Klotz, Michael

Working Paper

Regelwerke der IT-Compliance - Klassifikation und Übersicht, Teil 1: Rechtliche Regelwerke (2., überarbeitete und erweiterte Auflage)

SIMAT Arbeitspapiere, No. 04-12-020

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

Suggested Citation: Klotz, Michael (2012) : Regelwerke der IT-Compliance - Klassifikation und Übersicht, Teil 1: Rechtliche Regelwerke (2., überarbeitete und erweiterte Auflage), SIMAT Arbeitspapiere, No. 04-12-020, Fachhochschule Stralsund, Stralsund Information Management Team (SIMAT), Stralsund, https://nbn-resolving.de/urn:nbn:de:0226-simat04120202

This Version is available at:
https://hdl.handle.net/10419/65374

SIMAT Arbeitspapiere
Herausgeber: Prof. Dr. Michael Klotz

SIMAT AP 04-12-020

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

Prof. Dr. Michael Klotz

2., überarbeitete und erweiterte Auflage

Fachhochschule Stralsund
SIMAT Stralsund Information Management Team

September 2012

ISSN 1868-064X

Klotz, Michael: Regelwerke der IT-Compliance – Klassifikation und Übersicht, Teil 1: Rechtliche Regelwerke. In: SIMAT Arbeitspapiere. Hrsg. von Michael Klotz. 2., überarb. u. erw. Aufl. Stralsund: FH Stralsund, SIMAT Stralsund Information Management Team, 2012 (SIMAT AP, 4 (2012), 20), ISSN 1868-064X

Download über URN vom Server der Deutschen Nationalbibliothek:
http://nbn-resolving.de/urn:nbn:de:0226-simat04120202

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, aber auch Verträge. Die wichtigsten in der Praxis relevanten und in der Fachwelt diskutierten Regelwerke werden in ein „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 grundlegend hinsichtlich relevanter rechtlicher 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 – Erlass – EU-Verordnung – Informationstechnologie – IT-Compliance – IT-Vertrag – Rechtsprechung – Rechtsverordnung – Regelwerk – Satzung – Vertrag – Verwaltungsvorschrift

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

Hinweis: Aus Gründen der besseren Lesbarkeit wird in der Regel die männliche Schreibweise verwendet. Es sei an dieser Stelle ausdrücklich darauf hingewiesen, dass sowohl die männliche als auch die weibliche Schreibweise gemeint ist.

Vorwort zur 2. Auflage

Seit dem erstmaligen Erscheinen dieses Arbeitspapiers ist nunmehr ein gutes Jahr vergangen. Selbstverständlich haben sich in dieser Zeit diverse Aktualisierungen und Neuerungen ergeben. Nicht nur auf der Seite der Regelwerke, auch für den Zugang zu den verschiedenen Texten haben sich zahlreiche Änderungen vollzogen – das Internet ist an dieser Stelle schnelllebiger, als man sich dies manchmal wünscht.

Eine wesentliche Änderung betrifft die Anpassung des „House of IT-Compliance“, in das bei den rechtlichen Regelwerken einige neue „Etagen“ eingezogen werden mussten. So sind hier die Gruppen „EU-Verordnungen“, „Internationale Abkommen“, „Gesetze anderer Staaten“ sowie „Erlasse und Satzungen“ neu aufgenommen. Weiterhin wurden seit Mai 2011 weitere relevante Regelwerke identifiziert, sowohl zwischenzeitlich neu erschienene, also auch solche, die zum erstmaligen Erscheinungszeitpunkt des Arbeitspapiers zwar bereits vorhanden, aber vom Autor nicht berücksichtigt wurden. An dieser Stelle waren Hinweise von Leserinnen und Lesern des Arbeitspapiers hilfreich. All denjenigen, die die vorliegende Ausarbeitung in diesem Sinne gefördert haben, sei ausdrücklich gedankt. Auch für die Zukunft sind Rückmeldungen erbeten, die zur Aktualisierung und zur weiteren Komplettierung der Übersicht beitragen.

Außerdem wurden in dieser Vorlage einige Korrekturen vorgenommen, die Literaturgrundlage wurde ergänzt und das Literaturverzeichnis entsprechend aktualisiert.

Ich hoffe, dass diese 2. Auflage in der Praxis wieder auf geneigtes Interesse stößt und eine so gute Aufnahme findet, wie dies für die Erstauflage der Fall war.

Prof. Dr. Michael Klotz

Vorwort zur 1. Auflage

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

Abbildungsverzeichnis

Tabellenverzeichnis

Abkürzungsverzeichnis

AGB	Allgemeine Geschäftsbedingungen
AktG	Aktiengesetz
ASCII	American Standard Code for Information Interchange
AL	Ausfuhrliste
AO	Abgabenordnung
ArbSchG	Arbeitsschutzgesetz
Art	Artikel
AT	Allgemeiner Teil
AWV	Arbeitsgemeinschaft für wirtschaftliche Verwaltung e.V. Außenwirtschaftsverordnung
Az	Aktenzeichen
BADA	Bundesamt für Wirtschaft und Ausfuhrkontrolle
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
BIZ	Bank für Internationalen Zahlungsausgleich
BMF	Bundesfinanzministerium
BMI	Bundesministerium des Innern
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 Officer
COBIT	Control Objectives for Information and Related Techno- logy
CRM	Customer-Relationship-Management

DCGK	Deutsche Corporate Governance Kodex
DIN	Deutsches Institut der Normung e.V.
DV	Datenverarbeitung
EBGB	Einführungsgesetz zum Bürgerlichen Gesetzbuche
EDI	Electronic Data Interchange
EDIFACT	Electronic Data Interchange for Administration, Commerce and Transport
EFTA	European Free Trade Association
EG	Europäische Gemeinschaft
ElektroG	Elektro- und Elektronikgerätegesetz
E-Mail	Electronic Mail
EStG	Einkommensteuergesetz
EU	Europäische Union
EuGH	Europäischen Gerichtshofs
EVB-IT	Ergänzende Vertragsbedingungen für die Beschaffung von Informationstechnik
FATCA	Foreign Account Tax Compliance Act
FBI	Federal Bureau of Investigation
FG	Finanzgericht
FISC	Foreign Intelligence Surveillance Court
GenG	Gesetz betreffend die Erwerbs- und Wirtschaftsgenossen-schaften
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 Buchführungssysteme
GroMiKV	Großkredit- und Millionenkreditverordnung
GwG	Geldwäschegesetz
HGB	Handelsgesetzbuch
HIRE	Hiring Incentives to Restore Employment
IEC	International Electrotechnical Commission
IHK	Industrie- und Handelskammer
IKS	Internes Kontrollsystem

IMS	Identity Management Systems
IRC	Internal Revenue Code
ISACA	Information Systems Audit and Control Association
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 Unternehmensbereich
KWG	Kreditwesengesetz
LAG	Landesarbeitsgericht
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
PAuswG	Personalausweisgesetz
PCB	Polychlorierte Biphenyle
PCBAbfallV	PCB/PCT-Abfallverordnung
PCT	Polychlorierte Terphenyle
PublG	Gesetz über die Rechnungslegung von bestimmten Unternehmen und Konzernen
RR	referenziertes Regelwerk
RW	referenzierendes Regelwerk
SEC	Security and Exchange Commission
SOX	Sarbanes-Oxley Act
SigG	Signaturgesetz
SigV	Signaturverordnung
SIMAT	Stralsund Information Management Team
SLA	Service Level Agreement
SolvV	Solvabilitätsverordnung
TDDSG	Teledienstedatenschutzgesetz
TDG	Teledienstegesetz

TEDIS	Trade Electronic Data Interchange Systems
TKG	Telekommunikationsgesetz
TKÜV	Telekommunikations-Überwachungsverordnung
TMG	Telemediengesetz
UrhG	Gesetz gegen den unlauteren Wettbewerb
US	United States
USA	United States of America
USA PATRIOT	Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism
UStG	Umsatzsteuergesetz
UWG	Gesetz gegen den unlauteren Wettbewerb
VAG	Versicherungsaufsichtsgesetz
VermAnlG	Vermögensanlagengesetz
VO	Verordnung
VRRL	Verbraucherrechterichtlinie
WpAIV	Wertpapierhandelsanzeige- und Insiderverzeichnis-verordnung
WpDVerOV	Wertpapierdienstleistungs-Verhaltens- und Organisationsverordnung
WphG	Wertpapierhandelsgesetz
WpHMV	Wertpapierhandel-Meldeverordnung
WpÜG	Wertpapiererwerbs- und Übernahmegesetz
ZPO	Zivilprozessordnung
XBRL	eXtensible Business Reporting Language

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. einer Daten- und Dokumentenklassifizierung oder 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).[3]

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.
[3] Vgl. *Klotz 2011*, S. 593.

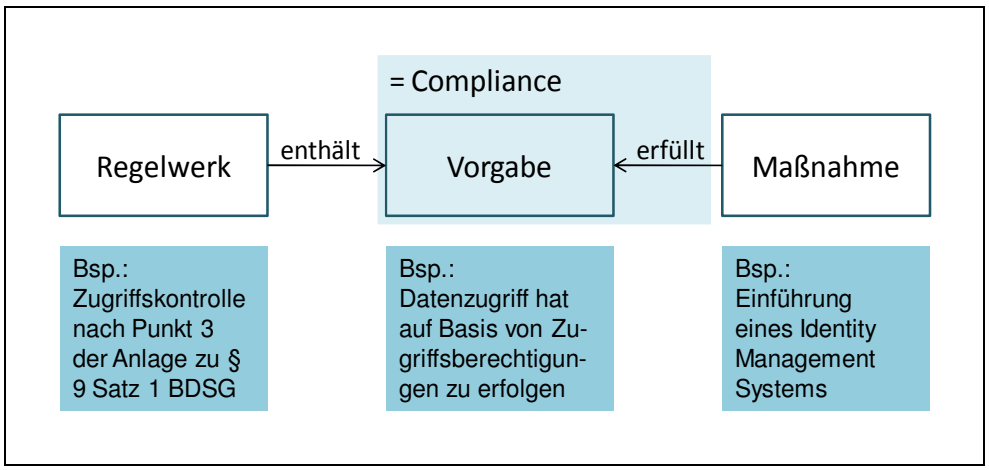

Abbildung 1
IT-Compliance als Erfüllung von Vorgaben[4]

Die Erfüllung von Vorgaben bildet somit die Basis für den Begriff der IT-Compliance. Dieser lässt sich damit 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.[5]

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.[6]

---

[4] Entnommen aus *ebd*.
[5] Vgl. *Klotz 2009*, S. 6.
[6] 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 die Compliance der IT-

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".[7] 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:[8]

Prozesse und der IT-gestützten Geschäftsprozesse auf Gesetze, Verordnungen und sonstige Rechtsvorschriften, aber auch auf vertragliche Vereinbarungen und sonstige externe Anforderungen bezieht, vgl. *ISACA 2012*, S. 213f.

[7] Vgl. *Teubner/Feller 2008*, S. 401.

[8] Nach *Klotz/Dorn 2008*, S. 9f.

