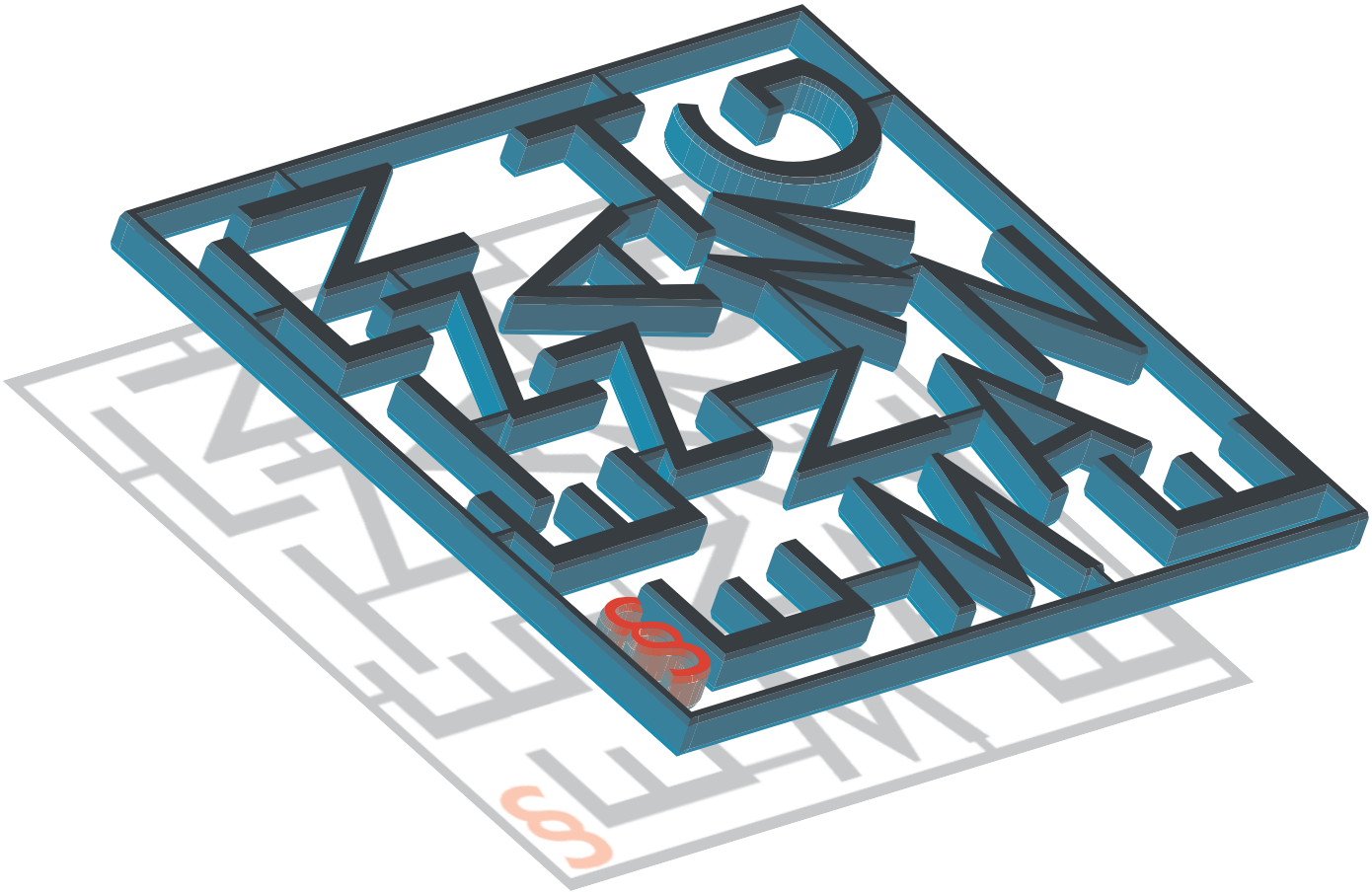
Aagon

Rechtsleitfaden Lizenzmanagement



Schnelle Orientierung im Labyrinth der Vorschriften

von Rechtsanwalt Horst Speichert
im Auftrag von Aagon Consulting GmbH

Vorwort

Liebe Leser,
als Hersteller der Aagon Client Management Plattform (ACMP) und als Berater unserer Kunden in den Bereichen Clientmanagement und Betriebssystem-Migrationen werden wir in der täglichen Arbeit oft auch mit Fragen aus dem rechtlichen Umfeld konfrontiert. Besonders groß ist der Informationsbedarf vor allem im Bereich des Lizenzmanagements und hier bei Fragen zu Lizenzmodellen und -bedingungen, der Lizenzkontrolle und dem Lizenznachweis, dem Datenschutz bei der Lizenzüberwachung und bei Fragen der Haftung bei Lizenzverstößen.

Um etwas Licht in die unübersichtliche da vielschichtige Thematik zu bringen, haben wir gemeinsam mit dem auf IT-Recht spezialisierten Rechtsanwalt Host Speichert diesen Leitfaden zum Thema Lizenzmanagement entwickelt. Der Ratgeber eignet sich einerseits dazu, sich grundsätzlich über die rechtlichen Rahmenbedingungen des Lizenzmanagements zu informieren. Andererseits liefert er auch bei Bedarf schnell die wichtigsten Informationen zu einem bestimmten Teilbereich. Und da Lizenzmanagement nicht für sich alleine steht, sondern fester Bestandteil von IT-Compliance und Risikomanagement ist, haben wir diese Themen ebenfalls in den Leitfaden aufgenommen.

Wir wünschen Ihnen eine interessante und lehrreiche Lektüre und hoffen, auf diese Weise nicht nur mit unseren Produkten zu mehr Klarheit und Transparenz in Ihrer IT-Administration beitragen zu können.

Ihr

Sebastian Weber

Product Manager bei Aagon Consulting

Aagon

Inhalt

Der Autor

Horst Speichert ist Rechtsanwalt in der Kanzlei esb Rechtsanwälte in Stuttgart und auf IT-Recht spezialisiert. Neben seiner Tätigkeit als Anwalt ist er Lehrbeauftragter der Universität Stuttgart für Informationsrecht, Seminarleiter für Internetrecht, IT-Sicherheit und Datenschutz, Ausbilder für Datenschutzbeauftragte, IT-Compliance-Audits und Vertragsgestaltung sowie Fachbuchautor von „Praxis des IT-Rechts“, erschienen im Vieweg Verlag in der 2. Auflage. Sie erreichen den Autor per E-Mail unter horst@speichert.de oder im Internet unter www.kanzlei.de und www.speichert.de.

Horst Speichert

I. Grundlagen des Lizenzmanagements

Ein Verstoß gegen eine Softwarelizenz ist schneller begangen als man meint. Denn schon die Installation eines gerade benötigten Programms von einem Originaldatenträger kann einen Lizenzverstoß verursachen, wenn keine entsprechende Nutzungslizenz für das Programm (mehr) frei ist. Die Gesetzeslage ist bei solchen Lizenzverstößen eindeutig. Denn das Urheberrecht stellt die unrechtmäßige Nutzung von Software unter Strafe. Haftbar sind dabei sowohl die Unternehmen selbst, als auch die für die Einhaltung von Lizenzverträgen verantwortlichen Personen also insbesondere Führungskräfte. Und es wird noch vertrackter: Denn um zu beweisen, dass man auch tatsächlich über eine gültige Lizenz für ein Programm verfügt, müssen die entsprechenden Lizenzen zu den installierten Programmen gut verwahrt und bei Bedarf nachweisbar sein. In Unternehmen mit einer Vielzahl von Nutzern stellt dies allein bereits eine eigene Verwaltungsaufgabe dar. Ohne ein effizientes Lizenzmanagement ist diese Herausforderung praktisch nicht zu meistern.

