtigungen durchgeführt?
7	Erfolgt ein Monitoring bzw. eine regelmäßige Kontrolle der Aktivitäten von Administratoren?

## Protokollierung und Protokollauswertung (siehe auch Zugangs-, Zugriffs- und Auftragskontrolle)

8	Existiert eine verbindliche Vorgabe, die den Umfang der Protokollierung definiert (unter Beachtung der Verhältnismäßigkeit/Angemessenheit)? Der Umfang der Protokollierung sollte sich am Schutzbedarf der Daten orientieren (unter Beachtung der Sensibilität der Daten und der Eintrittswahrscheinlichkeit einer Gefährdung).
9	<p>Erfolgt eine Protokollierung der administrativen Tätigkeiten (Protokollierung zum Nachweis einer korrekten Funktionsweise der Systeme/Applikationen sowie der Verwaltung von Berechtigungen = Systemüberwachung)?</p> <p>Beispiele:</p> <ul style="list-style-type: none"><li>• Installation, Modifikation und Konfiguration von Hard-/Software</li><li>• Einrichten von Benutzern, Verwalten von Berechtigungen</li><li>• Durchführen von Backup-, Restore- und sonstigen Datensicherungsmaßnahmen</li></ul>
10	<p>Erfolgt eine Protokollierung zum Nachweis einer korrekten und rechtskonformen Verarbeitung von Daten (Verfahrensüberwachung)?</p> <p>Beispiele:</p> <ul style="list-style-type: none"><li>• Versuche unbefugten Einloggens (Überschreitung von Befugnissen)</li><li>• Datenübertragungen</li><li>• Dateneingabe und -veränderung</li><li>• Dateneinsicht</li><li>• Datenlöschung</li></ul>

11	<p>Geben die Protokolldaten Auskunft über:</p> <ul style="list-style-type: none"> <li>• Wann (Zeitpunkt der Aktivität oder des Ereignisses)</li> <li>• Wer (die ausführende Person/Systemkomponente)</li> <li>• Was (Bezeichnung des Ereignisses/der Tätigkeit)</li> <li>• Wie (Ergebnis der Tätigkeit (erfolgreich ausgeführt?))</li> <li>• Wieviel (Datenmenge/betroffene Daten)</li> </ul>
12	Ist sichergestellt, dass alle Systeme protokollieren?
13	<p>Wenn eine zentrale Speicherung von Protokolldaten erfolgt: Ist sichergestellt, dass die Protokolldaten vollständig übertragen werden (TCP (verbindungsorientiertes Protokoll) statt UDP (verbindungsloses Protokoll))?</p>
14	Ist sichergestellt, dass ein Ausfall der Protokollierung umgehend bemerkt wird?
15	<p>Ist bei der Übertragung der Protokolldaten auf zentrale Server (z.B. zur Auswertung oder Archivierung) sichergestellt, dass die Daten ausreichend geschützt werden?</p> <p>Maßnahmenziele:</p> <ul style="list-style-type: none"> <li>• Vertraulichkeit: Kann eine Einsichtnahme durch Unberechtigte ausgeschlossen werden?</li> <li>• Integrität: Können nicht autorisierte Änderungen ausgeschlossen werden?</li> <li>• Authentizität: Kommen die Daten von dem angegebenen System?</li> </ul>
16	<p>Ist der Umfang der Auswertungen festgelegt?</p> <ul style="list-style-type: none"> <li>• Auswertungszyklus (zeitnah, z.B. täglich; zeitnahe Auswertungen sollen ermöglichen, bei aufgedeckten Verstößen Schäden abzuwenden)</li> <li>• Auswertungsumfang (z.B. vollständig oder in Stichproben)</li> </ul>

17	Sind die Verantwortlichkeiten für die Auswertung der Protokolle festgelegt?
18	Wird der Zugriff auf Protokolldaten für Unberechtigte verhindert („need-to-know“-Prinzip)? Die Zugriffsbefugnisse sollten in einem Berechtigungskonzept geregelt werden.
19	Ist die Aufbewahrungsdauer für die Protokolle festgelegt und dokumentiert? Werden Protokolle nach Ablauf der Aufbewahrungsdauer gelöscht?
20	Erfolgt eine Überwachung der Integrität bei den Protokolldaten (Schutz vor dem Löschen und Verändern von Ereignissen)? Wenn ja, werden Integritätsverletzungen gemeldet?

### Aufbewahrungsfristen von Dokumenten

21	Sind für alle Dokumente mit personenbezogenen Daten Aufbewahrungsfristen festgelegt (z.B. nach HGB, AO, etc.)?
22	Werden Dokumente mit personenbezogenen Daten nach Ablauf der Aufbewahrungsfristen gelöscht?

## Checkliste Auftragskontrolle

### Schriftliche Beauftragung

1	Existiert ein schriftlicher Vertrag i.S.d. § 11 BDSG zwischen Auftraggeber und Auftragnehmer?
2	Sind <u>alle</u> durch den Auftraggeber beauftragten Dienstleistungen ausreichend konkret beschrieben (u.a. Gegenstand, Umfang, Art und der Zweck der vorgesehenen Erhebung, Verarbeitung oder Nutzung von Daten)?
3	Beinhaltet der Vertrag die konkreten Pflichten des Auftragnehmers?
4	Sind Leistungsindikatoren festgelegt, an Hand derer die vertragskonforme Auftragsdatenverarbeitung überwacht werden kann?
5	Beinhaltet der Vertrag die Kontrollrechte des Auftraggebers und die entsprechenden Duldungs- und Mitwirkungspflichten des Auftragnehmers?
6	Beinhaltet der Vertrag, dass alle Rechte des Auftraggebers auch durch die Revision, Aufsichtsbehörde oder andere prüfungsberechtigte Stellen wahrgenommen werden können?
7	<p>Ist der Umgang mit Weisungen vertraglich eindeutig geregelt?</p> <p>Beispiele:</p> <ul style="list-style-type: none"> <li>• Ist der Umfang der Weisungsbefugnisse des Auftraggebers gegenüber dem Auftragnehmer vereinbart?</li> <li>• Wer darf wem gegenüber Weisungen erteilen?</li> <li>• Ist sichergestellt, dass Weisungen immer in schriftlicher Form erfolgen?</li> <li>• Ist vertraglich vereinbart, dass der Auftragnehmer den Auftraggeber unverzüglich informiert, wenn er der Meinung ist, eine Weisung verstoße gegen datenschutzrechtliche Vorschriften?</li> </ul>

8	Sind Arbeitsdokumente (z.B. Verfahrens-/Arbeitsanweisungen oder Prozessbeschreibungen) vorhanden, die Vorgaben zur konkreten Umsetzung bzw. Ausgestaltung der beauftragten Dienstleistungen machen, vorhanden?
---	--

### Beschäftigte des Auftragnehmers

9	Wurden alle Beschäftigten des Auftragnehmers i.S.d. § 5 BDSG sowie ggf. weiterer regulatorischer Anforderungen auf das Datengeheimnis verpflichtet?
10	Wurden die Beschäftigten des Auftragnehmers über die drohenden Konsequenzen informiert, wenn sie personenbezogene Daten unbefugt erheben, verarbeiten oder zu nutzen?
11	Werden Beschäftigten des Auftragnehmers regelmäßig mit den für den Datenschutz relevanten Vorschriften vertraut gemacht? Wenn ja, wird dieses dokumentiert? Begleitende Maßnahmen können sein: Merkblätter, Rundschreiben, Aushang von Gesetzestexten, Awareness-Kampagnen
12	Wurden die Beschäftigten des Auftragnehmers aufgefordert, eventuelle Datenschutzverstöße zu melden?

