Lexikon für das IT-Recht 2012

Die 140 wichtigsten Praxisthemen

Bearbeitet von
Dr. Eugen Ehmann

3. Auflage 2012. Buch. 426 S. Kartoniert
ISBN 978 3 7825 0531 4

2.2 Nachteile

- Keine Beschränkung der Mängelhaftung auf ein Jahr ab Überlassung, sondern Haftung für Mängel während der gesamten Überlassungszeit
- Erhöhte Sorgfaltspflichten gegenüber der einmaligen Leistung bei Verkauf von Software
- Bei Problemen mit der Internetverbindung ist keine Nutzung der Anwendung möglich. Der Provider haftet auch für diesen Nutzungsausfall.

Fazit

Der ASP-Vertrag bietet die Möglichkeit, Software zu mieten, die beim Provider installiert ist und nur für die Zeit zu vergüten, in der sich die Software tatsächlich im Einsatz befindet.

Der Vorteil des ASP ist in erster Linie Kosteneinsparung, die insbesondere dann stark ins Gewicht fällt, wenn eine teure Software selten genutzt wird. Der Nachteil ist die riskante Abhängigkeit, in die sich ein Kunde begibt, wenn er über seine IT-Lösung und seine Daten nicht allein verfügen kann.

Archivierung von E-Mails – Rechtliche Rahmenbedingungen

I. Einleitung: E-Mail-Archivierung als Teil eines professionellen Risikomanagements

Die nachfolgenden Ausführungen beschäftigen sich intensiv mit den rechtlichen Rahmenbedingungen der Archivierungspflicht von E-Mails (als Teil eines effektiven IT-Risikomanagements) und zeigen insbesondere auf, welche Konflikte im Zusammenhang mit dem Datenschutz bestehen und wie diese wiederum gemeistert werden können.

Heutzutage sind in der Geschäftswelt nahezu alle denkbaren Prozesse von einer Kommunikation per E-Mail abhängig. So machen manchen Schätzungen zufolge E-Mails bei mittelständischen Unternehmen und Konzernen 60–70 % (!) der Kommunikation aus. Man denke dabei an

- den Logistikbereich,
- das Marketing,
- die Produktion,
- die Kommunikation mit Lieferanten und Abnehmern,
- die Auftragserteilung,
- die Rechnungsstellung und etwa
- den firmeninternen Kommunikationsaustausch (etwa via Intranet) etc.

Vor dem Hintergrund erstaunt auch der Siegeszug der Kommunikationsform E-Mail nicht, ist sie doch

- leicht beherrschbar,
- flexibel,
- schnell und weltweit einsetzbar,
- und (im Vergleich zu Fax oder Telefon) ein preiswertes, ja fast kostenloses Kommunikationsmittel.

Die enge Verzahnung von unternehmerischem Handeln und dem Einsatz von Informationstechnik hat aber auch ihre Kehrseite.

1. Zeitaufwand

So verursacht das Phänomen „Spam“ im System der weltweiten E-Mail-Kommunikation einen erheblichen Schaden, da der Zeitaufwand enorm ist, den jeder Bearbeiter aufbringen muss, um Spam-Mail von geschäftsrelevanten Mails zu unterscheiden.

2. Sicherheitsrisiko

Die E-Mail hat sich gerade in den letzten Jahren als großes Viren-Einschleusetor erwiesen. Spätestens seit dem E-Mail-Virus „Worm“ ist dies einer breiteren Öffentlichkeit bekannt und bewusst.

3. Ordnungs- bzw. Speicherprobleme

Durch die gewaltige Zunahme des E-Mail-Aufkommens kommt es für die IT-Verantwortlichen einer Firma zu ganz praktischen Problemen:

- Wie behält man den Überblick?
- Wie begegnet man überquellenden Mailordnern?
- Welche E-Mails dürfen gelöscht werden und welche nicht?
- Auf welche Art und Weise sollte man E-Mails speichern?
- Wie lange hat man E-Mails zu speichern?

4. Ausfall der E-Mail-Kommunikation

So gut wie in allen Fällen haben ernstzunehmende Ausfälle oder Störungen der unternehmenseigenen IT-Infrastruktur direkte Auswirkungen auf den jeweiligen unternehmerischen Erfolg. Ließ sich beispielsweise in den 80er-Jahren ein Komplettausfall der IT-Umgebung noch halbwegs verkraften, so kann derselbe Ausfall heutzutage schnell existenzbedrohende Züge annehmen. So sei an dieser Stelle etwa eine Studie des Marktforschungsinstitut „Meta Group“ zitiert, welche zu dem Ergebnis kam, dass ein zehntägiger Ausfall von IT-Schlüsselsystemen mit einer Wahrscheinlichkeit von 50 Prozent zum Einstellen des Betriebs in den kommenden fünf Jahren führt.

5. Immer komplexer werdende rechtliche Anforderungen

Gerade angesichts der Relevanz der E-Mail in der Geschäftskorrespondenz ist es kein Wunder, dass gesetzliche wie auch behördliche Regelungsrahmen hinsichtlich des Umgangs mit E-Mails (und damit einhergehend die organisatorischen und technischen Herausforderungen) immer weitere Ausmaße annehmen:

- So ist etwa am 1.1.2007 das „Gesetz über elektronische Handelsregister und Genossenschaftsregister sowie das Unternehmensregister“ (EHUG) in Kraft getreten. Dieses bringt unter anderem für die im Handelsregister eingetragenen Unternehmen die Neuerung mit sich, dass diese nun auch bei ihrer via E-Mail oder via Fax geführten Korrespondenz bestimmte formale Anforderungen einhalten müssen, die bisher nur für gedruckte Geschäftsbriefe galten.
- Nicht zuletzt hat es der Gesetzgeber sich zum Ziel gesetzt, mittels einer ganzen Reihe von gesetzlichen Bestimmungen einen rechtlich verbindlichen Verhaltenskodex (s. dazu unten unter Abschnitt III) zu schaffen, um den Unternehmer zu einem gewissenhaften Risikomanagement, also dem planvollen Umgang mit unternehmerischen Risiken zu „erziehen“.

Das Thema „E-Mail-Archivierung“ stellt im Zusammenhang mit dem IT-Risikomanagement ein Teilaspekt dar, der aber gerade in den letzten Jahren Wellen geschlagen hat. So verlangt das Gesetz bereits seit ein paar Jahren von Kaufleuten, dass E-Mails, die in Bezug zu Rechtsgeschäften stehen oder sonst wie steuerrechtlich relevant sind, nach handelsrechtlichen sowie steuerrechtlichen Anforderungen mehrere Jahre ordnungsgemäß zu archivieren sind.

II. Rechtliche Risiken

Eine E-Mail wird in ihrer rechtlichen Bedeutung teilweise unterschätzt. Dies zu Unrecht, da die in einer E-Mail enthaltene Erklärung bzw. Information rechtsrelevant ist und im Geschäftsverkehr dieselbe rechtliche Bedeutung zukommt wie ihr Pendant in Papierform. Vor diesem Hintergrund ist es nicht nachvollziehbar, dass bislang nur relativ wenige Unternehmen das Kommunikationsmedium E-Mail wirklich „beherrschen“ – gerade in rechtlicher Hinsicht. Oftmals sind es die Firmenmitarbeiter, die für den Inhalt und die Verwertung der ausgetauschten Nachrichten zuständig sind, während die Unternehmen sich damit begnügen, eine stabile und kosteneffiziente Telekommunikationsinfrastruktur bereit zu stellen. Fragen der unternehmensgesteuerten Archivierung des eigenen E-Mail-Verkehrs kommen dabei oftmals zu kurz.

Diese Nachlässigkeit kann schnell nach hinten losgehen, wie etwa ein Fallbeispiel aus den USA zeigt. So wurde einem deutschen Unternehmen, nämlich der Deutschen Bank, Ende 2002 durch die US-Börsenaufsicht SEC eine Strafzahlung in Höhe von 1,65 Millionen US-Dollar auferlegt. Hintergrund: Anlageberater des Unternehmens hatten (entgegen den unternehmenseigenen Vorgaben) E-Mails nur unzureichend gespeichert. Dadurch waren Ermittlungsverfahren zu bestimmten umstrittenen Anlageempfehlungen erschwert bzw. vereitelt worden. Auch in Deutschland sind Sanktionen bei einer nur mangelhaften E-Mail-Archivierung durchaus möglich.

1. Verletzung der Buchführungspflicht

So kann etwa eine mangelhafte E-Mail-Archivierung als Verletzung der handelsrechtlichen Buchführungspflichten gewertet werden und wegen der Maßgeblichkeit zugleich eine Verletzung der steuerrechtlichen Buchführungspflicht gleichkommen. Da wiederum Mängel der Buchführung die steuerrechtliche Beweiskraft der Bücher beeinträchtigt, wäre die Finanzverwaltung in diesem Fall berechtigt, den steuerlichen Gewinn nach § 162 Abs. 2 AO zu schätzen. Zudem könnte die Finanzverwaltung die Buchführungspflicht durch ein Zwangsgeld erwirken (§ 328 Abs. 1 AO).

2. Straftat

Abgesehen von steuerrechtlichen Sanktionen kann die Verletzung der E-Mail-Archivierungspflicht strafbar sein, etwa wenn durch eine unzureichende oder gar manipulative Archivierung von E-Mails das Unternehmen vorsätzlich die Übersicht über dessen Vermögensstand erschwert mit dem Ziel, Vermögens-

spruch könne sich der Schuldner nicht auf Unkenntnis der maßgeblichen Preise berufen.

XXXIII. Wie kann man den jeweiligen Ladenpreis überhaupt sicher feststellen?

Tatsächlich ist die Frage, wie und wo man bei über 1 Millionen lieferbaren Büchern den jeweiligen gebundenen Ladenpreis sicher feststellen soll, nicht einfach zu beantworten. Gerade die semi-professionellen Buchhändler, die ihre Waren über die eBay und/oder die Amazon-Plattformen anbieten, sind hier oft überfordert. Zwar müssen Preisaufhebungen und Preissenkungen dem Buchhandel bekannt gemacht werden – etwa über die „Gelben Seiten" im Börsenblatt für den Deutschen Buchhandel oder über das „Verzeichnis lieferbarer Bücher". Doch häufig melden die Verlage ihre Preisänderungen oder Preisaufhebungen nicht.

TIPP!

Immerhin bietet sich auch die Möglichkeit der Recherche über ISBN-Nummern bei www.buchhandel.de/ oder etwa Web-Angebote wie www.libri.de.

XXXIV. Kann sich ein Händler (hinsichtlich gebrauchter Ware) gegen Abmahnungen schützen? Wie?

Abmahngefährdet ist ein Händler vor allem dann, wenn für die von ihm unterhalb des Buchbindungspreises angebotene Ware eigentlich noch eine Preisbindung besteht, d. h. wenn eine Umgehung des BuchPrG vorliegt. Häufig jedoch weiß möglicherweise der Händler gar nicht, dass für seine Ware noch eine Buchpreisbindung besteht, da er vermeintlich gebrauchte Ware (z. B. auf einem Flohmarkt) zur Weiterveräußerung gekauft hat.

Ein den Unterlassungsanspruch auslösender Verstoß gegen das BuchPrG ist jedoch verschuldensunabhängig, d. h. der Händler kann sich nicht darauf berufen, keine Kenntnis von der Preisgebundenheit der Ware gehabt zu haben. Vielmehr liegt es in seinem Verantwortungsbereich, die Ware ordnungsgemäß zu verkaufen. Er kann sich nicht ohne weiteres auf die Angaben seines Lieferanten verlassen, dass es sich bei der Ware um nicht mehr preisgebundene Ware handelt.

Einzig bliebe dem Händler eventuell die Möglichkeit, seinen Lieferanten für einen ihm entstandenen Schaden in Regress zu nehmen, was jedoch schwierig wäre bei Ware, die auf Flohmärkten erstanden wurde, da der Lieferant im Zweifel nicht greifbar ist. Letztlich könnte hier nur durch eine schriftliche Vereinbarung die Qualität der Ware festgehalten werden, so dass die Beweisführung später erleichtert würde.

BYOD (Bring Your Own Device)

I. Bedeutung von BYOD

Privat genutzte Notebooks und Smartphones entsprechen inzwischen in ihrer Leistungsfähigkeit den für betriebliche Zwecke angeschafften Geräten. Die Grenzen zwischen den Geräten für Verbraucher und Geschäftsanwender verschwimmen. Gleichzeitig nutzen Anwender ihre Privatgeräte für betriebliche Aufgaben und umgekehrt Geräte des Arbeitgebers zu privaten Zwecken.

Während die Privatnutzung von Smartphones und Notebooks, die der Arbeitgeber gestellt hat, häufig ohne ausdrückliche Erlaubnis erfolgt, wird die betriebliche Nutzung von Privatgeräten oftmals vom Arbeitgeber sogar gefördert. Man spricht in diesem Zusammenhang von „Bring Your Own Device" oder BYOD.

Mit BYOD verbinden viele Unternehmen eine Kostenersparnis bei der Anschaffung von Endgeräten und eine Produktivitätssteigerung bei den Beschäftigten, die zum einen mit dem von ihnen bevorzugten Gerät arbeiten können und zum anderen darüber auch außerhalb der reinen Arbeitszeit für Kunden und Arbeitgeber erreichbar sind.

Vergessen werden darf aber nicht, dass die Vermischung von betrieblicher und privater Datenverarbeitung deutliche Konsequenzen für den Datenschutz und die Datensicherheit haben kann. Das gilt insbesondere dann, wenn es keine klare Regelung für die betriebliche Nutzung von Privatgeräten gibt.

II. Risiken bei BYOD

1. BYOD ist beliebt und gefürchtet zugleich

87 Prozent der in der Studie „Consumerization of IT: A Survey of IT Professionals" von Dimensional Research befragten Unternehmen gaben an, dass sie ihre Daten nicht unter Kontrolle haben, weil Mitarbeiter private IT-Geräte zu geschäftlichen Zwecken verwenden. 64 Prozent wissen nicht, welche privaten IT-Geräte zu betrieblichen Zwecken genutzt werden. 62 Prozent sehen Bedarf an Werkzeugen, um die Geschäftsdaten auf privaten Smartphones oder Notebooks zu kontrollieren. 32 Prozent vermuten, dass ihre Mitarbeiter auch ohne Erlaubnis mit ihren Privatgeräten Firmendaten nutzen.

Laut einer Umfrage von Juniper Networks haben zum Beispiel 81 Prozent der Smartphone-Nutzer bereits mit ihrem Privatgerät unerlaubt auf Firmendaten zugegriffen, 58 Prozent machen dies jeden Tag.

WICHTIG!