1. Über- und Unterlizenzierung

Grundsätzlich unterscheidet man beim Thema Lizenzmanagement zwischen drei Situationen: der Überlizenzierung, der Unterlizenzierung und der korrekten Lizenzierung. Bei einer Unterlizenzierung sind weniger Lizenzen vorhanden, als tatsächlich benötigt würden. Das bedeutet, dass bei Unterlizenzierung strafbare Verstöße gegen das Urheberrecht begangen werden, die im Rahmen von IT-Compliance mit rechtmäßigen Unternehmensprozessen unvereinbar sind. Erkennt ein Softwarehersteller beispielsweise im Rahmen eines Audits eine Unterlizenzierung bei einem Kunden, führt dies meist zu kostspieligen Nachlizenzierungen. Denn Softwarehersteller nutzen dann gerne den drohenden Rechtsverstoß für überhöhte Lizenzgebühren aus.
Komplexe Lizenzverträge führen hingegen häufig zu wirtschaftlich nachteiligen Überlizenzierungen, da Unternehmen im Zweifel lieber zu viele Lizenzen erwerben, um auf der sicheren Seite zu sein. Zudem wird ein hoher Prozentsatz von ursprünglich notwendiger Software nach einem gewissen Zeitablauf im Unternehmen nicht mehr verwendet. Fehlt es an einem effizienten Lizenzmanagement, kommt es hierdurch zu kostspieliger Überlizenzierung.

Daher ist das Ziel von Lizenzmanagement, der perfekten Lizenzierung so nahe wie möglich zu kommen. Im Idealfall sind dann jederzeit genauso viele Lizenzen in Nutzung, wie auch vorhanden sind. Jeder Installation einer Software geht immer eine Lizenzprüfung voraus. Und regelmäßige Kontrollen stellen sicher, dass nicht Mitarbeiter versehentlich oder vorsätzlich gegen Lizenzbedingungen verstoßen haben.

2. Lizenzmanagement gehört zu IT-Compliance

IT-Compliance ist schon lange kein Marketing-Schlagwort mehr, sondern fordert von Unternehmen und Organisationen ganz konkrete Maßnahmen rechtlicher, organisatorischer und technischer Art. Der Begriff bedeutet dabei allgemein gesprochen die IT-spezifische Rechtskonformität, also die Einhaltung rechtlicher Vorgaben im IT-Umfeld. Hierzu zählen auch die lizenz- und urheberrechtlichen Bestimmungen, welche erst durch ein effizientes Lizenzmanagement überwacht und eingehalten werden können. Verbunden mit IT-Compliance ist die Etablierung von Prozessen und Verfahren zur Erlangung dieser Rechtstreue. Konkret bedeutet IT-Compliance die Konformität mit

- gesetzlichen Standards, das heißt eine Einhaltung von Gesetzen und eine Beachtung der Rechtsprechung,
- Vertragspflichten, insbesondere aus Verträgen mit Kunden, Geschäftspartnern, Mitarbeitern, Betriebsvereinbarungen etc.,
- (selbstgesetzten) Standards. Hierzu zählt die Einhaltung anerkannter Standards wie BSI oder ISO.

Aus der Blickrichtung der angestrebten Ziele definiert sich IT-Compliance als die wirksame Verhinderung von Informationsverlust (Wirtschaftsspionage), Rechts- und Lizenzverstößen, Straftaten und Falschbilanzierung.

Damit stellen IT-Compliance und Lizenzmanagement auch einen wichtigen Baustein für das Risikomanagement eines Unternehmens dar, da andernfalls gravierende Schäden durch Rechtsverletzungen und Imageverluste drohen.

Zentrale gesetzliche Vorschriften für das Informations- und Risikomanagement sind etwa das Gesetz zur Kontrolle und Transparenz im Unternehmensbereich (KonTraG), der Deutsche Corporate Governance Kodex, Basel II, die Mindestanforderungen an das Risikomanagement (MaRisk), die Grundsätze ordnungsmäßiger DV-gestützter Buchführungssysteme (GoBS) sowie die Grundsätze zum Datenzugriff und zur Prüfbarkeit digitaler Unterlagen (GDPdU). Die Aufzählung ist dabei bei Weitem nicht abschließend, sondern benennt nur wichtige Bestimmungen.

Der Deutsche Corporate Governance Kodex bestimmt beispielsweise in Punkt 4.1.3: „Der Vorstand hat für die Einhaltung der gesetzlichen Bestimmungen und der unternehmensinternen Richtlinien zu sorgen und wirkt auf deren Beachtung durch die Konzernunternehmen hin (Compliance)“.

Die Vorschrift benennt hier deutlich den Zusammenhang zwischen Compliance und der Einhaltung gesetzlicher Vorschriften und stellt klar, dass IT-Compliance und Lizenzmanagement originäre Aufgaben der Unternehmensleitung sind.

II. Lizenzmanagement als Prozess

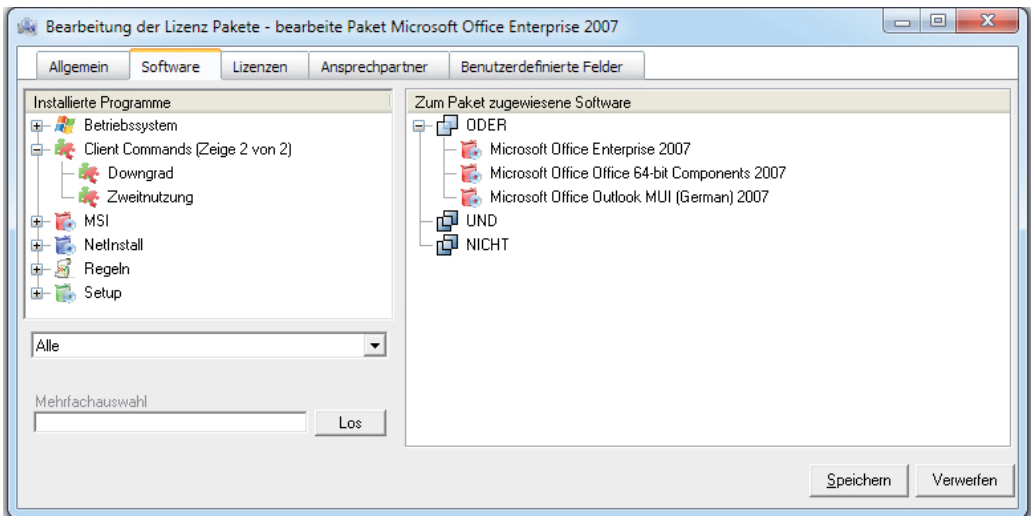
1. Lizenzmanagement ist Asset-Management für Software

Software macht sowohl bei den IT-Kosten wie auch beim Anlagevermögen eines Unternehmens einen immer größeren Prozentsatz aus. Um das Anlagevermögen eines Unternehmens im Bereich Software bewerten zu können, muss dessen Buchhaltung entsprechend wissen, welche Software(lizenzen) das Unternehmen tatsächlich besitzt. Anders gesagt: Erst durch ein effizientes Lizenzmanagement lässt sich das eigene Anlagevermögen im Bereich der Software-Assets detailliert und beweissicher führen!

Der angenehme Nebeneffekt des Software-Asset-Managements ist, das man dann auch auf Forderungen von Softwareherstellern nach Lizenzierungsnachweisen revisionssicher und konfliktfrei reagieren kann. Sofern im Unternehmen oder Konzern eine interne Verrechnung von IT-Dienstleistungen erfolgt, kann das moderne Lizenzmanagement schließlich auch dafür eine gute Unterstützung sein. Denn Lizenzmanagement verbessert auch die Budgetplanung und -kontrolle im IT-Umfeld.

2. Inventarisierung vorhandener Software und Lizenzen

Der erste Schritt eines Software-Asset-Managements ist die Inventarisierung aller im Unternehmen vorhandenen Programme und Lizenzen. Mit Hilfe eines Clientmanagement-Systems (CMS) wie beispielsweise ACMP von Aagon Consulting ermittelt hierbei ein Software-Agent regelmäßig auf allen Arbeitsplatzrechnern und Servern die dort installierte Software. Diese Daten speichert das CMS dann in einer zentralen Datenbank ab. Im nächsten Schritt muss ein Administrator, Lizenzverwalter oder eine andere dazu ermächtigte Person die im Unternehmen vorhandenen Lizenzen in dem Lizenzmanagement-Modul des CMS erfassen. Hierfür ist oftmals die rechtliche Prüfung und Auslegung der vorhandenen Lizenzverträge erforderlich, was sowohl Fachwissen als auch große Sorgfalt erfordert. Denn Software- oder Lizenzverträge können eine Vielzahl



von Chancen wie eine Ausdehnung von Nutzungsrechten (zum Beispiel bis wann ist ein Update kostenlos), aber auch Risiken wie Abmahnungen, Vertragsstrafen bis hin zur Strafanzeigen bei Falschauslegung für das Unternehmen enthalten.