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

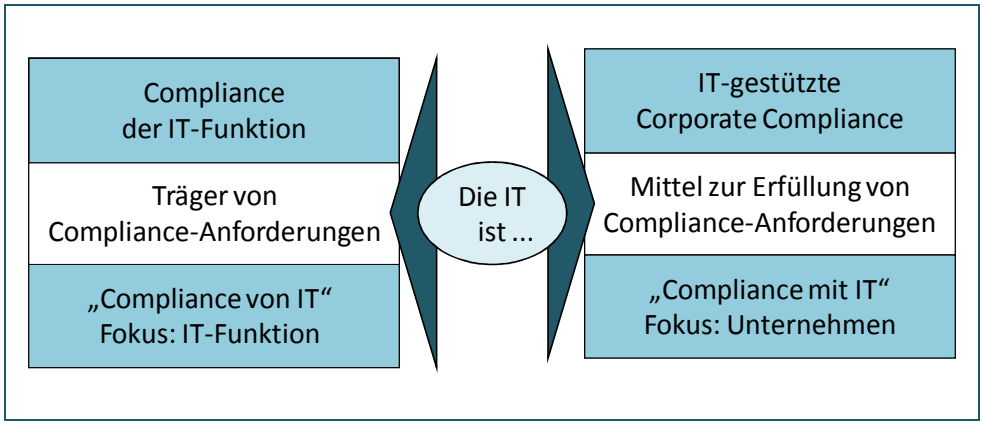

Abbildung 2
Compliance der IT-Funktion vs. IT-gestützte Corporate Compliance

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 Compliance 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 in dem vom Branchenverband BITKOM und dem DIN gemeinsam herausgegebenen „Kompass der IT-Sicherheitsstandards“[9], oder es werden zahlreiche Anwendungsbereiche, z. B. Archivierung, Datenschutz, Internes Kontrollsystem, Transparenz oder Risikomanagement, aufgeführt, 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. Hierzu gehören auch Verordnungen der Europäischen Union und ggf. auch ausländische Gesetze. EU-Verordnungen entfalten sie eine unmittelbare Durchgriffswirkung und bedürfen damit keiner Umsetzung in nationales Recht (anders als die Richtlinien der EU). So würde die derzeit als Entwurf vorliegende EU-Datenschutz-Grundverordnung[10] nach ihrer

---

[9] 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.

[10] Siehe den Vorschlag für eine „Verordnung des europäischen Parlaments und des Rates zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr (Datenschutz-Grundverordnung)“ unter

Verabschiedung und Veröffentlichung in den Mitgliedsstaaten unmittelbar geltendes Recht darstellen (und die deutschen Datenschutzgesetze wohl ganz oder in großen Teilen ablösen). Weiterhin können sich auch aus internationalen Abkommen Vorgaben für die Geschäftstätigkeit deutscher Unternehmen ergeben.

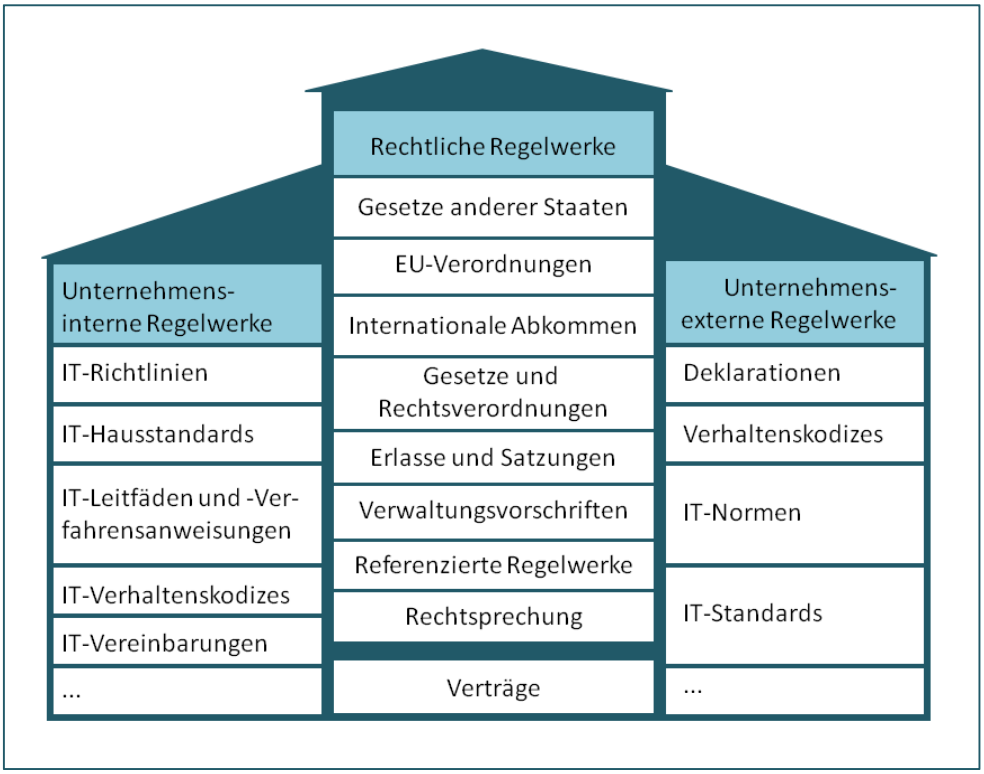

Abbildung 3
Das "House of IT-Compliance"

Offensichtlich relevant für IT-Compliance sind Gesetze, die sich schon vom Namen her auf die IT richten, wie beispielsweise das Bundesdatenschutzgesetz, das Signaturgesetz oder das Telemediengesetz.[11] 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.

Erlasse und Satzungen

Erlasse und Satzungen bilden eine weitere Gruppe. Erlasse stellen eine Anordnung von Behörden, z. B. eines Bundes- oder Landesministeriums, gegenüber ihnen nachgeordnete Dienststellen dar. Satzungen sind Rechtsnor-

http://ec.europa.eu/justice/data-protection/document/review2012/com_2012_11_de.pdf (der letzte Abruf dieser und aller folgenden Internetquellen erfolgte am 16.08.2012).

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

men, die von Gremien öffentlich-rechtlicher Körperschaften, z. B. Gemeinderäte oder Kreistage, beschlossen werden.

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.

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 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 oder des Betriebs kompletter Anwendungen an spezialisierte IT-Dienstleistungsunternehmen.

Unternehmensexterne Regelwerke

Die zweite Gruppe bilden unternehmensexterne Regelwerke[12], die sich auf die Art und Weise der IT-Nutzung beziehen. Sie reichen von Deklarationen, die im Rahmen internationaler Veranstaltungen verabschiedet wurden, über

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

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 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 111 Regelwerke, s. Tabelle 1.

Tabelle 1
Verteilung der rechtlichen Regelwerke

Gruppe			**Anzahl Regelwerke**
Gesetze anderer Staaten			3
EU-Verordnungen			3
Internationale Abkommen			1
Gesetze	IT-spezifische	6	31
	Nicht IT-spezifische	25	
Rechtsverordnungen	IT-spezifische	5	12
	Nicht IT-spezifische	7	
Erlasse, Satzungen			2
Verwaltungsvorschriften			8
Referenzierte Regelwerke			6
Rechtsprechung (Urteile)			18
Verträge	IT-Verträge	24	27
	Allgemeine Verträge	3	
Insgesamt			111

Abgrenzung: Nur aktuelle Regelwerke

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

nach zeitlichen und räumlichen Kriterien vorgenommen werden. 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. Ein anderes Beispiel sind die „Grundsätze ordnungsmäßiger Buchführung beim IT-Einsatz (GoBIT)“, die nun schon seit geraumer Zeit als Weiterentwicklung der GoBS (Grundsätze ordnungsgemäßer DV-gestützter Buchführungssysteme[13]) von der Arbeitsgemeinschaft für wirtschaftliche Verwaltung e.V. (AWV) in Zusammenarbeit mit den Finanzbehörden erarbeitet werden.[14] Als „Entwurf“ sollen an dieser Stelle auch EU-Richtlinien gelten, da ihre Vorgaben nach ihrer Verabschiedung durch den Rat der Europäischen Union und das Europäische Parlament auf der nationalen Ebene durch eine entsprechende Gesetzgebung erst noch umzusetzen sind. EU-Richtlinien mit IT-Bezug waren z. B.

- Die Richtlinie 95/46/EG vom 24.10.1995[15] zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien

---

13 Siehe unten Kap. 8.

14 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.).*

15 Siehe http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:1995:281:0031:0050:DE:PDF. 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 aufgefordert, dem Urteil des EuGH nachzukommen und die EU-Richtlinie umzusetzen. Die hierzu notwendigen

Datenverkehr wurde in Deutschland durch das „Gesetz zur Änderung des Bundesdatenschutzgesetzes und anderer Gesetze“ vom 18. Mai 2001 – allerdings verspätet – umgesetzt.

- Die Richtlinie 2010/45/EU vom 13.07.2010[16], die u. a. Vereinfachungen der elektronischen Rechnungsstellung vorsieht, wurde mit dem Steuervereinfachungsgesetz[17] vom 01.11.2011 in deutsches Recht umgesetzt.
- Der Begriff „Basel II“ steht für die im Juni 2004 veröffentlichte zweite Eigenkapitalvereinbarung des „Baseler Ausschuss für Bankenaufsicht“, der bei der „Bank für Internationalen Zahlungsausgleich“ (BIZ) angesiedelt ist. Basel II wurde auf europäischer Ebene durch die Neufassungen zweier Richtlinien[18] umgesetzt. Die nationale Umsetzung in Deutschland umfasste die Änderung des Kreditwesengesetzes (KWG), den Erlass der Solvabilitätsverordnung (SolvV) und die Neufassung der Großkredit- und Millionenkreditverordnung (GroMiKV).[19]

Für Unternehmen ist es jedoch durchaus sinnvoll, die Regelungsaktivitäten der EU im Auge zu behalten, um sich auf künftige Änderungen frühzeitig einstellen zu können. Dies gilt derzeit beispielsweise für die Richtlinie 2011/83/EU vom 25.10.2011[20], die so genannte Verbraucherrechterichtlinie (VRRL), die Informationspflichten im e-Commerce EU-weit harmonisiert und bis 13.12.2013 in nationales Recht umgesetzt sein muss.

Änderungen sind seitdem nach und nach in den einzelnen Bundesländern geregelt und vollzogen worden.

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

17 Siehe http://www.bundesfinanzministerium.de/Content/DE/Publikationen/Aktuelle_Gesetze/Gesetze_Verordnungen/010_a_StVereinfG2011.pdf?__blob=publicationFile&v=3

18 Dies sind die Richtlinie über die Aufnahme und Ausübung der Tätigkeit der Kreditinstitute (RL 2006/48/EG) und die Richtlinie über die angemessene Eigenkapitalausstattung von Wertpapierfirmen und Kreditinstituten (RL 2006/49/EG).

19 Von Relevanz für die IT-Sicherheit sind jedoch nicht die gesetzlichen Festlegungen, sondern vor allem die im Anhang der Rahmenvereinbarung aufgeführte Klassifikation der operationellen Risiken, in der sechs der sieben Risikobereiche Bezug auf IT-Risiken nehmen. Für eine umfangreiche Diskussion der Auswirkungen von Basel II auf das IT-Sicherheitsmanagement von Banken und kreditsuchenden Unternehmen siehe *Klotz 2007*.

20 Siehe http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2011:304:0064:0088:DE:PDF

Nur in D geltende Regelwerke

Weiterhin wird eine Einschränkung auf in Deutschland geltende Regelwerke vorgenommen. Aufgrund der Internationalität und der räumlichen Entgrenzung durch Informations- und Kommunikationstechnologien bedeutet dies aber nicht, dass ausländische, internationale und supranationale Regelwerke vollständig ausgeblendet werden. Entscheidend ist vielmehr, ob die Vorgaben ihre Bindungswirkung in Deutschland entfalten (auch wenn dies im Einzelfall nicht immer unumstritten ist).

