PC hinter Gittern? IT-Compliance im Unternehmen

RA **Dr. Michael Rath**, Luther Rechtsanwaltsgesellschaft mbH, Köln,
michael.rath@luther-lawfirm.com

IT-Compliance und IT-Governance umfassen nicht nur die Sicherstellung von Datenschutz (vgl. hierzu Mainzer, Datenschutzbeauftragter, S. 16 ff. in diesem Heft) und IT-Security (vgl. hierzu Münch, IT-Sicherheit, S. 7 ff. in diesem Heft). Dieser Rahmenbeitrag soll zeigen, welche Facetten und Potenziale in IT-Compliance stecken.

Was ist überhaupt „IT-Compliance"?

Der vor allem gesellschaftsrechtlich geprägte Begriff der „Corporate Governance" wird häufig mit „verantwortungsvoller Unternehmenssteuerung durch die Geschäftsführung" beschrieben. Danach sind sowohl der Vorstand einer AG als auch der Geschäftsführer einer „großen" GmbH als eigentliche Adressaten der Corporate Governance verpflichtet, neben der (eigentlich ja selbstverständlichen) Einhaltung von einschlägigen Gesetzen für eine transparente Organisation und ein angemessenes Risikomanagement zu sorgen.

Dies ist heutzutage angesichts der stetig zunehmenden Komplexität von Geschäftsprozessen in einem Unternehmen ohne den Einsatz von IT-Systemen nicht mehr vorstellbar. Corporate Governance ist daher untrennbar mit IT-Compliance verknüpft. IT-Compliance wird vorliegend verstanden als die Einhaltung und Umsetzung von regulatorischen Anforderungen im weitesten Sinne mit dem Ziel eines verantwortungsvollen Umgangs mit allen Aspekten von Informationstechnik (IT). Den mit der Umsetzung dieser Vorgaben einhergehenden Begriff IT-Governance kann man als Gesamtheit der Maßnahmen zur Organisation, Steuerung und Kontrolle der IT-Systeme eines Unternehmens beschreiben.

Anforderungen an Kontroll- und Informationssysteme enthält auch der **Sarbanes-Oxley-Act** (kurz: SOX oder SOA). Die Nichteinhaltung der Kontroll- und Dokumentationspflichten nach **SOX-404**, die nach der von der SEC gewährten Gnadenfrist (Geschäftsjahresende ab dem 15. Juli 2006) nunmehr auch für nicht an der U.S. Stock Exchange notierte Tochtergesellschaften von U.S.-amerikanischen Unternehmen gelten, wird streng sanktioniert: Abschnitt 802 SOX sieht bei Zerstörung und Veränderung von aufbewahrungspflichtigen Unterlagen drakonische Strafen vor (Strafmaß: bis zu 20 Jahren Freiheitsstrafe).

Das ist Chefsache!

IT-Compliance ist Aufgabe der Chefetage. Zur Vermeidung einer (persönlichen!) Haftung des Vorstandes oder der Geschäftsführung nach §§ 93 Abs. 2, 116 Abs. 1 AktG (analog) ist es nicht ausreichend, diese Aufgabe an die IT-Abteilung bzw. den „Chief Information Officer (CIO)" zu delegieren. Vielmehr ist das Management aufgerufen, sich persönlich um die Einhaltung von IT-Compliance zu kümmern. Die Unternehmensleitung muss nachweisen können, dass sie auch im Zusammenhang mit der IT im Unternehmen die erforderliche Sorgfalt angewendet hat.

IT-gestütztes „IKS"

IT-Compliance bedeutet damit zunächst die Einhaltung von gesetzlichen Sorgfaltsanforderungen (vgl. §§ 43 GmbHG, 93, 116 AktG) und Informations- sowie Dokumentationspflichten *durch und mit Hilfe der IT*. Die Etablierung eines solchen „Internen Kontrollsystems (IKS)", also eines IT-Risikomanagement-Systems, ist zwingend erforderlich, um eine ausreichende Basis zur Unternehmenslenkung und zur Erfüllung von gesetzlichen Berichts- und Dokumentationspflichten zu schaffen. Dieser Bestandteil von IT-Compliance wird daher teilweise auch als

„Information Security Governance (ISG)“ bezeichnet.