Bei vielen und komplexen Lizenzverträgen bietet es sich an, diese durch ein angebundenes Vertragsmanagement zu berücksichtigen und der internen Planung zuzuführen.

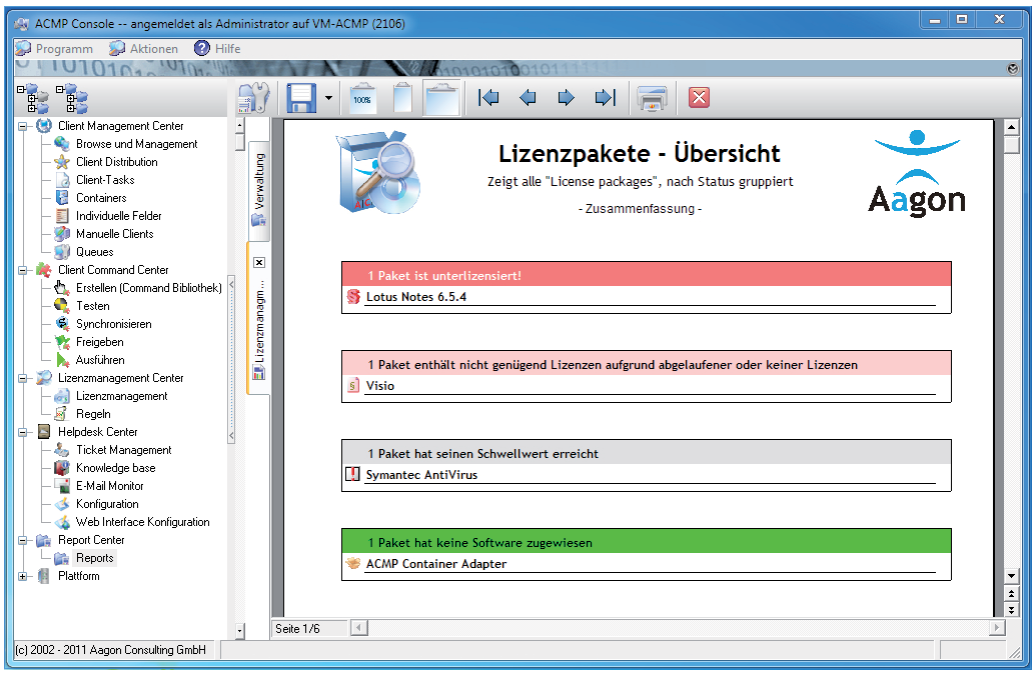
3. Gegenüberstellung und Bilanzierung

Sind inventarisierte Programme und vorhandene Lizenzen in dem Lizenzmanagement erfasst, ordnet im nächsten Schritt ein technisch versierter Mitarbeiter die bei der Inventarisierung gefundenen Softwarepakete den entsprechenden Lizenzpaketen zu. Dies kann in bestimmten Fällen ganz einfach und fast automatisch ablaufen. In komplexeren Szenarien wie beispielsweise bei besonderen Up- oder Downgrade-Rechten ist hier jedoch Handarbeit angesagt. Ist diese Zuordnung abgeschlossen, kann das Lizenzmanagement schließlich die Ergebnisse der Software- und Lizenzinventur gegenüberstellen. Das Ergebnis ist eine Lizenzbilanz die aufzeigt, welche Lizenzen aktuell fehlen oder überflüssig sind.

Status	Paketname	Kategorie	Hersteller	Liz. verfügbar	Liz. in Benutzung	Cont. Status
	Lotus Notes 6.5.4	Office	IBM	5	11	
	Visio	Office	Microsoft	0	2	
	Symantec AntiVirus	Security	Symantec	12	11	
	ACMP Container Adapter			0	0	
	Adobe Acrobat 6.0 Standard	PDF-Reader	Adobe Systems	Unbegrenzt	8	
	Adobe Photoshop CS2 Suite		Adobe Systems	13	0	
	Adobe Reader 9 - Deutsch	PDF-Reader	Adobe System Incorporated	30	2	
	Microsoft Office Enterprise 2007			2	1	
	Microsoft Office Excel Viewer 2003	Office	Microsoft	20	10	

4. Compliance-Check

Sofern Lizenzen fehlen, kann zudem ein Compliance-Check darüber informieren, ob in der Folge Rechtsverstöße begangen wurden. Da Compliance nicht nur Rechtskonformität, sondern auch eine prozessorientierte Lösung im Blick hat, sind darüber hinaus Wege aufzuzeigen, wie künftige Rechtsverstöße vermieden werden.



III. Lizenzrechtliche Rahmenbedingungen

1. Lizenzmodelle der Softwarehersteller

Eine der grundlegenden Weichenstellungen in Lizenzverträgen unterscheidet, ob eine Lizenz nur eine Bereitstellung erlaubt (Einzel-Lizenz) oder eine Mehrfach-Bereitstellung (Mehrfach-Lizenz) zulässig ist.
Je nach Lizenzmetrik können Mehrfach-Lizenzen dabei unterschiedlich definiert sein:

- Volumenlizenz (umfasst eine bestimmte, festgelegte Anzahl von Lizenzen),
- Standortlizenz (umfasst alle Bereitstellungen innerhalb eines festgelegten Standortes),
- Unternehmenslizenz (umfasst alle Bereitstellungen innerhalb eines bestimmten Unternehmens).

Eine urheberrechtliche Lizenz, also eine urheberrechtliche Nutzungs- bzw. Verwertungserlaubnis, ist bei Computerprogrammen grundsätzlich jedoch nur dann erforderlich, wenn eine Nutzung erfolgen soll, die nicht bereits durch eine gesetzliche Erlaubnis gemäß § 69d Urheberrechtsgesetz (UrhG) gedeckt ist. So darf beispielsweise gemäß Absatz 2 des § 69d UrhG einer Person, die zur Benutzung eines Programms berechtigt ist, die Erstellung einer Sicherungskopie vertraglich nicht untersagt werden, wenn sie für die Sicherung der künftigen Benutzung erforderlich ist.

2. Wirksamkeit von Lizenzbedingungen

a. Allgemeine Leitlinien

Während der Installation von Software werden dem Benutzer häufig Verträge angezeigt, die dieser bestätigen muss, um mit der Installation fortfahren zu können. Hierbei handelt es sich um sogenannte Endbenutzer-Lizenzverträge, englisch „End User License Agreement“, kurz EULA genannt. Diese erzwungenen Vereinbarungen sind jedoch nach europäischen Rechtsmaßstäben nur eingeschränkt gültig.
Schutzhüllenlizenzen (Shrink Wrap License) wiederum sind Lizenzbestimmungen, die nach der Vorstellung des Softwareherstellers automatisch durch das Öffnen der Verpackung (engl. „shrink wrap“) akzeptiert werden, obwohl der Nutzer den genauen Wortlaut erst nach dem Öffnen der Verpackung lesen kann. Ihre Wirksamkeit ist daher stark umstritten.

CPU-Klauseln schließlich sind Lizenzbestimmungen, welche die Benutzung der Software an eine bestimmte Hardware bindet. In der Praxis verbreitet sind vor allem nachfolgende Kategorien von CPU-Klauseln:

- Die Software darf ausschließlich auf einem bestimmten Rechner genutzt werden.
- Die Software darf nur gegen ein zusätzliches Entgelt auf einem anderen, insbesondere leistungsfähigerem Rechner eingesetzt werden.
- Die Software darf auf einem anderen Rechner nur genutzt werden, wenn die ursprünglich lizenzierte Hardware defekt ist.

CPU-Klauseln sind dann wirksam, wenn sie individuell mit dem Anwender vereinbart wurden und nicht Teil von AGB sind. Die Rechtsprechung hält CPU-Klauseln nach § 307 Abs. 2 Nr. 1 und 2 BGB überwiegend für unwirksam, wenn Kaufrecht auf die Programmüberlassung anwendbar ist. Nur ausnahmsweise können CPU-Klauseln durch ein schutzwürdiges Interesse des Softwareherstellers gerechtfertigt sein, beispielsweise wenn das Programm in seiner Ablauffähigkeit auf einen bestimmten Computertyp angewiesen ist und ein Einsatz auf einem anderen Rechner mit Ablaufschwierigkeiten verbunden ist, die den Ruf des Softwareherstellers gefährden würden.