Struktur der folgenden Darstellung

Die folgende Darstellung orientiert sich am „House of IT-Compliance“. 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 anderer Staaten

FATCA, SOX und USA PATRIOT Act

In dieser Gruppe der Gesetze anderer Staaten finden sich Regelwerke, die sowohl in der Öffentlichkeit als auch in der Fachdiskussion eine wesentliche Rolle spielen, allen voran der USA PATRIOT Act und der Sarbanes-Oxley Act (SOX).[21] Gleiches ist für die FATCA-Regelungen zu erwarten, die aktuell für Kreditinstitute und vor allem für Versicherungsunternehmen eine große Herausforderung darstellen.

Name	**Foreign Account Tax Compliance Act (FATCA)**
Inhalt	FATCA wurde am 18.03.2010 als Teil des US-Gesetzes „Hiring Incentives to Restore Employment Act“ (HIRE Act) erlassen. Durch FATCA werden (aus der Sicht der USA) ausländische Finanzinstitutionen verpflichtet, Daten über Kapitalerträge und Veräußerungserlöse US-amerikanischer Anleger an die US-amerikanische Steuerbehörde weiterzuleiten. Deutschland und andere europäische Staaten sowie die USA haben am 08.02.2012 eine gemeinsame Erklärung zur bilateralen Zusammenarbeit im Sinne von FATCA (d. h. zur Vermeidung der Steuerhinterziehung) herausgegeben. Am 26.07.2012 wurde ein Musterabkommen veröffentlicht, durch das die FATCA-Umsetzung auf eine zwischenstaatliche Grundlage gestellt werden soll.[22] Herausforderungen durch FATCA ergeben sich für die Unternehmens-IT hinsichtlich des Datenschutzes wegen der zustimmungspflichtigen Weitergabe personenbezogener Daten sowie für das Datenmanagement (beispielsweise hinsichtlich der Identifikation des betroffenen Personenkreises und der damit verbundenen Berechnungen und Berichtspflichten). Für die bestandsführenden Systeme ergibt sich ein entsprechender Anpassungsdarf.
Status	Die FATCA-Regelungen vom 18.03.2010 sind in den §§ 1471 bis 1474 des US-amerikanischen Bundessteuergesetzes „Internal Revenue Code“ (IRC) zu finden.
Link	zu den Texten: • FATCA-Regelungen im IRC: http://www.law.cornell.edu/uscode/text/26/subtitle-A/chapter-4 • Gemeinsame Erklärung: http://www.bundesfinanzministerium.de/Content/DE/Pressemitteilungen/Finanzpolitik/2012/02/20120208-PM-04-Anlage1.pdf?__blob=publicationFile&v=3

[21] Vgl. z. B. *Rath 2008*, S. 123f., *Grummer/Seeburg 2010*.
[22] Vgl. *Kring 2012*.

	• Musterabkommen: http://www.bundesfinanzministerium.de/Content/DE/Pressemitteilungen/Finanzpolitik/2012/07/2012-07-26-PM36-Anlage.pdf?__blob=publicationFile&v=2

Name	**Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act (USA PATRIOT Act)**
Inhalt	Der USA PATRIOT Act hat jüngst durch die Entwicklung des Cloud-Computing immens an Aktualität gewonnen. Beim USA PATRIOT Act handelt sich um ein US-amerikanisches Bundesgesetz, das am 25.10.2001 im Zuge des sog. „Krieges gegen den Terrorismus" verabschiedet wurde. Nach Section 215 (Access to Records and Other Items Under the Foreign Intelligence Surveillance Act) kann der Foreign Intelligence Surveillance Court (FISC)[23] dem FBI Zugang zu Daten aller Art bei einem Internet-Provider oder einen Cloud-Anbieter in den USA gewähren. Diese Verpflichtung kann aber auch entsprechende Unternehmen in Europa treffen, die Geschäftskontakte, sog. „minimum contacts", mit den USA pflegen (z. B. dort eine Betriebsstätte unterhalten) und Kontrolle über die von den US-amerikanischen Behörden gewünschten Zieldaten haben. Damit erweisen sich der USA PATRIOT Act und das deutsche Bundesdatenschutzgesetz als inkompatibel.[24]
Status	US-amerikanisches Bundesgesetz vom 25.10.2001
Link	zum Text: http://epic.org/privacy/terrorism/hr3162.html/

Name	**Sarbanes-Oxley Act (SOX)**
Inhalt	Der Sarbanes-Oxley Act ist ein im Jahr 2002 erlassenes US-Bundesgesetz, das in Folge diverser Unternehmensskandale um Manipulationen und Bilanzfälschungen[25] Regelungen für die Corporate Governance von Unternehmen traf. Dieses US-Gesetz ist für diejenigen Unternehmen relevant, die bei der US-Börsenaufsicht SEC (Security and Exchange Commission) registriert sind – inklusive deren Tochtergesellschaften – sowie deren Wirtschaftsprüfer.[26] Somit sind auch deutsche Tochtergesellschaften von bei der SEC registrierten

[23] Der FISC ist ein Bundesgericht der USA, das die Überwachungsaktivitäten der US-amerikanischen Auslandsgeheimdienste regelt.
[24] Vgl. die Ausführungen in *Noerr/Denton 2011*.
[25] In den USA waren dies vor allem die Betrugsfälle und Bilanzmanipulationen bei den Firmen Worldcom und Enron, in deren Folge es zu Unternehmenszusammenbrüchen, Strafverfolgungen und Verurteilungen, gar zu Selbstmorden der Verantwortlichen kam.
[26] Nach *Rüter/Schröder/Göldner 2006*, S. 117.

	Unternehmen betroffen. Dies trifft z. B. für die AXA Konzern AG zu, deren französische Muttergesellschaft an der New Yorker Börse NYSE notiert ist. [27] 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.
Status	US-Bundesgesetz, am 30.07.2002 in Kraft gesetzt
Link	zum Text: http://www.gpo.gov/fdsys/pkg/PLAW-107publ204/pdf/PLAW-107publ204.pdf

[27] Nach *Michels/Krzeminska 2006*, S, 141.

3. EU-Verordnungen

Im Rahmen der Terrorismusbekämpfung wurden von der EU folgende Anordnungen erlassen, die von allen importierenden und exportierenden Unternehmen sowie Kreditinstituten und Versicherungen zu beachten sind.

Name	**Verordnung (EG) Nr. 2580/2001 des Rates vom 27. Dezember 2001 über spezifische, gegen bestimmte Personen und Organisationen gerichtete restriktive Maßnahmen zur Bekämpfung des Terrorismus**
Inhalt	Mit der Verordnung (EG) Nr. 2580/2001 vom 27. Dezember 2001 hat die EU auf der Grundlage der Resolution 1373 (2001) des Sicherheitsrates der Vereinten Nationen Embargomaßnahmen gegen Personen und Organisationen getroffen, die terroristische Handlungen begehen, zu begehen versuchen, an diesen beteiligt sind, diese fördern oder erleichtern.
Status	Verordnung (EG) Nr. 2580/2001 des Rates vom 27. Dezember 2001, zuletzt geändert durch die Durchführungsverordnung (EU) Nr. 610/2010 des Rates vom 12. Juli 2010
Link	zum Text: http://p106764.typo3server.info/fileadmin/kost/Dokumetne/vo_eg_2580_2001.pdf

Name	**Verordnung (EG) Nr. 881/2002 des Rates vom 27. Mai 2002 über die Anwendung bestimmter spezifischer restriktiver Maßnahmen gegen bestimmte Personen und Organisationen, die mit Osama bin Laden, dem Al-Qaida-Netzwerk und den Taliban in Verbindung stehen, und zur Aufhebung der Verordnung (EG) Nr. 467/2001 des Rates über das Verbot der Ausfuhr bestimmter Waren und Dienstleistungen nach Afghanistan, über die Ausweitung des Flugverbots und des Einfrierens von Geldern und anderen Finanzmitteln betreffend die Taliban von Afghanistan**
Inhalt	Mit der Verordnung (EG) Nr. 881/2002 des Rates vom 27. Mai 2002 verabschiedete die EU auf der Grundlage der Resolution 1390 (2002) des Sicherheitsrates der Vereinten Nationen vom 16. Januar 2002 Maßnahmen zur Bekämpfung des Terrorismus. Sie richtet sich gegen Personen, Organisationen und Vereinigungen, die in der Namensliste des Sanktionsausschusses der Vereinten Nationen enthalten sind.
Status	Verordnung (EG) Nr. 881/2002 des Rates vom 27. Mai 2002, zuletzt geändert durch die Durchführungsverordnung (EU) Nr. 718/2012 der Kommission vom 07. August 2012
Link	zum Text: http://www.zoll.de/SharedDocs/Downloads/DE/Vorschriften/Aussenwirt

	schaft-Bargeldverkehr/vo_eg_881_2002.pdf zur Namensliste des Sanktionsausschusses der Vereinten Nationen: http://www.un.org/sc/committees/1267/aq_sanctions_list.shtml

Datenabgleich

Beide Verordnungen sehen vor, dass Gelder, andere finanzielle Vermögenswerte und wirtschaftliche Ressourcen der gelisteten Personen, Organisationen, Vereinigungen und Unternehmen eingefroren werden. Ihnen dürfen zudem keine Gelder, sonstigen finanziellen Vermögenswerte, wirtschaftliche Ressourcen oder Finanzdienstleistungen zur Verfügung gestellt werden.[28] Um diesen Verpflichtungen zu genügen, müssen Organisations- und Personenstammdaten mit den entsprechenden Sanktionslisten abgeglichen werden. Dies betrifft nicht nur die selbst erfassten und gepflegten Daten, sondern auch z. B. im Rahmen von Marketingaktionen zugekaufte Daten. Eine entsprechende Prüfsoftware sollte Treffer identifizieren und für eine weitere Überprüfung bzw. eine spätere Übermittlung zur Verfügung stellen. Nach Artikel 4 Absatz 1 VO (EG) Nr. 2580/2001 und Artikel 5 Absatz 1 VO (EG) Nr. 881/2002 sind bei Übereinstimmungen die Daten der betreffenden Geschäftsbeziehung an die zuständigen Behörden zu übermitteln.

Dual-Use-Verordnung

Auch die folgendete, so genannte „Dual-Use-Verordnung“ enthält Vorgaben, die sich explizit auch an die IT richten. In diesem Zusammenhang ist auch die Außenwirtschaftsverordnung (AWV) nebst zugehöriger Anlage zu sehen, die weitergehende verfahrenstechnische Vorgaben trifft.[29]

Name	**Verordnung (EG) Nr. 428/2009 des Rates vom 5. Mai 2009 über eine Gemeinschaftsregelung für die Kontrolle der Ausfuhr, der Verbringung, der Vermittlung und der Durchfuhr von Gütern mit doppeltem Verwendungszweck (EG-Dual-Use-VO)**
Inhalt	Die Dual-Use-Verordnung der EU soll sicherstellen, dass Güter mit doppeltem Verwendungszweck bei ihrer Ausfuhr aus der Europäischen Gemeinschaft wirksam kontrolliert werden. Hierbei werden Software und Technologie, also auch Informationstechnologie, ausdrücklich und umfangreich erwähnt. Als Ausfuhr wird auch die Übertragung von Software mittels elektronischer Medien (z. B. E-Mail, Datenträger) angesehen. Der Anhang I beinhaltet in der Liste der Güter mit doppeltem Verwendungszweck in der Kategorie 5 die Ausfuhrbeschränkungen für Telekommunikation und „Informationssicherheit“.
Status	Verordnung (EG) Nr. 428/2009 des Rates vom 5. Mai 2009

[28] Nach *BAFA 2009*, S. 5ff.
[29] Siehe Abschnitt 6.2.