In einem Unternehmen kann in der Regel ohnehin nur durch softwaregestützte Informationsmanagement-Prozesse sichergestellt werden, dass die unternehmerischen Entscheidungen auf der Grundlage angemessener Informationen getroffen werden. Es ist im Rahmen des zuvor beschriebenen allgemeinen Risk Management also notwendig, EDV-gestützte Maßnahmen zur Begleitung der Prozesse und zur Risikofrüherkennung zu etablieren und mit Hilfe der EDV auf ihre Brauchbarkeit hin zu kontrollieren.

Auch die ab dem 1. Januar 2007 qua Gesetz bindenden Eigenkapitalvorschriften **Basel II** berücksichtigen (ähnlich wie für Versicherungsunternehmen das neue System der Solvabilitätskontrolle nach **Solvency II**) bei der Beurteilung der Bonität und der wirtschaftlichen Lage des Unternehmens „weiche“ Faktoren wie das Vorhandensein und die Effektivität eines Dokumentations- und Informationsmanagements sowie etwaige IT-Risiken.

Das so genannte „COSO“-Modell („Internal Control Integrated Framework“) des Committee of Sponsoring Organizations of the Treadway-Commission stellt ein international anerkanntes und verbreitetes internes Kontrollsystem dar, welches das Ziel hat, die Ordnungsmäßigkeit und Verlässlichkeit der Rechnungslegung sowie die Einhaltung der für das Unternehmen zu beachtenden rechtlichen Vorschriften sicherzustellen. Bei der Etablierung einer solchen IT-Governance helfen zudem Enterprise-Content-Management (ECM)-Lösungen, den Überblick über die im Unternehmen vorhandenen Informationen zu behalten.

Auch der Abschlussprüfer hat im Rahmen von freiwilligen oder gesetzlich vorgeschriebenen Jahresabschlussprüfungen gemäß § 317 Abs. 4 HGB die im Unternehmen vorhandenen „Überwachungssysteme“, also auch die dort etablierten Risikomanagement-Prozesse und zugehörigen Risikofrüherkennungs- und IT-Systeme, zu beurteilen.
Die diversen **Prüfungsstandards (PS)** des Institutes der Wirtschaftsprüfer (**IDW**) und des Fachausschusses für IT (**FAIT**) spiegeln die Bedeutung der IT-Landschaft als wesentliche Komponente des IKS wieder. So sind bspw. nach **IDW PS 260, PS 330** und **PS 340** bei der Prüfung des IT-Systems auch Aufbau, Angemessenheit und Funktion des Risikomanagements (Risikofrüherkennung) zu beurteilen.

IT-Security

Risikomanagement in einem Unternehmen ist ohne IT-Security nicht denkbar. „IT-Sicherheit“ als ein weiterer Bestandteil von IT-Compliance bedeutet, dass die IT-Systeme (und die darin enthaltenen vertraulichen Informationen) gegen Angriffe von innen und außen geschützt werden müssen. Für wirklich effektive IT-Security sollte eine an den Bedürfnissen des Unternehmens (und nicht der jeweiligen Softwareanwendungen) ausgerichtete IT-Architektur (eine so genannte „Service Orientated Architecture“, SOA) vorhanden sein.

Die für IT-Security notwendigen Maßnahmen umfassen zunächst die Festlegung von Verantwortlichkeiten und Befugnissen der IT-User: Durch die sorgfältige Vergabe von Lese- und Editierrechten anhand interner Sicherheitsbestimmungen lässt sich erreichen, dass die betriebswesentlichen Informationen tatsächlich nur von den hierzu berechtigten Mitarbeitern gelesen und (über eine automatische Versionskontrolle der in der Datenbank vorhandenen Dokumente) bearbeitet werden können. Weiterer unerlässlicher Bestandteil von IT-Security ist auch der Einsatz von systemadäquaten und aktuellen Firewall-Systemen, Virenschutz-Programmen und Anti-Spam-Software.

Zur Eingrenzung von „IT-Risiken“ kann es je nach Bedeutung der IT-Systeme notwendig sein, diese redundant, ggf. sogar in dezidierten Serverräumen mit Zugangskontrolle und unterbrechungsfreier Stromversorgung vorzuhalten, um Schäden bei einem Ausfall der betriebsnotwendigen IT-Systeme vorzubeugen. Zudem muss das Management sich zur Vermeidung von Schäden durch Datenausfall bereits im Vorfeld Gedanken über Backup-Strategien gemacht haben.