### Unterauftragnehmer

13	Ist der Auftragnehmer im Rahmen der beauftragten Dienstleistung zur Begründung von Unterauftragsverhältnissen berechtigt?
14	Ist vereinbart, dass der Auftraggeber der Verlagerung der Erhebung, Verarbeitung oder Nutzung der Daten auf andere Standorte immer vorher zu genehmigen hat?
15	Setzt der Auftragnehmer im Rahmen der beauftragten Dienstleistung Unterauftragnehmer ein? Wenn ja, sind die folgenden Fragen zu beantworten:

16	Hat der Auftragnehmer Vereinbarungen zur Auftragsdatenvereinbarung mit den Unterauftragnehmern abgeschlossen, die den Anforderungen des § 11 BDSG gerecht werden?
17	Hat der Auftragnehmer den Unterauftragnehmer unter besonderer Berücksichtigung der Eignung der von ihm getroffenen technischen und organisatorischen Maßnahmen sorgfältig ausgewählt?
18	Sind die vertraglichen Vereinbarungen des Auftragnehmers mit dem/den Unterauftragnehmer/n so gestaltet, dass sie den Datenschutzbestimmungen im Vertragsverhältnis zwischen Auftraggeber und Auftragnehmer entsprechen?
19	Dürfen die vertraglichen Regelungen zwischen dem Auftragnehmer und dem Unterauftragnehmer auf Anfrage durch den Auftraggeber geprüft werden?
20	Überzeugt sich der Auftragnehmer regelmäßig von der Einhaltung der beim Unterauftragnehmer getroffenen technischen und organisatorischen Maßnahmen? Werden die Ergebnisse dokumentieren?
21	Wenn Frage 20 mit <i>ja</i> beantwortet wurde: Ist ein ausreichendes Datenschutzniveau beim Unterauftragnehmer sichergestellt (z.B. durch Safe Harbour, EU-Standardvertragsklausel, Corporate Binding Rules etc.)?
22	Wurden Unterauftragnehmer beauftragt, die ihren Standort außerhalb der EU oder eines anderen Vertragsstaats des Abkommens über den EWR haben?



## Protokollierung und Protokollauswertung (siehe auch Zugangs-, Zugriffs- und Eingabekontrolle)

23	Existiert eine verbindliche Vorgabe, die den Umfang der Protokollierung definiert (unter Beachtung der Verhältnismäßigkeit/Angemessenheit)? Der Umfang der Protokollierung sollte sich am Schutzbedarf der Daten orientieren (unter Beachtung der Sensibilität der Daten und der Eintrittswahrscheinlichkeit einer Gefährdung).
24	<p>Erfolgt eine Protokollierung der administrativen Tätigkeiten (Protokollierung zum Nachweis einer korrekten Funktionsweise der Systeme/Applikationen sowie der Verwaltung von Berechtigungen = Systemüberwachung)?</p> <p>Beispiele:</p> <ul style="list-style-type: none"><li>• Installation, Modifikation und Konfiguration von Hard-/Software</li><li>• Einrichten von Benutzern, Verwalten von Berechtigungen</li><li>• Durchführen von Backup-, Restore- und sonstigen Datensicherungsmaßnahmen</li></ul>
25	<p>Erfolgt eine Protokollierung zum Nachweis einer korrekten und rechtskonformen Verarbeitung von Daten (Verfahrensüberwachung)?</p> <p>Beispiele:</p> <ul style="list-style-type: none"><li>• Versuche unbefugten Einloggens (Überschreitung von Befugnissen)</li><li>• Datenübertragungen</li><li>• Dateneingabe und -veränderung</li><li>• Dateneinsicht</li><li>• Datenlöschung</li></ul>

26	<p>Geben die Protokolldaten Auskunft über:</p> <ul style="list-style-type: none"> <li>• Wann (Zeitpunkt der Aktivität oder des Ereignisses)</li> <li>• Wer (die ausführende Person/Systemkomponente)</li> <li>• Was (Bezeichnung des Ereignisses/der Tätigkeit)</li> <li>• Wie (Ergebnis der Tätigkeit (erfolgreich ausgeführt?))</li> <li>• Wieviel (Datenmenge/betroffene Daten)</li> </ul>
27	Ist sichergestellt, dass alle Systeme protokollieren?
28	<p>Wenn eine zentrale Speicherung von Protokolldaten erfolgt: Ist sichergestellt, dass die Protokolldaten vollständig übertragen werden (TCP (verbindungsorientiertes Protokoll) statt UDP (verbindungsloses Protokoll)?</p>
29	Ist sichergestellt, dass ein Ausfall der Protokollierung umgehend bemerkt wird?
30	<p>Ist bei der Übertragung der Protokolldaten auf zentrale Server (z.B. zur Auswertung oder Archivierung) sichergestellt, dass die Daten ausreichend geschützt werden?</p> <p>Maßnahmenziele:</p> <ul style="list-style-type: none"> <li>• Vertraulichkeit: Kann eine Einsichtnahme durch Unberechtigte ausgeschlossen werden?</li> <li>• Integrität: Können nicht autorisierte Änderungen ausgeschlossen werden?</li> <li>• Authentizität: Kommen die Daten von dem angegebenen System?</li> </ul>
31	<p>Ist der Umfang der Auswertungen festgelegt?</p> <ul style="list-style-type: none"> <li>• Auswertungszyklus (zeitnah, z.B. täglich; zeitnahe Auswertungen sollen ermöglichen, bei aufgedeckten Verstößen Schäden abzuwenden)</li> <li>• Auswertungsumfang (z.B. vollständig oder in Stichproben)</li> </ul>
32	Sind die Verantwortlichkeiten für die Auswertung der Protokolle festgelegt?

## Checkliste Auftragskontrolle

---

33	Wird der Zugriff auf Protokolldaten für Unberechtigte verhindert („need-to-know“-Prinzip)? Die Zugriffsbefugnisse sollten in einem Berechtigungskonzept geregelt werden.
34	Ist die Aufbewahrungsdauer für die Protokolle festgelegt und dokumentiert? Werden Protokolle nach Ablauf der Aufbewahrungsdauer gelöscht?
35	Erfolgt eine Überwachung der Integrität bei den Protokolldaten (Schutz vor dem Löschen und Verändern von Ereignissen)? Wenn ja, werden Integritätsverletzungen gemeldet?