	(Neufassung)
Link	zum Text: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2009:134:0001:0269:DE:PDF

4. Internationale Abkommen

Die Gruppe der internationalen Abkommen richtet sich auf bi- und multilaterale Verträge zwischen Staaten.

Name	**Abkommen zwischen der Europäischen Wirtschaftsgemeinschaft und der Schweizerischen Eidgenossenschaft über den elektronischen Datentransfer für kommerzielle Zwecke**
Inhalt	Dieses Abkommen regelt die Beteiligung der Schweiz am TEDIS-Programm[30] der Gemeinschaft. Hierdurch soll für den (elektronischen) Geschäftsverkehr die Errichtung neuer technischer Handelsschranken zwischen der Gemeinschaft und den Mitgliedstaaten der EFTA, in diesem Falle der Schweiz, verhindert werden
Status	Abkommen vom 07.12.1989
Link	zum Text: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:21989A1230(19):DE:NOT

[30] TEDIS steht für „Trade Electronic Data Interchange Systems“. Das TEDIS-Programm der Europäischen Gemeinschaft sollte die Einführung von EDI-Normen, die Verbesserung der europäischen Telekommunikatinsinfrastruktur und die Durchsetzung von Sicherheitsmaßnahmen bewirken. „Mit TEDIS wurden bis 1992 Normen vereinheitlicht und die internationale Norm Edifact in der Automobilbranche, der chemischen Industrie, der Elektronik- und Computerindustrie, dem Vertrieb und Einzelhandel und im Transportbereich eingeführt“ (http://www.europa-digital.de/service/abc/glossarstu.shtml#tedis).

5. Gesetze

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

5.1 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 damit von den Ermächtigungsvorschriften der §§ 27 ff. BDSG gedeckt ist.[31] Weiterhin werden u. a. die Bestellung eines Datenschutzbeauftragten, der Umfang der Betroffenenrechte, Transparenz und Dokumentation sowie die Nachvollziehbarkeit von Zugriffen, Änderungen und Weitergaben personenbezogener Daten an Dritte geregelt. Von besonderer Bedeutung für Unternehmen sind diesbezüglich die Regelungen des § 11 BDSG zur Auftragsdatenverarbeitung. Kommen einem Unternehmen Daten abhanden oder werden diese unrechtmäßig weitergeleitet, also im Falle typischer „Datenpannen“[32], regelt § 42a BDSG die Pflicht zur Mitteilung des Vorfalls an die Aufsichtsbehörde. 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.[33]
Status	Fassung vom 14. Januar 2003 (BGBl. I S. 66); zuletzt geändert durch

[31] Beschreibung der Gesetzesinhalte hier und im Folgenden nach *Klotz/Dorn 2009*.
[32] Beispiele für Datenpannen sind zu finden unter: http://www.datenleck.net/
[33] So beispielsweise *Schmidl 2009*, Rn. 13ff.

	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	**De-Mail-Gesetz**
Inhalt	Das De-Mail-Gesetz vom 28. April 2011 richtet sich an die Anbieter von De-Mail-Diensten und regelt die von ihnen erbrachten Dienste.
Status	Fassung vom 28. April 2011 (BGBl. I S. 666), geändert durch Artikel 2 Absatz 3 des Gesetzes vom 22. Dezember 2011 (BGBl. I S. 3044)
Link	zum Text: http://www.gesetze-im-internet.de/de-mail-g/BJNR066610011.html

Name	**BSIG – Gesetz über das Bundesamt für Sicherheit in der Informationstechnik (BSI-Gesetz)**
Inhalt	Das BSIG richtet sich zwar nur an das Bundesamt für Sicherheit in der Informationstechnik. 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. eine 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)

Link	zum Text: http://www.gesetze-im-internet.de/sigg_2001/BJNR087610001.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.[34] 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. § 109a enthält zudem Vorgaben zur Informationspflicht im Falle einer Verletzung des Schutzes personenbezogener Daten sowie Dokumentationspflichten in diesem Zusammenhang.
Status	Fassung vom 22. Juni 2004 (BGBl. I S. 1190), zuletzt geändert durch Artikel 1 des Gesetzes vom 3. Mai 2012 (BGBl. I S. 958)
Link	zum Text: http://www.gesetze-im-internet.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

[34] Diese Auffassung wird kontrovers diskutiert. Jüngst hat das LAG Berlin-Brandenburg anders entschieden und die Einstufung eines Unternehmens, das private E-Mail-Nutzung erlaubt hatte, als Telekommunikationsdiensteanbieter verneint, s. Kapitel 10.

	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

5.2 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 sowie an die Durchführung des elektronischen Geschäftsverkehrs) zu erfüllen.

Name	**AktG – Aktiengesetz**
Inhalt	Mehrere Reglungen des Aktiengesetzes beziehen sich auf die Nutzung der Kommunikationstechnik. So hat die Übermittlung von Eintragungen und Dokumenten nach § 45 AktG elektronisch zu erfolgen. Für die Durchführung der Hauptversammlung können nach § 118 elektronische Kommunikationsmittel genutzt werden. Zudem sind nach § 121 Abs. 3 i. V. m. § 124a AktG 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 AktG (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 AktG festgeschriebenen Sorgfaltspflichten[35] eine Verankerung für eine Verantwortung des Vorstands für IT-Compliance, IT-Risiko- und IT-Sicherheitsmanagement.[36]
Status	Fassung vom 6. September 1965 (BGBl. I S. 1089), zuletzt geändert durch Artikel 2 Absatz 49 des Gesetzes vom 22. Dezember 2011 (BGBl. I S. 3044)
Link	zum Text: http://bundesrecht.juris.de/aktg/BJNR010890965.html

[35] Für die GmbH findet sich die entsprechende Regelung in § 43 GmbHG.
[36] Vgl. *Rath/Sponholz 2009*, S. 68f.

Name	**AO – Abgabenordnung**
Inhalt	Die AO ist der Kern des deutschen Steuerrechts. Für IT-Compliance sind die §§ 145ff. 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 Unterlagen 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 9 des Gesetzes vom 21. Juli 2012 (BGBl. I S. 1566)
Link	zum Text: http://www.gesetze-im-internet.de/ao_1977/BJNR006130976.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 und § 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 zu (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 §§ 312 b bis f BGB Regelungen zur Nutzung von IT (u. a. E-Mails, Tele- und Mediendienste) und legt in § 312g Pflichten im elektronischen Geschäftsverkehr fest. So muss z. B. nach § 312g 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. Nach § 312g Absatz 3 BGB ist bei einer zahlungspflichtigen Bestellung eine ausdrückliche Bestätigung erforderlich. 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 BGB).
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 10. Mai 2012 (BGBl. I S. 1084)
Link	zum Text: http://www.gesetze-im-internet.de/bgb/BJNR001950896.html

Name	**EBGB – Einführungsgesetz zum Bürgerlichen Gesetzbuche**
Inhalt	Das EBGB enthält in Artikel 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. Art 246 § 3 EBGB trifft verschiedene Vorgaben zu den Informationspflichten bei Verträgen im elektronischen Geschäftsverkehr, z. B. nach Art 246 § 3 Nr. 1 EBGB über die einzelnen technischen Schritte, die zu einem Vertragsabschluss führen. Nach Art 246 § 3 Nr. 5 EBGB hat ein Unternehmen seine Kunden außerdem über Verhaltenskodizes, denen es sich unterwirft, sowie den Zugang zu diesen Regelwerken zu unterrichten.

Status	Fassung der Bekanntmachung vom 21. September 1994 (BGBl. I S. 2494; 1997 I S. 1061), zuletzt geändert durch Artikel 2 des Gesetzes vom 27. Juli 2011 (BGBl. I S. 1600, 1942)
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	Das ElektroG richtet sich entsprechend § 2 Abs. 1 auch auf Geräte der Informations- und Telekommunikationstechnik; diese werden in Anhang I explizit aufgeführt (z. B. Großrechner, Minicomputer, PCs, Drucker). Nicht mehr benötigte Hardware (z. B. infolge einer Ersatzbeschaffung) muss auch vom gewerblichen Nutzer entsorgt werden. Hierbei ist die Pflicht gemäß § 9 Abs. 1 ElektroG zu berücksichtigen, Altgeräte einer getrennten Versorgung bei einem öffentlich-rechtlichen Entsorgungsträger zuzuführen.
Status	Fassung vom 16. März 2005 (BGBl. I S. 762), zuletzt geändert durch Artikel 3 des Gesetzes vom 24. Februar 2012 (BGBl. I S. 212)
Link	zum Text: http://www.gesetze-im-internet.de/elektrog/BJNR076200005.html

Name	**EStG – Einkommensteuergesetz**
Inhalt	Nach § 5b EStG besteht die Pflicht, „Inhalt der Bilanz sowie der Gewinn- und Verlustrechnung nach amtlich vorgeschriebenem Datensatz durch Datenfernübertragung zu übermitteln“ (sog. E-Bilanz). Nach § 52 Abs. 15a gilt dies erstmals ab dem Wirtschaftsjahr 2011.
Status	Fassung vom 8. Oktober 2009 (BGBl. I S. 3366, 3862), zuletzt geändert durch Artikel 3 des Gesetzes vom 8. Mai 2012 (BGBl. I S. 1030)
Link	zum Text: http://www.gesetze-im-internet.de/estg/BJNR010050934.html

Name	**GmbHG – Gesetz betreffend die Gesellschaften mit beschränkter Haftung**
Inhalt	Nach § 12 Satz 2 GmbHG kann im Gesellschaftvertrag festgelegt werden, dass Bekanntmachungen der Gesellschaft in elektronischen Informationsmedien erfolgen.
Status	Bereinigte, im Bundesgesetzblatt Teil III, Gliederungsnummer 4123-1, veröffentlichte Fassung, zuletzt geändert durch Artikel 2 Absatz 51 des

	Gesetzes vom 22. Dezember 2011 (BGBl. I S. 3044)
Link	zum Text: http://www.gesetze-im-internet.de/gmbhg/BJNR004770892.html

Name	**GenG – Gesetz betreffend die Erwerbs- und Wirtschafts-genossenschaften (Genossenschaftsgesetz)**
Inhalt	§ 11 Abs. 4 GenG verweist auf § 12 Abs. 2 HGB. Damit sind Unterlagen für die Anmeldung der Eintragung der Genossenschaft in das Genossenschaftsregister elektronisch einzureichen.
Status	Fassung vom 16. Oktober 2006 (BGBl. I S. 2230), zuletzt geändert durch Artikel 10 des Gesetzes vom 25. Mai 2009 (BGBl. I S. 1102)
Link	zum Text: http://www.gesetze-im-internet.de/geng/BJNR000550889.html

Name	**GwG – Gesetz über das Aufspüren von Gewinnen aus schweren Straftaten (Geldwäschegesetz)**
Inhalt	Das GwG schreibt in § 4 Absatz 1 Satz 1 die Identifizierung von Vertragspartnern – also auch IT-Dienstleistern – bereits vor Begründung der Geschäftsbeziehung oder Durchführung der Transaktion vor. In § 4 GwG werden die Daten bzw. Dokumente genannt, auf die für diese Identifizierung zuzugreifen ist. Nach § 6 Absatz 2 Nr. 2 GwG kann ein elektronischer Identitätsnachweis nach § 18 des Personalausweisgesetzes oder eine elektronische Signatur bei der Feststellung der Identität zum Einsatz gelangen. Die erhobenen Informationen sind nach § 8 GwG aufzuzeichnen und für mindestens fünf Jahre aufzubewahren. Hierbei können nach § 8 Abs. 2 GwG Bild- oder andere Datenträger zum Einsatz gelangen. Hier bei „muss sichergestellt sein, dass die gespeicherten Daten mit den festgestellten Angaben übereinstimmen, während der Dauer der Aufbewahrungsfrist verfügbar sind und jederzeit innerhalb angemessener Frist lesbar gemacht werden können“.
Status	Fassung vom 13. August 2008 (BGBl. I S. 1690), zuletzt geändert durch Artikel 1 des Gesetzes vom 22. Dezember 2011 (BGBl. I S. 2959)
Link	zum Text: http://www.gesetze-im-internet.de/gwg_2008/BJNR169010008.html

