Klotz, Michael

Working Paper

Regelwerke der IT-Compliance - Klassifikation und Übersicht. Teil 1: Rechtliche Regelwerke

SIMAT Arbeitspapiere, No. 03-11-011

Provided in Cooperation with:
Hochschule Stralsund, Stralsund Information Management Team (SIMAT)

Suggested Citation: Klotz, Michael (2011) : Regelwerke der IT-Compliance - Klassifikation und Übersicht. Teil 1: Rechtliche Regelwerke, SIMAT Arbeitspapiere, No. 03-11-011, Fachhochschule Stralsund, Stralsund Information Management Team (SIMAT), Stralsund, https://nbn-resolving.de/urn:nbn:de:0226-simat03110110

This Version is available at:
https://hdl.handle.net/10419/60089

SIMAT Arbeitspapiere
Herausgeber: Prof. Dr. Michael Klotz

SIMAT AP 03-11-011

Regelwerke der IT-Compliance – Klassifikation und Übersicht Teil 1: Rechtliche Regelwerke

Prof. Dr. Michael Klotz

Fachhochschule Stralsund
SIMAT Stralsund Information Management Team

Mai 2011

ISSN 1868-064X

Klotz, Michael: Regelwerke der IT-Compliance – Klassifikation und Übersicht. In: SIMAT Arbeitspapiere. Hrsg. von Michael Klotz. Stralsund: FH Stralsund, SIMAT Stralsund Information Management Team, 2011 (SIMAT AP, 3 (2011), 11), ISSN 1868-064X

Download über URN vom Server der Deutschen Nationalbibliothek:
http://nbn-resolving.de/urn:nbn:de:0226-simat03110110

Impressum
Fachhochschule Stralsund
SIMAT Stralsund Information Management Team
Zur Schwedenschanze 15
18435 Stralsund
www.fh-stralsund.de
http://simat-stralsund.de/

Herausgeber
Prof. Dr. Michael Klotz
Fachbereich Wirtschaft
Zur Schwedenschanze 15
18435 Stralsund
E-Mail: michael.klotz@fh-stralsund.de

Autor

Prof. Dr. Michael Klotz lehrt und forscht am Fachbereich Wirtschaft der FH Stralsund auf den Gebieten der Unternehmensorganisation und des Informationsmanagements. Er ist u. a. Wissenschaftlicher Leiter des SIMAT, regionaler Ansprechpartner der gfo Gesellschaft für Organisation e.V., wissenschaftlicher Beirat und Academic Advocate der ISACA sowie Mitherausgeber der Zeitschrift „IT-Governance“.

Regelwerke der IT-Compliance – Klassifikation und Übersicht Teil 1: Rechtliche Regelwerke

Prof. Dr. Michael Klotz[1]

Zusammenfassung: IT-Compliance bezeichnet einen Zustand, in dem alle, die IT des Unternehmens betreffenden und verbindlich vorgegebenen bzw. als verbindlich akzeptierten Vorgaben nachweislich eingehalten werden. Sofern die Vorgaben aus Gesetzen stammen, bedeutet dies, dass sich Unternehmen an geltendes Recht zu halten haben. Neben Gesetzen hat ein Unternehmen jedoch auch Vorgaben aus weiteren internen und externen Regelwerken zu beachten. In diesem Arbeitspapier werden Regelwerke betrachtet, aus denen rechtliche Vorgaben für die IT des Unternehmens resultieren. Dies umfasst Gesetze und Rechtsverordnungen, Verwaltungsvorschriften, referenzierte Regelwerke und Urteile sowie Verträge. Die wichtigsten in der Praxis relevanten und in der Fachwelt diskutierten Regelwerke werden in ein sog. „House of IT-Compliance“ eingeordnet und in ihrer Bedeutung für IT-Compliance kurz beschrieben. Hierzu erfolgen die Nennung des Regelwerks und eine kurze Inhaltsangabe. Als Status wird die aktuelle Fassung oder Version angegeben. Ein Link zum Text des Regelwerks vereinfacht die eigene Recherche. Insgesamt bietet das Arbeitspapier damit eine Handreichung für die Praxis, die sich schnell hinsichtlich relevanter Regelwerke der IT-Compliance orientieren will.

Gliederung

---

[1] Prof. Dr. Michael Klotz, FH Stralsund, Fachbereich Wirtschaft, Zur Schwedenschanze 15, 18435 Stralsund, michael.klotz@fh-stralsund.de

Schlüsselwörter: Compliance – Gesetz – Governance – Informationstechnologie – IT-Compliance – IT-Vertrag – Rechtsprechung – Rechtsverordnung – Regelwerk – Vertrag – Verwaltungsvorschrift

JEL-Klassifikation: K12, K23, K31, K32, K34, M12, M41, M42

Vorwort

Funktionen und Systeme der Corporate Compliance haben sich in vielen Unternehmen in verschiedener Art und Weise durchgesetzt. Auch IT-Compliance hat sich mittlerweile als ein fester Bestandteil des IT-Managements etabliert. Gleichwohl liegt immer noch ein theoretisch-konzeptionelles Defizit für die Wissens- und Managementdomäne „IT-Compliance“ vor. Dies beginnt mit begrifflichen Abgrenzungen, setzt sich fort mit handlungsorientierten Strukturmodellen sowie vergleichenden Analysen und endet mit einer systemischen Integration mit anderen Gebieten des IT-Managements, insbesondere mit dem IT-Risikomanagement und dem IT-Sicherheitsmanagement.

Auf der begrifflichen Seite besteht Einigkeit im Grunde lediglich auf einer alltagssprachlichen Ebene, wenn unisono drauf verwiesen wird, dass Compliance als Befolgung, Einhaltung etc. von Vorgaben, Regeln oder Anforderungen verstanden werden kann. Woher diese Vorgaben/Regeln/Anforderungen stammen, wird dagegen oftmals nicht klar dargestellt. Hier soll das vorliegende Arbeitspapier zu einem Fortschritt verhelfen.

Als Quelle der einzuhaltenden Vorgaben wird im Folgenden der übergeordnete Begriff der Regelwerke verwendet. Diese werden systematisiert, wofür das Bild eines „House of IT-Compliance“ verwendet wird. In diese Systematik werden Regelwerke eingeordnet, die die IT eines Unternehmens direkt adressieren oder Anforderungen an andere Unternehmensfunktionen richten, die jedoch mehr oder weniger, mitunter aber auch nur ausschließlich mithilfe von IT erfüllt werden können. Aus dieser Zuordnung ergeben sich zahlreiche Klärungen, aber auch neue Fragestellungen zum Umfang von IT-Compliance. Deren Lösung ist wiederum Voraussetzung dafür, dass die Theorie der Praxis Orientierung vermitteln und praxistaugliche Modelle an die Hand geben kann.

In diesem Arbeitspapier werden Regelwerke betrachtet, aus denen rechtliche Vorgaben für die IT des Unternehmens resultieren. Dies umfasst z. B. Gesetze und Rechtsverordnungen ebenso wie Rechtsprechung und Verträge. In einem späteren Arbeitspapier werden sonstige unternehmensinterne und -externe Regelwerke (z. B. IT-Richtlinien, IT-Normen und -Standards) betrachtet.

Prof. Dr. Michael Klotz

1. IT-Compliance

1.1 Begriff der IT-Compliance

Vorgaben für die IT

IT-Compliance materialisiert sich im Vorhandensein und Funktionieren spezifischer informations- und kommunikationstechnischer Einrichtungen, im Vorliegen von Systemdokumentationen, Richtlinien, Kontrollergebnissen und Notfallplänen, korrekten und gesicherten Daten, Regelungen für den Datenzugriff u. v. a. m. Dennoch steht all dies nicht für die Bedeutung des Begriffs „IT-Compliance“. Nicht der unmittelbare Zweck, der mit dem Vorhandensein der verschiedenen Gerätschaften, Dokumente etc. verbunden ist, wird vom Compliance-Begriff adressiert, sondern eine Nebenbedingung steht hier im Vordergrund: die der Befolgung relevanter Vorgaben[2]. Diese Vorgaben, die technischer, organisatorischer oder personeller Art sein können, erweisen sich in der Regel als Mittel zum Zweck.

Beispiel Datenzugriff

So sollen beispielsweise durch eine Beschränkung des Datenzugriffs Datenverlust oder -beschädigung und damit letztlich eine Beeinträchtigung des Unternehmenswertes verhindert werden. Umfang und Art der Beschränkung des Datenzugriffs haben verschiedenen Regelwerken zu genügen:

- internen Vorgaben, z. B. eines Berechtigungskonzepts;
- vertraglichen Vereinbarungen, z. B. im Rahmen von Hosting-Verträgen;
- gesetzlichen Anforderungen, z. B. des Bundesdatenschutzgesetzes (BDSG);
- akzeptierten Normen, z. B. der ISO/IEC 27002;
- akzeptierten Standards, z. B. den Grundschutzkatalogen des Bundesamtes für Sicherheit in der Informationstechnik (BSI).

Aus diesen und ggf. weiteren Regelwerken resultieren verschiedene Vorgaben, die i. d. R. durch mehrere Maßnahmen adressiert werden. Eine dieser Maßnahmen kann die Einführung eines Identity Management Systems (IMS) darstellen. Durch die operative Nutzung des IMS werden die Vorgaben hinsichtlich der Beschränkung des Datenzugriffs schließlich erfüllt; im Ergebnis entsteht Compliance, s. Abbildung 1.

---

[2] Neben „Befolgung“ werden auch die Begriffe „Übereinstimmung“, „Einhaltung“, „Konformität“, „Erfüllung“ oder „Entsprechung“ verwendet; vgl. *Klotz 2009*, S. 3.

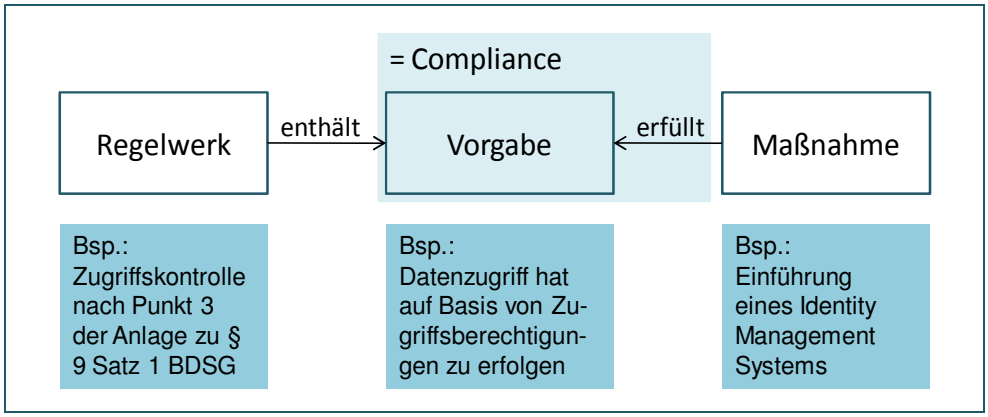

Abbildung 1
IT-Compliance als Erfüllung von Vorgaben

Die Erfüllung von Vorgaben bildet somit die Basis für den Begriff der IT-Compliance. Dieser lässt sich wie folgt fassen:

Definition IT-Compliance

> IT-Compliance bezeichnet einen Zustand, in dem alle, die IT des Unternehmens betreffenden und verbindlich vorgegebenen bzw. als verbindlich akzeptierten Vorgaben nachweislich eingehalten werden.

Hierbei ist es unerheblich, ob die IT-Leistungen ausschließlich unternehmensintern oder (teilweise) durch externe IT-Dienstleister (im Rahmen von Entwicklungs-, Hosting-, Outsourcing-Verträgen o. Ä.) erbracht werden.[3]

Sofern die Vorgaben aus Gesetzen stammen, bedeutet dies, dass sich Unternehmen an geltendes Recht zu halten haben – was eigentlich eine Selbstverständlichkeit sein sollte. Neben Gesetzen, oder besser Rechtsnormen, hat ein Unternehmen jedoch auch weitere Vorgaben aus unterschiedlichen internen und externen Regelwerken zu beachten.[4]

---

[3] Vgl. *Klotz 2009*, S. 6.

[4] Welche Regelwerke im Einzelnen zu behandeln sind, ist durchaus eine wichtige Frage, da hiervon der Umfang einer Compliance-Verantwortung abhängt. So begrenzt Hauschka Compliance auf gesetzliche Vorschriften (s. *Hauschka 2010*, Rn. 2), d. h. auf eine sog. „Legal Compliance". Dies ist für den Bereich der IT-Compliance als nicht ausreichend zu betrachten. Auch eine Bezugnahme auf „regulatorische Vorgaben und Anforderungen" (*Rath/Sponholz 2009*, S. 25) trägt hier kaum zur Klärung bei. Eine wichtige Orientierung gibt der DCGK (Deutsche Corporate Governance Kodex), der in Nr. 4.1.3 die Einhaltung von gesetzlichen Bestimmungen und unternehmensinternen Richtlinien als Compliance bezeichnet und als Aufgabe des Vorstands festschreibt. Am nächsten kommt dem hier vertretenen Begriffsumfang noch das IT-Governance-Referenzmodell „COBIT" (Control Objectives for Information and Related Technology), wo sich Compliance als Geschäftsanforderung auf Gesetze, Regulative und vertragliche Vereinbarungen in der Form externer Vorschriften und interner Richtlinien bezieht, vgl. *ITGI 2005*, S. 14.

1.2 Komplementäre Sichtweisen der IT-Compliance

In der Literatur und in Fachdiskussionen lassen sich häufig zwei Auffassungen von IT-Compliance ausmachen.

IT-Compliance als Hard- und Softwareeinsatz

- Die erste Sichtweise versteht IT-Compliance als Einsatz von Soft- und Hardwareprodukten, mit deren Hilfe die Einhaltung von Regelwerken – insbesondere der Corporate Governance – sichergestellt werden kann. In diesem Sinne handelt es sich um "IT-gestützte Corporate Compliance".5 Diese Interpretation wird vor allem von Herstellern vertreten, die Lösungen für Archivierung, Sicherheits- oder Content-Management, Datenverschlüsselung, Nutzer-, Zugangs- und Lizenzverwaltung u. a. m. anbieten. Aber auch auf Unternehmensseite wird dieser Sicht gerne gefolgt, belegt doch der Einsatz derartiger Systeme das Bemühen um Compliance. Dass diese Auffassung ihre Berechtigung hat, soll nicht im Geringsten bezweifelt werden. Im Gegenteil: Ohne die genannten Lösungen sind die zahlreichen Compliance-Anforderungen nicht in den Griff zu bekommen.

Compliance-Anforderungen an die IT-Funktion

- Die zweite Sichtweise fragt danach, welche Vorgaben aus Gesetzen, Normen, Standards, Verträgen und anderen Regelwerken die IT selbst als Unternehmensfunktion zu erfüllen hat. Hier richten sich Anforderungen direkt an die Planung, die Entwicklung und den Betrieb von Informationssystemen. Da diese Aufgaben ganz überwiegend im Verantwortungsbereich der IT-Abteilung eines Unternehmens liegen, steht hier somit die "Compliance der IT-Funktion" im Mittelpunkt der Betrachtung. Auch diese Sichtweise ist vollauf berechtigt, ist sie doch Teil der Führungsverantwortung der IT-Leitung.