Im Ergebnis zeigt sich, dass viele Lizenzbedingungen rechtlich angreifbar oder unwirksam sind, auch wenn sie üblicherweise in der Praxis von den großen Softwareherstellern verwendet werden. Demnach lohnt es sich also, ein kluges Lizenzmanagement unter Einbeziehung des lizenzrechtlichen Knowhows vorzuhalten.

b. Einzelplatzlizenz versus Netzwerknutzung

In Lizenzbedingungen häufig anzutreffen sind sogenannte Netzwerkverbote. Hierunter versteht man vertragliche Beschränkungen der Nutzung von Software über das lokale Netzwerk, beispielsweise im Rahmen einer Remote-Control-Sitzung. Urheberrechtlich ist dabei zweifelhaft, ob die Nutzung von Software über lokale Netzwerke überhaupt in die Verwertungsrechte des Softwareherstellers eingreift. Wird hingegen eine Software auf verschiedenen Rechnern fest gespeichert, liegt in der mehrfachen Festspeicherung in der Tat eine urheberrechtlich unzulässige Vervielfältigung durch den Nutzer vor. Das direkte Verbot der Nutzung über ein Netzwerk ist daher häufig unwirksam. Auch unzulässig sind sogenannte Site-, Installations- oder Gebäudelizenzen, die den Einsatzort einer Software festlegen. Zweifelhaft sind auch sogenannte Service-Büro-Beschränkungen sowie vertragliche und technische Beschränkungen auf eine bestimmte Anzahl von Nutzern. Trotzdem muss natürlich für jeden Nutzer eine entsprechende Lizenz vorhanden sein.

3. Umgang mit Gebrauchtsoftware

Ebenfalls unter Juristen umstritten ist die Zulässigkeit des Handels mit gebrauchter Software. Der BGH entschied in einem richtungsweisenden Urteil aus dem Jahr 2000, dass der Weiterverkauf von datenträgerbasierter Software grundsätzlich nicht über Lizenzbedingungen von den Herstellern eingeschränkt werden kann. In einem aktuellen Urteil vom 11.02.2010 (veröffentlicht im Oktober 2010) hat es der BGH jedoch für zulässig gehalten, dass der Hersteller eines Computerspiels den Weitervertrieb durch bestimmte Vertragsklauseln unmöglich macht, was im Ergebnis einem Verbot des Weiterverkaufs entspricht.

Im Kern geht es bei der Entscheidung darum, ob der Weitervertrieb von Software überhaupt untersagt werden darf. Dagegen spricht der sogenannte „Erschöpfungsgrundsatz“, welcher einem Softwarehersteller verbietet, die weitere Verbreitung eines einmal willentlich in den Verkehr gebrachten Softwareproduktes zu reglementieren. Der „Erschöpfungsgrundsatz“ dient dem allgemeinen Interesse an einem freien Warenverkehr und gilt nur für verkörperte Werke, also beispielsweise wenn eine Software auf einem Datenträger in den Handel kommt, nicht aber bei unkörperlichen Werken, also zum Beispiel beim bloßen Online-Vertrieb per Download.

Angesichts der aktuell unklaren Rechtslage empfiehlt es sich hier, Gebrauchtsoftware im Rahmen der Lizenzverwaltung gesondert auszuweisen.

4. Sonderfall Open-Source-Software (OSS)

Open-Source-Software (OSS) hat inzwischen alle denkbaren Bereiche des Softwareeinsatzes erreicht. Dabei trifft man in der Praxis auf verschiedene OSS-Lizenzen, welche sich durch die dem Nutzer der Software auferlegten Pflichten unterscheiden. Zu den gängigen OSS-Lizenzen gehören unter anderem folgende Lizenzformen:

- Die General Public License (GPL) verlangt, dass Software, welche GPL-Bestandteile verwendet, wiederum nur unter der GPL – also nicht proprietär – vertrieben werden darf (sogenanntes „Copyleft“).

- Charakteristisch für die BSD-Lizenz (Apache Software License) ist hingegen ihr geringer Pflichtenumfang. Mangels Copyleft ist es zulässig, Modifikationen und Weiterentwicklungen auch als proprietäre Software zu vertreiben.

- Eine abgeschwächte Form des Copyleft beinhaltet die Lesser General Public License (LGPL), die insbesondere für die Lizenzierung von Programmbibliotheken gedacht ist.

Trotz des großen wirtschaftlichen Vorteils, den freie Software Unternehmen bietet, hält ihr Einsatz in der Praxis zahlreiche juristische Fußangeln und Risiken bereit. So hat zwar das Landgericht München I in einem Urteil vom 19. Mai 2004 entschieden, dass OSS wie jede andere Software urheberrechtlichen Schutz genießt und die General Public License rechtlich wirksam ist. Doch sind die mit der freien Software aufgeworfenen Rechtsfragen noch nicht abschließend geklärt, woraus sich eine erhebliche Rechtsunsicherheit ergibt. So ist zum Beispiel, wenn nur Bestandteile von OSS in eine andere Software übernommen oder mit dieser verbunden werden, nicht sicher abgrenzbar, ob die neu entstandene Software proprietär verwertbar ist oder

das Copyleft gilt. Das programmierende und investierende Unternehmen weiß also unter Umständen nicht, woran es ist, zumal auch Verstöße gegen OSS-Lizenzen zunehmend stärker verfolgt werden.

Insgesamt ist festzustellen, dass sich freie Software keineswegs im rechtsfreien Raum bewegt, sondern genauso wie proprietäre Software an Lizenzbedingungen gebunden ist. In der Praxis werden dabei häufig durch Missverständnisse bedingte Rechtsverstöße begangen, weil unter freier Software irrtümlich „frei von Lizenzpflichten“ verstanden wird.

Zur Vermeidung von Missverständnissen sollte daher auch Open-Source-Software in die Lizenzverwaltung eines Unternehmens einbezogen werden.

IV. Lizenzkontrolle und Beweisproblematik

1. Audits durch Softwarehersteller

Häufig lassen sich die großen Softwarehersteller in ihren Lizenzbedingungen Auditrechte gegenüber ihren Kunden einräumen. Diese Auditrechte berechtigen die Hersteller, beim Kunden die Einhaltung ihrer Lizenzbestimmungen zu überprüfen. Dabei bedienen sich die Softwarehersteller häufig der großen Wirtschaftsprüfungsgesellschaften, um vor Ort beim Lizenznehmer die Lizenzunterlagen sowie dessen Hardware und Software zu kontrollieren.

Nach dem Besichtigungsanspruch gemäß § 809 BGB kann der Rechteinhaber, der gegen den Besitzer einer Sache einen Anspruch in Ansehung der Sache hat oder sich Gewissheit verschaffen will, ob ihm ein solcher Anspruch zusteht, verlangen, dass ihm der Besitzer die Sache zur Besichtigung vorlegt oder die Besichtigung gestattet, wenn die Besichtigung der Sache für den Rechteinhaber von Interesse ist.
So lässt sich zusammenfassend feststellen, dass sowohl vertragliche wie auch gesetzliche Pflichtenstrukturen bestehen, welche Softwareherstellern die Möglichkeit für Lizenzaudits eröffnen.

2. Mitwirkungspflichten der Lizenznehmer

Ob die Kunden beziehungsweise Lizenznehmer jedoch verpflichtet sind, das vertraglich bestehende Auditrecht zu dulden, oder die entsprechenden Lizenzklauseln AGB-rechtlich unzulässig sind, ist im Einzelnen stark umstritten. Denn die Auditrechte könnten als überraschende Klauseln unzulässig sein, weil nach dem Urheberrecht verdachtsunabhängige Überprüfungen nicht vorgesehen sind. Eingewandt wird auch, dass durch die Kontrollvorgänge beim Lizenznehmer die Rechte Dritter gefährdet oder verletzt werden.
Doch werden letztlich solche rechtlich unsicheren Einwände dem Lizenznehmer in der Praxis nur wenig weiterhelfen, da er im Falle einer Weigerung mit Rechtsstreitigkeiten oder der Beendigung der Geschäftsbeziehung rechnen muss.

Faktisch ist der Lizenznehmer daher gerade gegenüber den großen Softwareherstellern an die Lizenzbedingungen gebunden und tut gut daran, sich frühzeitig auf Lizenzaudits einzurichten. Hierbei hilft ihm die geordnete Darstellung durch eine professionelle Lizenzverwaltung.