Die unkontrollierte Nutzung von privaten IT-Geräten im Unternehmensumfeld gefährdet vertrauliche Daten und wichtige Infrastrukturen. Zum einen ist der Sicherheitsstatus der Privatgeräte unbekannt und kann nicht ohne weiteres durch betriebliche Sicherheitsmaßnahmen beeinflusst werden. Zum anderen können → *Schadprogramme* auf den Privatgeräten Zugang zum Unternehmensnetzwerk bekommen. Weiterhin besteht die Gefahr, dass Unternehmensdaten beim Ausscheiden eines Be-

schäftigten auf dem Privatgerät verbleiben, oder aber dass Beschäftigte ihre Privatgeräte nutzen, um Daten unerlaubt zu kopieren und zu verbreiten. Deshalb zählt das Information Security Forum (ISF) den Trend BYOD zu den Top-Risiken des Jahres 2012.

2. Risiken von BYOD werden noch unterschätzt

Der Trend zur Vermischung privater und geschäftlicher Datenverarbeitung wird trotzdem noch von vielen Unternehmen als ungefährlich gesehen. Die Umfrage „Consumerization of IT" von Symantec zeigt, dass 85 Prozent der befragten Unternehmen glauben, dass die freie Wahl des dienstlich genutzten Smartphones die Zufriedenheit der Nutzer erhöht, 71 Prozent meinen, die freie Wahl erhöhe die Mitarbeiterproduktivität, nur 52 Prozent glauben, die freie Smartphone-Wahl für dienstliche Zwecke könne ein gewisses Sicherheitsrisiko darstellen, und 23 Prozent der Befragten meinen sogar, dies hätte keinen Einfluss auf die Datensicherheit.

III. Regelungsbedarf bei BYOD

1. Benutzerrichtlinie muss für Daten- und Anwendungstrennung sorgen

Um die Vorteile von BYOD nutzen zu können, ohne die Privatsphäre des Anwenders (Kontrolle aller Daten auf den Privatgeräten) oder aber die betriebliche Datensicherheit (Verzicht auf Kontrolle) zu gefährden, sollten Unternehmen eine Benutzerrichtlinie (Policy) entwickeln und deren Umsetzung mit den betroffenen Beschäftigten vereinbaren. Die wesentlichen Fragen, die diese Policy klären sollte, sind:

WICHTIG!

Welche Ziele verfolgt das Unternehmen mit BYOD?

Welche verschiedenen Typen von Privatgeräten sind für die betriebliche Nutzung erlaubt?

Welche Art von Sicherheitsvorgaben gibt es und wie wirken sich diese aus?

Wie sind die personenbezogenen und alle privaten Daten dabei geschützt?

Wer trägt die Kosten für die betriebliche Nutzung der Privatgeräte?

Welchen Support erhalten die Nutzer für ihre betrieblich genutzten Privatgeräte?

Wie werden mögliche Verstöße gegen die Policy geahndet?

2. Spezielle Sicherheitslösung kann dabei unterstützen

Auf Basis der verabschiedeten Policy für BYOD können spezielle Sicherheitswerkzeuge bei der Umsetzung und stichprobenartigen Kontrolle der Einhaltung helfen. Die ausgewählte Sicherheitslösung muss dabei die intern festgelegte Benutzerrichtlinie abbilden können.

WICHTIG!

Unterstützen können Lösungen aus dem Bereich Device Management, also Inventurlösungen, die alle betrieblich zugelassenen Geräte – ob privat oder geschäftlich – erfassen, und verbotene Geräte bei versuchtem Datenzugriff im Unternehmensnetzwerk blockieren.

Zudem sind Lösungen hilfreich, die aus einem Gerät zwei virtuelle Geräte machen können. Im Prinzip werden dabei Daten und Anwendungen entweder der Kategorie „dienstlich" oder der Kategorie „privat" zugeordnet, wobei eine Vermischung verboten ist. Dienstliche Anwendungen können dann nicht auf private Daten zugreifen und umgekehrt.

Beispiel:

Mit der Benutzerrichtlinie und unterstützender Sicherheitssoftware muss bei Einführung von BYOD zum Beispiel verhindert werden:

die Übernahme von Firmendaten in private Anwendungen,

die Weiterleitung von Firmendaten mit privaten Mail-Programmen,

die Speicherung von Firmendaten in privaten Verzeichnissen und

die Übertragung von Firmendaten auf private Speichermedien,

aber auch der betriebliche Zugriff auf private Daten des Nutzers.

IV. Checkliste

WICHTIG!

Entwicklung und Freigabe einer Policy für die betriebliche Nutzung von Privatgeräten

Unterweisung der betroffenen Beschäftigten über die Inhalte der Policy

Inventarisierung der betrieblich genutzten Geräte

Klassifizierung der Anwendungen und Daten in „betrieblich" und „privat"

Prüfung der Einhaltung der BYOD-Policy

Einsatz einer Sicherheitssoftware zur Trennung der betrieblichen und privaten Datenverarbeitung auf Endgeräten, die parallel dienstlich und privat genutzt werden

Ziel: Erreichen einer betrieblichen Datensicherheit ohne Einschränkung der Privatsphäre des Nutzers, Erhöhung der Produktivität und Senkung der Kosten durch BYOD

CE-Kennzeichen – was ist zu tun?

Datenschutzerklärung

I. Wertlosigkeit allgemeiner „Privacy Policies“

Es ist im Internet inzwischen weithin üblich geworden, seinen Webauftritt mit einer „Datenschutzerklärung“ zu versehen, in der – oft wortreich – erklärt wird, wie wichtig dem Unternehmen der Datenschutz sei, was man mit den Daten alles nicht tun wolle usw. Auszug aus einer typischen Erklärung:

Beispiel:

> „Wir messen dem Schutz ihrer Privatsphäre höchste Bedeutung zu. Dies gilt insbesondere für die Verarbeitung ihrer personenbezogenen Daten. In bestimmten Fällen benötigen wir Ihren Namen und Ihre Adresse, um die von Ihnen gewünschten Leistungen erbringen zu können. Bei der Nutzung unserer Webseite speichern wir nur die Daten, die Sie uns automatisch zur Verfügung stellen.“

Solche allgemeinen Erklärungen sind wertlos. Der Trend, sie mehr und mehr zu benutzen, ist aus verschiedenen Gründen kritisch zu sehen:

- Sie sind in **dieser** Form nirgends gesetzlich vorgesehen oder gar vorgeschrieben.
- Sie schaffen keine Transparenz, sondern vernebeln eher den Blick darauf, was konkret geschieht. (So fragt sich im obigen Beispiel, welche Daten denn genau „automatisch zur Verfügung gestellt werden“.)
- Sie sind im schlimmsten Fall irreführend und falsch. (So wird oft behauptet, es würden beim Besuch einer Webseite keine Daten gespeichert, obwohl Cookies eingesetzt werden, um genau das zu tun.)

Der Blick ist also darauf zu richten, welche gesetzlichen Informationspflichten erfüllt werden müssen. Blumige Texte allgemeiner Art helfen dabei nicht weiter. Fragt man nach den Gründen für die zunehmende Verbreitung wertloser Erklärungen der geschilderten Art, so stößt man im Wesentlichen auf zwei Phänomene:

- Derartige Erklärungen setzen sich seit einigen Jahren in den USA mehr und mehr durch (vielleicht deshalb, weil dort in vielen Bereichen von Datenschutz auf europäischem Niveau gerade keine Rede sein kann, wollen Unternehmen dem Kunden doch insoweit zumindest ein gutes Gefühl geben) und Entwicklungen in den USA werden im Internet gerne nachgeahmt.
- Der Nachahmungstrieb bei der Gestaltung von Internetauftritten ist generell enorm. Dies hat sich etwa bei dem – in dieser Form rechtlich völlig unsinnigen – Disclaimer wegen einer etwaigen Haftung für Links gezeigt, in dem auf ein Urteil des Landgerichts Hamburg aus dem Jahr 1998 Bezug genommen wird (siehe dazu die kritische Darstellung unter http://www.internetrecht-rostock.de/SNewsH/link-disclaimer.htm). Ein ähnliches Phänomen erlebt man hier.

II. Rechtliche Anknüpfungspunkte für Datenschutzerklärungen

1. Ergebnisdarstellung bei einem Datenschutzaudit

Sofern – was auf freiwilliger Basis jetzt schon möglich ist und an sich (siehe § 9a BDSG) gesetzlich geregelt werden sollte – ein Datenschutzaudit durchgeführt wird, kann das Ergebnis eines solchen Audits in Form einer Datenschutzerklärung der Öffentlichkeit zugänglich gemacht werden.

Ein solches Vorgehen ist nur ernst zu nehmen, wenn die Begutachtung im Rahmen des Audits auch die Überprüfung der Datenschutzerklärung daraufhin erfasst, ob sie mit den Ergebnissen des Audits übereinstimmt (so zutreffend Roßnagel in Roßnagel, Handbuch Datenschutzrecht, München 2003, Teil 3.7, RN 118). Ansonsten ist die Objektivität unsicher und die Erklärung ist nicht geeignet, Transparenz herzustellen.

Da Audits bisher so gut wie nicht durchgeführt werden, haben Datenschutzerklärungen nur selten den Zweck, das Ergebnis eines Audits darzustellen.

2. Benachrichtigung des Betroffenen gemäß § 33 BDSG

Sofern – etwa beim Besuch einer Webseite – Daten des Betroffenen ohne dessen Kenntnis gespeichert werden, ist er gemäß § 33 Abs. 1 Satz 1 BDSG über Folgendes zu benachrichtigen:

- Tatsache der Speicherung,
- Art der gespeicherten Daten,
- Zweckbestimmung der Erhebung, Verarbeitung oder Nutzung,
- Identität der verantwortlichen Stelle.

Dabei ist zu beachten, dass diese Benachrichtigung seitens der verantwortlichen Stelle aktiv und unaufgefordert zu veranlassen ist. Es genügt also **nicht,** dass der Betroffene diese Informationen abrufen **kann.** Das ist vor allem bei der Gestaltung von Online-Shop-AGB zu beachten.

Auch der Zweck einer Benachrichtigung nach § 33 BDSG wird mit einer Datenschutzerklärung nur selten verfolgt.

3. Erfüllung von Informationspflichten nach § 13 Telemediengesetz (TMG)

Dieser Zweck steht bei Datenschutzerklärungen im Vordergrund. § 13 Abs. 1 TMG legt fest, dass ein Diensteanbieter den Nutzer zu **Beginn** des Nutzungsvorgangs über Folgendes zu unterrichten hat:

- Art,
- Umfang und
- Zweck der Erhebung und Verwendung personenbezogener Daten sowie
- eine etwaige Verarbeitung von Daten in Drittstaaten außerhalb der Europäischen Union.

Bei entsprechender Ausgestaltung ist eine Datenschutzerklärung dazu geeignet, in dieser Hinsicht Transparenz zu schaffen. Das gilt auch für die Verwendung von Elementen wie dem „Gefällt-mir-Button“ von Facebook.

Die Regelung des § 13 TMG gilt für alle elektronischen Informations- und Kommunikationsdienste (§ 1 Abs. 1 Satz 1 TMG), also insbesondere auch für das Bereitstellen von Webseiten, die nur der Information dienen sollen.

Inhaltlicher Maßstab dafür, ob bei einer Nutzung solcher Dienste Daten überhaupt gespeichert werden dürfen, ist § 15 TMG (Nutzungsdaten). Es genügt also (selbstverständlich) nicht, dem Nutzer zu sagen, welche Daten man tatsächlich speichert, vielmehr muss die Speicherung dieser Daten auch rechtmäßig erfolgen. Die entsprechende Prüfung hat einer Datenschutzerklärung vorauszugehen.

III. Konkrete Ausgestaltung einer Datenschutzerklärung

1. Beispiel: Bayerisches Staatsministerium der Justiz und für Verbraucherschutz (StMJV)

Die Datenschutzerklärung des StMJV eignet sich aus mehreren Gründen gut dazu, typische Elemente einer Datenschutzerklärung zu erläutern:

- Die Seite enthält zum einen Informationsangebote, die betrachtet oder teils auch heruntergeladen werden können.
- Sie bietet die Möglichkeit, Nachrichten an das Ministerium zu senden.
- Es ist möglich, Newsletter zu abonnieren und Druckpublikationen zu bestellen.
- Die Seite liegt auf einem externen Webserver (Landesamt für Statistik und Datenverarbeitung).

All diese Elemente sind auch auf Unternehmensseiten weithin üblich. Dass es sich um eine Behördenseite handelt, spielt also keine Rolle.

Die Erklärung (abrufbar unter www.justiz.bayern.de/ministerium/, Button „Impressum“) hat folgenden Wortlaut (Stand: 1.2.2012, die Nummerierung der Absätze wurde hier eingefügt):

„Datenschutz (Protokollierung)

(1) Der Web-Server des Bayerischen Staatsministeriums der Justiz und für Verbraucherschutz wird durch das Bayerische Landesamt für Statistik und Datenverarbeitung (webmaster@bayern.de [email]), Neuhauser Str. 8, 80331 München, Postanschrift 80228 München, betrieben.

(2) Bei jeder Anforderung einer Internetdatei werden folgende Zugriffsdaten im Bayerischen Landesamt für Statistik und Datenverarbeitung gespeichert:

1. *die Seite, von der aus die Datei angefordert wurde,*
2. *der Name der aufgerufenen Datei,*
3. *das Datum und die Uhrzeit der Anforderung,*
4. *die übertragene Datenmenge,*
5. *der Zugriffsstatus (Datei übertragen, Datei nicht gefunden etc.),*
6. *die Beschreibung des verwendeten Webbrowsertyps bzw. des verwendeten Betriebssystems,*
7. *die IP-Adresse des anfordernden Rechners.*

(3) Die gespeicherten Daten werden ausschließlich zu technischen oder statistischen Zwecken benötigt; ein Abgleich mit anderen Datenbeständen oder eine Weitergabe an Dritte, auch in Auszügen, findet nicht statt.

(4) Im Informationsangebot des StMJV können Cookies oder JAVA-Applets verwendet werden.

(5) Die Verwendung dieser Funktionalitäten kann durch Einstellungen des Browserprogramms vom jeweiligen Nutzer ausgeschaltet werden.

(6) Nach Auswertung der jährlichen Zugriffe werden die protokollierten Daten gelöscht. Die Auswertung erfolgt monatlich und jährlich, die Löschung erfolgt jeweils im Januar des Folgejahres. Auswertung und Löschung erfolgen durch Mitarbeiter des Bayerischen Landesamts für Statistik und Datenverarbeitung im Auftrag des StMJV.