In der Praxis sind beide Sichtweisen zusammenzubringen. Aus diesem Grunde ist es sinnvoll, sich die grundlegenden Unterschiede zwischen den beiden Interpretationsmöglichkeiten zu verdeutlichen, s. Abbildung 2.

Compliance der IT-Funktion

Die Sichtweise "Compliance der IT-Funktion" betrachtet die IT selbst als Träger von Compliance-Anforderungen. Hier stellen sich beispielsweise folgende Fragen:[6]

- Welche Rechtsnormen und ggf. sonstigen Regelwerke sind für die IT des Unternehmens relevant?

---

[5] Vgl. *Teubner/Feller 2008*, S. 401.
[6] Nach *Klotz/Dorn 2008, S. 9f.*

- Welche IT-gestützten Prozesse und Anwendungen sind betroffen und welche Anforderungen sind von ihnen zu erfüllen?
- Welche Risiken resultieren in welcher Höhe aus fehlender oder mangelhafter Compliance der IT?
- Welche Compliance-Anforderungen haben die einzelnen Bereiche der IT (Infrastruktur, Datenhaltung, Betrieb, Prozesse etc.) zu erfüllen?
- Welche technischen, organisatorischen und personellen Maßnahmen sind für die Gewährleistung von Compliance der IT zu ergreifen?

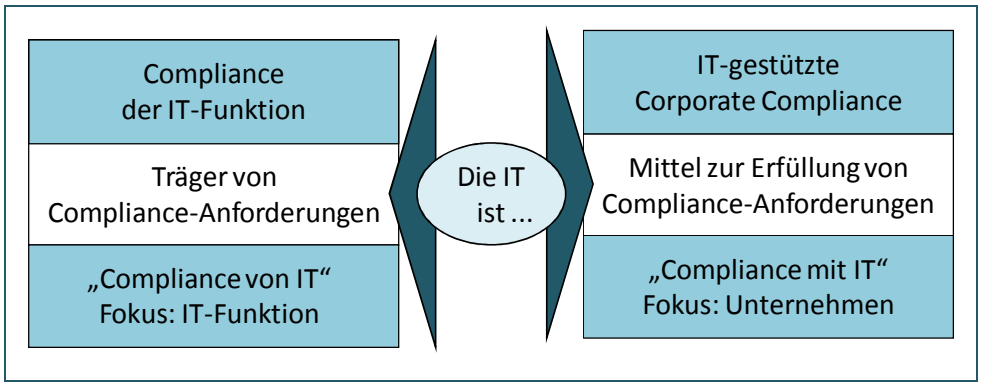

Abbildung 2
Compliance der IT-Funktion vs. IT-gestützte Corporate Compliance

IT-gestützte Corporate Compliance

IT-gestützte Corporate Compliance bedeutet, dass IT als Mittel zum Erreichen von Compliance in allen Unternehmensbereichen genutzt wird (vor allem im Rechnungs- und Finanzwesen, aber auch in der Beschaffung, im Personalwesen, im Vertrieb etc.). Bei dieser Sichtweise stellen sich beispielsweise folgende Fragen:

- Welche Compliance-Anforderungen haben die Geschäftsprozesse in den verschiedenen Geschäftsbereichen zu erfüllen?
- Welche Compliance-Anforderungen kann eine spezifische Hard- oder Software adressieren?
- Welche Hard- oder Softwarelösung ist für die Erfüllung der Compliance-Anforderungen am besten geeignet?
- Wie sind die verfügbaren Compliance-Mechanismen und -Tools aufeinander abzustimmen?

Es ist offensichtlich, dass beide Sichtweisen ineinandergreifen, da die Geschäftsprozesse überwiegend IT-gestützt erfolgen und schon hierdurch Fachfunktion und IT-Funktion gleichermaßen betroffen sind. Insofern sind beide Sichtweisen notwendig, um Compliance im Allgemeinen und Compli-

ance der IT im Speziellen zu erreichen. Aber auch für eine Klassifizierung der für IT-Compliance relevanten Regelwerke ist diese Unterscheidung hilfreich.

1.3 Klassifikation der Regelwerke

Grundgerüst

In Abhandlungen zu IT-Compliance werden relevante Regelwerke zumeist summarisch aufgelistet oder fachlich abgegrenzt. Im letzteren Fall wird entweder nur eine Perspektive eingenommen, wie z. B. für die Informationssicherheit im vom Branchenverband BITKOM und dem DIN herausgegebenen „Kompass der IT-Sicherheitsstandards“[7], oder es werden zahlreiche Anwendungsbereiche aufgeführt, z. B. Archivierung, Datenschutz, Internes Kontrollsystem, Transparenz, Risikomanagement, deren Abgrenzung untereinander wiederum nicht trennscharf ist, so dass die Regelwerke mehreren Bereichen zuzuordnen sind.

Klassifikation nach Herkunft

Für diese Arbeit orientiert sich die Klassifikation an der Herkunft der Regelwerke aus Unternehmenssicht. Es werden drei für IT-Compliance relevante Gruppen von Regelwerken unterschieden, die in ihrer Summe ein Grundgerüst für eine systematische Analyse von Compliance-Regelwerken und -Anforderungen darstellen. Diese drei Gruppen und ihre Regelwerke werden im Folgenden in ein so genanntes „House of IT-Compliance“ eingeordnet, s. Abbildung 3.

Rechtliche Regelwerke

Die erste Gruppe bilden die rechtlichen Regelwerke. Im Zentrum stehen hier Rechtsnormen, also vom Gesetzgeber erlassene Gesetze und Rechtsverordnungen. Offensichtlich relevant für IT-Compliance sind Gesetze, die sich schon vom Namen her auf die IT beziehen, wie beispielsweise das Bundesdatenschutzgesetz, das Signaturgesetz oder das Telemediengesetz.[8] Zudem beziehen sich zahlreiche weitere Gesetze auf den IT-Einsatz im Unternehmen, z. B. das Betriebsverfassungsgesetz oder hinsichtlich der Buchführungs- und steuerlichen Pflichten das Handelsgesetzbuch und die Abgabenordnung. In beiden Teilgruppen finden sich prinzipiell auch Gesetze anderer Staaten (z. B. der Sarbanes-Oylex Act, SOX) sowie Rechtsentwicklungen, die sich auf EU-Ebene vollziehen (z. B. die Richtlinie 95/46/EG des Euro-

[7] Siehe *BITKOM/DIN 2009*, wo für die IT-Sicherheit relevante ISO/IEC-Normen, DIN-Normen, Best-Practice-Frameworks, Branchenstandards, Verwaltungsanweisungen sowie nationale und ausländische Gesetze aufgeführt werden.

[8] Diese IT-spezifischen Gesetze werden mitunter unter dem Oberbegriff „IT-Recht“ oder „Informationstechnologierecht“ zusammengefasst.

päischen Parlaments und des Rates vom 24. Oktober 1995 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr[9]).

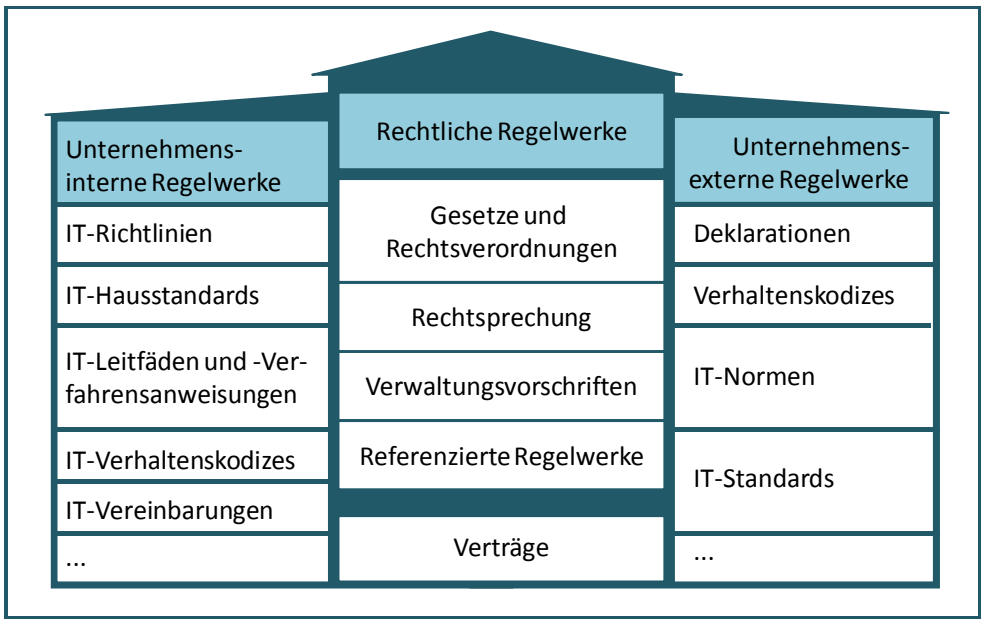

Abbildung 3
Das "House of IT-Compliance"

Rechtsprechung

Für die Auslegung von Gesetzen sind Gerichtsurteile von hoher praktischer Bedeutung. Insofern wird auch die Rechtsprechung als rechtliches Regelwerk in das „House of IT-Compliance" eingeordnet. Gleichwohl ist dies ein Bereich der IT-Compliance, in dem ein einigermaßen vollständiger und aktueller Überblick ohne den Einsatz spezialisierter juristischer Ressourcen fast unmöglich sein dürfte.

Verwaltungsvorschriften

Weitere für die IT relevante rechtliche Regelwerke stellen Verwaltungsvorschriften dar. Diese werden beispielsweise von Ministerien (z. B. dem Bundesfinanzministerium) oder Aufsichtsorganisationen (z. B. der Bundesanstalt für Finanzdienstleistungsaufsicht) zur Interpretation und Ausführung der Rechtsnormen aufgestellt.

[9] Diese Richtlinie wurde in Deutschland durch das „Gesetz zur Änderung des Bundesdatenschutzgesetzes und anderer Gesetze" vom 18. Mai 2001 verspätet umgesetzt. Im Juli 2005 rügte die EU-Kommission, dass den Stellen, die mit der Datenschutzaufsicht der Länder betraut sind, die erforderliche Unabhängigkeit von staatlicher Einflussnahme fehle. Nach einem Vertragsverletzungsverfahren urteilte der Europäische Gerichtshof (EuGH) am 09.03.2010, dass die EU-Vorgabe in Deutschland falsch umgesetzt sei. Am 06.04.2011 hat die Europäische Kommission Deutschland nunmehr aufgefordert, dem Urteil des EuGH nachzukommen und die EU-Richtlinie umzusetzen.

Referenzierte Regelwerke

Als „referenzierte Regelwerke“ sollen hier solche Regelwerke bezeichnet werden, auf die in Gesetzen, Rechtsverordnungen und Verwaltungsvorschriften verwiesen wird oder die von der Rechtsprechung zur Auslegung herangezogen werden. In anderen Wirtschaftsbereichen wird hiervon regelmäßig Gebrauch gemacht, beispielsweise im Bauwesen, wo in Urteilen DIN-Normen umfangreich zur Begründung herangezogen werden. In der IT-Branche sind derartige Verweise bisher jedoch noch kaum zu finden. Insbesondere haben Gerichte bisher (noch) nicht in ihren Urteilen auf die gängigen IT-Normen und -Standards zurückgegriffen.

Verträge

Verträge, die ein Unternehmen mit Kunden, Hard- und Software-Lieferanten und sonstigen Marktpartnern (z. B. Versicherungen) abschließt und die IT-relevante Vereinbarungen enthalten, ergänzen die Gruppe der rechtlichen Regelwerke. Im Gegensatz zu den bisher genannten Regelwerken besitzen Verträge jedoch keine allgemeine Verbindlichkeit, sondern verpflichten lediglich die jeweiligen Vertragspartner. Im Mittelpunkt stehen hier die zahlreichen Möglichkeiten, des IT-Outsourcings, z. B. durch Vergabe von Entwicklungs- und Wartungsaufträgen an spezialisierte IT-Dienstleistungsunternehmen.

Unternehmensexterne Regelwerke

Die zweite Gruppe bilden unternehmensexterne Regelwerke[10], die sich auf die Art und Weise der IT-Nutzung beziehen. Sie reichen von Deklarationen, die im Rahmen internationaler Veranstaltungen verabschiedet wurden, über Richtlinien intergouvernementaler Organisationen (wie der OECD) und Verhaltenskodizes von Berufsorganisationen bis hin zu IT-Normen oder -Standards vielfältiger Institutionen, die die Ausgestaltung oder Nutzung der IT durch Best-Practice-Modelle unterstützen oder hierfür mehr oder weniger verbindliche Vorgaben machen.

Unternehmensinterne Regelwerke

Die dritte Gruppe der unternehmensinternen Regelwerke ist notwendig, da die verschiedenen Regelwerke der anderen beiden Gruppen in aller Regel auf die Unternehmensspezifika angepasst werden müssen. Deshalb nutzen Unternehmen verschiedene interne Regelwerke, die Vorgaben für die unternehmensinterne IT enthalten. Dies können eher strategische Richtlinien für die IT sein oder operative IT-Leitfäden und -Verfahrensanweisungen. Hausstandards und interne Kodizes entstehen durch Adaption externer IT-Standards und -Verhaltenskodizes. Auch interne IT-Vereinbarungen, vor allem

[10] Im Grunde müsste es „der *sonstigen* unternehmensexternen Regelwerke heißen“, da natürlich auch die rechtlichen Regelwerke unternehmensexterne Regelwerke darstellen.

Service Level Agreements (SLAs), zählen zu dieser Gruppe.

Für die Gruppe der rechtlichen Regelwerke werden im Folgenden die wichtigsten in der Praxis verwendeten und in der Literatur diskutierten Gesetze, Verordnungen, Verwaltungsvorschriften etc. aufgelistet, in der Summe 74 Regelwerke, s. Tabelle 1.

Tabelle 1 Verteilung der rechtlichen Regelwerke

Gruppe			**Anzahl Regelwerke**
Gesetze	IT-spezifische	5	20
	Nicht IT-spezifische	15	
Rechtsverordnungen	IT-spezifische	5	6
	Nicht IT-spezifische	1	
Verwaltungsvorschriften			5
Referenzierte Regelwerke			6
Rechtsprechung			13
Verträge	IT-Verträge	21	24
	Allgemeine Verträge	3	
Insgesamt			74

Abgrenzung der Betrachtung

Eine Auflistung von Regelwerken, die der Forderung nach Systematik zumindest näherungsweise erfüllen will, erfordert eine Abgrenzung.

Nur aktuelle Regelwerke

- Es werden im Folgenden nur aktuelle Regelwerke aufgeführt. Damit entfallen solche Gesetze, deren Regelungen mittlerweile in andere Gesetze Eingang gefunden haben, wie z. B. das Teledienstegesetz (TDG) und das Teledienstedatenschutzgesetz (TDDSG), die beide 2007 durch das Telemediengesetz (TMG) abgelöst wurden. Ebenso werden Artikelgesetze, die Änderungen in mehreren anderen Gesetzen herbeiführen, nicht berücksichtigt. Ein Beispiel hierfür ist das Informations- und Kommunikationsdienste-Gesetz (IuKDG) von 1997, das sowohl neue Gesetze enthielt (z. B. das Signaturgesetz) als auch Änderungen bestehender Gesetze (z. B. des Strafgesetzbuches oder des Urheberrechtsgesetzes) herbeiführte.