## Checkliste Verfügbarkeitskontrolle

### Allgemeines

1	Wurde vertraglich eine Verfügbarkeit vereinbart und für was gilt diese (Service Level Agreement)?
2	<p>Auf welcher Basis wird die Verfügbarkeit ermittelt?</p> <ul style="list-style-type: none"> <li>• Verfügbarkeit von Komponenten (der Server funktioniert)</li> <li>• Verfügbarkeit der Leistung (der Server funktioniert und ist für Anwender erreichbar)</li> <li>• Nutzbarkeit der Leistung (der Server funktioniert und ist für Anwender erreichbar und nutzbar, etc.)</li> </ul>

### Technische Gebäudeausstattung

3	<p>Gibt es eine ausfallsichere Versorgung der IT-Infrastruktur?</p> <ul style="list-style-type: none"> <li>• Energieversorgung über zwei Wege</li> <li>• Netzersatzanlage (N+1)</li> <li>• USV-Anlage (N+1)</li> <li>• Klimatisierung (N+1)</li> </ul>
4	Wird die Infrastruktur regelmäßig gewartet? Liegen Wartungsprotokolle vor?
5	Sind die IT-Systeme redundant an PDUs (Power Distribution Systeme - Stromverteiler in Racks) angeschlossen?
6	<p>Sind Maßnahmen gegen Feuer getroffen (auch zur Reduzierung von Brandlasten), gibt es Brandmelder in den schutzbedürftigen IT-Räumen?</p> <p>Gibt es ein Rauchansaugsystem mit entsprechender Brandfrüherkennung?</p> <p>Existiert eine Löschanlage zur Löschung in IT-Räumen (z.B. mit Inertgas)?</p>

7	Sind Maßnahmen gegen Wassereinbruch getroffen, gibt es Leckagemelder in den schutzbedürftigen IT-Räumen?
---	--

## Netz- und Systemmanagement

8	Sind Netzwerk- und Systeminfrastruktur hochverfügbar aufgebaut? <ul style="list-style-type: none"><li>• Sind Netzpläne vorhanden?</li><li>• Gibt es Betriebshandbücher mit Wiederherstellungsplänen?</li></ul>
9	Gibt es ein Redundanzkonzept für geschäftskritische Anwendungen?
10	Ist der Ausfall eines Gebäudes in den Notfallplänen eingeplant?
11	Sind alle relevanten Komponenten lizenziert? (z.B. Software)
12	Liegen Supportverträge mit Drittherstellern vor?
13	Werden die Systeme hinsichtlich deren Verfügbarkeit in einem Monitoring-System überwacht?
14	Wie erfolgt die Datenlöschung oder Datenbereinigung? Werden Aufbewahrungsfristen eingehalten?
15	Gibt es Datenschnittstellen, über die personenbezogene Daten ausgetauscht werden können? Sind diese geschützt?
16	Gibt es ein Entsorgungskonzept für Datenträger (z.B. Festplatten aus IT-Systemen)?
17	Werden virtuelle Systeme eingesetzt? Wenn ja, ist festgelegt, <ul style="list-style-type: none"><li>• auf welchen physischen Systemen diese betrieben werden dürfen (z.B. werden Server in unterschiedlichen Sicherheitszonen betrieben)?</li></ul>

	<ul style="list-style-type: none"> <li>• wie viele virtuelle Systeme auf den physischen Systemen betrieben werden dürfen?</li> <li>• ob mehrere Mandanten in einem virtuellen System zusammengefasst werden?</li> </ul>
18	Erfolgt die Speicherung der Daten auf getrennten Systemen (z.B. NAS, SAN, RAID)?
19	Kommen Cloud-Dienste zum Einsatz?
20	Ist ein Kapazitätsmanagement vorhanden? Werden die verfügbaren Ressourcen regelmäßig ermittelt? Liegen Nachweise vor?

## Datensicherung & Notfallmanagement

21	<p>Gibt es ein angemessenes Konzept zur Erstellung von Backups der betriebskritischen Systeme?</p> <ul style="list-style-type: none"> <li>• Wird eine Datensicherung durchgeführt (z.B. full backup, incremental backup oder differential backup)?</li> <li>• Sind die Backupintervalle der Sensibilität der zu sichernden Daten angemessen (z.B. täglich)?</li> <li>• Wird das Ergebnis der Sicherung regelmäßig überprüft (erfolgreich, abgebrochen, Fehlermeldungen)?</li> <li>• Erfolgt die Lagerung der Sicherungsmedien an einem sicheren Ort (z.B. anderer Brandabschnitt oder Standort)?</li> <li>• Ist ein sicherer Datenträgertransport sichergestellt?</li> </ul>
22	<p>Sind die Voraussetzungen für die Wiederherstellung erfüllt?</p> <ul style="list-style-type: none"> <li>• Vollständigkeit der Sicherungsmedien</li> <li>• Ungeeignete Sicherungsmedien (z.B. überalterte Medien)</li> <li>• Kennwortgeschützten Sicherungsdatenträgern erfordern ein hinterlegtes Passwort</li> </ul>

	<ul style="list-style-type: none"><li>• Dokumentierte, revisionssichere Wiederanlaufpläne</li><li>• Kenntnis zur Datenintegrität und Risiken von Dateninkonsistenzen</li></ul>
23	Wird die Rückspielbarkeit der Datensicherungen regelmäßig getestet? Gibt es Nachweise für Rücksicherungen?
24	<p>Liegt ein Notfallhandbuch/BSM-Konzept mit folgendem Inhalt vor?</p> <ul style="list-style-type: none"><li>• Vorsorgeplanung</li><li>• Einsatzplanung</li><li>• Wiederanlaufplanung</li><li>• Regelmäßige Überprüfung</li><li>• Verantwortlichkeiten</li><li>• Kommunikationspartner (Notfall-Rufnummern)</li></ul>
25	Ist ein Ausweichrechenzentrum vorhanden (z.B. Hot-Standby, Cold-Standby)
26	Werden in regelmäßigen Abständen Notfallübungen durchgeführt? Gibt es Nachweise für die Notfallübungen?

## Sicherheitssysteme

27	<p>Sind Maßnahmen (Erkennung, Verhinderung, Beseitigung) zum Schutz vor Malware (u.a. Viren, Würmer, Cookies, Applets, CGI Skripte, Trojaner, ROOT Kits) umgesetzt?</p> <ul style="list-style-type: none"><li>• Ist eine regelmäßige Aktualisierung der Clients sichergestellt (Applikation, Scan-Pattern)?</li><li>• Gibt es Managementsysteme zur Alarmierung von Virenfunden?</li><li>• Wie werden Virenfunde behandelt (Löschen oder Quarantäne)?</li></ul> <p><b>Achtung:</b> Die Löschung eines Virus darf niemals undokumentiert erfolgen, ggf. werden relevante Informationen gelöscht!</p>
----	---

28	Ist das Netzwerk nach außen durch Firewalls abgeschottet?
29	<p>Existiert eine angemessene Netzwerkarchitektur bestehend aus einem mehrstufigen Firewallkonzept (Netzwerksegmente mit einem unterschiedlichen Schutzbedarf)? Beispiele:</p> <ul style="list-style-type: none"> <li>• Demilitarisierte Zone (DMZ)</li> <li>• interner Bereich</li> </ul>
30	Werden angemessene Filter zur Identifikation und Abwehr von Spam genutzt? (ggf. mehrstufige Filter )
31	Wird ein System zur Erkennung und zur Abwehr von Angriffen umgesetzt (Intrusion Detection System/Intrusion Prevention System)?
32	Gibt es eine Richtlinie zur Behandlung fremder Speichermedien?