3. Lizenznachweis, Beweislast

Ein Lizenznachweis ist eine dokumentierte Nutzungsberechtigung, die vom Hersteller oder Händler unmittelbar oder indirekt erteilt wird. Für die Frage, was bei einer Lizenzprüfung als gültiger Nachweis anerkannt wird, haben sich bislang soweit ersichtlich keine allgemein gültigen Standards heraus gebildet. Trotzdem kann sich der Lizenznehmer bei Beachtung der nachfolgenden Maßgaben rechtlich sicher aufstellen.

a. Verwahrung von Belegen

Häufig werden in den Unternehmen wertvolle Belege wie Quittungen, Rechnungen, Überweisungsträger etc. weggeworfen, die als Lizenznachweise dienen (können). Doch im Zweifel muss der Lizenznehmer beweisen, dass er für seinen Softwarebestand über gültige Lizenzen verfügt. Ebenfalls kommen als Lizenznachweise beispielsweise in Betracht:

- Original-Datenträger (CD-ROM, DVD etc.),
- Lizenzdokumente aller Art, zum Beispiel der „Endbenutzer-Lizenzvertrag“ (EULA),
- Siegel, Aufkleber des Softwareherstellers,
- Echtheitszertifikate, Lizenzverträge,
- Handbücher, Dokumentationen, Anleitungen etc.,
- Schriftverkehr (auch per E-Mail) bei der Vertragsanbahnung.

Bei der geordneten Verwahrung der notwendigen Lizenznachweise ist es hilfreich, wenn sich diese in digitaler Form direkt im Lizenzmanagement den dort erfassten Lizenzpaketen zuordnen lassen. Per Mausklick kann dann ein Administrator, Einkäufer, Auditor oder CIO sofort sehen, auf welcher Vertragsgrundlage das entsprechende Lizenzpaket beruht. Für den Nachweis, dass Software rechtmäßig erworben wurde, ist also neben den Belegen auch eine jederzeit verfügbare Übersicht über den aktuellen Softwarebestand durch eine Inventarisierung und sowie die Darstellung einer Lizenzbilanz im Rahmen einer Lizenzverwaltung erforderlich.

b. Einscannen von Belegen

Das Einscannen von Belegen im Rahmen von Dokumentenmanagementlösungen (DMS) führt bei Schriftstücken formalrechtlich zu einer Minderung der Beweisqualität, da der Vollbeweis durch den Medienwechsel beim Scannen verloren geht. Dies wird in der Praxis aber unschädlich sein, da gescannte Belege akzeptiert werden, sofern der Scanprozess in einem geordneten Verfahren organisiert wird. Hierzu gehört nach den Maßgaben der Grundsätze ordnungsmäßiger DV-gestützter Buchführungssysteme:

- eine genaue Organisationsanweisung und Dokumentation, wer was wann einscannt,
- unveränderliche Formate, zum Beispiel Bildformate oder PDF/A sowie die Speicherung auf WORM-Medien (Write Once Read Multiple) wie CD-R und DVD+-R,
- ausreichende Fehlerkontrolle mit Dokumentation,
- Datensicherheits- und Berechtigungskonzepte,
- Verfahrensdokumentationen.

V. Datenschutz und Mitbestimmung

1. Nutzungsüberwachung der Mitarbeiter

Datenschutzbestimmungen wie das Bundesdatenschutzgesetz, verschiedene Landesdatenschutzgesetze, das Telekommunikationsgesetz (TKG) sowie Mitbestimmungsrechte der Betriebs- und Personalräte sichern die Persönlichkeitsrechte der Mitarbeiter. Wenn daher Softwareagenten von Clientmanagement-Systemen neben ihren klassischen Aufgaben wie der Inventarisierung und Verteilung von Software zudem nutzungsabhängige Lizenzen überwachen oder rechtswidrige Softwarenutzung aufdecken sollen, müssen die erforderlichen Kontrollmaßnahmen die Vorgaben des Datenschutzes einhalten. Neben den urheberrechtlichen Anforderungen, muss also auch die Datenschutzkonformität der Lizenzverwaltung gewährleistet sein.

2. Zulässigkeit von Verhaltenskontrollen

a. Strafverfolgung im Unternehmen nach §32 BDSG

Nach § 32 Abs. 1 Satz 2 BDSG dürfen zur Aufdeckung von Straftaten personenbezogene Daten eines Beschäf-

tigten nur dann erhoben, verarbeitet oder genutzt werden, wenn zu dokumentierende, tatsächliche Anhaltspunkte den Verdacht begründen, dass der Betroffene im Beschäftigungsverhältnis eine Straftat begangen hat und die Kontrollmaßnahme verhältnismäßig ist. Hieraus ergeben sich folglich vier Voraussetzungen:

- konkreter Verdacht gegen einen bestimmten Mitarbeiter,
- tatsächliche Anhaltspunkte, die den Verdacht begründen,
- Dokumentationspflicht bezüglich dieser Anhaltspunkte,
- Verhältnismäßigkeit der Kontrollmaßnahme.

Die IT- und Datenschutzverantwortlichen sind somit gehalten, im Unternehmen einen Prozess zu etablieren, der die Prüfung eines konkreten Verdachts sowie der Verhältnismäßigkeit einschließt und die Dokumentation der konkreten Verdachtsmomente beinhaltet. Nach § 32 Abs. 3 BDSG sind die Betriebs- und Personalräte an diesem Prozedere zu beteiligen. Zu beachten ist, dass die Regelung zur Verhaltenskontrolle nach § 32 Abs. 1 Satz 2 BDSG nur die Aufdeckung von „Straftaten“ betrifft. Damit bleibt die Vorgehensweise bei Verdacht auf eine bloße Ordnungswidrigkeit oder Arbeitspflichtverletzung unterhalb der Strafbarkeitsgrenze offen. Zu empfehlen ist aber eine einheitliche Vorgehensweise für Straftaten und Arbeitspflichtverletzungen.

b. Das neue Beschäftigtendatenschutzgesetz

Der dritte Entwurf eines Gesetzes zur Regelung des Beschäftigtendatenschutzes ist mit Kabinettbeschluss vom 25.08.2010 vorgelegt worden. Seit Jahrzehnten wird über die Notwendigkeit gesetzlicher Regelungen für den Beschäftigtendatenschutz diskutiert. Der vorgelegte Entwurf soll in der Öffentlichkeit stark diskutierte Vorfälle aus den vergangenen Jahren regeln. Es gibt bereits heute zu vielen Fragen des Beschäftigtendatenschutzes eine einzelfallbezogene Rechtsprechung der Arbeitsgerichte, die oft uneinheitlich ist. Mit dem vorliegenden Gesetzentwurf soll die Schaffung umfassender gesetzlicher Regelungen für den Arbeitnehmerdatenschutz verwirklicht werden.

Das Ziel des neuen Beschäftigtendatenschutzgesetzes ist es, die Beschäftigten vor der unrechtmäßigen Erhebung und Verwendung ihrer personenbezogenen Daten besser zu schützen. Gleichzeitig wird jedoch auch das berechtigte Anliegen der Arbeitgeber, Straftaten zu bekämpfen und die Einhaltung geltender Regeln am Arbeitsplatz kontrollieren zu können (Compliance), beachtet. Der Gesetzentwurf trifft unter anderem auch Regelungen zur Nutzung von Telekommunikationsdiensten am Arbeitsplatz sowie zur Zulässigkeit der Datenerhebung, -verarbeitung und -nutzung zum Zweck der Leistungs- und Verhaltenskontrolle, der Korruptionsbekämpfung sowie der Überprüfung, ob die im Beschäftigungsverhältnis zu beachtenden Regeln eingehalten werden (Compliance).

Sobald der Gesetzesentwurf in seiner endgültigen Fassung in Kraft getreten ist, muss er von den Verantwortlichen in den Unternehmen umgesetzt werden.

c. Kontrollen als Organisationspflicht

Um Verstöße gegen Verkehrssicherungspflichten und ein Organisationsverschulden im Unternehmen zu vermeiden, haben die Verantwortlichen die Verfahren und Prozesse im Unternehmen so zu organisieren, dass keine Rechtsverstöße begangen werden. Nach der Rechtsprechung des BGH gilt:
„Wer eine Gefahrenquelle eröffnet oder sich an ihr beteiligt, muss Dritte schützen und hierfür geeignete Schutzmaßnahmen ergreifen.“

Diese Verkehrssicherungspflichten bestehen im Wesentlichen aus:

- Organisationspflichten bezüglich betrieblicher (technischer) Abläufe,
- Aufsichtspflichten des Arbeitgebers gegenüber seinen Mitarbeitern.