Keine Entwürfe

- Auf der anderen Seite werden aber auch keine Regelwerke aufgeführt, die lediglich als Entwurf vorliegen und noch nicht als Gesetz verabschiedet sind. Ein Beispiel hierfür ist der Gesetzentwurf zur Regelung des Beschäftigtendatenschutzes, der am 25.02.2011 im Bundestag in

erster Lesung erörtert wurde.[11] Ein anderes Beispiel sind die „Grundsätze ordnungsmäßiger Buchführung beim IT-Einsatz (GoBIT)“, die derzeit als Weiterentwicklung der GoBS (Grundsätze ordnungsgemäßer DV-gestützter Buchführungssysteme[12]) von der Arbeitsgemeinschaft für wirtschaftliche Verwaltung e.V. (AWV) in Zusammenarbeit mit den Finanzbehörden erarbeitet werden.[13]

Nur bundesdeutsche Regelwerke

- Weiterhin wird eine Einschränkung auf bundesdeutsche Regelwerke vorgenommen. Eine Berücksichtigung ausländischer, internationaler und supranationaler Regelwerke würde schnell ausufern und wäre letztlich willkürlich. Das Ausblenden supranationaler Regelwerke führt dazu, dass die Rechtsentwicklungen auf der EU-Ebene keinen Eingang in die Darstellung finden. Dies muss jedoch aus nationalstaatlicher Perspektive kein Mangel sein, da die entsprechenden Vorgaben ohnehin auf der nationalen Ebene umzusetzen sind. So sieht beispielsweise die Richtlinie 2010/45/EU vom 13.07.2010[14] Vereinfachungen der elektronischen Rechnungsstellung vor. Die Umsetzung in nationales Recht hat bis zum 01.01.2013 erfolgen.

SOX

Gleichwohl werden durch diese Einschränkung Regelwerke ausgeblendet, die in der Fachdiskussion eine wesentliche Rolle spielen, allen voran der Sarbanes-Oxley Act (SOX), der regelmäßig in Compliance-Abhandlungen erörtert wird.[15] Dieser soll deshalb auch an dieser Stelle zumindest kurz Erwähnung finden. Der Sarbanes-Oxley Act ist ein 2002 erlassenes US-Bundesgesetz[16], das in Folge von Bilanzfälschungen[17] Regelungen für die Corporate Governance von Unternehmen traf. Er ist für diejenigen deutschen Unternehmen relevant, deren Wertpapiere in den USA gehandelt oder angeboten werden (bzw. für Tochtergesellschaften von Unternehmen, die

---

11 Vgl. *Deutscher Bundestag o.J.*

12 Siehe unten Kap. 4.

13 Der in dem AWV-Arbeitskreis „erarbeitete Entwurf soll neuen Entwicklungen, Begrifflichkeiten, Schwerpunktverschiebungen und auch neu hinzutretenden Risiken bei der IT-gestützten Buchführung Rechnung tragen“ (*AWV o.J.)*

14 Siehe http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2010:189:0001:0008:DE:PDF .

15 Vgl. z. B. *Rath 2008*, S. 123f., *Grummer/Seeburg 2010*.

16 Siehe http://thomas.loc.gov/cgi-bin/query/z?c107:H.R.3763.ENR:.

17 In den USA waren dies vor allem die Betrugsfälle und Bilanzmanipulationen bei den Firmen Worldcom und Enron.

SOX unterliegen[18]). Section 404 des SOX schreibt die Implementierung und Bewertung eines Internen Kontrollsystems (IKS) für die Rechnungslegung vor. Da dieses gewöhnlich nicht ohne IT-Kontrollen auskommt, ergeben sich aus SOX indirekt Anforderungen an die IT eines Unternehmens, d. h. an das Konzipieren, Entwickeln, Testen und Überwachen rechnungslegungsrelevanter IT-Kontrollen.

Struktur der folgenden Darstellung

Es erfolgen jeweils die Nennung des Regelwerks, ggf. mit Abkürzung, sowie eine kurze Inhaltsangabe (die die Bedeutung des aufgeführten Regelwerks für IT-Compliance jedoch nicht erschöpfend darstellen kann). Als Status wird die aktuelle Fassung oder Version angegeben. Ein Link zum Text des Regelwerks vereinfacht die eigene Recherche.

2. Gesetze

Im Folgenden werden IT-spezifische Gesetze und allgemeine, nicht IT-spezifische Gesetze, die aber ebenso Anforderungen an die IT richten, aufgeführt.

2.1 IT-spezifische Gesetze

IT-spezifische Gesetze

Die IT-spezifischen Gesetze zeichnen sich dadurch aus, dass sie sich von ihrem Namen her bereits auf IT beziehen (z. B. Daten, Informationstechnik, Medien). Entsprechend enthält ein Großteil des jeweiligen Gesetzestextes Compliance-Anforderungen, die sich auf die Verwendung von Daten und Dokumenten oder die Durchführung spezifischer Verfahren (z. B. der Information oder Beteiligung von Betroffenen) beziehen.

Name	**BDSG – Bundesdatenschutzgesetz**
Inhalt	Das BDSG regelt die Erhebung, Verarbeitung und Nutzung personenbezogener Daten durch öffentliche und nicht-öffentliche Stellen (Unternehmen). Beim Umgang mit personenbezogenen Daten ist jeweils eine genaue Prüfung für jede Nutzung – z. B. für die interne Auswertung von Kundendaten in Data-Warehouse- bzw. CRM-Lösungen – vorzunehmen, ob diese Nutzung (weitere Speicherung, Übermittlung an andere Stellen, Auswertung) von den konkreten Vertragszwecken und

[18] Wie dies z. B. für die AXA Konzern AG zutrifft, deren französische Muttergesellschaft an der New Yorker Börse NYSE notiert ist, s. *Michels/Krzeminska 2006*, S, 141.

	damit von den Ermächtigungsvorschriften der §§ 27 ff. BDSG gedeckt ist.[19] Vor allem die Anlage zu § 9 gibt verschiedene technische und organisatorische Kontrollmaßnahmen vor, die einen Missbrauch personenbezogener Daten verhindern sollen. Hierin kann auch ein Ansatzpunkt für eine Verpflichtung des Unternehmens zu (deckungsgleichen) Maßnahmen der IT-Sicherheit gesehen werden.[20]
Status	Fassung vom 14. Januar 2003 (BGBl. I S. 66); zuletzt geändert durch Artikel 1 des Gesetzes vom 14. August 2009 (BGBl. I S. 2814)
Link	zum Text: http://www.gesetze-im-internet.de/bdsg_1990/BJNR029550990.html

Name	**BSIG – Gesetz über das Bundesamt für Sicherheit in der Informationstechnik (BSI-Gesetz)**
Inhalt	Das BSIG richtet sich zwar nur an das BSI. In § 2 Abs. 2 BSIG findet sich jedoch eine Legaldefinition für Sicherheit in der Informationstechnik: „Sicherheit in der Informationstechnik im Sinne dieses Gesetzes bedeutet die Einhaltung bestimmter Sicherheitsstandards, die die Verfügbarkeit, Unversehrtheit oder Vertraulichkeit von Informationen betreffen, durch Sicherheitsvorkehrungen 1. in informationstechnischen Systemen, Komponenten oder Prozessen oder 2. bei der Anwendung von informationstechnischen Systemen, Komponenten oder Prozessen.“
Status	Fassung vom 14. August 2009 (BGBl. I S. 2821)
Link	zum Text: http://www.gesetze-im-internet.de/bsig_2009/BJNR282110009.html

Name	**SigG – Gesetz über Rahmenbedingungen für elektronische Signaturen (Signaturgesetz)**
Inhalt	Das SigG regelt die Nutzung elektronischer Signaturen im Geschäftsverkehr, d. h. für E-Commerce und E-Government. Hinsichtlich der elektronischen Signatur definiert das SigG a) eine einfache elektronischen Signatur, b) eine fortgeschrittene elektronische Signatur und c) eine fortgeschrittene qualifizierte (d. h. auf einem Zertifikat basierende) elektronische Signatur.
Status	Fassung vom 16. Mai 2001 (BGBl. I S. 876); zuletzt geändert durch Artikel 4 des Gesetzes vom 17. Juli 2009 (BGBl. I S. 2091)

[19] Beschreibung der Gesetzesinhalte hier und im Folgenden nach *Klotz/Dorn 2009*.
[20] So bspw. *Schmidl 2009*, Rn 13ff.

Link	zum Text: http://bundesrecht.juris.de/sigg_2001/index.html

Name	**TKG – Telekommunikationsgesetz**
Inhalt	Das TKG dient der Regulierung des Wettbewerbs im Bereich der Telekommunikation. Für Unternehmen wird das TKG dann relevant, wenn die Einräumung der privaten Nutzung von Internet und E-Mail als Anbieten von Übertragungswegen an Dritte i. S. d. TKG angesehen wird und ein Unternehmen dadurch Telekommunikationsdienste i. S. d. TKG erbringt. Nach § 109 TKG hat jeder Diensteanbieter angemessene technische Maßnahmen zum Schutze des Fernmeldegeheimnisses und personenbezogener Daten sowie der Telekommunikations- und Datenverarbeitungssysteme zu ergreifen. Hierzu sind u. a. ein IT-Sicherheitskonzept zu erstellen und ein IT-Sicherheitsbeauftragter zu ernennen.
Status	Fassung vom 22. Juni 2004 (BGBl. I S. 1190), zuletzt geändert durch Artikel 3 des Gesetzes vom 24. März 2011 (BGBl. I S. 506)
Link	zum Text: http://bundesrecht.juris.de/tkg_2004/BJNR119000004.html

Name	**TMG – Telemediengesetz**
Inhalt	Das TMG regelt die elektronischen Informations- und Kommunikationsdienste und bildet damit eine wichtige Grundlage für Internet-Dienste. Den Anbieter entsprechender Dienste treffen nach den §§ 5, 6 TMG umfangreiche Informationspflichten (z. B. Angaben zum Unternehmen, Erreichbarkeit, zu eventuellen Aufsichtsbehörden sowie zur Erkennbarkeit einer kommerziellen Kommunikation). Wichtig für die Frage der Haftung des Diensteanbieters für fremde Inhalte sind die §§ 7 ff. TMG. Hierin ist ein Haftungsausschluss geregelt, der jedoch nach § 10 TMG nur dann gilt, wenn die fremden Inhalte dem Unternehmen nicht bekannt gewesen oder die beanstandeten Daten unverzüglich nach Kenntnis entfernt oder gesperrt worden sind. Auch datenschutzrechtliche Anforderungen finden sich im TMG. So richtet sich die Bearbeitung personenbezogener Daten nach den §§ 14, 15 TMG.
Status	Fassung vom 26. Februar 2007 (BGBl. I S. 179), zuletzt geändert durch Artikel 1 des Gesetzes vom 31. Mai 2010 (BGBl. I S. 692)
Link	zum Text: http://www.gesetze-im-internet.de/tmg/BJNR017910007.html

2.2 Nicht IT-spezifische Gesetze

Nicht IT-spezifische Gesetze

Die allgemeinen, nicht IT-spezifischen Gesetze adressieren teilweise direkt die Art und Weise des IT-Einsatzes (dann zumeist nur in wenigen Paragraphen), teilweise beziehen sie sich nicht direkt auf die IT, wobei die IT in diesen Fällen aber das Mittel darstellt, um Vorgaben (vor allem hinsichtlich Dokumentation und Archivierung) zu erfüllen.

Name	**AktG – Aktiengesetz**
Inhalt	Mit der Neufassung des AktG von 2009 können nach § 118 für die Durchführung der Hauptversammlung elektronische Kommunikationsmittel genutzt werden. Zudem sind nach § 121 Abs. 3 i. V. m. § 124a Informationen zur Hauptversammlung auf der Internetseite des Unternehmens zu veröffentlichen. Mitunter wird das AktG angeführt, um Compliance-Anforderungen an das IT-Sicherheits- oder das IT-Risikomanagement zu begründen. Hierfür bietet das AktG jedoch keine unmittelbaren Ansatzpunkte. Natürlich hat sich das nach § 91 Abs. 2 (der 1998 durch das KontraG eingeführt wurde) einzurichtende Überwachungssystem auch auf die IT zu erstrecken, wenn mit ihr bestandsgefährdende Risiken verbunden sind. Ebenso ergibt sich lediglich mittelbar über die in § 93 festgeschriebenen Sorgfaltspflichten[21] eine Verankerung für eine Verantwortung des Vorstands für IT-Compliance, IT-Risiko- und IT-Sicherheitsmanagement.[22]
Status	Fassung vom 6. September 1965 (BGBl. I S. 1089), zuletzt geändert durch Artikel 6 des Gesetzes vom 9. Dezember 2010 (BGBl. I S. 1900)
Link	zum Text: http://bundesrecht.juris.de/aktg/BJNR010890965.html

Name	**AO – Abgabenordnung**
Inhalt	Die AO ist der Kern des deutschen Steuerrechts. Für IT-Compliance sind die §§ 145 ff. relevant, die die Aufzeichnungs- und Aufbewahrungspflichten sowie den Datenzugriff durch die Finanzbehörden regeln. Von zentraler Bedeutung ist die Regelung des § 147 Abs. 2 AO, wonach eine Aufbewahrung von Unterlagen auf Bildträgern oder anderen Datenträgern erlaubt ist, wenn die Daten „während der Dauer der Aufbewahrungsfrist jederzeit verfügbar sind, unverzüglich lesbar gemacht und maschinell ausgewertet werden können“. Um den Finanzbehörden die Prüfung elektronisch gespeicherter Unter-

[21] Für die GmbH findet sich die entsprechende Regelung in § 43 GmbhG.
[22] Vgl. *Rath/Sponholz 2009*, S. 68f.

	lagen und Daten zu ermöglichen, hat ein Unternehmen nach § 147 Abs. 5 AO Hilfsmittel zur Verfügung zu stellen, um die Unterlagen lesbar zu machen. Noch weitergehend muss ein Unternehmen nach § 147 Abs. 6 AO bei einer Erstellung der Aufzeichnungen mit Hilfe eines IT-Systems nicht nur die „Einsicht" in diese Daten ermöglichen, sondern nach Vorgabe der Betriebsprüfung die Daten selbst auswerten oder den Finanzbehörden auf einem verwertbaren lesbaren Datenträger zur Verfügung stellen.
Status	Fassung vom 1. Oktober 2002 (BGBl. I S. 3866; 2003 I S. 61), zuletzt geändert durch Artikel 4 des Gesetzes vom 12. April 2011 (BGBl. I S. 615)
Link	zum Text: http://www.gesetze-im-internet.de/ao_1977/index.html