(7) Im Angebot des StMJV besteht die Möglichkeit zur Eingabe persönlicher oder geschäftlicher Daten (E-Mail-Adressen, Namen, Anschriften) bei Schreiben an das StMJV, für Bestellzwecke, für Feedbacks sowie ggf. zur Abonnierung von Newslettern und zur Teilnahme an Diskussionsforen. Die Nutzung der angebotenen Serviceleistungen und Dienste seitens des Nutzers erfolgt ausdrücklich auf freiwilliger Basis. Soweit ein Newsletterversand eingerichtet ist, werden die E-Mail-Adressen hierfür auf dem Newsletterserver im Bayerischen Landesamt für Statistik und Datenverarbeitung gespeichert und für keine anderen Zwecke als den Versand der Newsletter verwendet. Die Abonnenten der Newsletter können jederzeit selbst das Abonnement kündigen; die E-Mail-Adressen werden dadurch automatisch gelöscht. In jedem Fall (Bestellung, Newsletter, Feedback, Diskussionsforum) werden die angegebenen persönlichen Daten (insb. Name, E-Mail-Adresse) nur für die Übersendung der gewünschten Veröffentlichungen oder Informationen bzw. für die bei dem einzelnen Formular ggf. explizit genannten anderen Zwecke verarbeitet und nicht an Dritte weitergegeben.

(8) Zeitlich begrenzte Nutzerdaten (Cookies) werden auf dem Rechner des Nutzers gespeichert, wenn der Nutzer dies zur Erhöhung seines Komforts wünscht (dies betrifft die Speicherung des vom Nutzer evtl. ausgewählten CSS für die Kombination Hintergrund-/Schriftfarbe). Diese Speicherung kann vom Nutzer jederzeit durch entsprechende Einstellung des Internetbrowsers rückgängig gemacht bzw. verhindert werden.“

2. Erläuterungen zum Text des StMJV

(Die nachfolgend verwendeten Gliederungsziffern beziehen sich auf die in Klammer vorangestellten Zahlen im Beispieltext).

- Regeln über eine sichere Authentifizierung der Kommunikationspartner und deren Protokollierung;
- Vereinbarungen über Dauer und den Ort der Aufbewahrung der Protokollierungen;
- unverzügliche gegenseitige Informationspflicht, wenn Verstöße gegen das Datenschutzrecht oder die Pflicht zur Verschwiegenheit festgestellt werden;
- genaue Beschreibung zu den Maßnahmen zur IT-Sicherheit beim Anbieter.

Letztendlich ist bei Fernwartungsverträgen wie in allen IT-Verträgen eine gute und präzise Leistungsbeschreibung essentiell. Die besten rechtlichen Regelungen nützen wenig, wenn die vertraglichen Leistungen ungenau beschrieben sind.

Filesharing

I. Begriff

Unter Filesharing (dt. „gemeinsamer Dateizugriff“ oder „Dateien teilen“) versteht man das Weitergeben von Dateien zwischen Benutzern des Internets über sog. Tauschbörsen, die vollständig oder überwiegend auf dem Peer-to-Peer-Prinzip beruhen. Dabei stellen sich die Teilnehmer gegenseitig über die jeweilige Tauschplattform Daten zur Verfügung. Hierzu sind alle Computer der Nutzer über eine bestimmte Software in einem eigenen Netzwerk miteinander verbunden.

Um an dem Netzwerk teilnehmen zu können, ist es erforderlich, eine entsprechende Software, welche im Internet kostenlos angeboten wird, herunterzuladen und zu installieren, sowie sich selbst zu registrieren und einen Benutzernamen anzugeben. Jeder Nutzer der Internettauschbörse bietet den anderen Nutzern sodann Einblick in einen bestimmten Teil der Festplatte seines Computers. Die Daten werden dann gegenseitig über die Tauschplattform zur Verfügung gestellt. Dabei bietet jeder, der auch nur ein Datenpaket einer Datei von einem anderen Nutzer auf seine eigene Festplatte lädt, dieses Datenpaket bereits wieder anderen Nutzern für den Download durch diese an.

Bekannte Filesharing-Systeme sind z. B. BitTorrent, Morpheus und BearShare, die auf einem Gnutella genannten Projekt bzw. Protokoll beruhen. Weitere bekannte Anbieter bzw. Systeme mit überwiegend eigener Technik sind Kazaa, Audiogalaxy, Freenet und eDonkey2000.

Illegales wie legales Filesharing konnte sich lange Zeit relativ unbehelligt entwickeln. Entsprechend hoch ist der Anteil dieses netzbasierten Datenaustauschs am gesamten Internetdatenverkehr; man spricht von über 50 %. In jüngerer Zeit werden die anbietenden Teilnehmer jedoch zunehmend von Urheberrechtsinhabern sowie Staatsanwaltschaften verfolgt. Durch gezielte Einzel- sowie Massenverfahren sollen die Teilnehmer von Tauschbörsen in die Pflicht genommen und abgeschreckt werden.

II. Ermittlung und Verfolgung der Nutzer

Für die Ermittlung der Teilnehmer von Internettauschbörsen werden zunächst besondere Programme eingesetzt, die sich das Peer-to-Peer-Prinzip zunutze machen. Die eingesetzten Programme greifen auf die beteiligten Rechner eines Peer-to-Peer-Netzwerkes zu und durchsuchen diese auf urheberrechtlich geschützte Dateien. Die Rechner geben dabei ihre Kennung und Adresse, die sog. IP (Internet Protokoll Adresse) an. Da die IP dem jeweiligen Anschluss vom Zugangsprovider jedoch immer nur vorübergehend zugewiesen wird (dynamische IP), muss zusätzlich eine Datei heruntergeladen werden, um neben der IP auch den Moment ihrer Zuordnung zu einem bestimmten Anschluss dokumentieren zu können. Mit den so gewonnenen Daten kann man jedoch noch nicht auf die persönlichen Daten des jeweiligen Anschlussinhabers schließen.

Ermittlung der persönlichen Daten nach der früheren Rechtslage:

Da der Zugangsprovider den Rechteinhabern nach früherem Recht zivilrechtlich nicht zur Auskunft verpflichtet war, mussten diese einen „Umweg“ über die Strafverfolgungsbehörden gehen. Die Rechteinhaber zeigten daher die beobachteten Vorgänge bei den Staatsanwaltschaften an. Diese konnten dann auf Grundlage eines richterlichen Beschlusses die persönlichen Daten der Anschlussinhaber vom Zugangsprovider herausverlangen. Über die gewährte Akteneinsicht kamen die Rechteinhaber schließlich an die persönlichen Daten des jeweiligen Anschlussinhabers.

Ermittlung der persönlichen Daten nach der aktuellen Rechtslage:

Die nach der früheren Rechtslage erforderliche Ermittlungspraxis war jedoch für die Rechteinhaber äußerst umständlich, da diese stets auf die Mithilfe der Strafverfolgungsbehörden angewiesen waren. Gleichzeitig führte dieser Umstand zu einer regelrechten Flut von Strafanzeigen bei den Staatsanwaltschaften, die hierdurch wegen oftmals verhältnismäßig geringfügiger Urheberrechtsdelikte stark eingespannt wurden. Dieses Problem hat der Gesetzgeber durch eine Neuregelung des § 101 UrhG beseitigt. Darin ist nun u. a. ein zivilrechtlicher Auskunftsanspruch des Rechteinhabers gegen den Zugangsprovider geregelt (→ *Auskunftsanspruch UrhG*). Danach kann der Rechteinhaber die persönlichen Daten des Anschlussinhabers unter bestimmten Voraussetzungen selbst vom Zugangsprovider herausverlangen.

III. Haftung der Beteiligten

Bei der Nutzung von Filesharing-Systemen kommen drei Formen der Beteiligung in Betracht, die jeweils unterschiedlich rechtlich zu würdigen sind:

- Anbieten bzw. Hochladen,
- Herunterladen,
- bloßes Bereitstellen eines Anschlusses.

IV. Haftung des Anbietenden

1. Zivilrechtliche Haftung

Das Anbieten urheberrechtlich geschützter Daten über Filesharing-Netzwerke stellt ein öffentliches Zugänglichmachen nach § 19a UrhG dar. Dabei ist es unerheblich, ob die Daten tatsächlich hochgeladen werden. Ein **öffentliches Zugänglichmachen** im Sinne des Urheberrechts liegt bereits dann vor, wenn andere Teilnehmer auf die Daten Zugriff nehmen können. Werden urheberrechtlich geschützte Daten ohne Erlaubnis der Rechteinhaber öffentlich zugänglich gemacht, so stellt dies gemäß §§ 15 Abs. 2, 52 Abs. 3 UrhG einen Rechtsverstoß dar. Rechtsfolge sind Unterlassungs-, Beseitigungs-, Auskunfts-, Rechnungslegungs-, Besichtigungs- und Schadensersatzansprüche gemäß § 97 UrhG. In der Praxis stehen dabei naturgemäß der Unterlassungs- und der Schadensersatzanspruch im Vordergrund.

1.1 Anspruch auf Unterlassung

Mit dem Unterlassungsanspruch kann der Rechteinhaber gegen den Verletzer das Verbot durchsetzen, die urheberrechtlich geschützten Daten ohne seine Zustimmung zu nutzen. In prozessualer Hinsicht erfolgt dies meistens durch eine urheberrechtliche Abmahnung, verbunden mit der Aufforderung an den Gegner, innerhalb einer bestimmten Frist eine entsprechende strafbewehrte Unterlassungs- und Verpflichtungserklärung abzugeben. Unterwirft sich der Gegner trotz einer entsprechenden Aufforderung nicht, so kann der Rechteinhaber seinen Unterlassungsanspruch im Wege des vorläufigen Rechtsschutzes (einstweilige Verfügung) oder im Rahmen einer Hauptsacheklage gerichtlich durchsetzen.

Die Kosten für solche Verfahren beurteilen sich nach dem Streitwert der Angelegenheit. Wertbestimmend ist beim Unterlassungsanspruch die gemäß § 3 ZPO zu schätzende Beeinträchtigung, die für den Verletzten von dem beanstandeten Verhalten verständigerweise zu besorgen ist und die mit der begehrten Unterlassung beseitigt werden soll (vgl. Zöller, ZPO, § 3 Rn. 16 „Unterlassung“). Dieser Wert wird bei urheberrechtlichen Verstößen von den Gerichten relativ hoch angesetzt.

Mit Beschluss vom 9.8.2007 (Az. 308 O 273/07) entschied etwa das Landgericht Hamburg, dass gegenüber demjenigen, der durch den Betrieb eines eDonkey-Servers zum Funktionieren eines Filesharingsystems über das eDonkey-Netzwerk beiträgt, ein Streitwert von 20.000 € für jede einzelne öffentlich zugänglich gemachte Musikdatei gerechtfertigt ist. Für den Fall, dass der Unterlassungsschuldner nicht selbst aktiv zum Betrieb des Filesharing-Systems beigetragen hat, sondern sich als Anschlussinhaber nach den Grundsätzen der Störerhaftung das in einzelnen Filesharing-Handlungen liegende deliktische Verhalten seiner Kinder oder anderer Dritter zurechnen lassen muss, nimmt das Landgericht Hamburg eine Streitwertstaffelung an. In solchen Fällen erachtet das Gericht mittlerweile einen Streitwert von 6.000 € für den ersten Titel, von je 3.000 € für den zweiten bis fünften Titel, von je 1.500 € für den sechsten bis zehnten Titel und von je 600 € für jeden weiteren Titel für angemessen und ausreichend. Entsprechend hoch sind auch die zu erwartenden Prozesskosten, für den Fall, dass es trotz vorheriger Abmahnung zu einer gerichtlichen Auseinandersetzung kommt. Aber auch die außergerichtlichen Kosten einer anwaltlichen Abmahnung sind angesichts solcher Streitwerte schon sehr hoch anzusiedeln. Legt man einen Streitwert von 6.000 € zugrunde, ergeben sich für eine durchschnittliche anwaltliche Abmahnung bereits Kosten in Höhe von 546,69 € inkl. USt.

Hinweis:
Im Urheberrecht beschränkt sich seit Inkrafttreten des § 97a Abs. 2 UrhG der Ersatz der erforderlichen Aufwendungen für die Inanspruchnahme anwaltlicher Dienstleistungen für die erstmalige Abmahnung in einfach gelagerten Fällen mit einer nur unerheblichen Rechtsverletzung außerhalb des geschäftlichen Verkehrs auf 100 Euro (→ *100-€-Abmahnung*).

1.2 Anspruch auf Schadensersatz

Grundsätzlich kommt bei schuldhaft begangenen Urheberrechtsverletzungen auch immer ein Schadensersatzanspruch des Verletzten in Betracht. Für die Höhe des Schadensersatzes sind in der Rechtsprechung drei Berechnungsarten anerkannt:

- Ersatz der erlittenen Vermögenseinbuße einschließlich des entgangenen Gewinns
- Zahlung einer angemessenen Lizenz
- Herausgabe des Verletzergewinns

Da in den typischen Fällen von Filesharing der Nachweis eines konkret entstandenen Schadens bzw. die konkrete Bestimmung des Verletzergewinns naturgemäß sehr schwierig ist, behilft man sich in derartigen Fällen zumeist mit der **Geltendmachung einer angemessenen Lizenz.** Diese Berechnungsart beruht auf dem Gedanken, dass der schuldhaft handelnde Verletzer nicht besser gestellt sein soll als derjenige, der das Schutzrecht als vertraglicher Lizenznehmer rechtmäßig nutzt. Der größte Vorteil dieser Berechnungsart gegenüber den anderen beiden Berechnungsarten liegt darin, dass es keine Kausalitätsprobleme gibt. Die Lizenz ist als pauschalierter Mindestschaden anzusehen. In der Regel wird zur Berechnung ein Betrag zwischen 5.000 und 15.000 € pro angebotener Datei zu Grunde gelegt und dieser mit deren Anzahl multipliziert. Bei oft mehreren Hundert angebotenen Dateien ergibt dies Beträge im Millionen-Euro-Bereich. Da solche Forderungen auch den abmahnenden Kanzleien unverhältnismäßig hoch erscheinen, werden in der Praxis „aus Kulanz“ weitaus niedrigere Beträge (in der Regel zwischen 3.000 und 10.000 €) als Schadensersatz geltend gemacht. Für Schuldner mit geringen bis durchschnittlichen Einkommen stellen jedoch auch solche Beträge eine empfindliche „Strafe“ dar.