Kontrollen zur Einhaltung der urheberrechtlichen Lizenzbestimmungen gehören damit zu den betrieblichen Organisationspflichten eines jeden Unternehmens, das Softwareprodukte einsetzt.

d. Erlaubte Privatnutzung und das Fernmeldegeheimnis

Im Bereich der dienstlichen Nutzung eines Arbeitsplatzrechners misst sich die Datenschutzkonformität von

Kontrollmaßnahmen am Maßstab des BDSG. Bei erlaubter Privatnutzung von Telekommunikation greift hingegen das TKG ein, das als spezielle Regelung dem BDSG vorgeht. Damit verbunden ist die Geltung des Fernmeldegeheimnisses, welches die Datenschutzanforderungen verschärft. Allerdings ist die Anwendbarkeit des TKG beschränkt auf die Telekommunikation, also insbesondere die Verbindungsdaten und Inhalte aus der Internet-, E-Mail- und Telefonkommunikation. Sofern solche Daten bei der Lizenzverwaltung oder -kontrolle betroffen sind, kann das Fernmeldegeheimnis anwendbar sein.

Für den Datenschutz stellt sich zunächst die Ausgangsfrage, ob der Arbeitgeber die private Nutzung von E-Mail, Internet und Telefonie erlaubt oder verboten hat. Bei erlaubter Privatnutzung wird der Arbeitgeber zum Telekommunikationsanbieter, da die Möglichkeit des Arbeitnehmers zur Privatnutzung als Dienstleistung einzustufen ist. Daraus resultiert die Geltung des Fernmeldegeheimnisses (TKG), da sich der Arbeitnehmer auf die Vertraulichkeit der privaten Kommunikation verlassen darf. Kontrollmaßnahmen unter dem Regime des Fernmeldegeheimnisses sind aus Datenschutzgründen problematischer als bei rein dienstlicher Nutzung, welche nur dem BDSG unterfällt.

Auch sofern die Privatnutzung vom Arbeitgeber nicht ausdrücklich erlaubt, sondern nur geduldet wird, greift das Fernmeldegeheimnis ein, denn der Arbeitnehmer darf wegen der Duldung auf den Schutz seiner Privatsphäre vertrauen.

e. Dienstliche Nutzung und Verhältnismäßigkeitsprinzip

Ist dagegen die Privatnutzung verboten und nur eine dienstliche Nutzung möglich, kommt das Fernmeldegeheimnis nicht zur Anwendung. Die dienstliche Nutzung beurteilt sich lediglich nach dem BDSG, sodass Datenerhebungen und Kontrollen in weiterem Umfange zulässig sind.

Durch die Neuregelung beurteilt sich der Arbeitnehmerdatenschutz künftig nach § 32 BDSG, der den bisher anwendbaren § 28 Abs. 1 BDSG zum Teil verdrängt. Werden Daten eines Beschäftigten für Zwecke des Arbeitsverhältnisses erhoben, verarbeitet oder genutzt, findet § 28 Abs. 1 BDSG keine Anwendung mehr.
Für andere Zwecke können im Verhältnis Arbeitgeber zum Beschäftigten die übrigen Vorschriften des BDSG oder andere Gesetze auch weiterhin zur Anwendung kommen. Dazu gehören nach herrschender Meinung insbesondere die Regelungen über die Datenverarbeitung zur Wahrung berechtigter Interessen des Arbeitgebers nach § 28 Abs. 1 Nr. 2 BDSG.

Will also der Arbeitgeber im Rahmen des Lizenzmanagements zum Beispiel nutzungsabhängige Lizenzen überwachen oder rechtswidrige Softwarenutzung aufdecken, so beurteilt sich dies weiterhin nach § 28 Abs. 1 Nr. 2 BDSG. Die Lizenzkontrollen sind zulässig, wenn aufgrund einer Güterabwägung nach dem Verhältnismäßigkeitsprinzip die Maßnahme erforderlich und angemessen ist. In diese Gesamtabwägung der relevanten Belange sind alle beteiligten Interessen mit einzubeziehen. Verfolgt der Arbeitgeber allein den Zweck, Lizenzverstöße oder Überlizenzierung zu vermeiden, wird man im Regelfall von einem überwiegenden Arbeitgeberinteresse und damit von der Datenschutzkonformität ausgehen können. Nicht zulässig ist dagegen eine zweckwidrige Verwertung der Kontrolldaten, zum Beispiel zu Leistungskontrollen.

3. Mitbestimmung und Gestaltung

a. Mitbestimmungsrechte des Betriebsrats

Die soeben erörterten datenschutzkonformen Verhaltenskontrollen im Zusammenhang mit Compliance-Maßnahmen wie dem Lizenzmanagement betreffen speziell den Arbeitnehmerdatenschutz und unterliegen deshalb dem Mitbestimmungsrecht des Betriebsverfassungsgesetzes beziehungsweise des Personalvertretungsrechtes. Das Mitbestimmungsrecht des Betriebsrates besteht gemäß § 87 Abs. 1 Nr. 1 und 6 des Betriebsverfassungsgesetzes (BetrVG) für die Bereiche:

- Ordnung des Betriebes, Arbeitnehmerverhalten,
- technische Kontrolleinrichtungen.

Folglich müssen Betriebs- und Personalräte am Entscheidungsprozess über Verhaltenskontrollen im Zusammenhang mit Compliance-Maßnahmen wie dem Lizenzmanagement beteiligt werden, sofern sie ihre Mitbestimmungsrechte geltend machen. Diese Beteiligung erfolgt in Form von vertraglichen Absprachen mit dem Arbeitgeber, den sogenannten Betriebs- bzw. Dienstvereinbarungen.

Während der Arbeitgeber Missbrauch, Rechtsverstöße und Straftaten verhindern will, befürchtet der Betriebsrat die Ausforschung der Arbeitnehmer. Bei den Standardmaßnahmen der Lizenzkontrolle kann sich der Betriebsrat hier auf Kontrolloptionen und Stichproben beschränken. Zielgerichtete Kontrollen gegen bestimmte Mitarbeiter sollten möglichst unter Beteiligung des Betriebsrates und/oder Datenschutzbeauftragten nach dem Vier-Augen-Prinzip erfolgen.

b. Gestaltung durch Betriebsvereinbarungen

Für die Ausübung der Mitbestimmung kommen insbesondere der Abschluss von Betriebs- und Dienstvereinbarungen mit entsprechenden Nutzungs- und Kontrollregelungen unter anderem für die Lizenzkontrolle in Betracht. Bei einer Betriebs-/Dienstvereinbarung handelt es sich um einen schriftlichen Vertrag zwischen Arbeitgeber und Mitarbeitervertretung, der zur Lösung des Datenschutzproblems geschlossen wird. In Betrieben ab einer Größe von fünf Mitarbeitern sind Betriebsräte und damit Betriebsvereinbarungen möglich. Die Betriebs-/Dienstvereinbarung hat rechtssetzenden Charakter und wirkt modifizierend auf die Inhalte der Arbeitsverträge ein.

c. Einwilligung der Mitarbeiter

Im Bereich des Fernmeldegeheimnisses, das auf ein Grundrecht zurückgeht, ist neben Kollektivvereinbarungen die individuelle Zustimmung der beteiligten Arbeitnehmer von Vorteil. Ergänzend zu entsprechenden Betriebs- und Dienstvereinbarungen kann deshalb eine zusätzliche Legitimation und Information durch eine persönliche Zustimmung des betroffenen Arbeitnehmers erfolgen, sofern diese Einwilligung freiwillig getroffen wird.

VI. IT-Compliance und Risikomanagement

Risiko- und Informationssicherheitsmanagement (ISMS), interne Kontrollsysteme (IKS), Haftungsfragen und IT-Compliance stehen nicht beziehungslos nebeneinander, sondern bilden ein verzahntes Gesamtkonzept.
IT-Compliance verlangt die Einhaltung gesetzlicher Bestimmungen, vertraglicher Pflichten sowie anerkannter Standards und erfordert konkrete Maßnahmen. Werden diese nicht getroffen, können Rechtsverstöße zu gravierenden, bestandsgefährdenden Schäden führen. Deshalb ist im Rahmen des gesetzlich verbindlichen Risiko- und Informationssicherheitsmanagements (ISMS) ein Frühwarnsystem zur Risikoerkennung und -kontrolle einzurichten.