Name	**BetrVG – Betriebsverfassungsgesetz**
Inhalt	Das BetrVG regelt in Bezug auf den IT-Einsatz die Beteiligung des Betriebsrates, z. B. durch Mitwirkungsrechte in der Planungsphase oder ggf. Mitbestimmungsrechte in der Einführungsphase. So ist der Betriebsrat nach §§ 80 Abs. 2, 90 BetrVG über die geplante Einführung von IT-Systemen, die Erweiterung ihres Einsatzes und die Einführung neuer Programme unverzüglich zu unterrichten. Dem Betriebsrat steht darüber hinaus ein Mitbestimmungsrecht (und die Maßnahme bedarf somit seiner Zustimmung in Form einer Betriebsvereinbarung), wenn es sich beim betreffenden IT-System gemäß § 87 Abs. 1 Nr. 6 BetrVG um eine Einrichtung handelt, die dazu bestimmt ist, die Leistung oder das Verhalten von Arbeitnehmern zu überwachen.
Status	Fassung vom 25. September 2001 (BGBl. I S. 2518), zuletzt geändert durch Artikel 9 des Gesetzes vom 29. Juli 2009 (BGBl. I S. 2424)
Link	zum Text: http://www.gesetze.juris.de/betrvg/BJNR000130972.html

Name	**BGB – Bürgerliches Gesetzbuch**
Inhalt	Die Bezüge des BGB zur IT sind mittlerweile vielfältig. So trifft das BGB für Fernabsatzverträge in den §§ 312e, 312 c BGB Regelungen zur Nutzung von IT (E-Mails, Tele- und Mediendienste) und legt Pflichten im elektronischen Geschäftsverkehr fest. So muss z. B. nach § 312e Abs. 1 BGB eine Möglichkeit zur Korrektur von Eingabefehlern bestehen, der Vertrag muss durch das Unternehmen unverzüglich elektronisch bestätigt werden und der Inhalt und die Bedingungen des zu Stande gekommenen Vertrages müssen gespeichert werden und für den Kunden abrufbar sein. Außerdem gilt das Kauf- und Gewährleistungsrecht des BGB auch für

	Softwareerstellung und -kauf. So stellt das Gewährleistungsrecht des BGB sowohl im Kauf- als auch im Werkvertragsrecht in erster Linie auf die vereinbarte Sollbeschaffenheit ab (§§ 437 Abs.1, 633 Abs. 2 BGB), was in Verträgen eine möglichst genaue, ggf. funktionale Leistungsbeschreibung erfordert, deren Einhaltung durch Abgleich mit der tatsächlichen Beschaffenheit der jeweiligen Hard- oder Software zu überprüfen ist. In den §§ 126, Abs. 3, 126a BGB wird zudem die Verwendung von elektronischen Signaturen grundlegend geregelt. Diese ist hierdurch der Schriftform gleichgestellt, es sei denn, dass dies durch gesetzliche Regelung ausgeschlossen wird (wie z. B. in den §§ 623, 766, 780).
Status	Fassung der Bekanntmachung vom 2. Januar 2002 (BGBl. I S. 42, 2909; 2003 I S. 738), zuletzt geändert durch Artikel 1 des Gesetzes vom 17. Januar 2011 (BGBl. I S. 34)
Link	zum Text: http://www.gesetze-im-internet.de/bgb/BJNR001950896.html

Name	**EBGB – Einführungsgesetz zum Bürgerlichen Gesetzbuche**
Inhalt	Das EBGB enthält in den Artikeln 240 und 246 Regelungen zu den Informationspflichten bei Fernabsatzverträgen, also bei elektronischem Geschäftsverkehr. Diese Pflichten umfassen neben zahlreichen Angaben zum Unternehmen und zu den Produkten und Leistungen auch Vertragsbedingungen inkl. AGB sowie nach § 3 Nr. 5 Verhaltenskodizes, denen sich das Unternehmen unterwirft.
Status	Fassung der Bekanntmachung vom 21. September 1994 (BGBl. I S. 2494; 1997 I S. 1061), zuletzt geändert durch Artikel 2 des Gesetzes vom 12. April 2011 (BGBl. I S. 615)
Link	zum Text: http://bundesrecht.juris.de/bgbeg/BJNR006049896.html#BJNR006049896BJNG053200140

Name	**ElektroG – Gesetz über das Inverkehrbringen, die Rücknahme und die umweltverträgliche Entsorgung von Elektro- und Elektronikgeräten (Elektro- und Elektronikgerätegesetz)**
Inhalt	Nicht mehr benötigte Hardware (z. B. infolge einer Ersatzbeschaffung) muss entsorgt werden. Hierbei ist die Pflicht gemäß § 9 Abs. 1 ElektroG zu berücksichtigen, Altgeräte einer getrennten Versorgung zuzuführen.
Status	Fassung vom 16. März 2005 (BGBl. I S. 762), zuletzt geändert durch Artikel 5 des Gesetzes vom 11. August 2010 (BGBl. I S. 1163)
Link	zum Text:

	http://www.gesetze-im-internet.de/elektrog/BJNR076200005.html

Name	**HGB – Handelsgesetzbuch**
Inhalt	Das HGB stellt verschiedene Anforderungen an die elektronische Geschäftskommunikation sowie an die Verwendung von Bild- und Datenträgern im Rahmen der Buchführung. So ist bei der Gestaltung der Geschäftskorrespondenz zu beachten, dass gemäß § 37 a HGB auf allen Geschäftsbriefen, zu denen auch E-Mails gehören, Angaben zur Firmierung, Vertretung und Handelsregistereintragung enthalten sein müssen. Die Aufbewahrung von Handelsbriefen kann zwar nach den §§ 238 Abs. 2, 257 HGB auch auf Datenträgern erfolgen. Diese müssen jedoch während der Dauer der Aufbewahrungsfrist verfügbar und jederzeit lesbar sein.
Status	Bundesgesetzblatt Teil III, Gliederungsnummer 4100-1, veröffentlichte Fassung, zuletzt geändert durch Artikel 8 des Gesetzes vom 1. März 2011 (BGBl. I S. 288)
Link	zum Text: http://www.gesetze-im-internet.de/hgb/BJNR002190897.html

Name	**KWG – Gesetz über das Kreditwesen (Kreditwesengesetz)**
Inhalt	Als Teil einer ordnungsgemäßen Geschäftsorganisation haben Kredit- und Finanzdienstleistungsinstitute nach § 25 a Abs. 1 KWG ein Risikomanagement einzurichten, das ein Notfallkonzept insbesondere für IT-Systeme zu beinhalten hat. Der Paragraph enthält weitere Pflichten, die auf die IT anzuwenden sind, vor allem bei Auslagerung der IT.
Status	Fassung der Bekanntmachung vom 9. September 1998 (BGBl. I S. 2776), zuletzt geändert durch Artikel 2 des Gesetzes vom 1. März 2011 (BGBl. I S. 288)
Link	zum Text: http://www.gesetze.juris.de/kredwg/BJNR008810961.html

Name	**OWiG – Gesetz über Ordnungswidrigkeiten**
Inhalt	Im OWiG finden sich im Zweiten Abschnitt, § 116ff, Regelungen, nach denen Verstöße gegen die öffentliche Ordnung auch durch Verbreitung von Ton- oder Bildträgern sowie Datenspeichern begangen werden können.
Status	Fassung der Bekanntmachung vom 19. Februar 1987 (BGBl. I S. 602), zuletzt geändert durch Artikel 2 des Gesetzes vom 29. Juli 2009 (BGBl. I S. 2353)

Link	zum Text: http://www.gesetze-im-internet.de/owig_1968/BJNR004810968.html

Name	**StGB – Strafgesetzbuch**
Inhalt	Das StGB ist bereits ggf. bei Verstoß gegen die anderen hier genannten Gesetze relevant. Es enthält außerdem IT-spezifische Tatbestände, die Daten und IT-Systeme schützen sollen.[23] Dies sind die §§ 202a (Ausspähen von Daten), 202b (Abfangen von Daten), 202c (Vorbereiten des Ausspähens und Abfangens von Daten), 269 (Fälschung beweiserheblicher Daten), 274 (Unterdrücken beweiserheblicher Daten) und 303a (Datenveränderung).
Status	Fassung der Bekanntmachung vom 13. November 1998 (BGBl. I S. 3322), zuletzt geändert durch Artikel 1 des Gesetzes vom 28. April 2011 (BGBl. I S. 676)
Link	zum Text: http://www.gesetze-im-internet.de/stgb/BJNR001270871.html

Name	**UrhG – Gesetz gegen den unlauteren Wettbewerb**
Inhalt	Das UrhG regelt in § 4 UrhG das Datenbankurheberrecht. Dies ist vor allem deswegen für die IT-Compliance relevant, da auch Websites häufig als Datenbankwerke im Sinne des § 4 Abs. 2 UrhG geschützt sind. Jede Publikation von Inhalten auf einer Website erfordert entsprechende Nutzungs- und Verwertungsrechte, um nicht gegen Urheberrechte zu verstoßen. Soweit Texte, Bilder oder andere schutzfähige Werke für die Website erstellt werden, ist darauf zu achten, dass eine für diese Nutzungsart ausreichende Übertragung der Nutzungsrechte (§§ 31 ff. UrhG) erfolgt.
Status	Fassung vom 9. September 1965 (BGBl. I S. 1273), zuletzt geändert durch Artikel 83 des Gesetzes vom 17. Dezember 2008 (BGBl. I S. 2586)
Link	zum Text: http://www.gesetze-im-internet.de/urhg/BJNR012730965.html

Name	**UStG – Umsatzsteuergesetz**
Inhalt	Die relevanten Regelungen des UStG beziehen sich auf elektronische Rechnungen, deren Verwendung nach § 14 Abs. 1 der Zustimmung des Empfängers bedarf. Nach § 14 Abs. 3 UStG müssen bei einer auf elektronischem Wege übermittelte Rechnung Echtheit und Unver-

[23] Nach Schmidl 2010, Rn. 132.

	sehrtheit gewährleistet sein entweder a) durch eine qualifizierte elektronische Signatur nach dem Signaturgesetz oder b) durch elektronischen Datenaustausch (EDI) nach Artikel 2 der Empfehlung 94/820/EG der EU-Kommission. Die Aufbewahrung elektronischer Rechnungen ist in § 14b geregelt.
Status	Fassung der Bekanntmachung vom 21. Februar 2005 (BGBl. I S. 386), zuletzt geändert durch Artikel 2 des Gesetzes vom 5. April 2011 (BGBl. I S. 554)
Link	zum Text: http://www.gesetze-im-internet.de/ustg_1980/BJNR119530979.html

Name	**UWG – Gesetz gegen den unlauteren Wettbewerb**
Inhalt	Bei der Gestaltung einer Website sind die einzelnen in den §§ 4 bis 7 UWG aufgeführten Tatbestände unlauteren Wettbewerbs zu berücksichtigen. Zudem enthält § 7 UWG Vorgaben für die Nutzung werblicher E-Mails, die verhindern sollen, dass diese den Adressaten in unzumutbarer Weise belästigen.
Status	Fassung vom 3. März 2010 (BGBl. I S. 254)
Link	zum Text: http://www.gesetze.juris.de/uwg_2004/BJNR141400004.html

Name	**WphG – Gesetz über den Wertpapierhandel (Wertpapierhandelsgesetz)**
Inhalt	Nach § 33 Abs. 1 WphG haben Wertpapierdienstleistungsunternehmen die organisatorischen Pflichten nach § 25a Abs. 1 und 4 KWG (s. o.) einhalten, also vor allem ein IT-Notfallkonzept zu erstellen.
Status	Fassung der Bekanntmachung vom 9. September 1998 (BGBl. I S. 2708), zuletzt geändert durch Artikel 1 des Gesetzes vom 5. April 2011 (BGBl. I S. 538)
Link	zum Text: http://www.gesetze-im-internet.de/wphg/BJNR174910994.html

Name	**ZPO – Zivilprozessordnung**
Inhalt	Nach § 425 ZPO kann einem Unternehmen vom Gericht aufgegeben werden, in seinem Besitz befindliche Unterlagen vorzulegen. Dies stellt entsprechende Anforderungen an Dokumentation und Archivierung. Gemäß § 427 ZPO kann die Nichtvorlage dazu führen, dass der Beweis durch den Gegner als geführt gilt, insbesondere wenn, z. B. auf Grund der handelsrechtlichen Regelungen, eine Pflicht zur Aufbewahrung besteht.

Status	Fassung vom 5. Dezember 2005 (BGBl. I S. 3202; 2006 I S. 431; 2007 I S. 1781), zuletzt geändert durch Artikel 3 des Gesetzes vom 12. April 2011 (BGBl. I S. 615)
Link	zum Text: http://www.gesetze-im-internet.de/zpo/BJNR005330950.html

3. Rechtsverordnungen

Rechtsverordnungen

Rechtsverordnungen unterliegen keinem förmlichen Gesetzgebungsverfahren, sondern werden durch die Bundes- oder eine Landesregierung oder ein Ministerium aufgrund einer in einem Bundes- oder Landesgesetz geregelten Ermächtigung erlassen. Ein Beispiel hierfür ist die Bildschirmarbeitsverordnung (s. u.), die nach den im § 18 ArbSchG geregelten Verordnungsermächtigungen des Arbeitsschutzgesetzes von der Bundesregierung mit Zustimmung des Bundesrates erlassen wurde.

Abgrenzung

Rechtsverordnungen sind Gesetze im materiellen Sinn, d. h. der Sache nach, und stellen (untergesetzliche) Rechtsnormen dar. Die im Folgenden aufgeführten Verordnungen sind ausschließlich Bundesrechtsverordnungen; durch Landesregierungen erlassene Verordnungen bleiben außer Betracht. Analog zu den IT-Gesetzen wird auch für die Darstellung der Rechtsverordnungen wieder zwischen IT-spezifischen und nicht IT-spezifischen Regelwerken unterschieden.

3.1 IT-spezifische Rechtsverordnungen

IT-spezifische Rechtsverordnungen

Die IT-spezifischen Rechtsverordnungen beziehen sich vom Namen her wieder direkt auf die IT (Informationspflichten, Informationstechnik, elektronische Signatur) und regeln deren Gebrauch.