Buchhaltung und elektronische Archivierung

IT-Compliance ist außerdem bei der elektronischen Archivierung von Dokumenten tangiert. Kaufleute müssen nach Handelsrecht (§ 257 HGB), aber auch aus steuerrechtlichen Gründen (§ 147 AO) Handels- und Geschäftsbriefe aufbewahren. Die Aufbewahrungsfrist beträgt nach § 257 Abs. 4 HGB (ebenso wie nach § 147 Abs. 3, 4 AO) sechs, für Buchungsbelege, Jahresabschlüsse, Rechnungen, etc. bis zu zehn Jahre (vgl. auch § 14 b UStG).

Da der Rechtsverkehr heutzutage vielfach elektronisch erfolgt, sind neben den vorgenannten Dokumenten grundsätzlich auch E-Mails im Zusammenhang mit der Vorbereitung, dem Abschluss und der Durchführung des „Handelsgeschäftes“ i.S.v. § 343 HGB zu archivieren. Schätzungsweise erfüllen ca. 70% der E-Mails die Anforde-

rungen an einen solchen „Geschäftsbrief“, müssten also archiviert werden. Dies kann gemäß §§ 239 Abs. 4, 257 Abs. 3 HGB auch auf elektronischen Datenträgern geschehen, wenn dies den Grundsätzen ordnungsgemäßer Buchführung (GoB) und den Grundsätzen ordnungsgemäßer DV-gestützter Buchführungssysteme (GoBS) entspricht. Dann allerdings muss u.a. sichergestellt sein, dass die Daten mit den Originalen übereinstimmen, dass diese innerhalb der Aufbewahrungsfrist verfügbar sind und in angemessener Frist lesbar und maschinell auswertbar gemacht werden können (sog. Revisionssicherheit). Hierbei gelten die Standards ISO 17421 und 14589.

Elektronische Prüfung / GDPdU

Um Dritten (insbesondere dem Betriebsprüfer) eine Prüfung der häufig unmittelbar aus den internen ERP- und Buchhaltungssystemen generierten Informationen zu ermöglichen, muss die Archivierung zudem so erfolgen, dass die Dokumente periodengerecht den jeweiligen (Handels-) Geschäften zugeordnet werden können. Hierzu gehört, dass auch die Anlagen zu einer E-Mail aufbewahrt werden, da der in einer E-Mail verkörperte Handelsbrief ohne die zugehörigen Attachments regelmäßig zur Dokumentation des Geschäftsvorfalles unzureichend wäre. Manch geneigter Leser wird an dieser Stelle beim Gedanken an seine eigene Mailbox kurz zusammen zucken, was bei schätzungsweise 400.000 E-Mails, die weltweit pro Sekunde versendet werden, nicht verwunderlich ist.

Die Anforderungen an die Archivierung digitaler Unterlagen werden vom Bundesfinanzministerium durch die „Grundsätze zum Datenzugriff und zur Prüfbarkeit digitaler Unterlagen (GDPdU)“ konkretisiert. Der Finanzverwaltung steht danach seit dem 1. Januar 2002 bei Außenprüfungen das Recht zu, nach Maßgabe eben dieser GDPdU auf alle digitalen steuerrelevanten Unternehmensdaten zuzugreifen. Danach sind die Unternehmen auf Anfrage des Steuerprüfers dazu verpflichtet, ihre steuerrelevanten Daten auch maschinell auswertbar zur Verfügung zu stellen. Die Daten werden dann in der Regel in die Prüfsoftware „IDEA“ (Fa. Audicon) oder „ACL“ eingelesen.

Bei der **Außenprüfung** werden nach **GDPdU** drei Arten des Datenzugriffs unterschieden: der unmittelbare Lesezugriff durch Verwendung der unternehmenseigenen Hard- und Software (Z1), der mittelbare Zugriff über Auswertungen des Unternehmens nach den Vorgaben des Prüfers (Z2) und die (ggf. nach dem Standard des BSI verschlüsselte) Datenträgerüberlassung (Z3). Ein Online-Zugriff auf die Datenbestände des Unternehmens ist der Finanzverwaltung nicht gestattet.

Auch in diesem Zusammenhang wird die Bedeutung des zuvor skizzierten User-Management deutlich: dem Betriebsprüfer sollen schließlich nur die „steuerlich relevanten“ Informationen, also diejenigen Teile der Dokumentensammlung zur Verfügung gestellt werden, welche den richtigen Prüfungsbereich betreffen. Ein Verwertungsverbot für versehentlich überlassene Daten gibt es nicht. Das EDV-System muss daher von vornherein eine Trennung der steuerlich relevanten Daten von den übrigen Daten sowie eine Differenzierbarkeit nach Jahren und Steuerarten ermöglichen.