Name	**HGB – Handelsgesetzbuch**
Inhalt	Das HGB stellt verschiedene Anforderungen an die elektronische Geschäftskommunikation sowie an die Verwendung von Bild- und Daten-

	trägern im Rahmen der Buchführung. Nach § 8 Abs. 1 HGB wird das Handelsregister von den Gerichten elektronisch geführt. Entsprechend sind nach § 12 Abs. 1 HGB Anmeldungen zur Eintragung in das Handelsregister und Dokumente nach § 12 Abs. 2 HGB elektronisch einzureichen. Auch die Offenlegung von Jahresabschlüssen hat elektronisch zu erfolgen; § 325 Abs. 1 regelt dies für Kapitalgesellschaften. Bei der Gestaltung der Geschäftskorrespondenz ist 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	In Bundesgesetzblatt Teil III, Gliederungsnummer 4100-1, veröffentlichte Fassung, zuletzt geändert durch Artikel 2 Absatz 39 des Gesetzes vom 22. Dezember 2011 (BGBl. I S. 3044)
Link	zum Text: http://www.gesetze-im-internet.de/hgb/BJNR002190897.html

Name	**KunstUrhG – Gesetz betreffend das Urheberrecht an Werken der bildenden Künste und der Photographie (Kunsturhebergesetz)**
Inhalt	Die Veröffentlichung von Mitarbeiterfotos richtet sich nach dem KunstUrhG. Nach § 22 Satz 1 KunstUrhG dürfen Bildnisse, also auch Fotos „nur mit Einwilligung des Abgebildeten verbreitet oder öffentlich zur Schau gestellt werden“. Dies betrifft vor allem die Verbreitung von Mitarbeiterfotos zu Image- oder Werbezwecken im Internet. Ein Schriftformerfordernis für die Einwilligung gibt es nicht, allerdings liegt die Beweislast beim Unternehmen.[37]
Status	In Bundesgesetzblatt Teil III, Gliederungsnummer 440-3, veröffentlichte bereinigte Fassung, zuletzt geändert durch Artikel 3 § 31 des Gesetzes vom 16. Februar 2001 (BGBl. I S. 266)
Link	zum Text: http://www.gesetze-im-internet.de/kunsturhg/BJNR000070907.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-

[37] Nach *Franck 2010*, S. 4; vgl. das in Kapitel 10 aufgeführte Urteil des LAG Hessen.

	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 Artikel 9 des Gesetzes vom 26. Juni 2012 (BGBl. I S. 1375)
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	**PAuswG – Gesetz über Personalausweise und den elektronischen Identitätsnachweis (Personalausweisgesetz)**
Inhalt	Das PAuswG regelt die Voraussetzungen, unter denen ein Unternehmen gemäß § 2 Abs. 3 PAuswG als Diensteanbieter die Möglichkeiten des mit dem neuen Personalausweis verbundenen elektronischen Identitätsnachweises nutzen kann. § 18 Abs. 4 und § 21 PAuswG beinhalten die Vorgaben (insbesondere für den Erwerb eines Berechtigungszertifikats), die ein Unternehmen erfüllen muss, wenn es als Diensteanbieter auftreten will.
Status	Fassung der Bekanntmachung vom 18. Juni 2009 (BGBl. I S. 1346), zuletzt geändert durch Artikel 4 des Gesetzes vom 22. Dezember 2011 (BGBl. I S. 2959)
Link	zum Text: http://www.gesetze-im-internet.de/pauswg/BJNR134610009.html

Name	**PublG – Gesetz über die Rechnungslegung von bestimmten Unternehmen und Konzernen (Publizitätsgesetz)**
Inhalt	Die für den Bundesanzeiger einzureichenden Erklärungen nach § 2 Abs. 2 PublG und § 12 Abs. 2 PublG sind elektronisch abzugeben.
Status	Fassung vom 15. August 1969 (BGBl. I S. 1189), zuletzt geändert durch Artikel 2 Absatz 47 des Gesetzes vom 22. Dezember 2011

	(BGBl. I S. 3044)
Link	zum Text: http://www.gesetze-im-internet.de/publg/BJNR011890969.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.[38] Dies sind die §§ 202a (Ausspähen von Daten), 202b (Abfangen von Daten), 202c (Vorbereiten des Ausspähens und Abfangens von Daten), 263a (Computerbetrug), 269 (Fälschung beweiserheblicher Daten), 270 (Täuschung im Rechtsverkehr bei Datenverarbeitung), 274 (Unterdrücken beweiserheblicher Daten), 303a (Datenveränderung) und 303b (Computersabotage).
Status	Fassung der Bekanntmachung vom 13. November 1998 (BGBl. I S. 3322), zuletzt geändert durch Artikel 1 des Gesetzes vom 25. Juni 2012 (BGBl. I S. 1374)
Link	zum Text: http://www.gesetze-im-internet.de/stgb/BJNR001270871.html

Name	**UrhG – Gesetz über Urheberrecht und verwandte Schutzrechte (Urheberrechtsgesetz)**
Inhalt	Das UrhG regelt in den §§ 4 und 87a bis e 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 2 Absatz 53 des Gesetzes vom 22. Dezember 2011 (BGBl. I S. 3044)
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

[38] Nach *Schmidl 2010*, Rn. 132.

	Rechnungen, deren Verwendung nach § 14 Abs. 1 der Zustimmung des Empfängers bedarf. Nach § 14 Abs. 1 UStG müssen bei einer auf elektronischem Wege übermittelte Rechnung die Echtheit der Herkunft, die Unversehrtheit des Inhalts und die Lesbarkeit der Rechnung gewährleistet sein. Darüber, wie dies sichergestellt werden kann, entscheidet nach § 14 Abs. 1 UStG Satz 5 jedes Unternehmen selbst. Dies kann nach § 14 Abs. 3 UStG aber auch erfolgen durch a) eine qualifizierte elektronische Signatur nach dem Signaturgesetz oder b) elektronischen Datenaustausch (EDI) nach Artikel 2 der Empfehlung 94/820/EG der EU-Kommission. Die Aufbewahrung elektronischer Rechnungen ist in § 14b UStG geregelt.
Status	Fassung der Bekanntmachung vom 21. Februar 2005 (BGBl. I S. 386), zuletzt geändert durch Artikel 2 des Gesetzes vom 8. Mai 2012 (BGBl. I S. 1030)
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	**VermAnlG - Gesetz über Vermögensanlagen (Vermögensanlagengesetz)**
Inhalt	Das VermAnlG regelt in § 9 Abs. 2 die Form der Veröffentlichung von Verkaufsprospekten für inländische Vermögensanlagen, insbesondere die Veröffentlichung im elektronischen Bundesanzeiger sowie in einem „elektronischen Informationsverbreitungssystem“.
Status	Fassung vom 6. Dezember 2011 (BGBl. I S. 2481
Link	zum Text: http://www.gesetze-im-internet.de/vermanlg/BJNR248110011.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 einzuhalten, also vor allem ein IT-Notfallkonzept zu erstellen.
Status	Fassung der Bekanntmachung vom 9. September 1998 (BGBl. I S. 2708), zuletzt geändert durch Artikel 2 des Gesetzes vom 26. Juni 2012 (BGBl. I S. 1375)
Link	zum Text: http://www.gesetze-im-internet.de/wphg/BJNR174910994.html

Name	**WpÜG – Wertpapiererwerbs- und Übernahmegesetz**
Inhalt	Im Falle, dass ein Unternehmen sich entscheidet, ein Angebot zum Erwerb von Wertpapieren eines Zielunternehmens abzugeben, muss es diese Entscheidung nach § 10 Abs. 1 WpÜG unverzüglich veröffentlichen. Nach § 10 Abs. 3 WpÜG hat diese Veröffentlichung durch Bekanntgabe im Internet und über ein elektronisch betriebenes Informationsverbreitungssystem zu erfolgen. Die gleiche Veröffentlichungspflicht obliegt nach § 35 Abs. 1 WpÜG einem Unternehmen, das im Rahmen einer Übernahme die Kontrolle über eine Zielgesellschaft erlangt hat. Weiterhin ist die nach § 11 WpÜG zu erstellende Angebotsunterlage nach § 14 Abs. 3 durch Bekanntgabe im Internet zu veröffentlichen.
Status	Fassung der Bekanntmachung vom 20. Dezember 2001 (BGBl. I S. 3822), zuletzt geändert durch Artikel 2 Absatz 46 des Gesetzes vom 22. Dezember 2011 (BGBl. I S. 3044)
Link	zum Text: http://www.gesetze-im-internet.de/wp_g/BJNR382210001.html

Name	**ZPO – Zivilprozessordnung**
Inhalt	§ 416a ZPO regelt die Beweiskraft des Ausdrucks eines öffentlichen elektronischen Dokuments. Weiterhin von Bedeutung für die IT ist § 425 ZPO. Hiernach kann einem Unternehmen vom Gericht aufgegeben werden, in seinem Besitz befindliche Unterlagen (Urkunden) 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 2 des Gesetzes vom 21. Juli 2012 (BGBl. I S. 1577)
Link	zum Text: http://www.gesetze-im-internet.de/zpo/BJNR005330950.html

Name	**VAG – Gesetz über die Beaufsichtigung der Versicherungs-unternehmen (Versicherungsaufsichtsgesetz)**
Inhalt	§ 31 Abs. 2 VAG verweist auf § 12 Abs. 2 HGB. Damit sind Unterlagen für die Anmeldung zum Handelsregister elektronisch einzureichen.
Status	Fassung vom 17. Dezember 1992 (BGBl. 1993 I S. 2), zuletzt geändert durch Artikel 10 des Gesetzes vom 15. März 2012 (BGBl. I S. 462)
Link	zum Text: http://www.gesetze-im-internet.de/vag/BJNR001390901.html

6. 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.