Name	**BGB-InfoV – Verordnung über Informations- und Nachweispflichten nach bürgerlichem Recht (BGB-Informationspflichten-Verordnung)**
Inhalt	Die BGB-InfoV regelt ergänzend zum BGB Informationspflichten im elektronischen Geschäftsverkehr. Verschiedene Regelungen wurden allerdings zuletzt auf das EBGB übertragen.
Status	Fassung vom 5. August 2002 (BGBl. I S. 3002); zuletzt geändert durch Artikel 3 des Gesetzes vom 17. Januar 2011 (BGBl. I S. 34)
Link	zum Text:

	http://www.gesetze-im-internet.de/bgb-infov/index.html

Name	**BildscharbV – Verordnung über Sicherheit und Gesundheitsschutz bei der Arbeit an Bildschirmgeräten (Bildschirmarbeitsverordnung)**
Inhalt	Die BildscharbV regelt die Arbeit an Bildschirmen und dient insbesondere der Sicherheit und dem Gesundheitsschutz der Arbeitnehmer/innen. Ein Anhang enthält die an Bildschirmarbeitsplätze zu stellenden Anforderungen, z. B. hinsichtlich Geräten und Arbeitsumgebung, aber auch in Bezug auf die softwareergonomische Gestaltung.
Status	Fassung vom 4. Dezember 1996 (BGBl. I S. 1843); zuletzt geändert durch Artikel 7 der Verordnung vom 18. Dezember 2008 (BGBl. I S. 2768)
Link	zum Text: http://www.gesetze-im-internet.de/bildscharbv/BJNR184300996.html

Name	**BITV – Verordnung zur Schaffung barrierefreier Informationstechnik nach dem Behindertengleichstellungsgesetz (Barrierefreie Informationstechnik-Verordnung)**
Inhalt	Die BITV soll behinderten Menschen den Zugang und die Nutzung von Informationstechnik ermöglichen oder erleichtern. Sie betreffen vor allem die den IT-Nutzern angebotenen elektronischen Inhalte und Informationen. Hierfür werden Anforderungen in einer Anlage getroffen.
Status	Fassung vom 17. Juli 2002 (BGBl. I S. 2654)"
Link	zum Text: http://www.gesetze-im-internet.de/bitv/BJNR265400002.html

Name	**SigV – Verordnung zur elektronischen Signatur (Signaturverordnung)**
Inhalt	Die SigV ergänzt das SigG um Regelungen hinsichtlich der Tätigkeit von Zertifizierungsdiensteanbietern.
Status	Fassung vom 16. November 2001 (BGBl. I S. 3074), zuletzt geändert durch Artikel 1 der Verordnung vom 15. November 2010 (BGBl. I S. 1542)
Link	zum Text: http://bundesrecht.juris.de/sigv_2001/BJNR307400001.html

Name	**TKÜV – Verordnung über die technische und organisatorische Umsetzung von Maßnahmen zur Überwachung der Telekommunikation (Telekommunikations-Überwachungsverordnung)**

Inhalt	Die TKÜV schreibt Betreibern von Telekommunikationsanlagen vor, welche Vorkehrungen sie für den Fall einer Telekommunikationsüberwachung zu treffen haben.
Status	Fassung vom 3. November 2005 (BGBl. I S. 3136), zuletzt geändert durch Artikel 4 des Gesetzes vom 25. Dezember 2008 (BGBl. I S. 3083)
Link	zum Text: http://bundesrecht.juris.de/tk_v_2005/BJNR313600005.html

3.2 Nicht IT-spezifische Rechtsverordnungen

Nicht IT-spezifische Rechtsverordnungen

In nicht IT-spezifischen Rechtsverordnungen bezieht sich wieder nur ein geringer Teil der Regelungen auf IT-Belange.

Name	**PAngV – Preisangabenverordnung**
Inhalt	Die PAngV trifft für den E-Commerce wichtige Regelungen. So bestimmt § 5 Abs. 1, dass der Ort eines Leistungsangebotes auch die Bildschirmanzeige sein kann. § 4 Abs. 4 legt für diesen Fall den Ort der Preisauszeichnung fest.
Status	Fassung der Bekanntmachung vom 18. Oktober 2002 (BGBl. I S. 4197), zuletzt geändert durch Artikel 4 des Gesetzes vom 24. Juli 2010 (BGBl. I S. 977)
Link	zum Text: http://www.gesetze-im-internet.de/pangv/BJNR105800985.html

4. Verwaltungsvorschriften

Verwaltungsvorschriften

Auch ohne dass es sich um Rechtsnormen handelt, sind für IT-Compliance solche Regelwerke relevant, die von den zuständigen (Aufsichts-)Behörden zur Interpretation und Ausführung der Rechtsnormen aufgestellt oder erklärtermaßen herangezogen werden. Diese Regelwerke bewirken rechtlich eine Selbstbindung der Verwaltung, indem sie die Anwendung der Rechtsnormen durch die Verwaltung bestimmen. Zudem ist die Entwicklung zu beobachten, dass es zunehmend ergänzende Informationsschreiben gibt, in denen dargelegt wird, wie spezielle Fragen zur Nutzung von IT aus Sicht der Verwaltung handzuhaben sind. Diese ergänzenden Informationen haben allerdings in der Regel keine bindende Wirkung.

Name	**GDPdU – Grundsätze zum Datenzugriff und zur Prüfbarkeit digitaler Unterlagen**
Inhalt	Die GDPdU regeln als Verwaltungsanweisung des Bundesfinanzministeriums (BMF) die Aufbewahrung digitaler Unterlagen und die Mitwirkungspflicht der Steuerpflichtigen bei Betriebsprüfungen. So werden Unternehmen durch die GDPdU beispielsweise dazu verpflichtet, steuerrelevante Daten über einen Zeitraum von mindestens zehn Jahren unveränderbar sowie maschinell les- und auswertbar vorzuhalten.
Status	BMF-Schreiben vom 16. Juli 2001 - IV D 2 - S 0316 - 136/01 -
Link	zum Text: http://www.bundesfinanzministerium.de/DE/Wirtschaft__und__Verwaltung/Steuern/Veroeffentlichungen__zu__Steuerarten/Abgabenordnung/Datenzugriff__GDPdU/002,templateId=raw,property=publicationFile.pdf

Name	**(GDPdU) Fragen und Antworten zum Datenzugriffsrecht der Finanzverwaltung**
Inhalt	Der Fragen- und Antwortenkatalog des BMF bietet eine unverbindliche Orientierungshilfe für die Anwendung des Datenzugriffsrechts nach den GDPdU. Hier wird beispielsweise in I Nr. 10 erklärt, dass das Unternehmen verpflichtet sei, den Datenzugriff der Finanzverwaltung auf freiwillig geführte, digitale Aufzeichnungen zuzulassen. Weiterhin findet sich in I Nr. 15 die Aussage, dass für versehentlich überlassene Daten kein Verwertungsverbot besteht.
Status	BMF, Stand: 22. Januar 2009
Link	zum Text: http://www.bundesfinanzministerium.de/DE/BMF__Startseite/Service/Downloads/Abt__IV/009,property=publicationFile.pdf

Name	**(GDPdU) Information zum „Beschreibungsstandard für die Datenträgerüberlassung“**
Inhalt	Die Information enthält grundlegende Informationen zum XML-basierten Beschreibungsstandard. Dieser ist vor allem für die Datenträgerüberlassung (Z3-Zugriff) als häufigste angewendete Methode in der digitalen Betriebsprüfung relevant.
Status	BMF, Stand: 15. August 2002
Link	zum Text: http://www.bundesfinanzministerium.de/DE/BMF__Startseite/Service/Downloads/Abt__IV/010,property=publicationFile.pdf

Name	**GoBS – Grundsätze ordnungsmäßiger DV-gestützter Buchführungssysteme**
Inhalt	Die GoBS regeln als Verwaltungsanweisung des Bundesfinanzministeriums (BMF) die ordnungsmäßige Behandlung, insb. die Aufbewahrung und Archivierung elektronischer Dokumente. Sie beinhalten insb. auch die Verpflichtung zur Datensicherheit (Tz. 5 der GoBS). Nach Tz. 6 der GoBS ist zudem für jedes DV-gestützte Buchführungssystem eine sog. Verfahrensdokumentation zu erstellen.
Status	BMF-Schreiben vom 7. November 1995 - IV A 8 - S 0316 - 52/95- BStBl 1995 I S. 738
Link	zum Text: http://www.bundesfinanzministerium.de/nn_314/DE/BMF__Startseite/Service/Downloads/Abt__IV/BMF__Schreiben/015,templateId=raw,property=publicationFile.pdf

Name	**MaRisk – Mindestanforderungen an das Risikomanagement**
Inhalt	Die MaRisk konkretisieren das von Kreditinstituten nach § 25a Abs. 1 KWG (Kreditwesengesetz) einzurichtende Risikomanagement. Die der MaRisk zugehörige Anlage 1 enthält unter „AT 7.2 Technisch-organisatorische Ausstattung“ Vorgaben für den IT-Einsatz.
Status	Rundschreiben der Bundesanstalt für Finanzdienstleistungsaufsicht (BaFin) vom 20.12.2005, Anlage 1: MaRisk - Regelungstext mit Erläuterungen
Link	zum Text: http://www.bundesbank.de/download/bankenaufsicht/pdf/marisk/051220_anl1.pdf

5. Referenzierte Regelwerke

Referenzierte Regelwerke

Regelwerke, die als solche keinen Rechtsnormcharakter haben und sowohl von Verwaltungen wie auch von privatrechtlichen Institutionen (z. B. dem DIN, Deutsches Institut für Normung) stammen können, haben für die IT-Compliance die gleiche Bedeutung wie Rechtsnormen, wenn sie durch ausdrückliche Verweisung in diese einbezogen werden. Allerdings sind derartige Fälle zurzeit recht selten.

An erster Position erfolgt die Angabe des referenzierenden Regelwerks (RW). Die Inhaltsangabe bezieht sich auf den Verweis im referenzierenden Regelwerk. Dann erfolgt die Angabe des/der referenzierten Regelwerks/

Regelwerke (RR). Status und Link werden für die Regelwerke getrennt aufgeführt.

RW	**Anlage zu den §§ 3 und 4 Abs. 1 BITV – Barrierefreie Informations-technik-Verordnung**
Inhalt RW	In der der BITV zugehörigen Anlage wird in der Einleitung zu Teil 1 darauf verwiesen, dass Anforderungen und Bedingungen der Anlage grundsätzlich auf den Zugänglichkeitsrichtlinien für Web-Inhalte 1.0 (Web Content Accessibility Guidelines 1.0) des World Wide Web Consortiums vom 5. Mai 1999 basieren.
Status RW	Fassung vom 16. November 2001 (BGBl. I S. 3074), zuletzt geändert durch Artikel 1 der Verordnung vom 15. November 2010 (BGBl. I S. 1542)
Link RW	zum Text: http://www.bundesfinanzministerium.de/nn_314/DE/BMF__Startseite/Service/Downloads/Abt__IV/BMF__Schreiben/015,templateId=raw,property=publicationFile.pdf
RR	**Web Content Accessibility Guidelines 1.0**
Status RR	Version 1.0, W3C Recommendation 5-May-1999
Link RR	zum Text: http://www.w3.org/TR/WCAG10/

RW	**EBGB – Einführungsgesetz zum Bürgerlichen Gesetzbuche**
Inhalt RW	Art 248 § 3 Nr. 5 EBGB verweist auf Verhaltenskodizes, denen sich ein Unternehmen unterwirft. Bei elektronischem Geschäftsverkehr hat das Unternehmen diese Verhaltenskodizes anzugeben und elektronischen Zugang zu diesen zu gewähren.
Status RW	Fassung der Bekanntmachung vom 21. September 1994 (BGBl. I S. 2494; 1997 I S. 1061), das zuletzt durch Artikel 2 des Gesetzes vom 12. April 2011 (BGBl. I S. 615) geändert
Link	zum Text: http://bundesrecht.juris.de/bgbeg/BJNR006049896.html#BJNR006049896BJNG053200140
RR	**Verhaltenskodizes** Viele Unternehmen verweisen in ihren AGB darauf, dass sie sich keinen derartigen Verhaltenskodizes unterworfen haben. Mitunter

	finden sich jedoch Angaben, dass sich ein Unternehmen speziellen Sicherheitsrichtlinien oder Verbandskodizes unterworfen hat.[24]

RW	**Anlage 1: MaRisk - Regelungstext mit Erläuterungen – Mindestanforderungen an das Risikomanagement**
Inhalt RW	In der der MaRisk zugehörigen Anlage 1 verweist die Erläuterung zu AT 7.2 sowohl auf die vom Bundesamt für Sicherheit in der Informationstechnik (BSI) herausgegebenen IT-Grundschutzkataloge als auch auf die (mittlerweile zurückgezogene) ISO 17799.
Status RW	Rundschreiben der Bundesanstalt für Finanzdienstleistungsaufsicht (BaFin) vom 20.12.2005, Anlage 1: MaRisk - Regelungstext mit Erläuterungen
Link RW	zum Text: http://www.bundesbank.de/download/bankenaufsicht/pdf/marisk/051220_anl1.pdf
RR	**IT-Grundschutzkataloge**
Status RR	unterschiedlich
Link RR	zur Grundschutz-Information des BSI: https://www.bsi.bund.de/DE/Themen/ITGrundschutz/StartseiteITGrundschutz/startseiteitgrundschutz_node.html
RR	**ISO/IEC 17799**
Status RR	ISO stage code: Withdrawal stage 95.99 (2008-10-15) Withdrawal of International Standard
Link RR	zur ISO-Information: http://www.iso.org/iso/catalogue_detail?csnumber=39612

RW	**Anlage 1 zu § 11 Abs. 3, § 15 Abs. 5 und § 16 Abs. 2 SigV: Vorgaben für die Prüfung von Produkten für qualifizierte elektronische Signaturen**
Inhalt RW	Nach Nr. 1.1 der Anlage zur SigV hat die Prüfung von Produkten für qualifizierte elektronische Signaturen nach den "Gemeinsamen Kriterien für die Prüfung und Bewertung der Sicherheit von Informationstechnik" (Common Criteria for Information Technology Security Evaluation) bzw. der ISO/IEC 15408 oder nach den "Kriterien für die Bewertung der Sicherheit von Systemen der Informationstechnik" (ITSEC) in der jeweils geltenden Fassung zu erfolgen.

[24] Beispiele sind im Internet leicht recherchierbar und werden deshalb hier nicht angegeben.

Status RW	Fassung vom 16. November 2001 (BGBl. I S. 3074), zuletzt geändert durch Artikel 1 der Verordnung vom 15. November 2010 (BGBl. I S. 1542)
Link RW	zum Text: http://www.bundesfinanzministerium.de/nn_314/DE/BMF__Startseite/Service/Downloads/Abt__IV/BMF__Schreiben/015,templateId=raw,property=publicationFile.pdf
RR	**Common Criteria for Information Technology Security Evaluation**
Status RR	unterschiedlich
Link RR	zur Download-Seite des commoncriteriaportal: http://www.commoncriteriaportal.org/cc/
RR	**ISO/IEC 15408**
Status RR	ISO stage code: Publication stage 60.60 (2009-12-03) International Standard published
Link RR	zur ISO-Information: http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=50341
RR	**Kriterien für die Bewertung der Sicherheit von Systemen der Informationstechnik (ITSEC)**
Status RR	Version 1.2 vom 28.06.1991
Link RR	zum Text: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Zertifizierung/ITSicherheitskriterien/itsec-dt_pdf.pdf?__blob=publicationFile

6. Rechtsprechung

Rechtsprechung

Zu den rechtlichen Vorgaben zählt weiterhin die Rechtsprechung, die die Rechtsnormen auslegt und damit wesentlich deren Inhalt bestimmt. Dies betrifft in besonderem Maße so genannte unbestimmte Rechtsbegriffe bzw. Generalklauseln. Beispiele hierfür sind die „übliche Beschaffenheit“, die das Vorliegen eines Mangels im Werkvertragsrecht bestimmt, oder Sorgfaltspflichten, deren Missachtung den Vorwurf fahrlässigen Verhaltens begründet.[25]

[25] Bspw. die in § 347 HGB geregelte „Sorgfalt eines ordentlichen Kaufmanns“.

Einschränkung

Die folgende Auflistung kann nicht annähernd eine Vollständigkeit hinsichtlich der vor deutschen Gerichten verhandelten IT-Themen beanspruchen; sie ist insofern nur exemplarisch zu verstehen. Insbesondere können Verfahren über mehrere Instanzen oder Verweisungsstrukturen, die sich z. B. regelmäßig bei Reaktionen der Rechtsprechung auf BGH-Urteile ergeben, hier nicht dargestellt werden. Der Leser/die Leserin sei hierfür auf die juristische Fachliteratur verwiesen.