Speicherplatz und Encryption

Die ordnungsgemäße Archivierung wird in der Praxis dadurch erschwert, dass viele E-Mail-Programme bei der Archivierung aus Speicherplatzgründen die Anlagen zu den E-Mails einfach „abschneiden“; das spart zwar Speicherplatz, führt aber bei einer Betriebsprüfung zu unangenehmen Nachfragen.

Ein weiteres Problem kann die immer häufiger anzutreffende Verschlüsselung von E-Mails („Encryption“) darstellen. Selbstverständlich muss auch bei der Speicherung von verschlüsselten E-Mails während der gesetzlichen Aufbewahrungsfristen eine jederzeitige Entschlüsselung möglich sein, um den Datenzugriff der Finanzverwaltung zu ermöglichen. Dabei muss sichergestellt sein, dass hierdurch nicht in Rechte des Arbeitnehmers eingegriffen wird (der Blick des Arbeitgebers in das auch privat genutzte Postfach eines Mitarbeiters kann ein strafrechtlich relevantes Ausspähen von Daten i.S.v. § 202 a StGB darstellen).

IT-Compliance bedeutet hier, dass das Unternehmen eine interne Anweisung für die Archivierung von E-Mails (E-Mail-Management) vorsehen sollte. Dies geschieht häufig als Betriebsvereinbarung über die Nutzung von Internet und E-Mails (vgl. auch Mainzer, Datenschutzbeauftragter, Seite 18 in diesem Heft).

Releasewechsel / Migration auf neue IT-Systeme

Angesichts der kurzen Lebenszyklen von Softwareanwendungen ist es schwierig, die vorstehend ohnehin nur skizzierten Anforderungen zu gewährleisten. Trotzdem muss natürlich auch im Falle einer Betriebsübernahme oder einer sonstigen Änderung mit Auswirkung auf die IT ein neues EDV-System die Unveränderbarkeit des Datenbestandes gewährleistet sein (§ 146 Abs. 4 AO). Also müssen bspw. auch im Falle eines Releasewechsels, eines Austauschs des

Produktiv- oder E-Mail-Systems oder gar eines Providerwechsels die (unveränderten) Altdaten in das neue System übertragen werden. Neben Authentizität und Integrität der Dokumente muss im Langzeitarchiv aber auch noch die Lesbarkeit garantiert werden. Dies führt in der Praxis oft zu einer kostenträchtigen redundanten Datenhaltung.

Rechtskonforme IT-Systeme / Lizenzmanagement

IT-Compliance bedeutet aber auch, dass die IT-Systeme selbst rechtskonform sein müssen. Rechtmäßige IT-Systeme sind nur solche, die ihrerseits über ausreichende Lizenzen zum Betrieb der jeweiligen Software verfügen – einen gutgläubigen Erwerb von Rechten an einer Software gibt es nicht. Durch die Etablierung eines „Software Asset Management"-Systems (möglichst unter Einhaltung des ISO-Standards 19770) kann eine (im Übrigen auch strafrechtlich relevante) Unterlizenzierung ebenso vermieden werden wie eine kostenträchtige Überlizenzierung. Hier schlummern Einsparpotenziale. Berechnungen zufolge geben Unternehmen ohne ein effizientes Lizenzmanagementsystem bis zu 60% zu viel für Software aus.

Compliance mit und durch IT-Standards

Untersuchungen zeigen, dass bei Weitem nicht alle Unternehmen in Deutschland die hier aufgezeigten Anforderungen vollständig erfüllen. Gerade einmal 5% der Unternehmen haben bislang Compliance-Projekte umgesetzt.

Dies ist nicht verwunderlich, denn die Vorgaben für IT-Compliance sind entweder in einer ganzen Reihe von umfangreichen Normen „versteckt" oder aber so wenig konkret, dass selbst bei dem Versuch einer gewissenhaften Umsetzung noch immer berechtigte Zweifel bestehen, dass alle Vorgaben eingehalten sind. Zudem entfalten diese Vorgaben in der Regel weder unmittelbare Rechtswirkung (es gibt nur wenige Anforderungen an die Ausgestaltung der IT mit formalem Gesetzesrang wie etwa §§ 9, 11 BSDG, §§ 25 a KWG, 33 Abs. 2 WpHG) noch resultiert aus deren Anwendung eine Vermutung für die Rechtskonformität und damit die Einhaltung von IT-Compliance.