6.1 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, so dass die BGB-InfoV auf die Reisebranche beschränkt ist. So regelt § 4 BGB-InfoV die notwendigen Prospektangaben, die gemäß Absatz 3 auch bei Verwendung von Bild- und Tonträgern gelten.
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/BJNR034200002.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 in insgesamt 25 Einzelpunkten 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 2.0 – Verordnung zur Schaffung barrierefreier Informationstechnik nach dem Behindertengleichstellungsgesetz (Barrierefreie Informationstechnik-Verordnung)**
Inhalt	Die BITV 2.0 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 12. September 2011 (BGBl. I S. 1843)
Link	zum Text: http://www.gesetze-im-internet.de/bitv_2_0/BJNR184300011.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

6.2 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	**AWV – Verordnung zur Durchführung des Außenwirtschafts-gesetzes (Außenwirtschaftsverordnung)**
Inhalt	Die AWV regelt zusammen mit der Dual-Use-Verordnung[39] die deutsche Exportkontrolle. Für die Abwicklung des Verwaltungsverfahrens sieht sie in § 9 Abs. 1 die Nutzung spezifischer Systeme vor. Nach § 9 Abs. 6 AWV sind Ladungsverzeichnisse, die mittels einer Datenverarbeitungsanlage erstellt werden, auf maschinell verwertbaren Datenträgern oder durch Datenfernübertragung abzugeben. § 13 AWV regelt die Voraussetzungen für eine vereinfachte elektronische Ausfuhranmeldung. Für die Ausfuhrtätigkeit selbst sind die Regelungen von Bedeutung, dass gemäß § 4c auch eine Übermittlung von Datenverarbeitungsprogrammen oder Technologie durch Daten- oder Nachrichtenübertragungstechnik eine Ausfuhr darstellt und eine technische Unterstützungsleistung in Zusammenhang mit der Ausfuhr von Gütern auch in elektronischer Form erbracht werden kann.
Status	Fassung der Bekanntmachung vom 22. November 1993 (BGBl. I S. 1934, 2493), zuletzt geändert durch Artikel 1 der Verordnung vom 7. Juni 2012 (BAnz. 2012)
Link	zum Text: http://www.gesetze-im-internet.de/awv_1986/BJNR026710986.html

Name	**Anlage zur Einhundertneunten Verordnung zur Änderung der Ausfuhrliste – Anlage AL zur Außenwirtschaftsverordnung**
Inhalt	Teil I Abschnitt C der Ausfuhrliste benennt in Kategorie 5 Telekommunikation und „Informationssicherheit“ diejenigen IT-Güter (Waren, Datenverarbeitungsprogramme (Software) und Technologien), für die die Beschränkungen der Außenwirtschaftsverordnung und der EG-Dual-Use-VO gelten.
Status	Anlage AL zur Außenwirtschaftsverordnung – vom 31. März 2010,

[39] Siehe Kapitel 3.

	veröffentlicht im Bundesanzeiger, Jg. 62, Nr. 58a, vom 16.04.2010
Link	zum Text der Anlage: http://www.gesetze-im-internet.de/normengrafiken/banz_2010/j1351_0010.pdf

Name	**PCBAbfallV – Verordnung über die Entsorgung polychlorierter Biphenyle, polychlorierter Terphenyle und halogenierter Monomethyldiphenylmethane (Artikel 1 der Verordnung über die Entsorgung polychlorierter Biphenyle, polychlorierter Terphenyle sowie halogenierter Monomethyldiphenylmethane und zur Änderung chemikalienrechtlicher Vorschriften) (PCB/PCT-Abfallverordnung)**
Inhalt	Die PCBAbfallV regelt in § 2 Abs. 2 Nr. 2, dass Besitzer von Geräten der Informationstechnik und der Bürokommunikation, soweit technisch möglich und wirtschaftlich zumutbar, PCB-haltige Bauteile zu entfernen, getrennt zu halten und getrennt zu beseitigen haben. Zu Nachweiszwecken ist ein Register zu führen. Die diesbezügliche elektronische Speicherung regelt § 4 Abs. 3 PCBAbfallV.
Status	Fassung der Bekanntmachung vom 26. Juni 2000 (BGBl. I S. 932), zuletzt geändert durch Absatz 21 des Gesetzes vom 24. Februar 2012 (BGBl. I S. 212)
Link	zum Text: http://www.gesetze-im-internet.de/pcbabfallv/BJNR093210000.html

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 PAngV 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

Name	**WpAIV – Verordnung zur Konkretisierung von Anzeige-, Mitteilungs- und Veröffentlichungspflichten sowie der Pflicht zur Führung von Insiderverzeichnissen nach dem Wertpapierhandelsgesetz (Wertpapierhandelsanzeige- und Insiderverzeichnisverordnung)**
Inhalt	Die WpAIV regelt in Unterabschnitt 2 die Veröffentlichung und Mitteilung von Insiderinformationen. Nach § 5 WpAIV ist sicherzustellen,

	dass die Information über ein elektronisch betriebenes Informationsverbreitungssystem in die Öffentlichkeit gelangt. Für die Führung eines Insiderverzeichnisses wird in § 16 WpAIV auf § 257 Abs. 3 HGB verwiesen, wo die Aufbewahrung auf Bild- oder anderen Datenträgern geregelt wird.
Status	Fassung der Bekanntmachung vom 13. Dezember 2004 (BGBl. I S. 3376), zuletzt geändert durch Artikel 3 des Gesetzes vom 26. Juni 2012 (BGBl. I S. 1375)
Link	zum Text: http://www.gesetze-im-internet.de/wpaiv/BJNR337600004.html

Name	**WpDVerOV – Verordnung zur Konkretisierung der Verhaltensregeln und Organisationsanforderungen für Wertpapierdienstleistungsunternehmen (Wertpapierdienstleistungs-Verhaltens- und Organisationsverordnung)**
Inhalt	Die WpDVerOV regelt in § 3 die Voraussetzungen für die Bereitstellung von Informationen durch Wertpapierdienstleistungsunternehmen für ihre Kunden über das Internet. Die dem Kunden zur Verfügung zu stellenden Informationsblätter über Finanzinstrumente dürfen nach § 5 a Abs. 2 WpDVerOV auch als elektronisches Dokument bereitgestellt werden.
Status	Fassung der Bekanntmachung vom 20. Juli 2007 (BGBl. I S. 1432), zuletzt geändert durch Artikel 5 des Gesetzes vom 5. April 2011 (BGBl. I S. 538)
Link	zum Text: http://www.gesetze-im-internet.de/wpdverov/BJNR143200007.html

Name	**WpHMV – Verordnung über die Meldepflichten beim Handel mit Wertpapieren und Derivaten (Wertpapierhandel-Meldeverordnung)**
Inhalt	Die WpHMV regelt in Abschnitt 3 die technischen Voraussetzungen für die Übermittlung der Mitteilungen nach § 9 des Wertpapierhandelsgesetzes an die Bundesanstalt für Finanzdienstleistungsaufsicht. So regelt § 12 WpHMV das Format (ASCII), § 13 WpHMV trifft Vorgaben für die zulässigen Datenträger und Übertragungswege (z. B. Mailbox, Festverbindung, Diskette).
Status	Fassung der Bekanntmachung vom 21. Dezember 1995 (BGBl. I S. 2094; 1996 I S. 220), zuletzt geändert durch Artikel 1 der Verordnung vom 18. Dezember 2007 (BGBl. I S. 3014)
Link	zum Text: http://www.gesetze-im-internet.de/wphmv/BJNR209400995.html

7. Erlasse und Satzungen

Beispiele für Erlasse und Satzungen mit IT-Bezug finden sich eher der Ebene der Gemeinden oder Bundesländer. Insofern ist der Kreis der betroffenen Unternehmen begrenzt. Zudem sind lediglich einzelne Branchen und Verwaltungsbereiche betroffen. Insofern sollen die nachfolgend genannten Regelwerke als exemplarische Beispiele dienen.

Name	**Erlass über das Informationsmanagement der Naturschutzverwaltung in Rheinland-Pfalz (Informationserlass)**
Inhalt	Zweck dieses Erlasses ist die Gewinnung, Verarbeitung und Verbreitung raumbezogener digitaler Naturschutzinformationen. Der Erlass benennt informationspflichtige Stellen, Auskunftspersonen und raumbezogene digitale Naturschutzinformationen und konkretisiert den Zugang zu den Naturschutzinformationen bzw. ihre Verbreitung durch die Naturschutzverwaltung.
Status	Erlass vom 22. Juni 2001 in der Fassung vom 30. März 2006
Link	zum Text: http://www.naturschutz.rlp.de/index.php?id=22&pid1=43

Name	**Kurabgabesatzung für die Stadt Plau am See**
Inhalt	Die Kurabgabensatzung regelt in § 11 die Pflichten der Quartiergeber. In Absatz 5 werden die im Einzelnen zu erfassenden persönlichen Daten der Gäste verzeichnet. Weiterhin geregelt werden die Führung des Gästeverzeichnisses und in § 14 die datenschutzrelevanten Berechtigungen.
Status	Satzung über die Erhebung einer Kurabgabe der Stadt Plau am See vom 26.09.2007
Link	zum Text: http://www.bks-mv.de/cms/BKS_qa/BKS/Amt_Plau_am_See/_Behoerden/Amt_Plau_am_See_Geschaeftsfuehrende_Gemeinde_Stadt_Plau_/_Behoerden/2._Hauptamt/_Satzungen/Kurabgabe_2007.pdf

8. Verwaltungsvorschriften

Verwaltungs-vorschriften

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	**E-Bilanz** **- Verfahrensgrundsätze zur Aktualisierung der Taxonomien** **- Veröffentlichung der aktualisierten Taxonomien (Version 5.1)**
Inhalt	In BMF-Schreiben verweist das Bundesfinanzministerium darauf, dass für die Übermittlung der Inhalte der Bilanz sowie der Gewinn- und Verlustrechnung durch Datenfernübertragung die jeweils für dieses Wirtschaftsjahr geltende Taxonomie verwendet werden muss. Die aktualisierten Taxonomien (Kern- und Branchentaxonomien) stehen unter www.esteuer.de zur Ansicht und zum Abruf bereit.
Status	BMF Schreiben vom 5. Juni 2012
Link	zum Text: http://www.esteuer.de/download/BMF-Schreiben%20vom%205.%20Juni%202012.pdf

Name	**Elektronische Übermittlung von Bilanzen sowie Gewinn- und Verlustrechnungen; Anwendungsschreiben zur Veröffentlichung der Taxonomie**
Inhalt	In dem Anwenderschreiben stellt das Bundesfinanzministerium in Punkt IX. klar, dass es nicht beanstandet wird, wenn Unternehmen für das Wirtschaftsjahr 2012 ihre Bilanz sowie die Gewinn- und Verlustrechnung noch nicht durch Datenfernübertragung übermitteln.[40] Erneut

[40] In der Pressemeldung des BMF vom 30.05.2012 findet sich sogar die Aussage, dass die elektronische Übermittlung in den allermeisten Fällen erst für Wirtschaftsjahre ab 2013 verpflichtend wird, „also – zusammen mit den elektronischen Steuererklärungen – frühestens im Jahr 2014. Für das Wirtschaftsjahr 2012 oder 2012/2013 steht es den Unternehmen frei, die Bilanz noch auf Papier abzugeben oder bereits elektronisch“, siehe http://www.bundesfinanzministerium.de/Content/DE/Pressemitteilungen/Finanzpolitik/2012/05/2012-05-30-PM21.html.

	wird in dem Schreiben für die Übermittlung XBRL (eXtensible Business Reporting Language) als Übermittlungsformat festgelegt.
Status	BMF Schreiben vom 28. September 2011
Link	zum Text: http://www.bundesfinanzministerium.de/Content/DE/Downloads/BMF_Schreiben/Steuerarten/Einkommensteuer/051_a.pdf?__blob=publicationFile&v=4

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. Nach den GDPdU hat ein Unternehmen im Falle der Erstellung steuerrelevanter Aufzeichnungen mit Hilfe eines IT-Systems nicht nur die Einsichtnahme in diese Daten zu ermöglichen, sondern nach Vorgabe der Finanzbehörde die Daten selbst auszuwerten oder auf einem lesbaren Datenträger zur Verfügung zu stellen. Weiterhin 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/Content/DE/Downloads/BMF_Schreiben/Weitere_Steuerthemen/Abgabenordnung/Datenzugriff_GDPdU/002_GDPdU_a.pdf?__blob=publicationFile&v=4

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 durch die Finanzverwaltung besteht.
Status	BMF, Stand: 22. Januar 2009
Link	zum Text: http://www.bundesfinanzministerium.de/Content/DE/Standardartikel/Themen/Steuern/Weitere_Steuerthemen/Abgabeordnung/Datenzugriff_GDPdU/GdPdU-faq-anl.pdf?__blob=publicationFile&v=4