2. Strafrechtliche Haftung

Neben der zivilrechtlichen Haftung droht demjenigen, der urheberrechtlich geschützte Daten ohne die erforderliche Erlaubnis der Rechteinhaber über Filesharing-Systeme anbietet, auch noch eine strafrechtliche Verfolgung. Die Strafbarkeit ergibt sich insoweit aus § 106 UrhG, wonach mit Freiheitsstrafe bis zu drei Jahren oder mit Geldstrafe bestraft wird, wer in anderen als

dentlich gekündigt werden (§§ 620 Abs. 2, 621 BGB). Die Kündigungsfristen ergeben sich aus § 621 BGB und § 624 BGB.

- Bei Vorliegen eines wichtigen Grundes kann fristlos gekündigt werden (§ 626 BGB). Im Fall der Leistung von Diensten „höherer Art“ aufgrund einer besonderen Vertrauensstellung kann fristlos gekündigt werden, ohne dass ein wichtiger Grund vorliegt (§ 627 BGB). Folge der Kündigung ist ein Anspruch auf Teilvergütung (§ 628 Abs. 1 BGB) oder, wenn ein Teil durch vertragswidriges Verhalten des anderen zur Kündigung veranlasst worden ist, auf Schadensersatz (§ 628 Abs. 2 BGB). Zu beachten ist auch, dass eine unberechtigte und unwirksame Kündigung als Vertragsverletzung zum Schadensersatz gem. §§ 280 Abs. 1, 241 Abs. 2 BGB verpflichtet.

Die Folge der Kündigung ist ein Anspruch auf Teilvergütung (§ 628 Abs. 1 BGB) also der Vergütung für die Dienstleistungen, die bis zur Wirksamkeit der Kündigung erbracht wurden. Stützt sich die Kündigung auf eine Pflichtverletzung des Vertragspartners kann der andere Vertragspartner auch Schadensersatz (§ 628 Abs. 2 BGB) verlangen. Zu beachten ist auch, dass eine unberechtigte und unwirksame Kündigung als Vertragsverletzung zum Schadensersatz gem. §§ 280 Abs. 1, 241 Abs. 2 BGB verpflichtet.

Beide Seiten können einen einvernehmlichen Aufhebungsvertrag schließen. Die Kündigung bedarf im Gegensatz zum Arbeitsvertrag nicht der Schriftform. Aus Nachweisbarkeitsgründen sollte sie aber in Schrift- oder wenigstens in Textform erfolgen.

VIII. Geheimhaltung/Herausgabe von Unterlagen

Eine → *Geheimhaltungsvereinbarung* dient dem Schutz des Auftraggebers. So soll vermieden werden, dass der freie Mitarbeiter geheime Informationen eines Kunden des Auftraggebers, die der Auftraggeber nach besonderer Geheimhaltungsvereinbarung mit dem Kunden erhalten hat, verwendet. Es ist auch davon auszugehen, dass sich ein solches Verhalten des freien Mitarbeiters als wettbewerbswidrig darstellen dürfte.

IX. Wettbewerbsverbot

Es ist möglich, ein nachvertragliches Wettbewerbsverbot zu vereinbaren, welches wiederum mit einem Free-Lancer nicht den §§ 74 ff. HGB unterliegt, soweit nicht der freie Mitarbeiter vom Auftraggeber wirtschaftlich abhängig ist (arbeitnehmerähnlicher Selbstständiger). Jedoch sollte man sich bei der Verwendung dieser Klausel im Klaren sein, dass diese einer gerichtlichen Überprüfung nicht standhalten könnte, sofern man keine Karenzentschädigung (Orientierung am Mindestsatz des § 74 HGB, also 50 % der zuletzt bezogenen vertragsgemäßen Leistung) vorsieht. Sollte das Honorar des Free-Lancers variieren, kann der Durchschnitt des abgerechneten Honorars der vergangenen drei Monate angesetzt werden. Eine Garantie kann es jedoch nicht geben, dass trotz Karenzentschädigung ein Wettbewerbsverbot der gerichtlichen Überprüfung standhält, denn es darf dabei nicht übersehen werden, dass ein solches Verbot auch einen Eingriff in die grundgesetzlich garantierte Berufsfreiheit (Art. 12 GG) darstellt. Dasselbe gilt entsprechend für eine Vereinbarung, die ein Abwerbeverbot für den freien Mitarbeiter vorsieht.

TIPP!

Am sinnvollsten ist es, das Wettbewerbsverbot auf das örtliche und zeitliche Mindestmaß zu beschränken.

X. Haftung

Das Gesetz sieht die unbegrenzte Haftung des freien Mitarbeiters vor. Diese ist der freie Mitarbeiter aber selten gewillt einzugehen, insbesondere, wenn er z. B. an einer Software arbeitet, die in haftungsintensiven Bereichen (industrielle Fertigung, Bankenbereich, Krankenhausbereich) eingesetzt wird. Auch für den Auftraggeber stellt die Regressmöglichkeit auf seinen Mitarbeiter eine Scheinsicherheit dar. In den seltensten Fällen wird er hohe Schadensersatzansprüche gegen diesen faktisch durchsetzen können. Es ist daher sinnvoll, die Haftung gegen den Auftragnehmer zu begrenzen und dafür zu sorgen, dass der freie Mitarbeiter eine angemessene Vermögenshaftpflichtversicherung abschließt. Die Aufrechterhaltung dieser Versicherung sollte überwacht werden.

XI. Zurückbehaltungsrecht

Zuletzt kann noch der Ausschluss eines Zurückbehaltungsrechts vereinbart werden. Dabei sollte man auf eine individuelle Vereinbarung achten, da ein formularmäßiger Ausschluss (AGB) nach § 309 Nr. 2 BGB unwirksam ist.

Mit diesem Ausschluss kann man dem freien Mitarbeiter die Möglichkeit nehmen, durch die Zurückhaltung der Software und anderer Unterlagen, Druck auf den Auftraggeber auszuüben.

IT-Forensik

I. Bedeutung von IT-Forensik

Die IT-Forensik oder Computer-Forensik befasst sich mit der Untersuchung verdächtiger Vorfälle in IT-Systemen. Ähnlich wie die klassische Spurensicherung nach einem Verbrechen suchen die IT-Forensiker nach verwertbaren digitalen Spuren, zum Beispiel wenn es zu einem Hackerangriff auf einen Webserver gekommen ist oder wenn vertrauliche Daten im Unternehmensnetzwerk kopiert und missbraucht wurden. Die IT-Forensik ist Aufgabe von Spezialisten. Für Unternehmen als mögliche Opfer einer Computerstraftat ist es jedoch wichtig zu wissen, wie die IT-Forensik arbeitet, um die digitale Spurensuche nicht ungewollt zu behindern.

II. Vorgehen der IT-Forensiker

1. Ziel sind gerichtsverwertbare, digitale Beweise

Die digitale Spurensuche und Beweisaufnahme nach einem möglichen Einbruch in IT-Systeme erfolgt nach einem definierten Schema, das in der Regel so aussieht:

- Beauftragung durch die Unternehmensleitung zur Absicherung der Rechtmäßigkeit der Ermittlungsarbeiten,
- Klärung der datenschutzrechtlichen Regelungen,
- Schutz der betroffenen Systeme,
- Schutz der gerichtsverwertbaren Spuren oder der Spuren entsprechend dem konkreten Auftrag,
- Erzeugung von Arbeitskopien der zu untersuchenden Daten,
- Datenanalyse und Bewertung,
- forensische Dokumentation und
- Erstellung von Berichten für eine mögliche Gerichtsverhandlung.

WICHTIG!

Die Suche nach verwertbaren, digitalen Spuren darf niemals an den Originaldateien erfolgen, die mit dem verdächtigen Vorfall in Verbindung stehen. Deshalb sind grundsätzlich Arbeitskopien zu erzeugen. Nach Abschluss der forensischen Untersuchungen, nach erfolgter Beweisaufnahme und nach Rücksprache mit den Ermittlungsbehörden sollten die Arbeitskopien durch das betroffene Unternehmen oder die IT-Forensiker gelöscht werden.

Zur forensischen Analyse der IT-Systeme stehen den Experten zahlreiche Möglichkeiten zur Verfügung:

- die Überprüfung sämtlicher, relevanter Speichermedien, insbesondere auch externer und mobiler Medien, mit spezieller IT-Forensik-Software,
- die Durchsuchung der Protokoll- und Systemdateien nach Anhaltspunkten, die zu dem möglichen IT-Vorfall passen,
- die Aufstellung des zeitlichen Ablaufs eines Systemausfalls oder -einbruchs,
- die Suche nach möglicherweise ursächlicher → *Schadsoftware*,
- die Analyse des Angriffsmusters sowie
- die Dokumentation der aufgefundenen Schwachstellen in der Datensicherheit.

Die tatsächlich ergriffenen Maßnahmen werden durch die IT-Forensiker dokumentiert.

2. Die Daten Unbeteiligter sind zu schützen

Bei der Suche nach digitalen Spuren werden zu Beginn weite Teile der Datenbestände des betroffenen Unternehmens durch IT-Forensiker durchforstet. Dabei besteht eine hohe Wahrscheinlichkeit, dass auch Daten unbeteiligter Mitarbeiter, Geschäftspartner und Kunden in die Untersuchung einbezogen werden.

Mögliche Problemfelder sind insbesondere Datenbestände, die personenbezogene Daten enthalten, darunter ggf. private E-Mails und private Nutzungsspuren im Internetbrowser. Deshalb sollten die Mitarbeitervertretung und der Datenschutzbeauftragte immer in die Vorbereitungen für die IT-Forensik einbezogen werden.

WICHTIG!

Um die Daten Unbeteiligter so weit wie möglich zu schützen, sollten die Untersuchungen der IT-Forensiker gezielt begrenzt werden. Gleichzeitig sollte verhindert werden, für die Beweissicherung wichtige Bereiche bei der Untersuchung auszusparen. Dazu müssen der Zeitablauf des Systemeinbruchs und der Angriffsweg so genau wie möglich bestimmt werden, um betroffene Systeme und Datenbereiche von den nicht betroffenen unterscheiden zu können.

3. Die IT-Forensik ist zeitkritisch

Um noch digitale Spuren finden zu können, bevor die immer raffinierter vorgehenden Hacker mögliche Beweise gelöscht haben oder nichtsahnende Benutzer ungewollt die digitalen Beweise verwischen, muss schnell gehandelt werden, wenn ein Verdacht auf einen Systemeinbruch vorliegt. Dazu sollten Unternehmen auf mögliche Zeichen für Hackerangriffe und andere kriminelle IT-Aktivitäten achten.

Beispiel:

Mögliche Kennzeichen für einen Systemeinbruch könnten sein:

- Dritte kennen interne Details, bevor diese offiziell bekannt gegeben wurden.
- Wettbewerber bieten nach sehr kurzer Zeit ein vergleichbares Produkt an.
- Der Netzwerkverkehr des betroffenen Unternehmens hat unerklärlich stark zugenommen.
- Fehlermeldungen, die verschiedene Applikationen anzeigen, lassen sich nicht ohne weiteres erklären.
- IT-Systeme sind aus unerklärlichen Gründen langsamer geworden.
- Die Zahl an Einträgen in den Systemprotokollen hat massiv zugenommen.

WICHTIG!

Systemabstürze, das Löschen von Dateien und der Zugriff auf unerlaubte Systembereiche können auch ohne jede Absicht durch eigene Beschäftigte verursacht werden. Nicht immer muss hinter verdächtigen Vorkommnissen in IT-Systemen ein wirklicher Systemeinbruch stecken.

Wenn sich solche Vorkommnisse aber als ungewollt herausstellen, sollten trotzdem Maßnahmen (wie eine bessere Vergabe und Kontrolle der Zugriffsberechtigungen) ergriffen werden, die solche Fälle nach Möglichkeit ausschließen. Dadurch wird verhindert, dass tatsächliche Systemeinbrüche als harmlose Versehen behandelt werden und Beschäftigte unbegründet unter Verdacht geraten.

WICHTIG!

Systemeinbrüche finden nicht nur von außen statt. Die Zahl der Computerstraftaten durch Innentäter ist beträchtlich. Dabei werden in der Regel offizielle Systemprivilegien ausgenutzt, so dass sich gerade Attacken durch Innentäter nur schwierig aufspüren lassen.

- **Die technische Vermeidung einer Ortung setzt letztlich voraus, dass ein vorhandenes GPS- und WLAN-Modul deaktiviert wird und dass sich das Gerät bei keinem Mobilfunk-Dienst anmeldet. Dadurch sind jedoch viele Funktionen des Gerätes nicht verwendbar.**

Open-Source- oder Freie Software

I. Begriff

Open-Source-Software (OSS) oder auch „Freie Software“ ist eine Software, deren Quellcode veröffentlicht ist und die frei genutzt, vervielfältigt und verändert werden kann. Dabei kann es sich um einzelne Programme handeln, aber auch vollständige Betriebssysteme. Das wohl bekannteste ist hierbei das Linux-System, das heute über „Android“ sogar auf vielen Smartphones zu finden ist. Von Besonderer Relevanz ist dabei die Differenzierung zwischen „Quellcode“ und „Objektcode“ oder „Binärcode“. Letzteres ist der eigentlich ausführbare Code, also beispielsweise die .Exe-Datei die man auf einem Windows-System ausführt. Wer nur den ausführbaren Code hat, kann die Software zwar nutzen, aber eben nicht verändern – dazu benötigt man den Quellcode.

Der Begriff OSS, ganz besonders „freie Software“, darf auf keinen Fall mit Freeware verwechselt werden. Diese ist im allgemeinen Sprachgebrauch die übliche Bezeichnung für eine Software, die von jedermann unentgeltlich im Objektcode genutzt manchmal auch ohne Einschränkungen weiterverbreitet werden darf. Der Quellcode ist hierbei jedoch üblicherweise nicht frei zugänglich oder darf jedenfalls nicht frei modifiziert und verbreitet werden. Finanziell bedeutet dies auch eine Verschiebung der Einnahmequellen, weg vom reinen Verkauf, hin zu Dienstleistungen, also etwa Support und Schulungen. Juristisch kann die zunehmende Verbreitung von Open-Source-Software also auch bedeuten, dass hier das Kaufvertragsrecht weniger relevant wird, während Fragen rund um das Dienstleistungsrecht zunehmen.

II. Open-Source-Definition

Es gibt keine verbindliche Definition der Begriffe „freie Software“ oder „Open-Source“, wohl aber brauchbare Eingrenzungen. Freie Software ist insofern erst einmal von proprietärer Software zu unterscheiden, die dem Wortsinn nach „unfreie Software“ meint. Bei der Suche nach einer Open-Source-Definition sowie einer Definition für „freie Software“ sind zwei Kriterienkataloge hilfreich: Die Vorgaben der Free Software Foundation und die von Debian. Auch wenn diese auf den ersten Blick recht unterschiedlich sind, erkennt man schnell, dass es im Kern dabei um die gleichen Überlegungen geht, man also insofern schnell abstrakte Kriterien gewinnen kann.