## Checkliste Trennungskontrolle

1	<p>Ist sichergestellt, dass Daten, die zu unterschiedlichen Zwecken erhoben wurden (z.B. für unterschiedliche Auftraggeber), getrennt verarbeitet werden können?</p> <p>Beispiele (physische oder logische Trennung):</p> <ul style="list-style-type: none"><li>• Mandantenfähigkeit</li><li>• Dateiseparierung</li></ul>
2	<p>Wird durch ein Berechtigungskonzept sichergestellt, dass nur berechnigte Beschäftigte auf die Daten zugreifen können?</p>
3	<p>Werden die Daten des Auftraggebers im Rahmen der Datensicherung auf unterschiedlichen Datenträger getrennt von Daten von anderen Auftraggebern (z.B. Daten anderer Auftraggeber) gesichert?</p>
4	<p>Sind Entwicklungs- und Testsysteme von Produktionssystemen separiert?</p> <p>Beispiele:</p> <ul style="list-style-type: none"><li>• Unterschiedliche Netzsegmente (Trennung durch Firewalls)</li><li>• VLAN</li></ul>
5	<p>Ist sichergestellt, dass im Rahmen von Tests keine Produktionsdaten verwendet werden (z.B. durch Anonymisierung oder Pseudonymisierung)?</p>

## Die Autoren

Alle hier angegebene Autoren haben im Rahmen des Arbeitskreises Rechenzentrum an diesem GDD-Leitfaden „Datenschutz-Prüfung von Rechenzentren“ mitgearbeitet.

<p><b><i>Dipl.-Ing. Holger Brand</i></b> DAEQM Brand Inhaber hb@dae-hb.de www.dae-hb.de</p> 	<p>Seit 2009 ist Herr Dipl. Ing. (FH) Holger Brand externer Datenschutzbeauftragter und auf KMU's bundesweit spezialisiert. In dieser Tätigkeit werden die notwendigen Anforderungen des BDSG in den Unternehmen umgesetzt. Dies sind die technischen und organisatorischen Maßnahmen, Erstellen von Datenschutzkonzepten und Schulen der Mitarbeiter. Als vom TÜV Rheinland zertifizierter Datenschutzauditor werden interne Datenschutzaudits angeboten.</p> <p><u>Mitgliedschaft:</u> GDD Gesellschaft für Datenschutz und Datensicherheit e.V.</p>
<p><b><i>Axel Moritz (CISA, CISM)</i></b> Datenschutzbeauftragter, PCI DSS/IT-Security Manager B+S Card Service GmbH axel.moritz@bs-card-service.com www.bs-card-service.com</p> 	<p><u>Tätigkeit/Schwerpunkte:</u></p> <ul style="list-style-type: none"> <li>– Langjährige Erfahrung im Bereich Datenschutz, Qualitätsmanagement und Informationssicherheit</li> <li>– Als Datenschutzbeauftragter für die Pflege und Weiterentwicklung des Datenschutz-Managementsystems sowie für die Durchführung von Audits verantwortlich</li> <li>– Langjährige Verantwortung für die Aufrechterhaltung der PCI DSS Compliance</li> <li>– Als Projektleiter verantwortlich für den Aufbau von Managementsystemen nach ISO 9001 / 27001</li> </ul>

	<p><u>Ausbildung/Zertifizierungen:</u></p> <ul style="list-style-type: none"> <li>– Qualitätsmanager und interner Auditor (DGQ)</li> <li>– Fachkundig geprüfter Datenschutzbeauftragter (TA/Hochschule Ulm)</li> <li>– Zertifizierter Datenschutzauditor/-manager (TÜV)</li> <li>– Certified Information System Auditor (ISACA)</li> <li>– Certified Information Security Manager (ISACA)</li> <li>– Compliance Officer (Univ.)</li> </ul> <p><u>Mitgliedschaften:</u></p> <ul style="list-style-type: none"> <li>– ISACA - Berufsverband der IT-Revisoren, IT-Sicherheitsmanager sowie der IT-Governance Beauftragten</li> <li>– GDD Gesellschaft für Datenschutz und Datensicherheit e. V.</li> <li>– Mitglied des Leitungsteams des Erfa-Kreises Nord der GDD e.V.</li> <li>– Leiter der Arbeitsgruppe NordSec des Erfa-Kreises Nord der GDD e.V.</li> </ul>
<p><b>Volker Nehrhoff</b>          Datenschutzbeauftragter          Marli GmbH, Lübeck          datenschutz@marli.de          www.marli.de</p> 	<p>Interner Datenschutzbeauftragter</p> <p><u>Mitgliedschaften:</u></p> <ul style="list-style-type: none"> <li>– GDD Gesellschaft für Datenschutz und Datensicherheit e.V.</li> <li>– GDD-Erfa-Kreis Nord</li> <li>– GDD-Erfa-Kreis Mecklenburg-Vorpommern</li> </ul>

**Dipl.-Math. Birgit Pauls**

Seit 1998 als selbstständige Unternehmensberaterin mit den Schwerpunkten Datenschutz und Projektmanagement tätig.

pauls@birgitpauls.de  
www.birgitpauls.de



(Foto: S. Baouche)

- Fach- und Sachbuchautorin zu Datenschutzthemen seit 2007
- Mitautorin der Broschüre „Hilfe, ich soll Datenschutzbeauftragter werden“
- Texte für/von der GDD in Zusammenarbeit mit Datakontext herausgegebene Datenschutzposter
- Betriebliche Datenschutzbeauftragte (GDDcert.)
- Projektmanagement-Fachfrau (RKW/GPM)

Mitgliedschaften:

- GDD Gesellschaft für Datenschutz und Datensicherheit e.V.
- GDD-Erfa-Kreis Nord



**Marcus Pump**

akquinet system integration GmbH, Geschäftsführer

marcus.pump@akquinet.de  
www.akquinet.de




Langjährige erfolgreiche Tätigkeit als Berater und Projektleiter in Strategie- sowie Implementierungsprojekten mit Themenschwerpunkten in den Bereichen IT- Outsourcing, IT-Servicemanagement (ITIL), IT-Infrastruktur und IT-Sicherheit (BDSG, BSI IT-Grundschutz).

<p><b>Peer Reymann,</b> <b>Dipl.-Inform., B.Sc.</b></p> <p>ITQS GmbH, Geschäftsführer</p> <p>kontakt@itqs.de www.itqs.de</p> 	<ul style="list-style-type: none"><li>– CISA Certified Information System Auditor (ISACA)</li><li>– Lizenzierter Grundschutzauditor (BSI-GSL-0175-2005 - bis zur Ablösung des BSI-Auditschemas auf ISO 27001)</li><li>– Lizenzierter Auditor ISO 27001 auf Basis IT-Grundschutz (BSI-ZIG-0005-2014)</li><li>– IS-Revisor (BSI-ZISR-0003-2013)</li><li>– DE-Mail Auditor (BSI-ZADE-0015-2014)</li><li>– Lizenzierter Auditor QAR-IT</li><li>– Anerkannter Sachverständiger Datenschutzgütesiegel (Technik, ULD)</li><li>– Anerkannter Sachverständiger EuroPriSe (Technik)</li><li>– Geprüfter, fachkundiger Datenschutzbeauftragter (udis)</li><li>– Leiter GDD-Erfa-Kreis Nord (bis 2014) und AK Rechenzentrum (bis 10/2013) (udis)</li></ul>
<p><b>Curt-Jürgen Schädlich</b></p> <p>Diplom-Informatiker concept@rt GmbH</p> <p>EDV-und Organisationsberatung</p> <p>Geschäftsführer cjs@conceptart.it</p> 	<ul style="list-style-type: none"><li>– Seit 2005 als externer Datenschutzbeauftragter/IT-Sicherheitsbeauftragter tätig</li><li>– Datenschutzauditor (TÜV),</li><li>– IT-Security Auditor (TÜV)</li></ul> <p><u>Mitgliedschaften:</u></p> <ul style="list-style-type: none"><li>– Gesellschaft für Datenschutz und Datensicherheit e. V.</li><li>– GDD-Erfa-Kreis Nord</li><li>– NordSec des GDD-Erfa-Kreises Nord</li></ul>