Dennoch sind IT-Security und Information (Security) Governance ohne die Einrichtung und Beachtung anerkannter IT-Standards nicht möglich. Zudem können Standards bei der Festlegung des anzuwenden Sorgfaltsmaßstabes helfen.

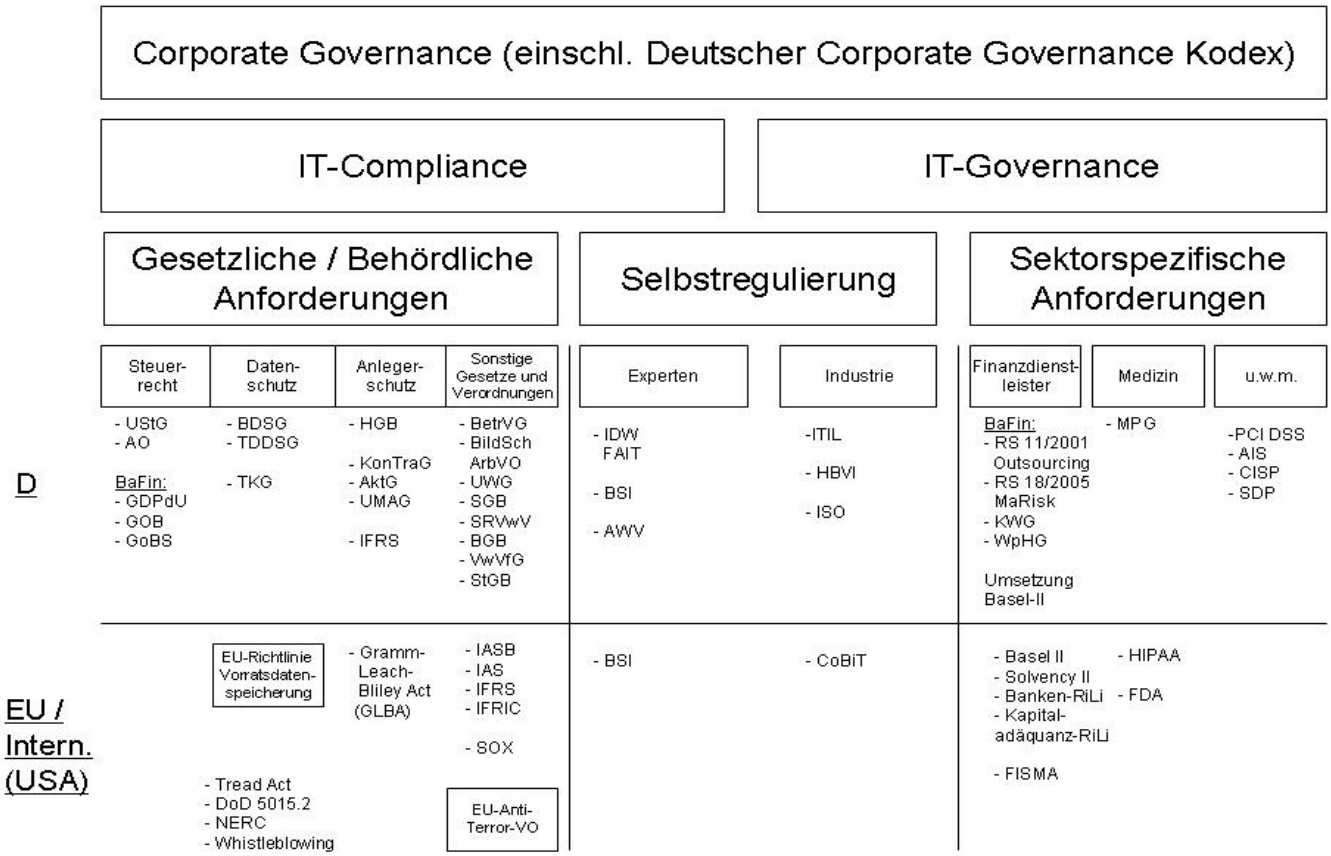

Abb. 1.: Überblick über Normative Vorgaben für IT-Compliance

Je nach Zielrichtung der IT-Governance kommen hierfür verschiedene Standards in Betracht: Für IT-Security bieten sich sicherlich die allgemein anerkannten Standards

für IT-Sicherheit des Bundesamtes für Sicherheit in der Informationstechnik (BSI) an, die BSI-Standards 100-1, 100-2 und 100-3 sowie die „IT-Grundschutz-Kataloge“ (vormals IT-Grundschutzhandbuch, vgl. hierzu nachfolgenden Beitrag von Münch, IT-Sicherheit, Seite 7 ff. in diesem Heft).