1. Free Software Foundation

Die 1985 von Richard Stallman gegründete „Free Software Foundation“ (FSF) ist eine gemeinnützige Gesellschaft deren Ziel es ist, freie Software zu fördern. Man kann sie in diesem Bereich getrost als den Pionier schlechthin bezeichnen. Neben diversen Kampagnen organisiert die FSF vor allem die Arbeit des GNU-Projekts, zu dem wiederum die bekannten Lizenzen GPL und LGPL gehören. Für beiden bekannten Lizenzen ist die Vereinbarkeit mit deutschem Recht heute allgemein anerkannt: Zur GPL siehe die wegweisende Entscheidung des LG München I, Az. 21 O 6123/04 sowie aktueller das LG Frankfurt, Az. 2-6 O 224/06. Zur LGPL siehe die Entscheidung des Landgerichts Bochum, Az. I-8 O 293/09.

Die FSF hat für sich vier Kriterien festgelegt, die erfüllt sein müssen, damit eine Software als „freie Software“ für die FSF gilt. Der Kriterienkatalog (zu finden unter http://fsfe.org/about/basics/freesoftware.de.html auf Deutsch) beinhaltet vier Freiheiten:

1. Die Freiheit, das Programm für jeden Zweck auszuführen.
2. Die Freiheit, die Funktionsweise eines Programms zu untersuchen, und es an seine Bedürfnisse anzupassen.
3. Die Freiheit, Kopien weiterzugeben und damit seinen Mitmenschen zu helfen.
4. Die Freiheit, ein Programm zu verbessern, und die Verbesserungen an die Öffentlichkeit weiterzugeben, sodass die gesamte Gesellschaft profitiert.

2. Debian Free Software Guidelines

Bei Debian handelt es sich um eine Linux-Distribution, die von einem Netzwerk von Entwicklern gepflegt wird. Die Ideologie freier Software wird hier aktiv gepflegt und ist Voraussetzung für die Mitarbeit. Gemäß der Open-Source-Definition der „Debian Free Software Guidelines“ (http://debiananwenderhandbuch.de/dfsg.html) wird Software als „freie Software“ angesehen, wenn ihre Lizenzbedingungen die folgenden Kriterien erfüllen.

Die Kriterien von Debian erinnern dabei teilweise an die vier Freiheiten der FSF, insgesamt gehen sie aber darüber hinaus und sehen bereits ein Copyleft vor. Das Copyleft verlangt, dass eine veränderte Software keiner Lizenz unterworfen werden

darf, die Einschränkungen gegenüber der ursprünglichen Lizenz vorsieht. Hintergrund ist der Gedanke, dass niemand von der freien Arbeit eines anderen profitieren soll, um seinerseits – mit teilweise minimalen Änderungen – dann daraus Profit zu Lasten der Freiheit der Software zu ziehen.

2.1 Freie Weitergabe

Die Lizenz darf niemanden in seinem Recht einschränken, die Software als Teil eines Software-Paketes, das Programme unterschiedlichen Ursprungs enthält, zu verschenken oder zu verkaufen. Die Lizenz darf für den Fall eines solchen Verkaufs keine Lizenz- oder sonstigen Gebühren festschreiben.

2.2 Quellcode

Das Programm muss den Quellcode beinhalten. Die Weitergabe muss sowohl für den Quellcode, als auch für die kompilierte Form zulässig sein. Wenn das Programm in irgendeiner Form ohne Quellcode weitergegeben wird, so muss es eine allgemein bekannte Möglichkeit geben, den Quellcode zum Selbstkostenpreis zu bekommen, vorzugsweise als gebührenfreien Download aus dem Internet. Der Quellcode soll die Form eines Programms haben, das ein Programmierer vorzugsweise bearbeitet. Ein absichtlich unverständlich geschriebener Quellcode ist daher nicht zulässig. Zwischenformen des Codes, so wie sie etwa ein Präprozessor oder ein Konverter („Translator“) erzeugt, sind unzulässig.

Hinweis:

Die Weitergabe des Quellcodes ist ein nicht zu unterschätzendes Problem, speziell bei der GPL, da diese recht restriktive Vorgaben macht und ein Verstoß den Verlust der Lizenz zur Folge hat. Gerade bei der GPLv2 besteht dabei das Problem, dass ein auf einem Datenträger ausgelieferter Objectcode nicht einfach mit einem Download-Angebot des Quellcodes kombiniert werden darf, sondern der Quellcode gleichsam auf einem Datenträger zu liefern ist. (Vertiefend dazu: http://www.ferner-alsdorf.de/?p=5692)

2.3 Abgeleitete Software

Die Lizenz muss Veränderungen und Derivate zulassen. Außerdem muss sie es zulassen, dass die solcherart entstandenen Programme unter denselben Lizenzbestimmungen weiter vertrieben werden können wie die Ausgangssoftware.

2.4 Unversehrtheit des Quellcodes des Autors

Die Lizenz darf die Möglichkeit, den Quellcode in veränderter Form weiterzugeben, nur dann einschränken, wenn sie vorsieht, dass zusammen mit dem Quellcode so genannte „Patch files“ weitergegeben werden dürfen, die den Programmcode bei der Kompilierung verändern. Die Lizenz muss die Weitergabe von Software, die aus einem veränderten Quellcode entstanden ist, ausdrücklich erlauben. Die Lizenz kann verlangen, dass die abgeleiteten Programme einen anderen Namen oder eine andere Versionsnummer als die Ausgangssoftware tragen.

2.5 Keine Diskriminierung von Personen oder Gruppen

Die Lizenz darf niemanden benachteiligen.

2.6 Keine Einschränkungen bezüglich des Einsatzfeldes

Die Lizenz darf niemanden daran hindern, das Programm in einem bestimmten Bereich einzusetzen. Beispielsweise darf sie den Einsatz des Programms in einem Geschäft oder in der Genforschung nicht ausschließen.

2.7 Weitergabe der Lizenz

Die Rechte an einem Programm müssen auf alle Personen übergehen, die diese Software erhalten, ohne dass für diese die Notwendigkeit besteht, eine eigene, zusätzliche Lizenz zu erwerben.

2.8 Die Lizenz darf nicht auf ein bestimmtes Produktpaket beschränkt sein

Die Rechte an dem Programm dürfen nicht davon abhängig sein, ob das Programm Teil eines bestimmten Software-Paketes ist. Wenn das Programm aus dem Paket herausgenommen und im Rahmen der zu diesem Programm gehörenden Lizenz benutzt oder weitergegeben wird, so sollen alle Personen, die dieses Programm dann erhalten, alle Rechte daran haben, die auch in Verbindung mit dem ursprünglichen Software-Paket gewährt wurden.

2.9 Die Lizenz darf die Weitergabe zusammen mit anderer Software nicht einschränken

Die Lizenz darf keine Einschränkungen enthalten bezüglich anderer Software, die zusammen mit der lizenzierten Software weitergegeben wird. So darf die Lizenz z. B. nicht verlangen, dass alle anderen Programme, die auf dem gleichen Medium weitergegeben werden, auch quelloffen sein müssen.

III. Thema: Lizenzverstöße bei der GPL

Immer noch umstritten ist, wie sich ein Lizenzverstoß bei der GPL auswirkt, insbesondere ob dieser einfach „heilbar“ ist. Diese Frage hat inzwischen besonders hohe Relevanz, etwa da gerade im Bereich des auf vielen Smartphones installierten Android-Betriebssystems die GPL eine besondere Rolle spielt. Wie im Falle eines Lizenzverstoßes für die zukünftige Verwendung zu verfahren ist, ist gerichtlich noch nicht geklärt. Einerseits wird die Auffassung vertreten, nach einem Lizenzverstoß sei zur erneuten Verwendung nicht nur die Heilung des bisherigen Verstoßes, sondern darüber hinaus die Zustimmung aller Urheber der Software nötig. Bei Software wie dem Linux-Kernel dürfte dies wohl unmöglich zu erfüllen sein. Andererseits aber gibt es die Auffassung, die darauf verweist, dass die Lizenz eine Nutzung ausdrücklich jedem zugesteht, der sich an die Bedingungen hält und gerade keine Ausnahmen für Vertragsbrüche gemacht werden (so Jaeger/Metzger, „Open Source Software“, bei Rn. 154). Letzteres erscheint derzeit, auf Grund des klaren Wortlautes der Lizenzvereinbarung, vorzugswürdig.

Festzuhalten ist nochmals ausdrücklich, dass die rechtliche Wirksamkeit der GPL heute allgemein anerkannt ist. Wer Software nutzt, die der GPL unterliegt, und dabei die Vorgaben der GPL nicht einhält, der sieht sich Unterlassungsansprüchen ausgesetzt (LG München I, Az. 7 O 5245/07; LG Berlin, Az. 16 O 134/06).

IV. Geschichte der OSS

In den 60er und 70er Jahren des letzten Jahrhunderts war der Quellcode der von Programmierern geschriebenen Computer-

programme sehr maschinennah. Die Software stellte noch keinen wesentlichen wirtschaftlichen Wert dar, diente sie doch alleine dazu, die aufwendigen Geräte bedienbar zu machen. Sie war stets offen und: war stets austauschbar. Erst durch die Entwicklung einer eigenen Softwareindustrie, die sich von der Hardwareindustrie erst emanzipierte und sie dann majorisierte, entstand die Vorstellung von Software als eigenem wirtschaftlichem Wert. Sie wurde daher auch entsprechend geschützt und zunehmend „proprietär" vermarktet. Das heißt, der Quellcode wurde als Betriebsgeheimnis geschützt und jeder Nutzer musste Lizenzen erwerben, um die Software nutzen zu können. Diese Entwicklung stieß bei vielen Programmierern auf Widerstand, da sie das Bedürfnis hatten, die auf dem Markt vorhandene Software an ihre eigenen Bedürfnisse anpassen zu können. Hierzu bestand aber keine (lizenz-)rechtliche Befugnis.

In den 80er Jahren des letzten Jahrhunderts wurde daher der Ruf nach „freier Software" laut. 1985 gründete dann der US-Amerikaner Richard Stallmann die „Free Software Foundation" (FSF), mit dem Ziel, ein vollkommen freies, uneingeschränkt nutzbares System von UNIX-kompatibler Software zu schaffen, das sog. GNU-System. Wirtschaftlich bedeutsam und für die gesamte Computerindustrie relevant wurde diese Bewegung aber erst durch den LINUX-Erfinder Linus Torvalds. Torvalds machte 1991 den Linux-Quellcode über das Internet mit dem Ziel zugänglich, dass andere Programmierer LINUX verändern und verbessern und ebenfalls die veränderten und verbesserten Versionen frei zugänglich veröffentlichen. Dazu setzte er auf die 1989 von Richard Stallman verfasste GNU GPL.

Seitdem hat die Verbreitung von OSS erheblich zugenommen und immer mehr Computer werden mit OSS verkauft. Da zunehmend auch Netzwerk-Router und Smartphones auf einem Linux-Kernel basieren, ziehen auch hier immer mehr OSS-Produkte ein. Ausschlaggebend für die Verbreitung ist auch das häufig in Lizenzen vorgesehene „Copyleft", da beim Rückgriff auf Software unter einem solchen Copyleft weiterhin die gleiche Open-Source-Lizenz genutzt werden muss.

Outsourcing und Auftragsdatenverarbeitung

I. Outsourcing – wirtschaftlich und rechtlich

1. Wirtschaftliche Betrachtungsweise

Outsourcingmaßnahmen sind normalerweise wirtschaftlich motiviert: Funktionen des Unternehmens, die es prinzipiell auch selbst intern wahrnehmen könnte, werden an Externe verlagert, weil

- diese die Aufgaben preisgünstiger erledigen können,
- sie die Aufgaben qualitativ höherwertiger erledigen können, mag das unter Umständen auch teurer sein oder
- sie über Know-how verfügen, das im eigenen Unternehmen nicht verfügbar ist.

Es trifft also **nicht** zu, dass es beim Outsourcing stets nur ums Sparen geht. Zugleich wird deutlich, dass es „das" einheitliche Motiv für Outsourcingmaßnahmen nicht gibt. Auch geschieht deren Umsetzung auf sehr unterschiedliche Art und Weise. Die Palette ist sehr breit.

Beispiele:

- Auslagerung von reinen Zuarbeiten (etwa Drucken und Kopieren)
- Auslagerung komplexer Tätigkeiten (etwa der Lohn- und Gehaltsabrechnung)
- Auslagerung ganzer Teilfunktionen des Unternehmens (etwa das Personalwesen insgesamt)

Extremfälle kommen in Konzernstrukturen vor, wo es so weit gehen kann, dass alle typischen Unternehmensfunktionen so zwischen mehreren Konzernunternehmen aufgeteilt sind, dass sie nur noch alle zusammen existenz- und handlungsfähig sind. Man spricht hier von „Matrixstrukturen". Diese Struktur wird – unter Vergleich mit anderen denkbaren Strukturen – erläutert auf der Seite http://www.themanagement.de/ressources/Strukturen.htm

Beispiel:

Es bestehen vier Konzernunternehmen A, B, C und D jeweils als eigene GmbH. A erledigt für alle vier Unternehmen das Rechnungswesen, B für alle das Personalwesen, C die Logistik usw.

Wer sich diese Bandbreite vorkommender Gestaltungen vor Augen hält, kann und wird nicht erwarten, dass alle Konstellationen rechtlich einheitlich behandelt werden können. Vom

Ausgangspunkt her geht es meist um die Frage, wie Datenflüsse, die aus personenbezogenen Daten bestehen, rechtlich einzuordnen sind. Es handelt sich daher primär um eine Frage des Datenschutzrechts, auf das sich die folgende Darstellung deshalb konzentriert.

2. Rechtliche Einordnung von Datenflüssen

2.1 Irrelevanz einer Konzernzugehörigkeit

Vorab ist darauf hinzuweisen, dass die Zugehörigkeit von Beteiligten zu ein und demselben Konzern in keinem Fall den Ausschlag für die rechtliche Einordnung von Datenflüssen gibt. Das deutsche Datenschutzrecht kennt kein „Konzernprivileg". Das bedeutet, Datenflüsse zwischen (rechtlich ja selbstständigen) Konzernunternehmen sind genauso zu behandeln, wie wenn die Beteiligten nicht durch einen Konzern verbunden sind. Das gilt auch im Verhältnis von „Mutter" und „Tochter" oder bei „gemeinsamen Töchtern" mehrerer Konzernunternehmen (etwa einer ausgelagerten früheren IT-Abteilung).