<p><b>Eric Schreiber</b></p> <p>akquinet system integration GmbH</p> <p>IT-Sicherheitsbeauftragter, Qualitätsmanagementbeauftragter Auditor</p> <p>eric.schreiber@akquinet.de www.akquinet.de</p> 	<p>Seit 2009 als IT-Sicherheitsbeauftragter und Prozessbeauftragter tätig. Langjährige Erfahrung in der Erstellung, Umsetzung und Weiterentwicklung von IT-Sicherheitskonzepten nach ISO 27001 oder BSI-Grundschutz.</p> <p>Verantwortlich für die Prüfung von Unternehmensprozessen und Managementsystemen nach Qualitäts- und IT-Service Managementstandards (beispielsweise nach ISO 9001 oder ISO 20000) und Beratung in der Optimierung oder Vereinheitlichung von Prozessen. Dies wird methodisch unterstützt durch Business Process Modelling nach BPMN- oder EPK-Notation.</p> <p><u>Ausbildung/Zertifizierungen:</u></p> <p>Qualitätsmanagementbeauftragter und interner Auditor (DAkkS akkreditiert) ISO 27001 Lead Auditor (DAkkS akkreditiert)</p>
<p><b>Uwe Steen</b></p> <p>Revisor und Datenschutzbeauftragter Medizinischen Dienst der Krankenversicherung Nord (KdöR)</p> <p>uwe.steen@mdk-nord.de www.mdk-nord.de</p> 	<p>– Diplom-Volkswirt, Handelsfachwirt und Groß- und Außenhandelskaufmann</p> <p>– Datenschutzbeauftragter seit 1999 Spezialgebiet: Sozialdatenschutz</p> <p><u>Mitgliedschaften:</u></p> <p>– GDD Gesellschaft für Datenschutz und Datensicherheit e.V. – GDD-Erfa-Kreis Nord – GDD AK GSW</p>

<p><b><i>Carmen Ullrich</i></b></p> <p>Hamburger Sparkasse AG</p> <p>Spezialistin Abteilung Datenschutz bei der Haspa AG und für Mandanten</p> 	<p>Langjährige Erfahrung im Bereich Datenschutz für die Haspa AG und als externe Spezialistin für Mandanten</p> <p>Betriebswirtin</p> <p>EDV-Kauffrau</p> <p>Zertifizierte Fachkraft für Datenschutz der DEKRA</p> <p>Zertifizierte Datenschutzbeauftragte der GDD (GDDcert.)</p> <p><u>Mitgliedschaften:</u></p> <ul style="list-style-type: none"><li>– GDD Gesellschaft für Datenschutz und Datensicherheit e.V.</li><li>– GDD-Erfa-Kreis Nord</li></ul>
<p><b><i>Dipl.-Ing. Berthold Weghaus</i></b></p> <p>Konzerndatenschutzbeauftragter und IT-Revisor</p> <p>TÜV Nord Group</p> <p><a href="mailto:bweghaus@tuev-nord.de">bweghaus@tuev-nord.de</a></p> <p><a href="http://www.tuev-nord.de">www.tuev-nord.de</a></p> 	<p>Revision von IT-Prozessen und -Systemen, Optimierung regelkonformer Geschäftsprozesse und deren, sicherheitstechnische Analysen/Technikfolgeabschätzungen und Projektmanagement aus dem Blickwinkel des Datenschutzrechts.</p> <p>IT-Audits (von Produkten, Prozessen und Systemen) insbesondere in den Bereichen eGovernment und elektronischer Zahlungsverkehr,</p> <p>Entwicklung und Einführung risikoorientierter Prüfungsplanung für datenschutzrelevante Audits.</p> <p>Certified Information Systems Auditor (CISA)</p>

	<p><u>Mitgliedschaften:</u></p> <ul style="list-style-type: none"> <li>– Berufsverband der EDV-Revisoren und IT Sicherheitsmanager ISACA Germany Chapter e.V.</li> <li>– DIIR, Deutschen Institut für Interne Revision e.V.</li> <li>– Gesellschaft für Datenschutz und Datensicherheit e.V.</li> <li>– GDD-Erfa-Kreis Nord</li> </ul>
<p><b>Dipl.-Ing. Doris Wolf</b></p> <p>schernus projekte + seminare GmbH &amp; Co. KG, Hamburg</p> <p>Geschäftsführerin</p> <p>doris.wolf@schernus.com</p> <p>www.schernus.com</p> 	<p>Externe Datenschutzbeauftragte, Projektleiterin, Beraterin und Referentin für Datenschutz</p> <p>Autorin</p> <p>Anerkannte Sachverständige Datenschutzgütesiegel (Technik, ULD)</p> <p>Zertifizierte Datenschutzauditorin TÜV Rheinland</p> <p>Zertifizierte Projektmanagement-Fachfrau (RKW/GPM)</p> <p><u>Mitgliedschaften:</u></p> <ul style="list-style-type: none"> <li>– GDD Gesellschaft für Datenschutz und Datensicherheit e.V.</li> <li>– GDD-Erfa-Kreis Nord</li> <li>– NordSec des GDD-Erfa-Kreises Nord</li> <li>– VDI Verband Deutscher Ingenieure</li> <li>– Leiterin AK „Rechenzentrum“ des Erfa-Kreises Nord der GDD (seit 11/2013)</li> </ul>



# Satzung

**der Gesellschaft für Datenschutz und Datensicherheit (GDD) e.V.  
(in der Fassung der Beschlüsse vom 10.11.1983, 16.11.1984, 14.11.1990,  
04.11.1991, 20.11.2002, 18.11.2009, 21.11.2012 und 19.11.2014  
der ordentlichen Mitgliederversammlung in Köln)**

## Präambel

Datenschutz und Datensicherheit sind mit Blick auf die modernen Informations- und Kommunikationstechnologien sowie den wachsenden wirtschaftlichen Wert personenbezogener Daten wichtige Grundpfeiler der Informationsgesellschaft. Ein angemessener Datenschutz hat dabei sowohl dem Recht auf informationelle Selbstbestimmung als auch der Informationsfreiheit Rechnung zu tragen. Die Gesellschaft für Datenschutz und Datensicherheit (GDD) e.V. tritt für einen sinnvollen, vertretbaren und technisch realisierbaren Datenschutz ein. Sie hat zum Ziel, die Daten verarbeitenden Stellen und deren Datenschutzbeauftragte bei der Lösung der vielfältigen technischen, rechtlichen und organisatorischen Fragen zu unterstützen, die durch das Erfordernis nach rechtmäßiger, ordnungsgemäßer und sicherer Datenverarbeitung aufgeworfen werden. Die Gesellschaft tritt hierzu für die Prinzipien der Selbstkontrolle und Selbstregulierung ein. Im Rahmen ihrer Aktivitäten pflegt sie eine intensive Zusammenarbeit mit Wirtschaft, Verwaltung, Wissenschaft und Politik. Die Gesellschaft vertritt die Belange der Daten verarbeitenden Stellen - insbesondere auch der mittelständischen Wirtschaft -, deren Datenschutzbeauftragten und der betroffenen Bürger gegenüber Regierungen und Gesetzgebungsorganen; sie will ferner die politische Willensbildung durch fachlichen Rat unterstützen.