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/Content/DE/Standardartikel/Themen/Steuern/Weitere_Steuerthemen/Abgabeordnung/Datenzugriff_GDPdU/info-beschreibungsstandard-anl.pdf?__blob=publicationFile&v=4

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/Content/DE/Downloads/BMF_Schreiben/Weitere_Steuerthemen/Betriebspruefung/015.pdf?__blob=publicationFile&v=3

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 enthält im Allgemeinen Teil (AT) unter „AT 7.2 Technisch-organisatorische Ausstattung“ Vorgaben für den IT-Einsatz. In den Erläuterungen zu AT 7.2 in der der MaRisk zugehörigen Anlage 1 werden zudem Hinweise für die operative Umsetzung gegeben.
Status	Rundschreiben 11/2010 (BA) der Bundesanstalt für Finanzdienstleistungsaufsicht (BaFin) vom 15.12.2010: Mindestanforderungen an das Risikomanagement - MaRisk
Link	zum Text der MaRisk: http://www.bafin.de/SharedDocs/Veroeffentlichungen/DE/Rundschreiben/rs_1011_ba_marisk.html?nn=2818068#doc2676948bodyText20 zum Text der Anlage 1:

	http://www.bafin.de/SharedDocs/Downloads/DE/Bericht/dl_rs_1011_ba_anlage1.pdf?__blob=publicationFile&v=6

Name	**Umsatzsteuer; Vereinfachung der elektronischen Rechnungsstellung zum 1. Juli 2011 durch das Steuervereinfachungsgesetz 2011**
Inhalt	Mit seinem Schreiben vom 2. Juli 2012 erläutert das Bundesministerium der Finanzen, wie elektronische Rechnungen steuerlich korrekt zu nutzen sind, insbesondere im Hinblick auf den Vorsteuerabzug nach dem Umsatzsteuergesetz.
Status	Schreiben BMF vom 15.12.2010, IV D 2 - S 7287-a/09/10004 :00, Dokument 2012/0449475
Link	zum Text: http://www.bundesfinanzministerium.de/Content/DE/Downloads/BMF_Schreiben/Steuerarten/Umsatzsteuer/Umsatzsteuer-Anwendungserlass/2012-07-02-Vereinfachung-der-elektronischen-Rechnungsstellung.pdf?__blob=publicationFile&v=3

9. 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	**EBGB – Einführungsgesetz zum Bürgerlichen Gesetzbuche**
Inhalt RW	Art 246 § 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), zuletzt geändert durch Artikel 2 des Gesetzes vom 27. Juli 2011 (BGBl. I S. 1600, 1942)
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.[41]

RW	**MaRisk – Mindestanforderungen an das Risikomanagement: Anlage 1 – Regelungstext mit Erläuterungen**
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 Normenreihe ISO/IEC 2700X.

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

Status RW	Anlage 1: Erläuterungen zu den MaRisk in der Fassung vom 15.12.2010
Link RW	zum Text: http://www.bafin.de/SharedDocs/Downloads/DE/Bericht/dl_rs_1011_ba_anlage1.pdf?__blob=publicationFile&v=6
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 2700X**
Status RR	Die Normenreihe ISO/IEC 2700X ist in ständiger Entwicklung begriffen. Neue Normen kommen hinzu, bestehende werden überarbeitet, ältere zurückgezogen. Insofern muss der Staus jeder Norm der Reihe einzeln recherchiert werden.
Link RR	zur ISO-Website: http://www.iso.org/iso/home/ Normenbeispiel: ISO/IEC 27002:2005 http://www.iso.org/iso/home/store/catalogue_ics/catalogue_detail_ics.htm?csnumber=50297

RW	**SigV (Signaturverordnung) – 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.
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://bundesrecht.juris.de/sigv_2001/BJNR307400001.html
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 15408-1:2009**
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

RW	**UStG – Umsatzsteuergesetz**
Inhalt RW	§ 14 Abs. 3 UStG verweist auf Artikel 2 der Empfehlung 94/820/EG der EU-Kommission. Derartige Empfehlungen sind rechtsunverbindliche Rechtsakte der Europäischen Union. In Artikel 2 werden die Begriffsbestimmungen erläutert und damit festgelegt, welche Formen des Datenaustausches durch das UStG akzeptiert werden.
Status RW	Fassung der Bekanntmachung vom 21. Februar 2005 (BGBl. I S. 386), zuletzt geändert durch Artikel 2 des Gesetzes vom 8. Mai 2012 (BGBl. I S. 1030)
Link RW	zum Text: http://www.gesetze-im-internet.de/ustg_1980/BJNR119530979.html
RR	**94/820/EG: Empfehlung der Kommission vom 19. Oktober 1994 über die rechtlichen Aspekte des elektronischen Datenaustausches**
Status RR	Fassung der Veröffentlichung im Amtsblatt Nr. L 338 vom 28/12/1994
Link RR	zum Text: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31994H0820:de:HTML

10. 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.[42]

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 oder entsprechende Internetportale[43] 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

[42] Bspw. die in § 347 HGB geregelte „Sorgfalt eines ordentlichen Kaufmanns“.
[43] Eine Übersicht über aktuelle und geplante Gesetzesänderungen findet sich auf: http://www.buzer.de

	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.[44]
Status	Urteil vom 11.03.2004 (Az. I ZR 304/01)
Link	zum Text: http://www.jurpc.de/rechtspr/20040265.htm

Name	**BGH – Bundesgerichtshof, I 5 StR 394/08**
Inhalt	Im konkret entschiedenen Fall verurteilte das Gericht den Leiter der Innenrevision eines Entsorgers als Anstalt des öffentlichen Rechts. Dieser hatte entgegen der ihm zuerkannten Garantenstellung nicht verhindert, dass der Betrieb seinen Kunden überhöhte Gebühren in Gesamthöhe von 23 Mio. € in Rechnung stellte. Für Compliance insgesamt sind die Ausführungen des BGH interessant, da dieser explizit auf die Position und Verantwortung eines „Compliance Officer", auch in Unternehmen, eingeht. Diesem wird regelmäßig eine Garantenpflicht zukommen, die darauf abzielt, „im Zusammenhang mit der Tätigkeit des Unternehmens stehende Straftaten von Unternehmensangehörigen zu verhindern".[45]
Status	Urteil vom 17.07.2009 (Az. 5 StR 394/08)
Link	zum Text: http://juris.bundesgerichtshof.de/cgi-bin/rechtsprechung/document.py?Gericht=bgh&Art=en&nr=48874&pos=0&anz=1

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

[44] Vgl. die Diskussion des Urteils und seiner Folgen bei *Weber/Dittrich 2010*, Rn. 17-20.
[45] Vgl. die Erörterung des Urteils von *Münzenberg* und seine Hinweise für die Gestaltung der Compliance-Organisation, s. *Münzenberg 2009*.

Status	Urteil vom 15.12.1983 (Az. 1 BvR 209, 269, 362, 420, 440, 484/83)
Link	zum Text: https://cdn.zensus2011.de/live/fileadmin/material/pdf/gesetze/volkszaehlungsurteil_1983.pdf

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.[46]
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**
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

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

	zur Verfügung, um die mangelnde Umsetzung des digitalen Datenzugriffs zu sanktionieren.[47]
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	**LAG Berlin-Brandenburg – Landesarbeitsgericht Berlin-Brandenburg, 4 Sa 2132/10**
Inhalt	Das Gericht gab einem Unternehmen recht, das auf die dienstlichen E-Mails einer Mitarbeiterin, die längere Zeit krankgeschrieben war, zugriff. Außerdem hat das Gericht bestätigt, dass ein Unternehmen nicht allein dadurch zum Dienstanbieter i. S. d. Telekommunikationsgesetzes wird, dass es seinen Beschäftigten gestattet, einen dienstlichen E-Mail-Account auch privat zu nutzen.
Status	Urteil vom 16.02.2011 (Az. 4 Sa 2132/10)
Link	zum Text: http://openjur.de/u/168249.html

Name	**LAG Hessen – Landesarbeitsgericht Hessen, 19 SaGa 1480/11**
Inhalt	Im entschiedenen Fall erließ das Gericht mit Bezugnahme auf §§ 22, 23 Kunsturhebergesetz eine einstweilige Verfügung. Die beklagte Organisation hatte zu Unrecht nach Ausscheiden einer Mitarbeiterin deren Daten (Bild, Name, Profil) nicht aus dem News-Blog entfern. Im Ergebnis folgt daraus, dass bei Austritt von Mitarbeitern stets alle betreffenden Einträge auf den Internetseiten des Unternehmens zu beseitigen sind.
Status	Urteil vom 24.01.2012 (Az. 19 SaGa 1480/11)
Link	zum Text: http://www.lareda.hessenrecht.hessen.de/jportal/portal/t/s15/page/bslaredaprod.psml?&doc.id=JURE120005100%3Ajuris-r01&showdoccase=1&doc.part=L

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.

[47] Nach *Kaminski 2010*, S. 28f.

Status	Urteil vom 19.12.2003 (Az. 10 O 387/01)
Link	zum Text: http://www.jurpc.de/rechtspr/20040109.htm

Name	**LG Heidelberg – Landgericht Heidelberg, 1 S 58/11**
Inhalt	Urteil des LG Heidelberg zum Versuch der Abwerbung von Mitarbeitern von Wettbewerbern durch gezielte Zusendung von Nachrichten über Social Media-Plattformen (im vorliegenden Fall XING). Das Gericht beurteilte den Versuch als Wettbewerbsverstoß gemäß §§ 4 Nr. 7 und 10 UWG.
Status	Urteil vom 23.05.2012 (Az. 1 S 58/11)
Link	zum Text: http://lrbw.juris.de/cgi-bin/laender_rechtsprechung/document.py?Gericht=bw&nr=15730

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 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 ein 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

Name	**OLG Oldenburg – Oberlandesgericht Oldenburg, 2 U 98/11**
Inhalt	Das OLG Oldenburg hat in diesem Fall entschieden, dass derjenige, der einen Stromausfall verursacht, durch den Daten auf einem Datenträger verloren gehen, zum Schadensersatz verpflichtet ist. Das gericht qualifizierte den Datenverlust als Eigentumsverletzung vor, da der betroffene Datenträger mit dem darin verkörperten Programm eine körperliche Sache sei.
Status	Urteil vom 24.11.2011 (Az. 2 U 98/11)
Link	zum Text: http://app.olg-ol.niedersachsen.de/efundus/volltext.php4?id=5864

11. Verträge

11.1 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

11.2 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.[48] 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-Anlagen und -Geräten sowie von DV-Programmen anzuwenden.[49] In einem offenen Verfahren haben Bieter die EVB-IT zu beachten, ansonsten droht ein 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.[50]

---

48 Zur Information der Bundesbeauftragten der Bundesregierung für Informationstechnik: http://www.cio.bund.de/DE/IT-Beschaffung/EVB-IT-und-BVB/evb-it_bvb_node.html

49 Siehe Nr. 3.1.1 VV-BHO zu §55 BHO: http://www.verwaltungsvorschriften-im-internet.de/bsvwvbund_14122011_DokNr20110981762.htm

50 Nach *Bachmann 2009*, S. 679f.

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 Lieferung eines IT-Systems (EVB-IT Systemlieferungs-AGB)**
Inhalt	Die EVB-IT Systemlieferungs-AGB richten sich auf die Lieferung eines IT- Systems auf der Grundlage eines Kaufvertrages und, soweit vereinbart, Schulung und Systemservice.
Status	Version 1.0 vom 01.02.2010
Link	zum Text: http://www.cio.bund.de/SharedDocs/Publikationen/DE/IT-Beschaffung/EVB-IT_Vertragstypen/EVB-IT_Systemlieferung/evb_it_agb_pdf_download.pdf?__blob=publicationFile