Der Begriff „Konzern" knüpft an einen wirtschaftlichen, nicht an einen rechtlichen Sachverhalt an. In der Sprache des Datenschutzrechts sind auch Konzernunternehmen im Verhältnis zueinander „Dritte" (§ 3 Abs. 8 Satz 2 BDSG).

2.2 Ausschließlichkeit einer Einordnung

Die rechtliche Einordnung eines Datenflusses ist im Ergebnis immer eindeutig, eine wie immer geartete Wahlfreiheit besteht nicht. Wenn im Folgenden verschiedene Möglichkeiten behandelt werden, dann fällt ein und derselbe Sachverhalt also immer nur in den Bereich einer Möglichkeit. Erscheinen die rechtlichen Konsequenzen dieser Möglichkeit nicht passend, dann muss der **Sachverhalt** so verändert und gestaltet werden, bis die Voraussetzungen der anderen Möglichkeit erfüllt sind. Ein bloßes „Jonglieren mit Begriffen" führt nicht weiter.

Beispiel:

Eine Übermittlung von Daten zwischen zwei Stellen auf der Basis von § 28 BDSG (Datenverarbeitung für eigene Zwecke) setzt in den meisten Fällen eine Interessensabwägung voraus, bei der auch die Interessen des Betroffenen einbezogen werden. Liegt eine Auftragsdatenverarbeitung nach § 11 BDSG vor, bedarf die Weitergabe von Daten einer solchen Abwägung dagegen nicht. Wer die Vorteile der einen oder der anderen Bestimmung genießen will, muss den Sachverhalt so (um)gestalten, dass die Voraussetzungen für die Anwendbarkeit der jeweiligen Regelung erfüllt sind.

2.3 Einordnung als Auftragsdatenverarbeitung

Diese in § 11 BDSG geregelte Möglichkeit setzt das Vorliegen eines „Auftrags" voraus. Der Begriff wird allgemein recht eng verstanden und lässt sich etwa als „intensiv ausgeprägtes Weisungsverhältnis" charakterisieren. Fehlt es daran, weil der „Auftragnehmer" zu große eigene Handlungsspielräume hat, wird ein Auftragsverhältnis verneint. Eine Weitergabe von Daten auf der Basis von § 11 BDSG ist dann nicht möglich.

In solchen „Negativfällen" wird das bestehende Rechtsverhältnis in der Regel durch den Begriff der „Funktionsübertragung" charakterisiert. Er bedeutet im Ergebnis, dass eine Weitergabe von Daten nur zulässig ist, wenn die rechtlichen Voraussetzungen für eine Datenübermittlung erfüllt sind (in der Regel also § 28 BDSG oder Vorliegen einer Einwilligung).

2.4 Haltung der Aufsichtsbehörden

Ein Papier der Datenschutzbeauftragten des Bundes und der Länder vom Oktober 2008 möchte den Begriff der Auftragsdatenverarbeitung sehr eng auslegen und ihn „ausschließlich als Rechtsgrundlage für Aufträge zur Datenverarbeitung (im rein technischen Sinn) … verstehen." Daraus wird dann gefolgert: „Für eine inhaltliche Aufgabenverlagerung kann § 11 BDSG danach niemals eine rechtliche Grundlage sein." (Siehe http://www.bfdi.bund.de/SharedDocs/Publikationen/Arbeitshilfen/AuftragsdatenverarbeitungOutsourcing.html;jsessionid=38E632BE849913903173FEECBDD2356C.1_cid136?nn=409924). Das würde bedeuten, dass nur reine „Rechenaufträge" im Weg der Auftragsdatenverarbeitung erledigt werden könnten. Zwar richtet sich das genannte Arbeitspapier ausdrücklich nur an die öffentliche Verwaltung. Da alle Landesbeauftragte für den Datenschutz (außer in Bayern) auch für die Aufsicht über die Privatwirtschaft zuständig sind, kann man davon ausgehen, dass über kurz oder lang versucht wird, diese Überlegungen auch auf Privatunternehmen zu übertragen. Das würde deren Spielraum für Auslagerungen erheblich einengen.

2.5 Einordnung als Datenübermittlung

„Übermitteln" bedeutet, dass vorhandene Daten in der Weise an einen Dritten bekannt gegeben werden, dass

- die Daten an den Dritten weitergegeben werden oder
- der Dritte die Daten einsieht oder abruft.

So die Definition in § 3 Abs. 4 Satz 2 Nr. 3 BDSG.

Diese Voraussetzungen sind für sich gesehen rein begrifflich auch erfüllt, wenn ein Auftragsverhältnis vorliegt. Für diese Fälle trifft aber das Gesetz die Abgrenzung, dass ein Auftragnehmer im Sinn von § 11 BDSG nicht als Dritter gilt (§ 3 Abs. 8 Satz 3 BDSG).

Letztlich kommt es bei Outsourcingmaßnahmen also entscheidend darauf an, ob es gelingt, die Voraussetzungen einer Auftragsdatenverarbeitung zu erfüllen:

- Ist das der Fall, dann ist die Weitergabe von Daten zwischen den Beteiligten ohne besondere Voraussetzungen zulässig.
- Falls nicht, müssen für die Weitergabe die oft nicht leicht zu erfüllenden Voraussetzungen für eine rechtmäßige Datenübermittlung eingehalten sein.

II. Gestaltung als Auftragsdatenverarbeitung (§ 11 BDSG)

1. Abgrenzung Auftragsdatenverarbeitung/ Funktionsübertragung

Eine Auftragsdatenverarbeitung liegt nur dann vor, wenn detaillierte Vorgaben dafür bestehen, wie mit den überlassenen Daten umzugehen ist.

Beispiel:

Ein Dienstleister wird damit beauftragt, auf der Basis eines bestimmten Tarifvertrages die Löhne der gesamten Belegschaft zu berechnen. Spielräume bei der Anwendung des Tarifvertrages bestehen für den Dienstleister nicht.

Anders sieht es dagegen aus, wenn nur eine allgemeine, nicht im Einzelnen definierte Aufgabenstellung vorgegeben ist:

Beispiel:

Die vorhandene Personalabteilung wird aufgelöst, alle vorhandenen Unterlagen werden einem externen Dienstleister übergeben. Gegen Zahlung eines monatlichen Pauschalbetrags je Mitarbeiter übernimmt der Dienstleister „die Abwicklung aller Arbeitgeberpflichten, insbesondere Durchführung von Einstellungsverfahren, Lohnberechnungen, Kündigungsabwicklung (außergerichtlich) und das Erstellen von Zeugnissen".

Diese Aufgabenstellung ist so pauschal, dass keine Auftragsdatenverarbeitung gemäß § 11 BDSG mehr vorliegt. Man spricht dann von einer „Funktionsübertragung", weil der Dienstleister letztlich funktional gesehen an die Stelle seines Auftraggebers tritt und nach eigenem Ermessen tun kann, was er für richtig hält.

Wie der Kontrast zwischen den beiden Beispielen zeigt, lässt es sich in gewissen Grenzen über die Gestaltung des Vertrages zwischen den Beteiligten steuern, welcher der beiden Begriffe „Auftragsdatenverarbeitung" und „Funktionsübertragung" erfüllt ist.

Welcher der beiden Begriffe erfüllt ist, lässt sich also in gewissen Grenzen über die Gestaltung des Vertrages zwischen den Beteiligten steuern. Beim letztgenannten Beispiel wäre wie folgt zu verfahren, um eine Wertung als Auftragsdatenverarbeitung zu erreichen:

- Es wird nicht die Übernahme „aller Arbeitgeberpflichten" vereinbart, vielmehr wird ein (abschließender!) Katalog der einzelnen Pflichten erstellt, die zu übernehmen sind.
- Für jede einzelne Pflicht wird vorgegeben, wie zu verfahren ist (Vorgabe von Checklisten, Mustertexten, Ablaufplänen).
- Es wird ausdrücklich festgelegt, dass bestimmte wichtige Ergebnisse (etwa ein Kündigungsschreiben oder ein Zeugnis) in jedem Einzelfall zur Billigung vorgelegt werden müssen – wobei die Billigung dann recht formalisiert erfolgen kann.

Dies führt rein äußerlich zu relativ umfangreichen Verträgen mit vielen Auflagen, Handbüchern usw. Anders gelingt es jedoch nicht, nach außen zu dokumentieren, dass der Auftraggeber „Herr des Geschehens" bleibt.

Auf dieser Basis ist es möglich, auch relativ komplexe Tätigkeiten als Auftragsdatenverarbeitung auszugestalten. Dabei ist es keineswegs verboten, dass der Auftragnehmer im Vorfeld die nötigen umfangreichen Verträge und Muster ausarbeitet und der Auftraggeber diese Vorschläge übernimmt. Es stört auch nicht, wenn die entsprechenden „Dokumentenpakete" in mehreren Fällen verwendet werden.

Beispiel:

Die DATEV e. G. führt für zahlreiche Auftraggeber relativ komplexe Tätigkeiten nach einer Reihe einheitlicher Schemata durch, die sehr umfangreich dokumentiert sind und dem Auftraggeber eine Reihe von Wahlmöglichkeiten lassen.

2. Schriftform

Ein Auftrag muss stets schriftlich erteilt werden (§ 11 Abs. 2 Satz 2 BDSG). Kern des Auftrags muss die Festlegung bilden, was genau mit welchen Daten geschehen soll (siehe dazu vorstehend 1). Hinzu kommen muss laut § 11 Abs. 2 Satz 2 BDSG, der zum 1.9.2009 erheblich erweitert wurde, ein ganzer Katalog an weiteren Festlegungen, der aus insgesamt zehn Ziffern besteht:

1. Gegenstand und die Dauer des Auftrags,
2. Umfang, die Art und der Zweck der vorgesehenen Erhebung, Verarbeitung oder Nutzung von Daten, die Art der Daten und der Kreis der Betroffenen,
3. nach § 9 zu treffende technische und organisatorische Maßnahmen,
4. Berichtigung, Löschung und Sperrung von Daten,
5. nach Absatz 4 bestehende Pflichten des Auftragnehmers, insbesondere die von ihm vorzunehmenden Kontrollen,
6. etwaige Berechtigung zur Begründung von Unterauftragsverhältnissen,
7. Kontrollrechte des Auftraggebers und die entsprechenden Duldungs- und Mitwirkungspflichten des Auftragnehmers,
8. mitzuteilende Verstöße des Auftragnehmers oder der bei ihm beschäftigten Personen gegen Vorschriften zum Schutz personenbezogener Daten oder gegen die im Auftrag getroffenen Festlegungen,
9. Umfang der Weisungsbefugnisse, die sich der Auftraggeber gegenüber dem Auftragnehmer vorbehält,
10. Rückgabe überlassener Datenträger und die Löschung beim Auftragnehmer gespeicherter Daten nach Beendigung des Auftrags.

Besonders Ziffer 3 (nach § 9 BDSG zu treffende technische und organisatorische Maßnahmen) erfordert detaillierte Festlegungen, die deshalb gesondert betrachtet werden müssen (siehe dazu den folgenden Gliederungspunkt).

3. Festlegung technischer und organisatorischer Maßnahmen nach § 9 BDSG

Pragmatisch kann man wie folgt vorgehen:

- Schon deutlich vor der Auftragserteilung wird der potenzielle Auftragnehmer aufgefordert, sein Datenschutzkonzept vorzulegen.
- Dieses wird auf Tauglichkeit geprüft, nötigenfalls ergänzt und als Pflichten, die vom Auftragnehmer einzuhalten sind, zum Bestandteil des Vertrages gemacht.

So wird sichergestellt, dass nur Auftragnehmer ausgewählt werden, die geeignete derartige Maßnahmen getroffen haben (§ 11 Abs. 2 Satz 1 BDSG).

Für die Beurteilung des Datenschutzkonzepts können Checklisten hilfreich sein, die auf die üblichen „Hauptschwachstellen" zielen.

Beispiel einer solchen Checkliste (siehe Ehmann, Sicherheit beim Outsourcing, Datenschutz Praxis 9/2007, S. 1, 9):

❑ Wie sieht die Datenanlieferung aus?

Klären Sie die Anlieferung der Daten: Wann, wo, wie (auf Datenträger oder elektronisch)? Legen Sie Maßnahmen zur Prüfung der Vollständigkeit und Unversehrtheit fest.

Legen Sie fest, an wen und wie schnell eine Rückmeldung gemacht werden soll, wenn die Daten nicht pünktlich eintreffen.

Ausgangspunkt her geht es meist um die Frage, wie Datenflüsse, die aus personenbezogenen Daten bestehen, rechtlich einzuordnen sind. Es handelt sich daher primär um eine Frage des Datenschutzrechts, auf das sich die folgende Darstellung deshalb konzentriert.

2. Rechtliche Einordnung von Datenflüssen

2.1 Irrelevanz einer Konzernzugehörigkeit

Vorab ist darauf hinzuweisen, dass die Zugehörigkeit von Beteiligten zu ein und demselben Konzern in keinem Fall den Ausschlag für die rechtliche Einordnung von Datenflüssen gibt. Das deutsche Datenschutzrecht kennt kein „Konzernprivileg". Das bedeutet, Datenflüsse zwischen (rechtlich ja selbstständigen) Konzernunternehmen sind genauso zu behandeln, wie wenn die Beteiligten nicht durch einen Konzern verbunden sind. Das gilt auch im Verhältnis von „Mutter" und „Tochter" oder bei „gemeinsamen Töchtern" mehrerer Konzernunternehmen (etwa einer ausgelagerten früheren IT-Abteilung).

Der Begriff „Konzern" knüpft an einen wirtschaftlichen, nicht an einen rechtlichen Sachverhalt an. In der Sprache des Datenschutzrechts sind auch Konzernunternehmen im Verhältnis zueinander „Dritte" (§ 3 Abs. 8 Satz 2 BDSG).

2.2 Ausschließlichkeit einer Einordnung

Die rechtliche Einordnung eines Datenflusses ist im Ergebnis immer eindeutig, eine wie immer geartete Wahlfreiheit besteht nicht. Wenn im Folgenden verschiedene Möglichkeiten behandelt werden, dann fällt ein und derselbe Sachverhalt also immer nur in den Bereich einer Möglichkeit. Erscheinen die rechtlichen Konsequenzen dieser Möglichkeit nicht passend, dann muss der **Sachverhalt** so verändert und gestaltet werden, bis die Voraussetzungen der anderen Möglichkeit erfüllt sind. Ein bloßes „Jonglieren mit Begriffen" führt nicht weiter.