## § 1

### **Name, Sitz, Geschäftsjahr**

- (1) Der Verein führt den Namen „Gesellschaft für Datenschutz und Datensicherheit (GDD) e.V.“ Die Gesellschaft hat ihren Sitz in Bonn; sie ist in das Vereinsregister eingetragen.
- (2) Das Geschäftsjahr der Gesellschaft ist das Kalenderjahr.

## § 2

### **Zweck und Gemeinnützigkeit**

(1) Die Gesellschaft mit Sitz in Bonn verfolgt ausschließlich und unmittelbar gemeinnützige Zwecke im Sinne des Abschnitts „Steuerbegünstigte Zwecke“ der Abgabenordnung. Zweck der Gesellschaft ist die Förderung der Volks- und Berufsbildung auf dem Gebiet des Datenschutzes und der Datensicherheit im Sinne der dieser Satzung vorangestellten Präambel. Der Satzungszweck wird verwirklicht insbesondere durch

1. die Zurverfügungstellung von Informationen und Materialien an die betroffenen Bürger und Daten verarbeitenden Stellen zur Meinungsbildung und Entscheidungsfindung,
2. die Bildung von Arbeits- und Erfahrungsaustauschkreisen,
3. die Entwicklung und Veröffentlichung von Methoden zur Sicherung der Qualifikation von Datenschutzverantwortlichen, insbesondere Datenschutzbeauftragten,
4. die Zusammenarbeit mit den in der Datenschutzgesetzgebung vorgesehenen staatlichen Kontrollorganen.

(2) Die Gesellschaft ist selbstlos tätig; sie verfolgt nicht in erster Linie eigenwirtschaftliche Zwecke. Mittel der Gesellschaft dürfen nur für die satzungsmäßigen Zwecke verwendet werden. Die Mitglieder erhalten keine Zuwendungen aus Mitteln der Gesellschaft. Es darf keine Person durch Ausgaben, die dem Zweck der Gesellschaft fremd sind, oder durch unverhältnismäßig hohe Vergütungen begünstigt werden.

## § 3

### **Mitgliedschaft**

- (1) Ordentliche Mitglieder der Gesellschaft können natürliche und juristische Personen, Handelsgesellschaften, nicht rechtsfähige Ver-

eine sowie Anstalten und Körperschaften des öffentlichen Rechts werden.

(2) Die Beitrittserklärung erfolgt schriftlich gegenüber dem Vorstand. Über die Annahme der Beitrittserklärung entscheidet der Vorstand. Die Mitgliedschaft beginnt mit Annahme der Beitrittserklärung.

(3) Die Mitgliedschaft endet durch Austrittserklärung, durch Tod von natürlichen Personen oder durch Auflösung und Erlöschen von juristischen Personen, Handelsgesellschaften, nicht rechtsfähigen Vereinen sowie Anstalten und Körperschaften des öffentlichen Rechts oder durch Ausschluss; die Beitragspflicht für das laufende Geschäftsjahr bleibt hiervon unberührt.

(4) Der Austritt ist nur zum Schluss eines Geschäftsjahres zulässig; die Austrittserklärung muss spätestens drei Monate vor Ablauf des Geschäftsjahres gegenüber dem Vorstand schriftlich abgegeben werden.

(5) Die Mitgliederversammlung kann solche Personen, die sich besondere Verdienste um die Gesellschaft oder um die von ihr verfolgten satzungsgemäßen Zwecke erworben haben, zu Ehrenmitgliedern ernennen. Ehrenmitglieder haben alle Rechte eines ordentlichen Mitglieds. Sie sind von Beitragsleistungen befreit.

#### § 4

##### **Rechte und Pflichten der Mitglieder**

(1) Die Mitglieder sind berechtigt, die Leistungen der Gesellschaft in Anspruch zu nehmen.

(2) Die Mitglieder sind verpflichtet, die satzungsgemäßen Zwecke der Gesellschaft zu unterstützen und zu fördern. Sie sind ferner verpflichtet, die festgesetzten Beiträge zu zahlen.

#### § 5

##### **Ausschluss eines Mitgliedes**

(1) Ein Mitglied kann durch Beschluss des Vorstandes ausgeschlossen werden, wenn es das Ansehen der Gesellschaft schädigt, seinen Beitragsverpflichtungen nicht nachkommt oder wenn ein sonstiger wichtiger Grund vorliegt. Der Vorstand muss dem auszuschließenden Mitglied den Beschluss in schriftlicher Form unter der Angabe der Gründe mitteilen und ihm auf Verlangen eine Anhörung gewähren.

(2) Gegen den Beschluss des Vorstandes ist die Anrufung der Mitgliederversammlung zulässig. Bis zum Beschluss der Mitgliederversammlung ruht die Mitgliedschaft.

#### § 6

##### **Beitrag**

(1) Die Gesellschaft erhebt einen Jahresbeitrag. Er ist für das Geschäftsjahr im ersten Quartal des Jahres im Voraus zu entrichten. Das Nähere regelt die Beitragsordnung, die von der Mitgliederversammlung beschlossen wird.

(2) Im begründeten Einzelfall kann für ein Mitglied durch Vorstandsbeschluss ein von der Beitragsordnung abweichender Beitrag festgesetzt werden.

#### § 7

##### **Organe der Gesellschaft**

Die Organe der Gesellschaft sind

1. die Mitgliederversammlung,
2. der Vorstand.

#### § 8

##### **Mitgliederversammlung**

(1) Oberstes Beschlussorgan ist die Mitgliederversammlung. Ihrer Beschlussfassung unterliegen

1. die Genehmigung des Finanzberichtes und der Haushaltspläne,
2. die Entlastung des Vorstandes,
3. die Wahl der einzelnen Vorstandsmitglieder,
4. die Bestellung von Finanzprüfern,
5. Satzungsänderungen,
6. die Genehmigung der Beitragsordnung,
7. die Richtlinie für die Erstattung von Reisekosten und Auslagen,
8. Anträge des Vorstandes und der Mitglieder,
9. die Ernennung von Ehrenmitgliedern,
10. die Auflösung der Gesellschaft.

(2) Die ordentliche Mitgliederversammlung findet einmal im Jahr statt. Außerordentliche Mitgliederversammlungen werden auf Beschluss des Vorstandes abgehalten, wenn die Interessen der Gesellschaft dies erfordern, oder wenn ein Viertel der Mitglieder dies unter Angabe des Zweckes schriftlich beantragt. Die Einberufung der Mitgliederversammlung erfolgt schriftlich durch den Vorstand mit einer Frist von mindestens zwei Wochen.