Es wurden nur solche Urteile ausgewählt, deren Urteilstext im Internet frei verfügbar ist. Die Inhaltsangaben richten sich überwiegend nach den jeweils angegebenen Leitsätzen.

Name	**BGH – Bundesgerichtshof, X ZR 129/01**
Inhalt	Urteil des BGH zu der Frage, ob im Rahmen der Erfüllung eines Werkvertrages über die Erstellung eines Softwareprogramms dem Auftraggeber auch der Quellcode überlassen werden muss. Dies richtet sich mangels ausdrücklicher Vereinbarung nach den Umständen des Einzelfalls.
Status	Urteil vom 16.12.2003 (Az. X ZR 129/01)
Link	zum Text: http://juris.bundesgerichtshof.de/cgi-bin/rechtsprechung/document.py?Gericht=bgh&Art=en&sid=f01be94677eaded74e96437fcbe7f322&client=3&nr=28600&pos=4&anz=91

Name	**BGH – Bundesgerichtshof, I ZR 304/01**
Inhalt	Urteil des BGH („Rolex ./. Ricardo“), aus dem sich in die Zukunft gerichtete, verschuldensunabhängige Unterlassungsansprüche an Diensteanbieter ergeben können. Wird diesem ein Fall einer Markenverletzung bekannt, muss er nicht nur das konkrete Angebot unverzüglich sperren, sondern auch technisch mögliche und zumutbare Maßnahmen ergreifen, um dafür zu sorgen, dass es nicht zu weiteren entsprechenden Verletzungen kommt.[26]
Status	Urteil vom 11.03.2004 (Az. I ZR 304/01)
Link	zum Text: http://www.jurpc.de/rechtspr/20040265.htm

Name	**BVerfG – Bundesverfassungsgericht, 1 BvR 209, 269, 362, 420, 440, 484/83 („Volkszählungsurteil)**

[26] Vgl. die Diskussion des Urteils und seiner Folgen bei *Weber/Dittrich 2010*, Rn. 17-20.

Inhalt	Das sog. „Volkszählungsurteil“ ist eine Grundsatzentscheidung des Bundesverfassungsgerichts. Mit diesem Urteil hat das BVerfG das Recht auf informationelle Selbstbestimmung als von Art 2 Abs. 1 in Verbindung mit Art 1 Abs. 1 GG umfasst anerkannt. Die zentrale Aussage lautet: „Freie Entfaltung der Persönlichkeit setzt unter den modernen Bedingungen der Datenverarbeitung den Schutz des Einzelnen gegen unbegrenzte Erhebung, Speicherung, Verwendung und Weitergabe seiner persönlichen Daten voraus.“
Status	Urteil vom 15.12.1983 (Az. 1 BvR 209, 269, 362, 420, 440, 484/83)
Link	zum Text: http://www.lfd.m-v.de/dschutz/ges_ver/guv/guv_a_20.html

Name	**BVerfG – Bundesverfassungsgericht, 1 BvR 370/07, 595/07**
Inhalt	Das Bundesverfassungsgerichts hat mit diesem Urteil ein „IT-Grundrecht“ formuliert, indem es klarstellt, dass das allgemeine Persönlichkeitsrecht nach Art. 2 Abs. 1 i. V. m. Art. 1 Abs. 1 GG ein Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme umfasst.
Status	Urteil vom 27.02.2008 (Az. 1 BvR 370/07, 595/07)
Link	zum Text: http://www.bundesverfassungsgericht.de/entscheidungen/rs20080227_1bvr037007.html

Name	**FG Rheinland-Pfalz – Finanzgericht Rheinland-Pfalz, 4 K 2167/04**
Inhalt	In diesem Fall hat eine Bank ihre Datenbestände für die Betriebsprüfung nicht so organisiert, dass das Bankgeheimnis nach § 30a AO bei einer Betriebsprüfung gewahrt bleiben konnte. Das Finanzgericht bestätigt mit diesem Urteil das GDPdU-Schreiben im Hinblick auf die Pflicht des Geprüften, die Buchhaltungsdaten abzugrenzen und dabei für steuerlich nicht relevante Daten gesetzliche Vorgaben wie Datenschutz und Berufsgeheimnis, aber eben auch das Bankgeheimnis, zu beachten.[27]
Status	Urteil vom 20.01.2005 (Az. 4 K 2167/04)
Link	zum Text: http://www.iww.de/index.cfm?pid=1307&opv=050565

Name	**FG Schleswig-Holstein – Finanzgericht Schleswig-Holstein, 3 V 243/09**

[27] Nach *Kaminski 2010*, S. 22f.

Inhalt	Von der Finanzverwaltung wurde ein Verzögerungsgeld gegen eine GmbH mit inländischen Buchhaltungssystemen verhängt, da diese der Aufforderung zur Datenträgerüberlassung nach mehrmaligen Anforderungen nicht nachkam. Nachdem die GmbH dem Verlangen genügte, beharrte die Finanzverwaltung jedoch auf der Forderung des Verzögerungsgeldes. Mit dem Verzögerungsgeld steht der Finanzverwaltung ein wirksames Mittel mit einem repressiven und präventiven Charakter zur Verfügung, um die mangelnde Umsetzung des digitalen Datenzugriffs zu sanktionieren.[28]
Status	Urteil vom 03.02.2010 (Az. 3 V 243/09)
Link	zum Text: http://www.iww.de/index.cfm?pid=1307&opv=101678

Name	**LG Bonn – Landgericht Bonn, 10 O 387/01**
Inhalt	Urteil des LG Bonn zu Leistungsstörungen im Softwarepflegevertrag. Es werden Vorgaben zur Softwaredokumentation gemacht. Diese ist z. B. als mangelhaft einzustufen, wenn in der Dokumentation abgebildete Bildschirmdialoge nicht mehr aktuell sind.
Status	Urteil vom 19.12.2003 (Az. 10 O 387/01)
Link	zum Text: http://www.jurpc.de/rechtspr/20040109.htm

Name	**LG Köln – Landgericht Köln, 4 Sa 1018/04**
Inhalt	Nach dem LG Köln ist private Internet- und E-Mail-Nutzung, die die Betriebstätigkeit nicht stört, keine erheblichen unzumutbaren Kosten verursacht und das Betriebssystem nicht gefährdet, gestattet.
Status	Urteil vom 11.02.2005 (Az. 4 Sa 1018/04)
Link	zum Text: http://www.justiz.nrw.de/nrwe/arbgs/koeln/lag_koeln/j2005/4_Sa_1018_04urteil20050211.html

Name	**LG Landshut – Landgericht Landshut, HK O 2392/02**
Inhalt	Nach dem LG Landshut ist der Lieferung einer Standard-Software Kaufrecht zu Grunde zu legen. Werkvertragsrecht kommt nur dann in Frage, wenn die Standard-Software in einem Umfang entsprechend der individuellen Bedürfnisse des Kunden angepasst werden muss, dass im Ergebnis eine Individual-Software vorliegt. Zudem darf nach

[28] Nach *ebd.*, S. 28f.

	diesem Urteil ein Handbuch als CD-ROM übergeben werden.
Status	Urteil vom 20.08.2003 (Az. 2 HK O 2392/02)
Link	zum Text: http://www.jurpc.de/rechtspr/20040101.htm

Name	**LG Stuttgart – Landgericht Stuttgart, 8 O 274/99**
Inhalt	Nach dem LG Stuttgart stellt die Übergabe eines Handbuches beim Verkauf von Hard- und Software eine Hauptleistungspflicht dar.
Status	Urteil vom 24.01.2002 (Az. 8 O 274/99)
Link	zum Text: http://www.jurpc.de/rechtspr/20020108.htm

Name	**OLG Hamm – Oberlandesgericht Hamm, 13 U 133/03**
Inhalt	Das OLG Hamm hat eine unterlassene Datensicherung bei Schäden, die durch Datenverluste entstehen, als Mitverschulden gewertet. Das Gericht stellte fest, dass eine Datensicherung täglich zu erfolgen hat, eine Vollsicherung mindestens einmal wöchentlich.
Status	Urteil vom 01.12.2003 (Az. 13 U 133/03)
Link	zum Text: http://www.justiz.nrw.de/nrwe/olgs/hamm/j2003/13_U_133_03urteil20031201.html

Name	**OLG Hamburg – Oberlandesgericht Hamburg, 3 W 44/10**
Inhalt	Als vorvertragliche Informationspflicht im elektronischen Geschäftsverkehr hat nach dem OLG Hamburg eine Online-Händler „den Verbraucher darüber zu informieren, wie mit den gemäß § 312 e Abs. 1 Satz 1 Nr. 1 des Bürgerlichen Gesetzbuchs zur Verfügung gestellten technischen Mitteln Eingabefehler vor Abgabe der Bestellung erkannt und berichtigt werden können“.
Status	Urteil vom 14.05.2010 (Az. 3 W 44/10)
Link	zum Text: http://www.landesrecht.hamburg.de/jportal/portal/page/bshaprod.psml;jsessionid=D0EE59E4F4B727BF37EAB3766448FAB8.jpj4?showdoccase=1&doc.id=KORE536532010&st=ent

Name	**OLG Köln – Oberlandesgericht Köln, 19 U 4/05**
Inhalt	Zum Anforderungsprofil einer Individualsoftware hat das OLG Köln entschieden, dass es grundsätzlich die Aufgabe des Auftraggebers ist,

	das für die Softwareentwicklung erforderliche Anforderungsprofil zu erstellen. Der Auftragnehmer muss hieran in geeigneter Weise mitwirken.
Status	Urteil vom 29.07.2005 (Az. 19 U 4/05)
Link	zum Text: http://www.jurpc.de/rechtspr/20060016.htm

7. Verträge

7.1 Allgemeine Verträge

Gruppierung

Ähnlich wie bei Gesetzen und Rechtsverordnungen sind hier zwei Gruppen von Verträgen von Bedeutung:

- Verträge allgemeiner Art, deren Vertragsgegenstand sich nicht auf IT-Belange konzentriert, die aber einzelne IT-relevante Regelungen enthalten (beispielsweise zum Austausch oder zur Aufbewahrung von Informationen) oder die dem Vertragsdokument als IT-Objekt einen schutzwürdigen Status zuerkennen (was gewöhnlich durch eine Geheimhaltungsvereinbarung geschieht);
- spezifische IT-Verträge, deren Vertragsgegenstand sich auf IT-Leistungen bezieht und die dadurch direkt relevant sind für IT-Compliance (z. B. IT-Entwicklungs- oder Schulungsverträge, Softwareüberlassungs- und Softwarepflegeverträge, Providerverträge).

Verträge allgemeiner Art

Für die erste Gruppe sollen im Folgenden einige Beispiele angeführt werden. Die zweite Gruppe wird im nächsten Abschnitt behandelt.

Name	**Beratungsvertrag**
Inhalt	Muster eines allgemein gehaltenen Beratungsvertrages, der Regelungen zur Vertraulichkeit, zum Datenschutz sowie zur Aufbewahrung und Rückgabe von Unterlagen enthält.
Status	Stand: nicht angegeben
Link	zum Text: http://www.go.nrw.de/files/muster-beratungsvertrag_bpw_010710_1.pdf

Name	**LOI – Letter of Intent (Absichtserklärung)**
Inhalt	Muster einer Absichtserklärung, bereitgestellt von der IHK Frankfurt am Main, in der eine Geheimhaltungsvereinbarung enthalten ist.

Status	Stand: nicht angegeben
Link	zum Text: http://www.frankfurt-main.ihk.de/recht/mustervertrag/intent/index.html

Name	**Geheimhaltungsvereinbarung**
Inhalt	Muster einer Geheimhaltungsvereinbarung, bereitgestellt von der IHK Frankfurt am Main, in dem zahlreiche Pflichten zum Umgang mit vertraulichen Informationen festgehalten werden.
Status	Stand: 1. Januar 2011
Link	zum Text: http://www.frankfurt-main.ihk.de/recht/mustervertrag/geheimhaltungsvereinbarung/index.html#html

7.2 IT-Verträge

IT-Verträge

IT-Verträge finden sich im Internet in großer Anzahl, schon weil Unternehmen ihre Vertragsbedingungen auf ihre Homepage stellen (müssen). Im Folgenden sollen jedoch keine Individualverträge angeführt werden, sondern nur solche, die von unabhängigen Organisationen als Muster angeboten werden. Hier finden sich Beispiele bei Industrie- und Handelskammern (IHK) sowie bei der Bundesbeauftragten der Bundesregierung für Informationstechnik („Bundes-CIO“). In jedem Fall ist aber darauf hinzuweisen, dass Muster nie eine auf den jeweiligen Anwendungsfall individuell angepasste Vertragsgestaltung ersetzen können.

EVB-IT

Auf der Homepage der Bundesbeauftragten der Bundesregierung für Informationstechnik werden die „Ergänzenden Vertragsbedingungen für die Beschaffung von Informationstechnik“ (EVB-IT) zum Download angeboten.[29] Die EVB-IT sind für IT-Beschaffungen der öffentlichen Hand maßgebend. Sie lösen die älteren BVB (Besondere Vertragsbedingungen für die Beschaffung von DV-Leistungen) ab. Nach 3.1.1 der Allgemeinen Verwaltungsvorschriften zu § 55 BHO (Bundeshaushaltsordnung) sind die EVB-IT bei öffentlichen Ausschreibungen bzgl. Beschaffung und Betrieb von DV-

[29] Zur Information der Bundesbeauftragten der Bundesregierung für Informationstechnik: http://www.cio.bund.de/DE/IT-Angebot/IT-Beschaffung/EVB-IT_BVB/evb-it_bvb_node.html

Anlagen und -Geräten sowie von DV-Programmen anzuwenden.[30] In einem offenen Verfahren haben Bieter die EVB-IT zu beachten, ansonsten droht Ausschluss aus dem Verfahren. Trotzdem ist die Anwendung nicht zwingend, beispielsweise im Rahmen eines Verhandlungsverfahrens. Da die EVB-IT letztlich Allgemeine Geschäftsbedingungen (AGB) darstellen, unterliegen sie auch deren, durch die §§ 305 bis 310 BGB festgelegten Beschränkungen.[31]

Jeder EVB-IT-Vertrag umfasst mehrere vertragliche Regelungen, insbesondere die AGB und den individuell auszufüllenden Vertragstext. Hinzu kommen ergänzende Regelungen bzw. Muster, z. B. für Leistungsnachweise oder Störungsmeldungen.