Name	**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 1.0 vom 01.02.2010
Link	zum Text: http://www.cio.bund.de/SharedDocs/Publikationen/DE/IT-Beschaffung/EVB-IT_Vertragstypen/EVB-IT_Systemlieferung/evb_it_systemlieferungsvertrag_pdf_download.pdf?__blob=publicationFile

Name	**Störungsmeldeformular zum EVB-IT Systemlieferungsvertrag**[51]
Inhalt	Muster für eine Störungs- bzw. Mängelmeldung zum EVB-IT Systemlieferungsvertrag
Status	Version 1.0 vom 01.02.2010
Link	zum Text: http://www.cio.bund.de/SharedDocs/Publikationen/DE/IT-Beschaffung/EVB-IT_Vertragstypen/EVB-IT_Systemlieferung/evb_it_muster_1_pdf_download.pdf?__blob=public

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

	ationFile

Name	**Leistungsnachweis zum EVB-IT Systemlieferungsvertrag**
Inhalt	Muster für einen Leistungsnachweis zum EVB-IT Systemlieferungsvertrag
Status	Version 1.0 vom 01.02.2010
Link	zum Text: http://www.cio.bund.de/SharedDocs/Publikationen/DE/IT-Beschaffung/EVB-IT_Vertragstypen/EVB-IT_Systemlieferung/evb_it_muster_2_pdf_download.pdf?__blob=publicationFile

Name	**Nutzungsrechtsmatrix zum EVB-IT Systemlieferungsvertrag**[52]
Inhalt	Muster für eine Nutzungsrechtsmatrix zum EVB-IT Systemlieferungsvertrag
Status	Version 1.0 vom 01.02.2010
Link	zum Text: http://www.cio.bund.de/SharedDocs/Publikationen/DE/IT-Beschaffung/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-Beschaffung/EVB-IT_Vertragstypen/EVB-IT_System/evb_it_dienstleistungen_ergaenzende_vertragsbedingungen_Erstellung_e_it_Systems_pdf_download.pdf?__blob=publicationFile

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

Name	**EVB-IT 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-Beschaffung/EVB-IT_Archiv/System/Vertragsformular_Systemvertrag/version_vom_051107_pdf_download.pdf?__blob=publicationFile

Name	**Änderungsverfahren Systemvertrag zu den EVB-IT System**
Inhalt	Muster für ein Änderungsverfahren (Change Request) bei der Erstellung eines IT-Gesamtsystems
Status	Version 1.0 vom 22.08.2007
Link	zum Text: http://www.cio.bund.de/SharedDocs/Publikationen/DE/IT-Beschaffung/EVB-IT_Vertragstypen/EVB-IT_System/evb_it_muster4_aenderungsverfahren_systemvertrag_pdf_download.pdf?__blob=publicationFile

Name	**Ergänzende Vertragsbedingungen für die Beschaffung von Informationstechnik (EVB-IT Kauf)**
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-Beschaffung/EVB-IT_Vertragstypen/EVB-IT_Kauf/evb_it_dienstleistungen_ergaenzende_vertragsbedingungen_Kauf_Hardware_pdf_download.pdf?__blob=publicationFile

Name	**EVB-IT 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-Beschaffung/EVB-IT_Vertragstypen/EVB-

	IT_Kauf/evb_it_kaufvertrag_langf_pdf_download.pdf?__blob=publicationFile

Name	**EVB-IT 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-Beschaffung/EVB-IT_Vertragstypen/EVB-IT_Kauf/evb_it_kaufvertrag_kurzf_pdf_download.pdf?__blob=publicationFile

Name	**Ergänzende Vertragsbedingungen für die Beschaffung von IT-Dienstleistungen (EVB-IT Dienstleistung)**
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-Beschaffung/EVB-IT_Vertragstypen/EVB-IT_Dienstleistung/evb_it_dienstleistungen_ergaenzende_vertragsbedingungen_beschaffung_it_dienstl_pdf_download.pdf?__blob=publicationFile

Name	**EVB-IT 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-Beschaffung/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-Beschaffung/EVB-IT_Vertragstypen/EVB-IT_Ueberlassung_Typ_A/evb_it_dienstleistungen_ergaenzende_vertragsbedingungen_ueberlassung_typ_a_pdf_download.pdf?__blob=publicationFile

Name	**EVB-IT Überlassungsvertrag Typ A (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-Beschaffung/EVB-IT_Vertragstypen/EVB-IT_Ueberlassung_Typ_A/evb_it_ueberlassungsvertrag_typ_a_langf_pdf_download.pdf?__blob=publicationFile

Name	**EVB-IT Überlassungsvertrag Typ A (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-Beschaffung/EVB-IT_Vertragstypen/EVB-IT_Ueberlassung_Typ_A/evb_it_ueberlassungsvertrag_typ_a_kurzf_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-Beschaffung/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-Beschaffung/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-Beschaffung/EVB-IT_Vertragstypen/EVB-IT_Instandhaltung/evb_it_instandhaltung_ergaenzende_vertragsbedingungen_hardware_pdf_download.pdf?__blob=publicationFile

Name	**EVB-IT Instandhaltungsvertrag**
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-Beschaffung/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-Beschaffung/EVB-IT_Vertragstypen/EVB-IT_Pflege_S/evb_it_dienstleistungen_ergaenzende_vertragsbedingungen_beschaffung_it_dienstl_pdf_download.pdf?__blob=publicationFile

Name	**EVB-IT Pflegevertrag S**
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-Beschaffung/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

Für den Bereich der Auftragsdatenverarbeitung nach § 11 BDSG wird vom und für das Bundesministerium des Innern (BMI) eine Mustervereinbarung angeboten.

Name	**Mustervereinbarung zur Auftragsdatenverarbeitung**
Inhalt	Mustervereinbarung zur Auftragsdatenverarbeitung nach § 11 BDSG für BMI und Geschäftsbereich
Status	Stand: Juni 2010
Link	zum Text: http://www.cio.bund.de/SharedDocs/Publikationen/DE/IT-Beschaffung/mustervereinbarung_auftragsdatenverarbeitung_pdf_download.pdf?__blob=publicationFile

12. Ausblick

Fortsetzung

In fortsetzenden Arbeitspapieren werden unternehmensinterne und unternehmensexterne Regelwerke aufgelistet. Für die unternehmensinternen Regelwerke werden hierbei im Wesentlichen Beispiele angegeben, während für die unternehmensexternen Regelwerke ein Verweis vor allem auf Standards und Normen erfolgt.

Aktualisierung

Die in diesem Arbeitspapier genannten Regelwerke unterliegen einer kontinuierlichen Veränderung. Aus diesem Grunde ist weiterhin eine jährliche Aktualisierung geplant.[53]

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

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 16.08.2012).

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.

BAFA 2009: Bundesamt für Wirtschaft und Ausfuhrkontrolle: Merkblatt Länderunabhängige Embargomaßnahmen zur Terrorismusbekämpfung, Stand 28.08.2009. Online verfügbar unter: http://www.ausfuhrkontrolle.info/ausfuhrkontrolle/de/arbeitshilfen/merkblaetter/merkblatt_ebt.pdf (Zugriff am 16.08.2012).

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 16.08.2012).

Franck 2010: Franck, J.: Veröffentlichung von Arbeitsnehmerdaten im Internet. In: DFN-Infobrief, Nov. 2010, S. 2-5. Online verfügbar unter: http://www.dst.kit.edu/downloads/DFN_Infobrief_11-2010_Seiten_1-5.pdf (Zugriff am 16.08.2012).

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.

ISACA 2012: Information Systems Audit and Control Association (ISACA): COBIT 5: Enabling Processes, Rolling Meadows: ISACA 2012.

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 2007: Klotz, M.: Basel II als Treiber des IT-Sicherheitsmanagements - Eine Klarstellung. In: HMD Praxis der Wirtschaftsinformatik, 2007, 44. Jg., Heft 256, S.93-104.

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

Klotz 2011: Klotz, M.: IT-Compliance. In: Tiemeyer, E. (Hrsg.): Handbuch IT-Management – Konzepte, Methoden, Lösungen und Arbeitshilfen für die Praxis, 4., überarb. u. erw. Aufl., München: Hanser, 2011, S. 585-639.

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.

Kring 2012: Kring, W.: BMF veröffentlicht Musterabkommen zu US-FATCA, Steuerboard DB0485095 vom 09.08.2012. Online verfügbar unter: http://blog.handelsblatt.com/steuerboard/2012/08/09/bmf-veroffentlicht-musterabkommen-zu-us-fatca/ (Zugriff am 16.08.2012).

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.

Münzenberg 2009: Münzenberg, Th.: Der Leiter der Innenrevision als Straftäter – das Urteil des Bundesgerichtshofs vom 17. Juli 2009. Online verfügbar unter: http://www.diir.de/fileadmin/fachwissen/downloads/DerLeiterderInnenrevisionalsStraftaeter.pdf (Zugriff am 16.08.2012).

Noerr/Denton 2011: Noerr LLP, SNR Denton US LLP (Hg.): Der USA PATRIOT Act – Implikationen für das Cloud Computing, 2011. Online verfügbar unter: http://www.noerr.com/PortalData/1/Resources/8_broschueren_newsletter/Noerr_US_Patriot_Act.pdf (Zugriff am 16.08.2012).

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.

Rüter/Schröder/Göldner 2006: Rüter, A.; Schröder, J.; Göldner, A. (Hrsg.): IT-Governance in der Praxis, Berlin-Heidelberg: Springer 2006.

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 werden Labore als Demonstrationsbereiche unterhalten. In den Laboren 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.

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 Informations-arbeiter
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 Projektmanagement-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. Kaminski	Grundlagen und aktuelle Entwicklungen der digitalen Betriebsprüfung
02-10-009	12.2010	D. Engel/ N. Zdrowomyslaw	Benchmarking-Studie Stralsund 2010
03-11-010	02.2011	E. Tiemeyer	Kennzahlengestütztes IT-Projektcontrolling – Projekt-Scorecards einführen und erfolgreich nutzen
03-11-011	05.2011	M. Klotz	Regelwerke der IT-Compliance – Klassifikation und Übersicht, Teil 1: Rechtliche Regelwerke
03-11-012	06.2011	M. Klotz	Konzeption des persönlichen Informations-managements
03-11-013	08.2011	H. Auerbach/ N. Zdrowo-myslaw	9. STeP-Kongress „Region gestalten! Gesundheits-wirtschaft und Zukunftsmanagement“
03-11-014	08.2011	M. Klotz	Rollen der Information im Unternehmen
03-11-015	08.2011	Ahlfeldt	eGuides in kulturellen Einrichtungen – deutsch-sprachige Museums-Apps
03-11-016	11.2011	S. Saatmann / I. Sulk / M. Klotz	Studie zu gewerblichen Strompreisen in Meck-lenburg-Vorpommern – Strom als Wettbewerbsfaktor und Gegenstand der Standortvermarktung
04-12-017	04.2012	M. Klotz / I. Sulk / E. Wieck	GDPdU-Konformität von Projektmanagement-software – Exemplarische Konzeption und Um-setzung
04-12-018	07.2012	M. Horn-Vahlefeld	Projektdesign als organisatorischer Rahmen des Projektmanagements
04-12-019	08.2012	M. Klotz / J. Kriegel	ITIL und Datenschutz – Überlegungen für eine Integration des Datenschutzes in die IT-Prozesse nach ITIL
04-12-020	09.2012	M. Klotz	Regelwerke der IT-Compliance – Klassifikation und Übersicht, Teil 1: Rechtliche Regelwerke, 2. Aufl.