Hierbei sind die Tagesordnung bekannt zugeben und ihr die nötigen Informationen beizufügen, insbesondere Geschäftsbericht, Finanzbericht, Haushaltsplan, Satzungsänderungen, Änderungen der Beitragsordnung und - soweit bekannt - Wahlvorschläge und Anträge an die Mitgliederversammlung. Anträge zur Tagesordnung sind mindestens drei Tage vor der Mitgliederversammlung bei der Geschäftsstelle einzureichen. Über die Behandlung von Initiativanträgen entscheidet die Mitgliederversammlung.

(3) Die Mitgliederversammlung ist beschlussfähig, wenn mindestens 30 stimmberechtigte Mitglieder anwesend sind. Beschlüsse sind jedoch gültig, wenn die Beschlussfähigkeit vor der Beschlussfassung nicht angezweifelt worden ist.

(4) Beschlüsse über Satzungsänderungen und über die Auflösung der Gesellschaft bedürfen zu ihrer Rechtswirksamkeit der Dreiviertelmehrheit der anwesenden und ordnungsgemäß vertretenen Mitglieder. In allen anderen Fällen genügt die einfache Mehrheit.

(5) Jedes Mitglied hat eine Stimme. Juristische Personen haben einen Stimmberechtigten schriftlich zu bestellen. Jedes Mitglied hat das Recht, sich durch eine andere stimmberechtigte natürliche Person vertreten zu lassen; eine Person kann höchstens zehn Stimmen auf sich vereinigen. Die Bestellung des Vertreters hat schriftlich zu erfolgen.

(6) Auf Antrag des Mitglieds ist geheim abzustimmen. Über die Beschlüsse der Mitgliederversammlung ist ein Protokoll anzufertigen, das vom Versammlungsleiter und dem Protokollführer zu unterzeichnen ist; das Protokoll ist allen Mitgliedern zuzustellen und auf der nächsten Mitgliederversammlung genehmigen zu lassen.

### § 9

#### Vorstand

(1) Der Vorstand besteht aus mindestens sieben und höchstens elf Mitgliedern:

1. dem Vorsitzenden,
2. zwei stellvertretenden Vorsitzenden,
3. dem Schatzmeister,
4. mindestens zwei und maximal sechs Beisitzern und
5. dem Erfa-Repräsentanten.

Der Vorstand ist berechtigt, bei entsprechendem Bedarf bis zu zwei Mitglieder zu kooptieren. Diese haben kein Stimmrecht.

(2) Vorstand im Sinne des § 26 Abs. 2 BGB sind der Vorsitzende, im Verhinderungsfall sein Stellvertreter, zusammen mit einem der anderen Vorstandsmitglieder. Die Vertretungsmacht ist durch Beschlüsse des gesamten Vorstandes begrenzt.

(3) Der Vorstand beschließt mit der Mehrheit seiner satzungsgemäßen Mitglieder. Sind mehr als zwei Vorstandsmitglieder dauernd an der Ausübung ihres Amtes gehindert, so sind unverzüglich Nachwahlen anzuberaumen.

(4) Die Amtsdauer der Vorstandsmitglieder beträgt zwei Jahre; Wiederwahl ist zulässig.

(5) Der Vorstand gibt sich eine Geschäftsordnung.

(6) Der Vorstandsvorsitzende ist Dienstvorgesetzter der Geschäftsführer.

(7) Der Schatzmeister überwacht die Haushaltsführung und verwaltet das Vermögen der Gesellschaft. Er hat auf eine sparsame und wirtschaftliche Haushaltsführung hinzuwirken. Mit Ablauf des Geschäftsjahres stellt er unverzüglich die Abrechnung sowie die Vermögensübersicht und sonstige Unterlagen von wirtschaftlichem Belang den Finanzprüfern der Gesellschaft zur Prüfung zur Verfügung.

(8) Die Vorstandsmitglieder sind grundsätzlich ehrenamtlich tätig; sie haben Anspruch auf Erstattung notwendiger Auslagen im Rahmen einer von der Mitgliederversammlung zu beschließenden Richtlinie über die Erstattung von Reisekosten und Auslagen.

(9) Der Vorstand kann einen 'Wissenschaftlichen Beirat' einrichten, der für die Gesellschaft beratend und unterstützend tätig wird; in den Beirat können auch Nicht-Mitglieder berufen werden.

(10) Auf Vorschlag des Vorstandes kann die Mitgliederversammlung einen Vorsitzenden des Vorstandes nach dessen Ausscheiden aus dem Vorstand wegen herausragender Verdienste um die Gesellschaft zum Ehrenvorsitzenden ernennen. Der Ehrenvorsitzende wird zu den Sitzungen des Vorstandes eingeladen, er hat aber kein Stimmrecht.

## § 10

### Geschäftsführung

- (1) Die Geschäftsführung besteht aus bis zu zwei Geschäftsführern. Die Rechte und Pflichten werden in einem Dienstvertrag geregelt.
- (2) Die Geschäftsführung führt die Geschäfte der Gesellschaft. Sie ist an die Vorgaben und Weisungen des Vorstandes gebunden. Die Geschäftsführung erstellt insbesondere den Jahreshaushaltsplan, den Rechnungsabschluss sowie den Geschäftsbericht und bereitet die Sitzungen des Vorstandes, der Mitgliederversammlung, des wissenschaftlichen Beirates und des Erfa-Beirates vor.
- (3) Innerhalb des laufenden Geschäftsverkehrs ist die Geschäftsführung im Rahmen der ihr erteilten Vollmacht ermächtigt, den Verein zu verpflichten und Rechte für ihn zu erwerben.

## § 11

### Finanzprüfer

- (1) Zur Kontrolle der Haushaltsführung bestellt die Mitgliederversammlung Finanzprüfer. Nach Durchführung ihrer Prüfung geben sie dem Vorstand Kenntnis von ihrem Prüfungsergebnis und erstatten der Mitgliederversammlung Bericht.
- (2) Die Finanzprüfer dürfen dem Vorstand nicht angehören.

## § 12

### Erfa-Organisation

- (1) Die Gesellschaft bildet zur Durchführung ihrer Aufgaben Erfahrungsaustauschkreise (Erfa-Kreise). Aufgabe der Erfa-Kreise ist es insbesondere, in Zusammenarbeit mit den zuständigen Aufsichtsbehörden und sonstigen Fachleuten für Fragen des Datenschutzes und der Datensicherheit,
  1. die Teilnehmer bei der Lösung und Klärung bestehender Datenschutzprobleme zu unterstützen,
  2. auf lokaler oder regionaler Ebene Ziele und Belange der Gesellschaft und ihrer Mitglieder zu vertreten,

3. auf lokaler oder regionaler Ebene die Belange der betrieblichen und behördlichen Datenschutzbeauftragten zu vertreten.
- (2) Aufgabe der Erfa-Kreise ist es ferner,
  1. die Entscheidungsbildung in der Gesellschaft zu fördern und vorzubereiten,
  2. Mitglieder für die Gesellschaft zu werben.
- (3) Beabsichtigt ein Erfa-Kreis, bestimmte Themen oder Aktivitäten mit überregionalem Bezug an die Öffentlichkeit zu tragen, ist dies vorher mit dem Vorstand der Gesellschaft abzustimmen.
- (4) Jeder Erfa-Kreis wählt einen Erfa-Kreis-Leiter. Die Erfa-Kreise sollten sich eine Geschäftsordnung geben, die mit dem Erfa-Beirat abzustimmen ist.