Name	**Ergänzende Vertragsbedingungen für die Beschaffung von Informationstechnik (EVB-IT), Systemlieferungs-AGB**
Inhalt	Die EVB-IT Systemlieferungs-AGB richten sich auf die Lieferung eines IT- Systems, wobei neben dem Kauf von Komponenten zusätzlich Service-Leistungen in Anspruch genommen werden (nach 1.1 EVB-IT).
Status	Version 1 vom 01.02.2010
Link	zum Text: http://www.cio.bund.de/SharedDocs/Publikationen/DE/IT-Angebot/EVB-IT_Vertragstypen/EVB-IT_Systemlieferung/evb_it_agb_pdf_download.pdf;jsessionid=DBE12415907A81B78C832F56CB891C9B.2_cid093?__blob=publicationFile

Name	**Ergänzende Vertragsbedingungen für die Beschaffung von Informationstechnik (EVB-IT), Systemlieferungsvertrag**
Inhalt	Der EVB-IT Systemlieferungsvertrag enthält auf der Basis der EVB-IT Systemlieferungs-AGB die im konkreten Anwendungsfall auszufüllenden Regelungen.
Status	Version 1 vom 01.02.2010
Link	zum Text: http://www.cio.bund.de/SharedDocs/Publikationen/DE/IT-Angebot/EVB-IT_Vertragstypen/EVB-IT_Systemlieferung/evb_it_systemlieferungsvertrag_pdf_download.pdf;jsessionid=DBE12415907A81B78C832F56CB891C9B.2_cid093?__blo

[30] Siehe Nr. 3.1.1 VV-BHO zu §55 BHO: http://www.verwaltungsvorschriften-im-internet.de/bsvwvbund_14032001_II.htm#ivz60

[31] Nach *Bachmann 2009*, S. 679f.

	b=publicationFile

Name	**Störungsmeldeformular zu EVB-IT, Systemlieferungsvertrag**[32]
Inhalt	Muster für eine Störungs- bzw. Mängelmeldung.
Status	Version 1 vom 01.02.2010
Link	zum Text: http://www.cio.bund.de/SharedDocs/Publikationen/DE/IT-Angebot/EVB-IT_Vertragstypen/EVB-IT_Systemlieferung/evb_it_muster_1_pdf_download.pdf?__blob=publicationFile

Name	**Ergänzende Vertragsbedingungen für die Erstellung eines IT-Systems (EVB-IT System)**
Inhalt	Die EVB-IT System richten sich als allgemeine Regelung auf die Erstellung eines Gesamtsystems auf der Grundlage eines Werkvertrages. Soweit vereinbart werden zudem noch Serviceleistungen (z. B. Beratung, Schulung) oder auch die Weiterentwicklung und Anpassung des Gesamtsystems nach der Abnahme geregelt.
Status	Version 1.01 vom 01.10.2007
Link	zum Text: http://www.cio.bund.de/SharedDocs/Publikationen/DE/IT-Angebot/EVB-IT_Vertragstypen/EVB-IT_System/evb_it_dienstleistungen_ergaenzende_vertragsbedingungen_Erstellung_e_it_Systems_pdf_download.pdf?__blob=publicationFile

Name	**Ergänzende Vertragsbedingungen für die Erstellung eines IT-Systems, Systemvertrag**
Inhalt	Der EVB-IT Systemvertrag enthält auf der Basis der EVB-IT System die im konkreten Anwendungsfall auszufüllenden Regelungen.
Status	Version 1.02 vom 05.11.2007
Link	zum Text: http://www.cio.bund.de/SharedDocs/Publikationen/DE/IT-Angebot/EVB-IT_Archiv/System/Vertragsformular_Systemvertrag/version_vom_051107_pdf_download.pdf?__blob=publicationFile

[32] Die Störungsmeldeformulare für die anderen EVB-IT-Verträge sind ähnlich strukturiert, so dass auf ihre Beschreibung an dieser Stelle verzichtet wird.

Name	**Ergänzende Vertragsbedingungen für die Beschaffung von Informationstechnik, Kauf von Hardware**
Inhalt	Die EVB-IT für den Kauf von Hardware regeln die Lieferung von Hardware inkl. Nebenpflichten (z. B. Entsorgung, Datensicherung).
Status	Version vom 01.04.2002
Link	zum Text: http://www.cio.bund.de/SharedDocs/Publikationen/DE/IT-Angebot/EVB-IT_Vertragstypen/EVB-IT_Kauf/evb_it_dienstleistungen_ergaenzende_vertragsbedingungen_Kauf_Hardware_pdf_download.pdf?__blob=publicationFile

Name	**Ergänzende Vertragsbedingungen für die Beschaffung von Informationstechnik, Kaufvertrag (Langfassung)**
Inhalt	Der EVB-IT Kaufvertrag enthält die im konkreten Anwendungsfall auszufüllenden Regelungen für den Kauf sowohl von Hardware als auch von Standardsoftware (Langfassung).
Status	Version vom 01.04.2002
Link	zum Text: http://www.cio.bund.de/SharedDocs/Publikationen/DE/IT-Angebot/EVB-IT_Vertragstypen/EVB-IT_Kauf/evb_it_kaufvertrag_langf_pdf_download.pdf?__blob=publicationFile

Name	**Ergänzende Vertragsbedingungen für die Beschaffung von Informationstechnik, Kaufvertrag (Kurzfassung)**
Inhalt	Der EVB-IT Kaufvertrag enthält die im konkreten Anwendungsfall auszufüllenden Regelungen für den Kauf sowohl von Hardware als auch von Standardsoftware (Kurzfassung).
Status	Version vom 01.04.2002
Link	zum Text: http://www.cio.bund.de/SharedDocs/Publikationen/DE/IT-Angebot/EVB-IT_Vertragstypen/EVB-IT_Kauf/evb_it_kaufvertrag_kurzf_pdf_download.pdf?__blob=publicationFile

Name	**Ergänzende Vertragsbedingungen für die Beschaffung von IT-Dienstleistungen**
Inhalt	Die EVB-IT Dienstleistung regeln die Erbringung von Dienstleistungen, wobei der Auftraggeber die Projekt- und Erfolgsverantwortung trägt. Außerdem obliegt im explizit die Pflicht zur Datensicherung.

Status	Version vom 01.04.2002
Link	zum Text: http://www.cio.bund.de/SharedDocs/Publikationen/DE/IT-Angebot/EVB-IT_Vertragstypen/EVB-IT_Dienstleistung/evb_it_dienstleistungen_ergaenzende_vertragsbedingungen_beschaffung_it_dienstl_pdf_download.pdf?__blob=publicationFile

Name	**Ergänzende Vertragsbedingungen für die Beschaffung von Informationstechnik, Dienstvertrag**
Inhalt	Der EVB-IT Dienstvertrag enthält die im konkreten Anwendungsfall auszufüllenden Regelungen für die Beschaffung von IT-Dienstleistungen.
Status	Version vom 01.04.2002
Link	zum Text: http://www.cio.bund.de/SharedDocs/Publikationen/DE/IT-Angebot/EVB-IT_Vertragstypen/EVB-IT_Dienstleistung/evb_it_dienstleistungen_dienstvertrag_pdf_download.pdf?__blob=publicationFile

Name	**Ergänzende Vertragsbedingungen für die zeitlich unbefristete Überlassung von Standardsoftware gegen Einmalvergütung – EVB-IT Überlassung Typ A –**
Inhalt	Die EVB-IT Überlassung Typ A regeln die zeitlich unbefristete Überlassung von Standardsoftware gegen Einmalvergütung.
Status	Version vom 01.04.2002
Link	zum Text: http://www.cio.bund.de/SharedDocs/Publikationen/DE/IT-Angebot/EVB-IT_Vertragstypen/EVB-IT_Ueberlassung_Typ_A/evb_it_dienstleistungen_ergaenzende_vertragsbedingungen_ueberlassung_typ_a_pdf_download.pdf?__blob=publicationFile

Name	**Vertrag über die zeitlich unbefristete Überlassung von Standardsoftware gegen Einmalvergütung (Langfassung)**
Inhalt	Der EVB-IT Überlassungsvertrag Typ A enthält die im konkreten Anwendungsfall auszufüllenden Regelungen für die Überlassung von Standardsoftware gegen Einmalvergütung (Langfassung).
Status	Version vom 01.04.2002
Link	zum Text:

	http://www.cio.bund.de/SharedDocs/Publikationen/DE/IT-Angebot/EVB-IT_Vertragstypen/EVB-IT_Ueberlassung_Typ_A/evb_it_ueberlassungsvertrag_typ_a_langf_pdf_download.pdf?__blob=publicationFile

Name	**Vertrag über die zeitlich unbefristete Überlassung von Standardsoftware gegen Einmalvergütung (Kurzfassung)**
Inhalt	Der EVB-IT Überlassungsvertrag Typ A enthält die im konkreten Anwendungsfall auszufüllenden Regelungen für die Überlassung von Standardsoftware gegen Einmalvergütung (Kurzfassung).
Status	Version vom 01.04.2002
Link	zum Text: http://www.cio.bund.de/SharedDocs/Publikationen/DE/IT-Angebot/EVB-IT_Vertragstypen/EVB-IT_Ueberlassung_Typ_A/evb_it_ueberlassungsvertrag_typ_a_langf_pdf_download.pdf?__blob=publicationFile

Name	**Ergänzende Vertragsbedingungen für die zeitlich befristete Überlassung von Standardsoftware – EVB-IT Überlassung Typ B –**
Inhalt	Die EVB-IT Überlassung Typ B regeln die zeitlich befristete Überlassung von Standardsoftware gegen Einmalvergütung.
Status	Version vom 01.04.2002
Link	zum Text: http://www.cio.bund.de/SharedDocs/Publikationen/DE/IT-Angebot/EVB-IT_Vertragstypen/EVB-IT_Ueberlassung_Typ_B/evb_it_dienstleistungen_ergaenzende_vertragsbedingungen_ueberlassung_typ_b_pdf_download.pdf?__blob=publicationFile

Name	**Vertrag über die zeitlich befristete Überlassung von Standardsoftware**
Inhalt	Der EVB-IT Überlassungsvertrag Typ B enthält die im konkreten Anwendungsfall auszufüllenden Regelungen für die Überlassung von Standardsoftware.
Status	Version vom 01.04.2002
Link	zum Text: http://www.cio.bund.de/SharedDocs/Publikationen/DE/IT-Angebot/EVB-IT_Vertragstypen/EVB-IT_Ueberlassung_Typ_B/evb_it_ueberlassungsvertrag_typ_b_pdf_download.pdf?__blob=publicationFile

Name	**Ergänzende Vertragsbedingungen für die Instandhaltung von Hardware**
Inhalt	Die EVB-IT Instandhaltung regeln die Verpflichtung zur Aufrechterhaltung und Wiederherstellung der Betriebsbereitschaft von Hardware. Hierzu zählen Instandsetzungs-, Inspektions- und Wartungsarbeiten.
Status	Version vom 01.04.2002
Link	zum Text: http://www.cio.bund.de/SharedDocs/Publikationen/DE/IT-Angebot/EVB-IT_Vertragstypen/EVB-IT_Instandhaltung/evb_it_instandhaltung_ergaenzende_vertragsbedingungen_hardware_pdf_download.pdf?__blob=publicationFile

Name	**Vertrag über die Instandhaltung von Hardware**
Inhalt	Der EVB-IT Instandhaltungsvertrag enthält die im konkreten Anwendungsfall auszufüllenden Regelungen für die Instandhaltung von Hardware.
Status	Version vom 01.04.2002
Link	zum Text: http://www.cio.bund.de/SharedDocs/Publikationen/DE/IT-Angebot/EVB-IT_Vertragstypen/EVB-IT_Instandhaltung/evb_it_instandhaltung_instandhaltungsvertrag_pdf_download.pdf?__blob=publicationFile

Name	**Ergänzende Vertragsbedingungen für die Pflege von Standardsoftware (EVB-IT Pflege S)**
Inhalt	Die EVB-IT Pflege S regeln Pflegeleistungen an Standardsoftware.
Status	Version vom 27.03.2003
Link	zum Text: http://www.cio.bund.de/SharedDocs/Publikationen/DE/IT-Angebot/EVB-IT_Vertragstypen/EVB-IT_Pflege_S/evb_it_dienstleistungen_ergaenzende_vertragsbedingungen_beschaffung_it_dienstl_pdf_download.pdf?__blob=publicationFile

Name	**Vertrag über die Pflege von Standardsoftware**
Inhalt	Der EVB-IT Pflegevertrag S enthält die im konkreten Anwendungsfall auszufüllenden Regelungen für die Pflege von Standardsoftware.
Status	Version vom 13.02.2003
Link	zum Text: http://www.cio.bund.de/SharedDocs/Publikationen/DE/IT-

	Angebot/EVB-IT_Vertragstypen/EVB-IT_Pflege_S/evb_it_pflegevertrag_s_pdf_download.pdf?__blob=publicationFile

Name	**Vertrag zur Pflege von Software**
Inhalt	Mustervertrag der IHK Magdeburg zur Softwarepflege
Status	Stand: 01. Januar 2008
Link	zum Text: http://www.magdeburg.ihk24.de/linkableblob/926596/data/Softwaren_Pflegevertrag_2008-data.pdf

Name	**Vertrag zur Softwareerstellung**
Inhalt	Mustervertrag der IHK Magdeburg zur Softwareerstellung
Status	Stand: 01. Januar 2008
Link	zum Text: http://www.magdeburg.ihk24.de/linkableblob/926594/data/Softwareerstellungsvertrages_2008-data.pdf

8. Ausblick

Fortsetzung

Im fortsetzenden Arbeitspapier werden unternehmensinterne und unternehmensexterne Regelwerke aufgelistet. Für die unternehmensinternen Regelwerke werden hierbei im Wesentlichen Beispiele angegeben, während für die unternehmensexternen Regelwerke wieder ein Verweis auf die Originaltexte erfolgt, soweit diese kostenfrei zugänglich sind.

Aktualisierung

Die in diesem Arbeitspapier genannten Regelwerke unterliegen einer kontinuierlichen Veränderung. Aus diesem Grunde ist eine mindestens jährliche Aktualisierung geplant.[33] Aktuellere Angaben sind zwischenzeitlich der SIMAT-Website[34] zu entnehmen, wo die Liste der Regelwerke, allerdings ohne Inhaltsbeschreibung, im Forschungsbereich unter „House of IT-Compliance“ quartalsweise gepflegt wird.