Beispiel:

Eine Übermittlung von Daten zwischen zwei Stellen auf der Basis von § 28 BDSG (Datenverarbeitung für eigene Zwecke) setzt in den meisten Fällen eine Interessensabwägung voraus, bei der auch die Interessen des Betroffenen einbezogen werden. Liegt eine Auftragsdatenverarbeitung nach § 11 BDSG vor, bedarf die Weitergabe von Daten einer solchen Abwägung dagegen nicht. Wer die Vorteile der einen oder der anderen Bestimmung genießen will, muss den Sachverhalt so (um)gestalten, dass die Voraussetzungen für die Anwendbarkeit der jeweiligen Regelung erfüllt sind.

2.3 Einordnung als Auftragsdatenverarbeitung

Diese in § 11 BDSG geregelte Möglichkeit setzt das Vorliegen eines „Auftrags" voraus. Der Begriff wird allgemein recht eng verstanden und lässt sich etwa als „intensiv ausgeprägtes Weisungsverhältnis" charakterisieren. Fehlt es daran, weil der „Auftragnehmer" zu große eigene Handlungsspielräume hat, wird ein Auftragsverhältnis verneint. Eine Weitergabe von Daten auf der Basis von § 11 BDSG ist dann nicht möglich.

In solchen „Negativfällen" wird das bestehende Rechtsverhältnis in der Regel durch den Begriff der „Funktionsübertragung" charakterisiert. Er bedeutet im Ergebnis, dass eine Weitergabe von Daten nur zulässig ist, wenn die rechtlichen Voraussetzungen für eine Datenübermittlung erfüllt sind (in der Regel also § 28 BDSG oder Vorliegen einer Einwilligung).

2.4 Haltung der Aufsichtsbehörden

Ein Papier der Datenschutzbeauftragten des Bundes und der Länder vom Oktober 2008 möchte den Begriff der Auftragsdatenverarbeitung sehr eng auslegen und ihn „ausschließlich als Rechtsgrundlage für Aufträge zur Datenverarbeitung (im rein technischen Sinn) … verstehen." Daraus wird dann gefolgert: „Für eine inhaltliche Aufgabenverlagerung kann § 11 BDSG danach niemals eine rechtliche Grundlage sein." (Siehe http://www.bfdi.bund.de/SharedDocs/Publikationen/Arbeitshilfen/AuftragsdatenverarbeitungOutsourcing.html;jsessionid=38E632BE849913903173FEECBDD2356C.1_cid136?nn=409924). Das würde bedeuten, dass nur reine „Rechenaufträge" im Weg der Auftragsdatenverarbeitung erledigt werden könnten. Zwar richtet sich das genannte Arbeitspapier ausdrücklich nur an die öffentliche Verwaltung. Da alle Landesbeauftragte für den Datenschutz (außer in Bayern) auch für die Aufsicht über die Privatwirtschaft zuständig sind, kann man davon ausgehen, dass über kurz oder lang versucht wird, diese Überlegungen auch auf Privatunternehmen zu übertragen. Das würde deren Spielraum für Auslagerungen erheblich einengen.

2.5 Einordnung als Datenübermittlung

„Übermitteln" bedeutet, dass vorhandene Daten in der Weise an einen Dritten bekannt gegeben werden, dass

- die Daten an den Dritten weitergegeben werden oder
- der Dritte die Daten einsieht oder abruft.

So die Definition in § 3 Abs. 4 Satz 2 Nr. 3 BDSG.

Diese Voraussetzungen sind für sich gesehen rein begrifflich auch erfüllt, wenn ein Auftragsverhältnis vorliegt. Für diese Fälle trifft aber das Gesetz die Abgrenzung, dass ein Auftragnehmer im Sinn von § 11 BDSG nicht als Dritter gilt (§ 3 Abs. 8 Satz 3 BDSG).

Letztlich kommt es bei Outsourcingmaßnahmen also entscheidend darauf an, ob es gelingt, die Voraussetzungen einer Auftragsdatenverarbeitung zu erfüllen:

- Ist das der Fall, dann ist die Weitergabe von Daten zwischen den Beteiligten ohne besondere Voraussetzungen zulässig.
- Falls nicht, müssen für die Weitergabe die oft nicht leicht zu erfüllenden Voraussetzungen für eine rechtmäßige Datenübermittlung eingehalten sein.

II. Gestaltung als Auftragsdatenverarbeitung (§ 11 BDSG)

1. Abgrenzung Auftragsdatenverarbeitung/ Funktionsübertragung

Eine Auftragsdatenverarbeitung liegt nur dann vor, wenn detaillierte Vorgaben dafür bestehen, wie mit den überlassenen Daten umzugehen ist.

Beispiel:

Ein Dienstleister wird damit beauftragt, auf der Basis eines bestimmten Tarifvertrages die Löhne der gesamten Belegschaft zu berechnen. Spielräume bei der Anwendung des Tarifvertrages bestehen für den Dienstleister nicht.

Anders sieht es dagegen aus, wenn nur eine allgemeine, nicht im Einzelnen definierte Aufgabenstellung vorgegeben ist:

Beispiel:

Die vorhandene Personalabteilung wird aufgelöst, alle vorhandenen Unterlagen werden einem externen Dienstleister übergeben. Gegen Zahlung eines monatlichen Pauschalbetrags je Mitarbeiter übernimmt der Dienstleister „die Abwicklung aller Arbeitgeberpflichten, insbesondere Durchführung von Einstellungsverfahren, Lohnberechnungen, Kündigungsabwicklung (außergerichtlich) und das Erstellen von Zeugnissen".

Diese Aufgabenstellung ist so pauschal, dass keine Auftragsdatenverarbeitung gemäß § 11 BDSG mehr vorliegt. Man spricht dann von einer „Funktionsübertragung", weil der Dienstleister letztlich funktional gesehen an die Stelle seines Auftraggebers tritt und nach eigenem Ermessen tun kann, was er für richtig hält.

Wie der Kontrast zwischen den beiden Beispielen zeigt, lässt es sich in gewissen Grenzen über die Gestaltung des Vertrages zwischen den Beteiligten steuern, welcher der beiden Begriffe „Auftragsdatenverarbeitung" und „Funktionsübertragung" erfüllt ist.

Welcher der beiden Begriffe erfüllt ist, lässt sich also in gewissen Grenzen über die Gestaltung des Vertrages zwischen den Beteiligten steuern. Beim letztgenannten Beispiel wäre wie folgt zu verfahren, um eine Wertung als Auftragsdatenverarbeitung zu erreichen:

- Es wird nicht die Übernahme „aller Arbeitgeberpflichten" vereinbart, vielmehr wird ein (abschließender!) Katalog der einzelnen Pflichten erstellt, die zu übernehmen sind.
- Für jede einzelne Pflicht wird vorgegeben, wie zu verfahren ist (Vorgabe von Checklisten, Mustertexten, Ablaufplänen).
- Es wird ausdrücklich festgelegt, dass bestimmte wichtige Ergebnisse (etwa ein Kündigungsschreiben oder ein Zeugnis) in jedem Einzelfall zur Billigung vorgelegt werden müssen – wobei die Billigung dann recht formalisiert erfolgen kann.

Dies führt rein äußerlich zu relativ umfangreichen Verträgen mit vielen Auflagen, Handbüchern usw. Anders gelingt es jedoch nicht, nach außen zu dokumentieren, dass der Auftraggeber „Herr des Geschehens" bleibt.

Auf dieser Basis ist es möglich, auch relativ komplexe Tätigkeiten als Auftragsdatenverarbeitung auszugestalten. Dabei ist es keineswegs verboten, dass der Auftragnehmer im Vorfeld die nötigen umfangreichen Verträge und Muster ausarbeitet und der Auftraggeber diese Vorschläge übernimmt. Es stört auch nicht, wenn die entsprechenden „Dokumentenpakete" in mehreren Fällen verwendet werden.

Beispiel:

Die DATEV e. G. führt für zahlreiche Auftraggeber relativ komplexe Tätigkeiten nach einer Reihe einheitlicher Schemata durch, die sehr umfangreich dokumentiert sind und dem Auftraggeber eine Reihe von Wahlmöglichkeiten lassen.

2. Schriftform

Ein Auftrag muss stets schriftlich erteilt werden (§ 11 Abs. 2 Satz 2 BDSG). Kern des Auftrags muss die Festlegung bilden, was genau mit welchen Daten geschehen soll (siehe dazu vorstehend 1). Hinzu kommen muss laut § 11 Abs. 2 Satz 2 BDSG, der zum 1.9.2009 erheblich erweitert wurde, ein ganzer Katalog an weiteren Festlegungen, der aus insgesamt zehn Ziffern besteht:

1. Gegenstand und die Dauer des Auftrags,
2. Umfang, die Art und der Zweck der vorgesehenen Erhebung, Verarbeitung oder Nutzung von Daten, die Art der Daten und der Kreis der Betroffenen,
3. nach § 9 zu treffende technische und organisatorische Maßnahmen,
4. Berichtigung, Löschung und Sperrung von Daten,
5. nach Absatz 4 bestehende Pflichten des Auftragnehmers, insbesondere die von ihm vorzunehmenden Kontrollen,
6. etwaige Berechtigung zur Begründung von Unterauftragsverhältnissen,
7. Kontrollrechte des Auftraggebers und die entsprechenden Duldungs- und Mitwirkungspflichten des Auftragnehmers,
8. mitzuteilende Verstöße des Auftragnehmers oder der bei ihm beschäftigten Personen gegen Vorschriften zum Schutz personenbezogener Daten oder gegen die im Auftrag getroffenen Festlegungen,
9. Umfang der Weisungsbefugnisse, die sich der Auftraggeber gegenüber dem Auftragnehmer vorbehält,
10. Rückgabe überlassener Datenträger und die Löschung beim Auftragnehmer gespeicherter Daten nach Beendigung des Auftrags.

Besonders Ziffer 3 (nach § 9 BDSG zu treffende technische und organisatorische Maßnahmen) erfordert detaillierte Festlegungen, die deshalb gesondert betrachtet werden müssen (siehe dazu den folgenden Gliederungspunkt).

3. Festlegung technischer und organisatorischer Maßnahmen nach § 9 BDSG

Pragmatisch kann man wie folgt vorgehen:

- Schon deutlich vor der Auftragserteilung wird der potenzielle Auftragnehmer aufgefordert, sein Datenschutzkonzept vorzulegen.
- Dieses wird auf Tauglichkeit geprüft, nötigenfalls ergänzt und als Pflichten, die vom Auftragnehmer einzuhalten sind, zum Bestandteil des Vertrages gemacht.

So wird sichergestellt, dass nur Auftragnehmer ausgewählt werden, die geeignete derartige Maßnahmen getroffen haben (§ 11 Abs. 2 Satz 1 BDSG).

Für die Beurteilung des Datenschutzkonzepts können Checklisten hilfreich sein, die auf die üblichen „Hauptschwachstellen" zielen.

Beispiel einer solchen Checkliste (siehe Ehmann, Sicherheit beim Outsourcing, Datenschutz Praxis 9/2007, S. 1, 9):

❑ Wie sieht die Datenanlieferung aus?

Klären Sie die Anlieferung der Daten: Wann, wo, wie (auf Datenträger oder elektronisch)? Legen Sie Maßnahmen zur Prüfung der Vollständigkeit und Unversehrtheit fest.

Legen Sie fest, an wen und wie schnell eine Rückmeldung gemacht werden soll, wenn die Daten nicht pünktlich eintreffen.

- ❑ Wie ist der Datentransport geregelt?

  Beim Versenden von Datenträgern hat sich das „Zweischlüsselsystem“ bewährt. Dabei werden die Datenträger vom Auftraggeber in ein stabiles Behältnis gelegt, das verschlossen wird. Der Transporteur hat keinen Schlüssel, der Auftragnehmer natürlich schon. Der Datentransport ist eine gefährliche potenzielle Schwachstelle, die oft zu wenig beachtet wird.

- ❑ Wie werden die Daten verschlüsselt?

  Überlegen Sie, welche Verschlüsselungssysteme Sie bei der elektronischen Übertragung der Daten einsetzen wollen.

- ❑ Wie bewahrt der Auftragnehmer die Daten auf?

  Prüfen Sie, wie die Sicherung gegen unbefugten Zugriff durch Dritte und durch Personen im Unternehmen des Auftragnehmers erfolgt. Gerade Letzteres wird oft als Gefahr übersehen!

- ❑ Ist gewährleistet, dass jederzeit zu reproduzieren ist, wohin die Daten kopiert wurden? Beachten Sie die Gefahr der Industriespionage.

- ❑ Wie geht der Auftragnehmer mit der Datenlöschung und mit Ausschussmaterial um?

  - ❑ Legen Sie die Löschung der Daten nach Abschluss des Auftrags fest. Fordern Sie eine Protokollierung und Nachprüfbarkeit der Löschvorgänge!

  - ❑ Prüfen Sie, wie mit Ausschussmaterial umgegangen wird. Dies ist wichtig, wenn das Erstellen von Ausdrucken oder das Brennen einer CD zum Gegenstand des Auftrags gehört.

- ❑ Kann der Auftragnehmer jederzeit nachvollziehen, wer bei ihm die Daten in der Hand gehabt hat?

- ❑ Die folgende Frage löst bisweilen Panik aus: Können Sie uns auch im Nachhinein lückenlos auflisten, welche Personen bei Ihnen mit unseren Daten befasst waren?

Ob die nötigen technischen und organisatorischen Maßnahmen auch tatsächlich eingehalten werden, ist **vor** Beginn der Arbeiten und – vor allem bei länger dauernden Vertragsverhältnissen – stichprobenartig auch danach zu prüfen (siehe § 11 Abs. 2 Satz 4 BDSG).

Völlig untauglich sind die in der Praxis oft anzutreffenden kurzen Erklärungen folgender Art: „Wir verpflichten uns, bei der Verarbeitung der Daten alle Vorschriften des Datenschutzes (BDSG und weitere Vorschriften) einzuhalten.“ Dies wird der gesetzlichen Verpflichtung, Einzelfestlegungen zu treffen (§ 11 Abs. 2 Satz 2 BDSG), in keiner Weise gerecht. Im Ernstfall entsteht zudem nur Streit darüber, was eigentlich konkret aus den gesetzlichen Regelungen folgt.

4. Unterauftragsverhältnisse

Unterauftragsverhältnisse bringen **besondere Risiken** mit sich. Der Auftraggeber kann oft nicht mehr überblicken, wer mit den von ihm zur Verfügung gestellten Daten umgeht. Ob Maßnahmen, zu denen sich der „Erst-Auftragnehmer“ verpflichtet hat, auch beim Unterauftragnehmer noch eingehalten werden, ist unsicher und oft kaum zu kontrollieren.

Grundregel sollte deshalb sein, die Vergabe von Unteraufträgen auszuschließen. Rechtlich sind sie jedoch möglich (Folgerung aus § 11 Abs. 2 Satz 2 Nr. 6 BDSG).