1. Gesetzliche Regelungen zum Risikomanagement

Die Unternehmensleitung von Kapitalgesellschaften (z. B. AG, GmbH) hat für ein wirksames Risikomanagement-System zu sorgen. Im Gesetz zur Kontrolle und Transparenz im Unternehmensbereich (KonTraG) schreibt der Gesetzgeber entsprechende Sicherungsmaßnahmen vor. Ein Vorstand einer Aktiengesellschaft hat ebenfalls nach § 91 Abs. 2 des Aktiengesetzes (AktG) geeignete Maßnahmen zu treffen, insbesondere ein Überwachungssystem einzurichten, das bestandsgefährdende Entwicklungen frühzeitig erkennt. Dieses Frühwarnsystem erfordert unter anderem eine präventive Überwachung und Erkennung von Fehlentwicklungen in den Bereichen IT-Compliance, Informationssicherheit und Datenschutz. Auch das BSI verweist in seinen Standards ausdrücklich auf das KonTraG. Ähnliche oder gleichlautende Vorgaben machen auch Bestimmungen aus den Bereichen Basel II (MaRisk), Deutscher Corporate Governance Kodex, SOX oder GoBS.

2. Interne Kontrollsysteme (IKS) und Risikomanagement

Die gesetzliche Regulierung des internen Kontrollsystems in GoBS, KonTraG, SOX etc. sowie die gleichlaufenden Anforderungen der Wirtschaftsprüfer sind ein wesentlicher Bestandteil des Risikomanagements, aber auch des Informationssicherheitsmanagements (ISMS). Das IKS ist die Gesamtheit aller aufeinander abgestimmten Kontrollen und Regelungen zum Schutz des Vermögens und der Informationen vor Verlusten aller Art durch Bereitstellung aussagefähiger Aufzeichnungen und deren Auswertung.
Im Rahmen der internen Kontrollsysteme ist insbesondere die Einrichtung IT-spezifischer Schlüsselkontrollen (Key Controls), wie zum Beispiel die regelmäßige Überprüfung kritischer Berechtigungen, Datensicherungs- und Virenschutzmaßnahmen, Verhinderung von Straftaten und Rechtsverstößen etc. erforderlich.

3. Lizenzmanagement als Teil der internen Kontrollsysteme

Wenn in einem Unternehmen Lizenzverstöße und damit Straftaten und Schadensersatzforderungen durch Unterlizenzierung oder wirtschaftliche Schäden durch Überlizenzierung drohen, ist es aufgrund der Vorgaben des Risikomanagements Aufgabe der Unternehmensleitung, Rechtsverstöße oder Vermögensverluste zu verhindern.

Adäquates Mittel hierfür ist nach der Struktur der internen Kontrollsysteme die Einrichtung der dazu notwendigen Lizenzkontrollen durch ein geeignetes Lizenzmanagementsystem das in der Lage ist, sowohl Rechtsverstöße wie auch unnötige Vermögensverluste rechtzeitig zu erkennen (Frühwarnsystem).

VII. Haftungsfragen

1. Rechtsfolgen von Lizenzverstößen

a. Zivilrechtliche Folgen – Abmahnung, Unterlassung, Schadensersatz

Einem Rechtsverstoß im Urheberrecht folgt zumeist eine Abmahnung, um den Verletzer über die Urheberrechtsverletzung zu informieren und ein aufwendiges und teures Gerichtsverfahren zu vermeiden. In der Abmahnung fordert der Rechteinhaber (Softwareunternehmen) den Verletzer zur Abgabe einer strafbewehrten Unterlassungserklärung auf, die der Verletzer abgeben muss, um die Wiederholungsgefahr für weitere Rechtsverstöße zu beseitigen. Für den Fall der Weigerung droht dem Verletzer der Erlass einer einstweiligen Verfügung. Sofern der Verletzer nach Abgabe der strafbewehrten Unterlassungserklärung erneut gegen Lizenzbedingungen verstößt, verwirkt er eine hohe Vertragsstrafe.

Beschränkt sich der Rechtsverstoß auf die Verletzung von zumutbaren Prüfungs- und Sicherungspflichten (die sogenannte Störerhaftung), so hat der Verletzer zumindest die angefallenen Rechtsanwaltskosten zu ersetzen. Liegt wie in den meisten Fällen darüber hinaus ein Verschulden vor (Vorsatz oder Fahrlässigkeit bezüglich der Lizenzverletzung), so muss der Verletzer auch Schadensersatz leisten. Die Höhe des Schadensersatzes bemisst sich nach der Höhe der zu zahlenden Lizenzgebühren, der sogenannten Lizenzanalogie.

b. Voraussetzungen der Strafbarkeit

Eine Urheberrechtsverletzung kann auch strafbar sein. Nach § 106 Abs. 1 UrhG droht demjenigen eine Freiheitsstrafe bis zu drei Jahren oder eine Geldstrafe, der ohne eine Lizenz und ohne Einwilligung des Rechteinhabers ein Werk vervielfältigt, verbreitet oder öffentlich wiedergibt. Das Kopieren von Software ohne Einwilligung des Rechteinhabers ist demnach verboten, sofern nicht gesetzliche Ausnahmen wie zum Beispiel zulässige Sicherungskopien, Reverse Engineering oder Dekompilierung eingreifen. Handelt der Täter gewerbsmäßig, beträgt die maximale Freiheitsstrafe sogar fünf Jahre. Voraussetzung für eine strafrechtliche Verantwortlichkeit ist aber stets ein vorsätzliches Handeln des Rechtsverletzers.

Nach deutschem Strafrecht kann nur eine natürliche Person zu einer Geld- oder Freiheitsstrafe verurteilt werden. Eine juristische Person kann sich nicht strafbar machen.

Wird also in einem Unternehmen eine Straftat durch Unterlizenzierung begangen, so werden die handelnden Personen (zum Beispiel Administrator, IT-Leiter, Geschäftsführer) zur Rechenschaft gezogen. Weist die Staatsanwaltschaft beispielsweise nach, dass die Geschäftsführung die Lizenzrechtsverstöße vorsätzlich etwa um Kosten zu sparen begangen oder in Kauf genommen hat, liegt Strafbarkeit der Geschäftsführung vor.

Auch Bußgeldtatbestände sind bei unzureichender Lizenzkontrolle denkbar. Wer als Inhaber eines Betriebes oder Unternehmens vorsätzlich oder fahrlässig die Aufsichtsmaßnahmen unterlässt, die erforderlich sind, um in dem Betrieb oder Unternehmen Pflichtverletzungen zu verhindern, kann gemäß § 130 des Ordnungswidrigkeitengesetzes (OwiG) mit einer Geldbuße bis zu einer Million Euro belegt werden.

2. Unternehmenshaftung

a. Zumutbare Prüfungs- und Organisationspflichten

Das Unterlassen von Verkehrssicherungspflichten führt zur Haftung. Umgekehrt ist die Erfüllung von Verkehrssicherungspflichten ein präventiver Schutz gegen Schadensersatzansprüche und Strafbarkeit. Wer das notwendige Maß an Sicherheit erbringt, indem er erforderliche technische und organisatorische Schutz- und Kontrollmaßnahmen im Rahmen eines angemessenen Lizenzmanagements ergreift, dem kann, wenn gleichwohl ein Schaden eintritt, kein Verschuldensvorwurf gemacht werden. Mit anderen Worten: Die Erfüllung der Verkehrssicherungspflichten führt zur Haftungsfreizeichnung, auch wenn ein Schaden eintritt. Der Sorgfältige, vorausschauend Planende wird für seine Vorsorgemaßnahmen belohnt, auch wenn sich das verbliebene Restrisiko in einem Schaden realisiert hat.

b. Störerhaftung bei illegalem Download

Nicht in jedem Fall setzt die Haftungsverantwortlichkeit ein Verschulden (Vorsatz oder Fahrlässigkeit) voraus. Für die sogenannte Störerhaftung genügt bereits die Verletzung zumutbarer Sicherungs- und Prüfungspflichten. Der Umfang der Prüfungspflichten bestimmt sich danach, ob und inwieweit dem als Störer in Anspruch Genommenen nach den Umständen eine Prüfung zuzumuten ist. Diese Zumutbarkeit wird man für den Abgleich der installierten Software mit den vorhandenen Lizenzen in jedem Falle annehmen können.
Selbst wenn also lizenzwidrige Softwareprodukte zum Beispiel durch Mitarbeiter illegal aus dem Internet heruntergeladen werden, greift eine Haftungsverantwortlichkeit des Arbeitgebers nach den Maßgaben der Störerhaftung ein.