[33] Hinweise in Bezug auf notwendige Ergänzungen und Aktualisierungen nimmt der Autor jederzeit gerne entgegen: michael.klotz@fh-stralsund.de

[34] http://simat-stralsund.de/component/content/article/306-it-compliance-regelwerke/312-it-compliance-regelwerke.html

Abkürzungsverzeichnis

AGB	Allgemeine Geschäftsbedingungen
AktG	Aktiengesetz
AO	Abgabenordnung
ArbSchG	Arbeitsschutzgesetz
AWV	Arbeitsgemeinschaft für wirtschaftliche Verwaltung e.V.
BaFin	Bundesanstalt für Finanzdienstleistungsaufsicht
BDSG	Bundesdatenschutzgesetz
BetrVG	Betriebsverfassungsgesetz
BGB	Bürgerliches Gesetzbuch
BGB-InfoV	BGB-Informationspflichten-Verordnung
BGBl	Bundesgesetzblatt
BGH	Bundesgerichtshof
BHO	Bundeshaushaltsordnung
BildscharbV	Bildschirmarbeitsverordnung
BITKOM	Bundesverband Informationswirtschaft, Telekommunikation und neue Medien e. V.
BITV	Barrierefreie Informationstechnik-Verordnung
BMF	Bundesfinanzministerium
BSI	Bundesamt für Sicherheit in der Informationstechnik
BSIG	BSI-Gesetz
BVB	Besondere Vertragsbedingungen für die Beschaffung von DV-Leistungen
BVerfG	Bundesverfassungsgericht
CD-ROM	Compact Disc Read-Only Memory
CIO	Chief Information Oficer
COBIT	Control Objectives for Information and Related Technology
DCGK	Deutsche Corporate Governance Kodex
DIN	Deutsches Institut der Normung e.V.
DV	Datenverarbeitung
EBGB	Einführungsgesetz zum Bürgerlichen Gesetzbuche
EDI	Electronic Data Interchange
ElektroG	Elektro- und Elektronikgerätegesetz
E-Mail	Electronic Mail
EVB-IT	Ergänzende Vertragsbedingungen für die Beschaffung von Informationstechnik
EU	Europäische Union
EuGH	Europäischen Gerichtshofs

FG	Finanzgericht
GG	Grundgesetz
GDPdU	Grundsätze zum Datenzugriff und zur Prüfbarkeit digitaler Unterlagen
GmbH	Gesellschaft mit beschränkter Haftung
GmbHG	Gesetz betreffend die Gesellschaften mit beschränkter Haftung
GoBIT	Grundsätze ordnungsmäßiger Buchführung beim IT-Einsatz
GoBS	Grundsätze ordnungsmäßiger DV-gestützter Buchführungs-systeme
HGB	Handelsgesetzbuch
IEC	International Electrotechnical Commission
IHK	Industrie- und Handelskammer
IKS	Internes Kontrollsystem
IMS	Identity Management Systems
ISO	International Organization for Standardization
IT	Informationstechnologie
ITSEC	Information Technology Security Evaluation Criteria (dt. *Kriterien für die Bewertung der Sicherheit von Systemen der Informationstechnik*)
IuKDG	Informations- und Kommunikationsdienste-Gesetz
KontraG	Gesetz zur Kontrolle und Transparenz im Unternehmens-bereich
KWG	Kreditwesengesetz
LG	Landgericht
LOI	Letter of Intent
MaRisk	Mindestanforderungen an das Risikomanagement
NYSE	New York Stock Exchange
OECD	Organisation for Economic Co-operation and Development (dt. *Organisation für wirtschaftliche Zusammenarbeit und Entwicklung*)
OLG	Oberlandesgericht
OWiG	Gesetz über Ordnungswidrigkeiten
RR	referenzieretes Regelwerk
RW	referenzierendes Regelwerk
SOX	Sarbanes-Oxley Act
SigG	Signaturgesetz
SigV	Signaturverordnung
SIMAT	Stralsund Information Management Team
SLA	Service Level Agreement

TDDSG	Teledienstedatenschutzgesetz
TDG	Teledienstegesetz
TKG	Telekommunikationsgesetz
TKÜV	Telekommunikations-Überwachungsverordnung
TMG	Telemediengesetz
UrhG	Gesetz gegen den unlauteren Wettbewerb
US	United States
USA	United States of America
UStG	Umsatzsteuergesetz
UWG	Gesetz gegen den unlauteren Wettbewerb
W3C	World Wide Web Consortium
WphG	Wertpapierhandelsgesetz
ZPO	Zivilprozessordnung

Quellenangaben

AWV o.J.: AWV Arbeitsgemeinschaft für wirtschaftliche Verwaltung e.V.: Auslegung der GoB beim Einsatz neuer Organisationstechnologien, Arbeitskreis 3.4. Online verfügbar unter: http://www.awv-net.de/cms/index-b-80-136.html (Zugriff am 13.05.2011).

Bachmann 2009: Bachmann, W.: Rechtliche Rahmenbedingungen für das IT-Management. In: Tiemeyer, E. (Hrsg.): IT-Management – Konzepte, Methoden, Lösungen und Arbeitshilfen für die Praxis , 3. Aufl., München: Carl Hanser Verlag 2009, S. 666-707.

BITKOM/DIN 2009: Bundesverband Informationswirtschaft, Telekommunikation und neue Medien e. V. (BITKOM), Deutsches Institut der Normung e.V. (DIN) (Hrsg.): Kompass der IT-Sicherheitsstandards – Leitfaden und Nachschlagewerk 4. Auflage, Berlin: BITKOM 2009. Online verfügbar unter: http://www.bitkom.org/files/documents/Kompass_der_IT-Sicherheitsstandards_web.pdf (Zugriff am 13.05.2011).

Deutscher Bundestag o.J.: Deutscher Bundestag: Regierung will Datenschutz der Arbeitnehmer stärken. Online verfügbar unter: http://www.bundestag.de/bundestag/aktuell/33464449_kw08_sp_arbeitnehmer_datenschutz.jsp (Zugriff am 13.05.2011).

Grummer/Seeburg 2010: Grummer, J.-M.; Seeburg, J.: SOX Compliance. In: Behringer, S. (Hrsg.): Compliance kompakt – Best Practice im Compliance-Management. Berlin: Erich Schmidt Verlag 2010, S.211-232.

Hauschka 2010: Hauschka, Ch. E.: § 1, Einführung. In: Hauschka, Ch. E. (Hrsg.): Corporate Compliance – Handbuch der Haftungsvermeidung im Unternehmen, 2. überarb. und erw. Aufl., München: Beck 2010, S. 1-25.

ITGI 2005: IT Governance Institute (ITGI): COBIT 4.0. Deutsche Ausgabe, Rolling Meadows: ITGI 2005.

Kaminski 2010: Kaminski, I.: Grundlagen und aktuelle Entwicklungen der digitalen Betriebsprüfung. In: Klotz, M. (Hrsg.): SIMAT Arbeitspapiere, Stralsund: FH Stralsund, SIMAT Stralsund Information Management Team, 2010 (SIMAT AP, 2 (2010), 8).

Klotz 2009: Klotz, M.: IT-Compliance – Ein Überblick. Heidelberg: dpunkt-Verlag 2009.

Klotz/Dorn 2008: Klotz, M.; Dorn, D.-W., IT-Compliance – Begriff, Umfang und relevante Regelwerke. In: HMD Praxis der Wirtschaftsinformatik, Jg. 45 (2008), Nr. 263, S. 5-14.

Klotz/Dorn 2009: Klotz, M.; Dorn, D.-W.: IT-Compliance in KMU. In: Der Betriebswirt 2009, 50. Jg., Heft 1, S. 23-27 und: IT-Compliance in KMU (Teil 2), in: Der Betriebswirt 2009, 50. Jg., Heft 2, S. 17-20.

Michels/Krzeminska 2006: Michels, Th.; Krzeminska, A.: Sarbanes-Oxley Act und Six Sigma als Instrumente des Prozess-Controllings bei der AXA Konzern AG. In: v. Werder, A.; Stöber, H.; Grundei, J. (Hrsg.): Organisations-Controlling – Konzepte und Praxisbeispiele. Wiesbaden: Gabler 2006, S. 135-151.

Rath 2008: Rath, M.: Rechtliche Aspekte von IT-Compliance. In: Wecker, G.; van Laak, H. (Hrsg.). Compliance in der Unternehmenspraxis – Grundlagen, Organisation und Umsetzung. Wiesbaden: Gabler 2008, S. 119-143.

Rath/Sponholz 2009: Rath, M.; Sponholz, R.: IT-Compliance – Erfolgreiches Management regulatorischer Anforderungen. Berlin: Erich Schmidt Verlag 2009.

Schmidl 2009: Schmidl, M.: Recht der IT-Sicherheit. In: Hauschka, Ch. E. (Hrsg.): Corporate Compliance – Handbuch der Haftungsvermeidung im Unternehmen. 2. überarb. und erw. Aufl., München: Beck 2010, S. 701-807.

Teubner/Feller 2008: Teubner, A.; Feller, T.: Informationstechnologie, Governance und Compliance. In: Wirtschaftsinformatik, 2008, Jg. 50, Nr. 5, S. 400-407.

Weber/Dittrich 2010: Weber, D.; Dittrich, J.: E-Business und Internet. In: Hauschka, Ch. E. (Hrsg.): Corporate Compliance – Handbuch der Haftungsvermeidung im Unternehmen, 2. überarb. und erw. Aufl., München: Beck 2010, S. 1082-1099.

Das Stralsund Information Management Team (SIMAT)

Das von Prof. Dr. Michael Klotz geleitete „Stralsund Information Management Team“ (SIMAT) ist am Fachbereich Wirtschaft der FH Stralsund angesiedelt. Es bündelt akademische Lehre und Forschung, Weiterbildungsangebote und Projekte im Themenbereich des betrieblichen Informationsmanagements. Informationsmanagement richtet sich auf die effektive und effiziente Nutzung der informationellen Ressourcen eines Unternehmens. Diese Zielsetzung wird heute von verschiedenen spezialisierten Fachrichtungen in der Informatik, der Wirtschaftsinformatik und der Betriebswirtschaftslehre verfolgt. Das SIMAT arbeitet insofern interdisziplinär, wobei die inhaltlichen Schwerpunkte in Kompetenzzentren (Competence Center) fokussiert werden. Im Rahmen des RD&D-Ansatzes (Research, Development and Demonstration) dienen Labore, die mit aktuellen Tools des Informationsmanagements ausgestattet sind, sowohl der fachlichen Arbeit als auch zu Demonstrationszwecken. Eine intensive Kooperation mit ausgewiesenen Expertinnen und Experten sowie mit privatwirtschaftlichen Unternehmen und die Mitarbeit in anwendungsnahen Fachorganisationen gewährleisten eine praxis- und lösungsorientierte Vorgehensweise. Die Zusammenarbeit mit Lehrstühlen anderer Hochschulen, wissenschaftlichen Einrichtungen und eine umfangreiche Publikationstätigkeit stellen sicher, dass sich das SIMAT am State-of-the-Art des Informationsmanagements orientiert und diesen mitprägt. Auf diese Weise sind die Mitarbeiterinnen und Mitarbeiter des SIMAT in der Lage, anspruchsvolle Konzepte und Lösungen zu konzipieren und zu realisieren.

Das SIMAT versteht sich als Mittler zwischen akademischer Forschung und Lehre auf der einen, und der Wirtschaftspraxis auf der anderen Seite. Diese Transferaufgabe, verankert im Landeshochschulgesetz Mecklenburg-Vorpommerns, bildet den Schwerpunkt der Arbeit des SIMAT. Forschung und Lehre werden nicht als Selbstzweck begriffen, sondern führen zu handlungsrelevanten, innovativen Konzepten und Lösungen, die in die Unternehmenspraxis transferiert werden. Die berufliche Weiterbildung bildet hierbei ein wesentliches Element.

Die anwendungsnahe Forschung am SIMAT ist auf eine ökonomische Verwertung hin orientiert. Es sollen Innovationen entwickelt und in Kooperation mit anderen wissenschaftlichen Einrichtungen, Fach-Institutionen und Unternehmen in eine nachhaltige und profitable Praxis umgesetzt werden. Hierzu werden eigene F&E-Projekte auf dem Gebiet des Informationsmanagements und Innovationsprojekte mit Partnern durchgeführt. Zudem hat sich das SIMAT auf die betriebswirtschaftliche Begleitberatung bei IT-nahen Technologieprojekten spezialisiert. Studierenden und wissenschaftlichen Mitarbeiterinnen und Mitarbeitern wird die Möglichkeit eröffnet, an

der Lösung praktischer Problemstellungen zu arbeiten und sich so optimal auf das spätere Berufsleben vorzubereiten.

Die studentischen Mitarbeiterinnen und Mitarbeiter erhalten im SIMAT Einblick in die Arbeitsmethodik sowohl auf wissenschaftlichem als auch auf wirtschaftlichem Gebiet. Aus den Projekten des SIMAT entstehen zahlreiche Abschlussarbeiten, die den Studierenden der FH Stralsund offen stehen. Das SIMAT bietet zudem eine berufliche Perspektive für Studierende, die sich als wissenschaftliche Mitarbeiter in der anwendungsnahen Forschung qualifizieren wollen.

Das SIMAT beteiligt sich zudem an der Diskussion der wissenschaftlichen Gemeinschaft. Hierzu werden regelmäßig Arbeitspapiere veröffentlicht, die den Stand der Arbeit des SIMAT in die Öffentlichkeit tragen und zur Diskussion anregen sollen. Das SIMAT lädt zudem andere Wissenschaftler, aber auch Referenten aus der Praxis als Vortragende ein. Auf diese Weise lernen die SIMAT-Mitarbeiterinnen und -Mitarbeiter sowie andere interessierte Studierende aktuelle Forschungsergebnisse und praktische Fragestellungen aus erster Hand kennen. Erkenntnisse aus diesen Aktivitäten sowie aus den verschiedenen F&E-Projekten werden systematisch in die Lehre überführt, so dass alle Studierenden von der Forschungsarbeit des SIMAT profitieren können.

Zum Zwecke des ökonomischen Transfers verfolgt das SIMAT den RD&D-Ansatz (Research, Development and Demonstration). Hierzu wird ein Labor als Demonstrationsbereich unterhalten, das einerseits als Testbed, andererseits als Showroom dient.

- Testbed: Im Rahmen des Testbed werden Produkte und Lösungen von Kooperationspartnern des SIMAT in den Bereichen des Informations-, Projekt- und Prozessmanagements betrieben. Auf dieser technischen Grundlage werden im Rahmen von Projekten durch das SIMAT-Team prototypische Lösungen erarbeitet.
- Showroom: Im Showroom werden die erarbeiteten Lösungen und komplexe Nutzungen der verfügbaren Technologie einem Auditorium präsentiert. Hierbei werden sowohl prototypische als auch praktisch erprobte Realisierungen gezeigt.

Kontakt

FH Stralsund • SIMAT • Zur Schwedenschanze 15 • 18435 Stralsund
Ansprechpartner: Prof. Dr. Michael Klotz (Wissenschaftlicher Leiter)
☎ +49 (0)3831 45-6946
✉ michael.klotz@fh-stralsund.de
🌍 www.simat-stralsund.de

Verzeichnis der SIMAT-Arbeitspapiere

AP	Datum	Autor	Titel
01-09-001	01.2009	M. Klotz	Datenschutz in KMU – Lehren für die IT-Compliance
01-09-002	02.2009	M. Klotz	Von der Informationsgesellschaft zum Informationsarbeiter
01-09-003	09.2009	L. Ramin M. Klotz	Aufgaben und Verantwortlichkeiten von IT-Nutzern anhand von COBIT
01-09-004	10.2009	S. Kubisch	Corporate Governance gemäß BilMoG und SOX
02-10-005	06.2010	M. Klotz	PMBOK-Compliance der Projekt-management-Software Projektron BCS
02-10-006	07.2010	A. Woltering	Kontinuierliche Verbesserung von Desktop-Services mittels Benchmarking
02-10-007	09.2010	M. Klotz	Grundlagen der Projekt-Compliance
02-10-008	11.2010	I. Karminski	Grundlagen und aktuelle Entwicklungen der digitalen Betriebsprüfung
02-10-009	12.2010	D. Engel/ N. Zdrowomyslaw	Benchmarking Studie Stralsund
03-11-010	02.2011	E. Tiemeyer	Kennzahlengestütztes IT-Projektcontrol-ling – Projekt-Scorecards einführen und erfolgreich nutzen
03-11-011	05.2011	M. Klotz	Regelwerke der IT-Compliance – Klassifikation und Übersicht Teil 1: Rechtliche Regelwerke