Lassen sie sich nicht vermeiden, sind folgende Festlegungen sinnvoll:

- Erteilung von Unteraufträgen nur mit vorheriger schriftlicher Zustimmung,
- Mitteilung von Name und Anschrift des Unterauftragnehmers,
- Übernahme aller Pflichten des Auftragnehmers auch durch den Unterauftragnehmer,
- Einräumung des Rechts zur direkten Kontrolle vor Ort auch beim Unterauftragnehmer.

5. Vertrauen ist gut, Kontrolle ist besser

Stets sollte zumindest vor Vergabe eines Auftrags eine Besichtigung vor Ort stattfinden. Der unmittelbare persönliche Eindruck hat schon manches schriftlich beeindruckende Datenschutzkonzept als Makulatur entlarvt. Eine Besichtigung muss dokumentiert werden. § 11 Abs. 2 Satz 4 BDSG verpflichtet aber nicht zwingend zu einer Besichtigung vor Ort. Unterbleibt sie, muss auf sonstige Weise überprüft werden, ob die notwendigen Maßnahmen eingehalten sind. Die hierfür denkbaren Wege (etwa Vorlage von Dokumenten, Bescheinigungen des Datenschutzbeauftragten des Auftragnehmers) schließen Manipulationsmöglichkeiten jedoch selten so zuverlässig aus wie eine Besichtigung vor Ort. Eine Dokumentation ist stets notwendig (§ 11 Abs. 2 Satz 5 BDSG).

6. Verantwortungsverteilung bei einem Auftragsverhältnis

Das Gesetz formuliert klar, dass der Auftraggeber auch (und gerade) nach Vergabe eines Auftrags nach außen datenschutzrechtlich verantwortlich bleibt (§ 11 Abs. 1 Satz 1 BDSG). Dies ist auch der Grund dafür, warum er detaillierte Vorgaben für den Auftragnehmer festlegen muss.

Sofern ein Betroffener Rechte nach dem BDSG geltend machen will (etwa das Auskunftsrecht, § 34 BDSG), ist nach wie vor der Auftraggeber sein Adressat, nicht der Auftragnehmer. Der Betroffene kann nicht an den Auftragnehmer verwiesen werden.

7. Musterverträge

7.1 Muster für die Privatwirtschaft

Im Internet gibt es inzwischen schon genügend kostenlose Musterverträge, die schon an die Änderungen des § 11 BDSG im Jahr 2009 angepasst wurden:

- Muster der GDD:

  https://www.gdd.de/nachrichten/news/neues-gdd-muster-zur-auftragsdatenverarbeitung-gemas-a7-11-bdsg

- Muster des Unabhängigen Landeszentrums für Datenschutz (ULD) Schleswig-Holstein

  https://www.datenschutzzentrum.de/wirtschaft/vertrgad.htm

V. Umschreibung im Markenregister

Die Eintragung des Rechtsübergangs im Markenregister ist nicht obligatorisch und keine Voraussetzung eines wirksamen Rechtserwerbs. Allerdings ist die sogenannte Umschreibung im Register auf jeden Fall zu empfehlen, da die (widerlegliche) Vermutung besteht, dass derjenige materieller Rechtsinhaber der Marke ist, der als Inhaber im Register vermerkt ist. Dies kann bei markenrechtlichen Streitigkeiten oder in einem Verfahren gegenüber dem Amt relevant werden, wenn es gilt, die Inhaberschaft nachzuweisen.

Die Umschreibung der Marke ist beim Deutschen Patent- und Markenamt zu beantragen. Sie ist kostenlos, weil die Richtigkeit des Registerinhalts auch im öffentlichen Interesse liegt.

VI. Übertragung von Nutzungsrechten – die Lizenz

Die Übertragung von Nutzungsrechten sowohl an einer eingetragenen als auch angemeldeten Marke ist durch Einräumung einer Lizenz gem. § 30 MarkenG möglich. Damit gestattet der Lizenzgeber dem Lizenznehmer in der Regel gegen Zahlung einer bestimmten Lizenzgebühr die Benutzung der Marke. Es können jedoch auch kostenlose Lizenzen erteilt werden.

1. Lizenzarten

Bei Lizenzverträgen sind unterschiedliche Ausgestaltungen möglich. Zum einen können ausschließliche Lizenzen, mit denen ein alleiniges Nutzungsrecht an der Marke dem Lizenznehmer eingeräumt wird, zum anderen einfache (nicht ausschließliche) Lizenzen, mit denen der Markeninhaber weiterhin über das Nutzungsrecht verfügen kann, entweder durch eigene Nutzung der Marke oder auch durch Vergabe weiterer Lizenzen an Dritte. Natürlich ist auch die Erteilung von Unterlizenzen möglich, soweit dieses Recht dem Lizenznehmer vom Lizenzgeber eingeräumt wurde oder sich durch Auslegung des Lizenzvertrages ergibt. Das Recht zur Abtretung des Lizenzrechts hat der Lizenznehmer in der Regel nur, wenn die Zustimmung des Lizenzgebers vorliegt.

2. Inhalt und Form der Lizenz

Gegenstand des Benutzungsrechts an der Marke kann die Dauer der Lizenz, die Form der Markenbenutzung, der räumliche Geltungsbereich, die Waren und Dienstleistungen und die Qualität der unter der Marke angebotenen Produkte sein. Hierbei sind auch Teillizenzen möglich. Eine Kombinierung von ausschließlicher und einfacher Lizenz ist im Hinblick auf die unterschiedlichen Regelungspunkte möglich, beispielsweise durch Einräumung einer ausschließlichen Lizenz für ein bestimmtes Teilgebiet, während für das andere Teilgebiet die Vergabe weiterer Lizenzen möglich bleibt.

Der Abschluss einer Lizenz ist formlos möglich. Allerdings ist natürlich aus Gründen der Rechtsklarheit der schriftliche Abschluss zu empfehlen.

3. Rechte des Lizenznehmers gegenüber Dritten

Rechte wegen Verletzung der Markenrechte kann der Lizenznehmer gem. § 30 Abs. 3 MarkenG nur mit Zustimmung des Lizenzgebers durchsetzen. Dies gilt sowohl für das außergerichtliche Vorgehen im Wege der Abmahnung als auch für die Markenverletzungsklage. Er macht dann das fremde Recht des Markeninhabers in eigenem Namen geltend.

Kann der Lizenznehmer keine markenrechtlichen Ansprüche gegenüber Dritten mangels Zustimmung geltend machen, so räumt ihm § 30 Abs. 4 MarkenG die Möglichkeit ein, der vom Markeninhaber erhobenen Markenverletzungsklage beizutreten, um auf diese Weise Schadensersatz geltend zu machen.

Wird die Marke gem. § 27 MarkenG übertragen, bleiben bestehende Lizenzen davon unberührt.

Urheberrecht

I. Begriff

Das Urheberrecht schützt geistige und künstlerische Leistungen, z. B. Kompositionen, Gemälde, Skulpturen, Texte, Theaterinszenierungen, Fotografien, Filme, Rundfunksendungen, Musik- und Tonaufnahmen, aber auch **Software, Spiele** und **Computerprogramme.** Ziel des Urheberrechtes ist es, **die** berechtigten Interessen der Kreativen zu schützen. Das Urheberrecht berücksichtigt damit die wirtschaftlichen Interessen und die Ideale des Urhebers am Werk, wird aber zum Teil zur Wahrung der Interessen der Allgemeinheit eingeschränkt (z. B. → *Schranken des Urheberrechts*). Entscheidend ist, dass das Urheberrecht nur das **Werk,** nicht aber die dem Werk zugrunde liegenden **Ideen** schützt. Solange also ein Werk noch nicht existiert, sondern lediglich in der Vorstellung des Schaffenden vorliegt, bestehen keine Urheberrechte. Das Werk ist aber nicht nur geschützt in seiner Endform. Bereits alle Entwürfe und festgehaltenen Pläne von Gestaltungen können bereits urheberrechtlichen Schutz genießen.

II. Schöpfungshöhe

Nicht jedes Werk ist geschützt. Erforderlich für einen urheberrechtlichen Schutz ist eine gewisse „**Schöpfungshöhe**“ eines Werkes. Ein Werk muss nach § 2 Abs. 2 UrhG eine persönliche geistige Schöpfung des Urhebers sein. Es versteht sich, dass

ein so allgemeiner Begriff wie Schöpfungshöhe sich nicht festlegen lässt. Die Ansprüche werden aber nicht allzu hoch gesetzt. Es gilt der sogenannte „Schutz der kleinen Münze".

Beispiel für Werke, die den Urheberschutz genießen:

Als Minimalschutz werden im Rahmen eines „Schutzes der kleinen Münze" von der Rechtsprechung

- Preislisten,
- Telefonbücher,
- Newsticker,
- Kataloge und Sammlungen von Kochrezepten

gerade noch als schutzwürdig erachtet.

Beispiel für Werke, die keinen Urheberrechtsschutz genießen:

Die Rechtsprechung sprach Urheberrechtsschutz folgenden Werken ab:

- Anwaltsschriftsätzen, mit der Ausnahme besonders umfangreicher bzw. anspruchsvoller Werke
- Handy-Logos,
- einfachen Bildbearbeitungen von Fotos am Computer.

ACHTUNG!

Anderes gilt nach der Rechtsprechung hingegen im Bereich der angewandten Kunst, also bei Gebrauchsgegenständen mit künstlerischer Formgebung und damit bei Werken, die nicht nur zur Betrachtung bestimmt sind, sondern zugleich einen Gebrauchszweck haben. Hier stellt die Rechtsprechung höhere Anforderungen an die Gestaltungshöhe und verlangt für die Werkqualität und damit für den Urheberrechtsschutz ein deutlich überragendes Niveau der Durchschnittsgestaltung. Maßgeblich für einen Schutz nach diesem Gesetz ist, dass das Designwerk eine eigenständige kreative Leistung darstellt, welche künstlerisch geprägt ist sowie eine nicht unerhebliche Schöpfungshöhe erreicht haben muss. Unter den Möbeldesign-Klassikern wurden beispielsweise Möbelmodellen von Le Corbusier oder den bekannten Thonet-Stühlen Urheberrechtsschutz gewährt. Begründet wird das mit der Möglichkeit des hier gegebenen Geschmacksmusterschutzes nach dem Geschmacksmustergesetz. Es belastet, so die Rechtsprechung, den Schöpfer des Werkes – beziehungsweise seinen Rechtsnachfolger – in den Nutzungsrechten nicht unbillig, bei einem Designwerk, das in seiner Schöpfungshöhe keine besondere künstlerische Höhe erreicht, um geschmacksmusterrechtlichen Schutz durch Eintragung nachzusuchen, falls er eine absolute Rechtsposition erstrebt und sich durch das nicht eingetragene Gemeinschaftsgeschmacksmuster nicht ausreichend geschützt sieht.

Liegt die erforderliche Schöpfungshöhe nicht vor, bleibt das Werk gemeinfrei, d. h. der Urheber hat keinen Anspruch auf einen Schutz.

III. Urheberrecht

Das Urheberrecht wird durch das Urheberrechtsgesetz (UrhG) geschützt. Wesentliche Änderungen brachte der sogenannte „zweite Korb" im Jahre 2008. Die jüngsten Änderungen traten am 1.9.2009 in Kraft.

IV. Entstehung und Erlöschen des Urheberrechts

Das Urheberrecht entsteht im Moment der Schaffung. Es muss im Gegensatz zu Markenrechten oder Patentrechten **nicht angemeldet werden.** Werke, die die notwendige Schöpfungshöhe erreichen, sind somit „automatisch" urheberrechtlich geschützt, ohne dass sie mit dem bekannten **Copyright-Vermerk** gekennzeichnet werden müssen. Es kann aber dennoch sinnvoll sein, sein Werk mit einem Copyright-Vermerk zu versehen. Der Urheber kann auf diese Weise dokumentieren, dass sein Werk urheberechtlich geschützt ist und den oft vorgebrachten Einwand abschneiden, man habe vom Urheberrecht „nichts gewusst". Der Copyright-Vermerk kann auch nach außen dokumentieren, dass der Urheber willens ist, seine Rechte zu verteidigen.

Gemäß § 64 UrhG erlischt das Urheberrecht siebzig Jahre nach dem Tode des Urhebers. Mit dem Tode des Urhebers geht das entsprechende Recht auf die Erben über. Steht das Urheberrecht mehreren Personen gemeinsam zu, so erlischt es 70 Jahre nach dem Tod des längstlebenden Miturhebers. Bei anonymen Werken endet das Urheberrecht 70 Jahre nach der Veröffentlichung.

V. Urheber und Miturheberschaft

Urheber ist der Schöpfer des Werkes. Urheber kann nur eine natürliche Person sein.

Erstellen mehrere Personen gemeinsam ein einheitliches Werk, so gelten sie als Miturheber. Das Urheberrecht steht dann allen Miturhebern gemeinsam zu, d. h. sie müssen einstimmig über die Veröffentlichung/Verwertung des Werkes entscheiden.

Dem Urheber steht das alleinige Recht an der Verwertung seines Werkes zu.

VI. Inhalt des Urheberrechts

Inhalte des Urheberrechts sind gemäß § 11 UrhG der Schutz des Urheberrechts in seinen geistigen und persönlichen Beziehungen zum Werk (Urheberpersönlichkeitsrechte gemäß §§ 12 ff. UrhG), die Nutzung des Werkes (Verwertungsrechte gemäß §§ 15 ff. UrhG) sowie die Sicherung einer angemessenen Vergütung für die Nutzung des Werkes.

1. Urheberpersönlichkeitsrecht

Der Urheber hat an allen urheberrechtlich geschützten Arbeitsergebnissen Urheberpersönlichkeitsrechte.

Hierzu gehören:

- das **Veröffentlichungsrecht** gem. § 12 UrhG. Das Veröffentlichungsrecht ist besonders eng mit den Verwertungsrechten verbunden. Ein Werk kann nur veröffentlicht, d. h. der Allgemeinheit zugänglich gemacht werden, indem es verbreitet, öffentlich ausgestellt oder öffentlich wiedergegeben, also zugleich verwertet wird. Die Veröffentlichung des Werkes schließt somit stets eine Verwertung des Werkes ein.
- das **Recht auf Anerkennung der Urheberschaft** gem. § 13 Satz 1 UrhG. Ein Dritter darf somit nicht vorgeben, selbst Urheber zu sein.
- Das Recht auf **Urheberbezeichnung** gem. § 13 Satz 2 UrhG. Dies bedeutet, dass nur der Urheber entscheiden darf, ob das Werk unter seinem Namen, anonym oder unter Pseudonym veröffentlicht wird.