Neben diesem IT-Security-Standard des BSI gibt es beispielsweise für das Risikocontrolling (in enger Anlehnung an COSO) das international akzeptierte Referenzmodell CobiT („Control Objectives for Information and Related Technology“) mit seinen 34 Kernprozessen und über 300 Kontrollzielen. Darüber hinaus empfiehlt sich die Einhaltung des De-facto-Standards für methodenorientierte IT-Abteilungen, die sehr umfassende „Best Practices“-Sammlung ITIL (IT Infrastructure Library), die übrigens aus dem angelsächsischen Behördenumfeld stammt. Auf Basis des Prozessrahmenwerkes ITIL arbeitet inzwischen mehr als die Hälfte aller deutschen Unternehmen.

Daneben sind in ISO 20000 die Mindestanforderungen an das Service-, Security- und Relationship-Management geregelt; ISO 27001 spezifiziert die Anforderungen an ein Informations-Sicherheits-Management-System und ermöglicht eine international anerkannte Zertifizierung der im Unternehmen angewandten IT-Sicherheit.

Was kann denn schon passieren?

Etwaige Nachlässigkeiten bei IT-Compliance werden nicht erst bei einer Betriebsprüfung oder einem eklatanten Verstoß gegen Datenschutzrecht nach § 43 BDSG bestraft. Vielmehr sind die Grenzen unternehmerischer Handlungsfreiheit dann erreicht, wenn ein Vorstandsmitglied gegen die vorstehend skizzierten, in der IT-Branche anerkannten Erfahrungsgrundsätze verstößt.

Diese Branchenkenntnisse sind naturgemäß nicht von jeder Geschäftsleitung zu erwarten. Es stellt jedoch sicherlich keine Lösung dar, sich nur auf den Sachverstand eines externen IT-Dienstleisters zu verlassen, denn eine vollständige Delegation der Compliance-Pflichten ist ohnehin nicht möglich. Dennoch wird oft nur auf die Verbesserung der Kostenquote geschielt, anstatt auf die notwendige law compliance zu achten.

Trotz der komplexen Kombination aus Recht, Steuern und Technik müssen die im Unternehmen eingesetzten IT-Systeme den hohen Anforderungen von IT-Compliance und IT-Governance genügen und dürfen nicht als zu vernachlässigende „Commodity“ angesehen werden. Zu den Pflichten einer vorausschauenden Unternehmensleitung gehört es daher, ein angemessenes Informations- und Risikomanagement zu etablieren und rechtskonforme IT-Systeme einzusetzen.

IT-Compliance bietet aber neben der Vermeidung einer persönlichen Haftung der Geschäftsleitung auch die Möglichkeit, erhebliche Kosteneinsparungspotenziale zu identifizieren (etwa bei der Vermeidung eines Parallelbetriebes von IT-Systemen oder der Überlizenzierung). Zudem bietet es dem Management eine gute Chance zum Aufbau wirklich prozessorientierter IT-Systeme (SOA) und damit zur Steigerung der Effektivität.

Auf dem Markt gibt es bereits eine große Auswahl an Compliance-Management-Software. Ziel muss es allerdings sein, keine Insellösungen für einzelne Anforderungen zu schaffen, sondern eine IT-Strategie zu finden, die neben der Erfüllung von IT-Compliance-Anforderungen auch für den eigentlichen Geschäftsbetrieb nutzbringend ist.

Tipps und Termine

Service Level Agreements (SLA) - Gestaltungshinweise aus Recht und Praxis

Unter diesem Titel bietet der Arbeitskreis EDV und Recht Köln e.V. am 24.1.2007 in Köln eine Vortragsveranstaltung an.

Im Mittelpunkt stehen die rechtlichen Fallstricke von SLA sowie die praktische Handhabung entsprechender SLA aus der Sicht der Dienstleister.

Nähere Informationen unter:
www.edv-und-recht.de