3. Haftung der Mitarbeiter

a. Eigenhaftung nach der Rechtsprechung des Bundesarbeitsgerichts

Die Vermeidung persönlicher Eigenhaftung ist für die handelnden Mitarbeiter ein entscheidender Faktor. Hierbei ist zwischen der:

- zivilrechtlichen (Schadensersatz),
- arbeitsrechtlichen (Abmahnung, Kündigung) und
- strafrechtlichen (Geld- oder Freiheitsstrafe).

Haftung zu unterscheiden.

Aus dem Arbeitsverhältnis treffen grundsätzlich jeden Mitarbeiter sogenannte arbeitsvertragliche Nebenpflichten wie Schutz-, Mitwirkungs-, Geheimhaltungs- und Aufklärungspflichten. Als Sorgfaltsmaßstab gilt hierbei ein besonnener Mensch mit durchschnittlichen Fähigkeiten in der Situation des Arbeitnehmers. In der Praxis bedeutet dies, dass die Maßstäbe individuell unterschiedlich sind: So werden an leitende Mitarbeiter höhere Sorgfaltsanforderungen gestellt. Bei Fragen der Pflichtverletzung trifft nach § 619a BGB die Beweislast hier den Arbeitgeber. Das heißt, der Arbeitgeber muss Rechtsverstöße des Arbeitnehmers beweisen (Beweislastumkehr zugunsten des Arbeitnehmers).

Schadensersatzansprüche des Arbeitgebers wegen Verletzung der arbeitsvertraglichen Nebenpflichten sind in der Praxis nicht häufig, aber möglich. Aufgrund der Fremdbestimmtheit der Arbeitsleistung trägt der Arbeitgeber das Unternehmensrisiko. Für den Arbeitnehmer im Arbeitsverhältnis gelten deshalb nach der Rechtsprechung des BAG die nachfolgenden Haftungsregeln:

- für vorsätzliches / grobfahrlässiges Verhalten: volle Haftung des Mitarbeiters,
- mittlere Fahrlässigkeit: Schadensteilung zwischen Arbeitgeber und Mitarbeiter,
- leichte Fahrlässigkeit: keine Haftung des Mitarbeiters.

Im Ergebnis ist der Arbeitnehmer für Lizenzverstöße insbesondere dann verantwortlich, wenn er Kenntnis von den rechtswidrigen Lizenzverhältnissen hat oder grob fahrlässig handelt. Macht er lediglich Fehler (einfache Fahrlässigkeit), führt dies in der Regel nicht zur schadensersatzrechtlichen Verantwortlichkeit. Diese Haftungserleichterung für den Mitarbeiter gilt grundsätzlich nur im Verhältnis zum Arbeitgeber. Im Verhältnis zu geschädigten Dritten besteht ein Freistellungsanspruch des Arbeitnehmers gegen den Arbeitgeber.
Nicht von der Haftungserleichterung erfasst sind die arbeitsrechtlichen Sanktionen der Abmahnung oder Kündigung, welche bei Pflichtverstößen des Mitarbeiters stets eintreten können.

b. Strafrechtliche Verantwortlichkeit

Für eine mögliche Strafbarkeit greift keine Haftungserleichterung. Vielmehr gilt der Grundsatz der vollständigen Eigenverantwortung. Ein Arbeitnehmer macht sich also selbst strafbar, die arbeitsvertragliche Haftungserleichterung ist nicht anwendbar. Auch gilt kein Befehlsnotstand, sodass ein Mitarbeiter, der zum Beispiel auf Anweisung seines Vorgesetzten Lizenzverstöße begeht, nicht allein wegen der Anweisung straflos ist.

c. Haftung der Verantwortlichen, Garantenstellung

Sofern Mitarbeiter für die Einhaltung der Lizenzbestimmungen funktionell zuständig sind (zum Beispiel Lizenzmanager, Compliance-Officer, IT-Verantwortliche), obliegt ihnen eine Garantenstellung nach § 13 StGB für die Verhinderung von Lizenzverstößen. Solche Funktionsträger können sich in der Folge ihrer Garantenstellung auch durch Unterlassen von Sicherungsmaßnahmen oder die Verletzung von Sorgfaltspflichten strafbar machen (vergleichbar mit der Garantenstellung des Compliance-Officers nach der BGH-Entscheidung vom 17.07.09).

Funktionsträger haften also strafrechtlich, aber auch zivilrechtlich unter verschärften Bedingungen.

4. Persönliche Haftung der Leitungsebene

In arbeitsteiligen Organisationen (Unternehmen, Behörden) hat nach der Rechtsprechung des BGH die Leitungsebene durch Anordnungen und Kontrollen dafür zu sorgen, dass durch die betrieblichen Arbeitsabläufe Dritte nicht geschädigt werden. Bei Verletzung dieser Organisationspflichten liegt ein selbstständiges Organisationsverschulden vor, dass zur eigenen Haftung nach § 823 BGB führt. Die Verletzung von Verkehrssicherungspflichten kann in Schadensersatzansprüche und Strafbarkeit münden.

Gemäß § 93 Abs. 2 Satz 1 AktG sind Vorstandsmitglieder, die ihre Pflichten verletzen, der Gesellschaft als Gesamtschuldner zum Schadenersatz verpflichtet. Damit ist im Schadensfalle nicht nur die Gesellschaft, sondern auch das einzelne Vorstandsmitglied persönlich haftbar. Die Beweislast für die Entkräftung von vorgeworfenen Pflichtverletzungen trägt die Leitungsebene selbst.

Bei Verstößen gegen das Risikofrüherkennungssystem kann dem Vorstand in der Aktionärsversammlung die Entlastung verweigert werden (LG München vom 05.04.2007).

Aagon Consulting GmbH

Aagon Consulting hat es sich zum Ziel gesetzt, IT-Verantwortliche in Unternehmen und Organisationen bei der Senkung ihrer IT-Kosten zu unterstützen. Zu diesem Zweck entwickelt und vertreibt die deutsche Firma Lösungen zur Einführung eines unternehmensweiten Betriebssystemstandards auf Clients und Servern sowie für das effektive Clientmanagement. Ein Modul der Aagon Client Management Plattform (ACMP) ist das Lizenzmanagement, das fest mit den weiteren Komponenten von ACMP wie der Inventarisierung von Hard- und Software, der Verteilung von Betriebssystemen und Anwendungen sowie einem Helpdesk integriert ist. Die Produkte und Lösungen von Aagon helfen IT-Administratoren, in weniger Zeit und mit weniger Mitteln mehr Dinge zu erledigen und so die Total Cost of Ownership ihrer IT-Landschaft nachhaltig zu senken. Die über 15-jährige Erfahrung bei Migrationsprojekten und Rollouts jeder Größenordnung sowie bei der Erstellung von Softwarepaketen kommt nicht nur den Produkten von Aagon zugute. Im Rahmen von professionellen Consulting-Services können auch Unternehmen von der Expertise der Spezialisten profitieren. Der Hauptsitz von Aagon Consulting ist in Soest.

Hinweis

Dieses Dokument stellt einen generellen Leitfaden dar. Es ersetzt nicht die verbindliche Rechtsauskunft durch einen Fachanwalt. Bitte haben Sie Verständnis, dass trotz Sorgfalt bei der Erstellung eine Garantie oder Haftung für die inhaltliche Richtigkeit nicht übernommen wird. Grundsätzlich ist jedem Unternehmen anzuraten, sich bei lizenz- oder datenschutzrechtlichen Fragen vor jeglicher Implementierung individuell rechtlich beraten zu lassen.

Lange Wende 33
D-59494 Soest

Fon: +49 (0) 29 21 - 78 92 00
Fax: +49 (0) 29 21 - 78 92 44
www.aagon.de