## § 13

### Erfa-Beirat

- (1) Der Erfa-Beirat besteht aus den Erfa-Kreis-Leitern, die Mitglieder der Gesellschaft sind.
- (2) Der Erfa-Beirat schlägt der Mitgliederversammlung aus seiner Mitte den Erfa-Repräsentanten zur Wahl in den Vorstand vor.
- (3) Der Erfa-Beirat wirkt bei der Führung der Geschäfte der Gesellschaft beratend und unterstützend mit. Er hat insbesondere die Aufgabe, die Belange der Erfa-Kreise zu vertreten.
- (4) Der Erfa-Beirat gibt sich eine Geschäftsordnung; in ihr ist die Mitgliederstärke der einzelnen Erfa-Kreise angemessen zu berücksichtigen.

## § 14

### Auflösung der Gesellschaft

Bei der Auflösung oder Aufhebung der Gesellschaft oder bei Wegfall steuerbegünstigter Zwecke fällt das Vermögen der Gesellschaft an eine juristische Person des öffentlichen Rechts oder eine andere steuerbegünstigte Körperschaft zwecks Verwendung für die Förderung der Volks- und Berufsbildung.

**Nähere Informationen über die GDD finden Sie unter [www.gdd.de](http://www.gdd.de) oder rufen Sie uns unter 0228/96 96 75 00 an.**

## Mitgliedschaft

GDD-Mitglieder können natürliche und juristische Personen, Personengesellschaften, nicht-rechtsfähige Vereine sowie Einrichtungen des öffentlichen Rechts im In- und Ausland werden. Bei Wirtschaftsunternehmen, Behörden, Verbänden u.ä. wird ein nach Größe der Vereinigung gestaffelter Jahresbeitrag erhoben. Einzelheiten ergeben sich aus unserer Beitragsordnung. Firmenmitglieder können neben den regelmäßigen Serviceleistungen der GDD zusätzlich die Unterstützung bei Datenschutzfragen aus der betrieblichen Praxis ihres Unternehmens in Anspruch nehmen. Wenn Sie Mitglied werden möchten, senden Sie bitte folgende Beitrittserklärung ausgefüllt an die

## Gesellschaft für Datenschutz und Datensicherheit e.V. (GDD)

Heinrich-Böll-Ring 10 · 53119 Bonn · F +49 228 96 96 75 25 · info@gdd.de

.....

## Beitrittserklärung

Für eine ordentliche Mitgliedschaft gem. § 3 Abs. 1 der GDD-Satzung:

- ☐ Firmenmitgliedschaft
- ☐ Anzahl der Beschäftigten: .....
- ☐ Persönliche Mitgliedschaft (nur Privatpersonen)
- ☐ Persönliche Mitgliedschaft als betrieblicher Datenschutzbeauftragter

Firma: .....

Name: .....

Straße/Ort: .....

Abteilung/Branche: .....

Telefon-/Fax-Nr.: .....

E-Mail: .....

Wie wurden Sie auf die GDD aufmerksam? .....

Mit der Aufnahme meiner Daten in die offizielle Mitgliederliste erkläre ich mich

- ☐ einverstanden
- ☐ nicht einverstanden

.....

Datum und Unterschrift

Wir verarbeiten Ihre Daten zu Ihrer Betreuung im Rahmen der Mitgliedschaft, ggf. auch unter Einsatz von Dienstleistern. Darüber hinaus geben wir Ihre Adressdaten an unseren Kooperationspartner Verlagsgruppe Huthig Jehle Rehm GmbH - Datakontext - weiter, um Sie über Produkte und Fachveranstaltungen zum Thema Datenschutz und IT-Sicherheit zu informieren. Der Verwendung Ihrer Daten zu Werbezwecken können Sie jederzeit bei uns widersprechen.

## >> GDD-Support für Wirtschaft, Verwaltung, Wissenschaft und Politik

Die GDD tritt für die Prinzipien der Selbstkontrolle und Selbstregulierung auf dem Gebiet des Datenschutzes ein. Sie unterstützt die politische Willensbildung durch fachlichen Rat.

Bei der Umsetzung der datenschutzrechtlichen Vorgaben bietet die GDD folgende Leistungen:

- >> Beratung in Einzelfragen
- >> Schulungen und Praktikerforen
- >> Online-Datenbanken, u.a.:  
GDD-Rechtsprechungsarchiv  
GDD-Literaturarchiv
- >> GDD-Praxis-Ratgeber
- >> Fachzeitschrift „Recht der  
Datenverarbeitung (RDV)“
- >> Fachpublikationen
- >> Erfahrungsaustausch

Wie Sie  
noch mehr  
erfahren

# GDD

Gesellschaft für  
Datenschutz und  
Datensicherheit e.V.

Heinrich-Böll-Ring 10  
53119 Bonn  
Telefon (0228) 96 96 75 00  
Telefax (0228) 96 96 75 25  
E-Mail: [info@gdd.de](mailto:info@gdd.de)  
Internet: [www.gdd.de](http://www.gdd.de)

# GDD

Gesellschaft für Datenschutz  
und Datensicherheit e.V.

# Das Datenschutzsiegel

Ist das Unternehmen in Sachen Datenschutz zuverlässig? Vor dieser Frage stehen nicht nur Verbraucher, sondern auch viele Unternehmen, die vertrauenswürdige Partner suchen.

## Das Problem

Gerade im Bereich der Auftragsdatenverarbeitung sind Auftraggeber gesetzlich verpflichtet, Auftragnehmer sorgfältig auszuwählen. Im Rahmen dieser Auswahl und auch im Verlauf der Vertragsbeziehung muss der Auftraggeber sich vom Datenschutzniveau des Auftragnehmers überzeugen. Für beide Seiten ein aufwändiges und kostenintensives Unterfangen.

## Unsere Lösung

Die Fachverbände „Berufsverband der Datenschutzbeauftragten Deutschlands (BvD) e.V.“ und „Gesellschaft für Datenschutz und Datensicherheit (GDD) e.V.“ haben deshalb ein Datenschutzsiegel basierend auf dem Datenschutzstandard „DS-BvD-GDD-01“ speziell für die Auftragsdatenverarbeitung entwickelt.



## Ihre Vorteile

- Auftraggeber können das Siegel ihrem eigenen Kontrollermessen zu Grunde legen.
- Auftragnehmer signalisieren ihr gesetzteskonformes Datenschutzniveau
- Der Landesbeauftragte für Datenschutz und Informationsfreiheit Nordrhein-Westfalen (LDI NRW) befürwortet die zu Grunde liegende Gesamtkonzeption aus Standard und Zertifizierungsablauf.

## Der Zertifizierer

Das Gütesiegel kann bei der DSZ Datenschutz Zertifizierungsgesellschaft mbH ([www.dsz-audit.de](http://www.dsz-audit.de)) beantragt werden.