



IT-Recht: Projekte • eBusiness • AGB

IP-Recht: Marken • Domains • Urheberrecht

Verträge • Schlichtung • Compliance

Rechtsanwältin Berlin & Lissabon
Fachanwältin für Informationstechnologierecht
Dr. Astrid Auer-Reinsdorff

Schumannstraße 18 • 10117 Berlin
www.dr-auer.de • anfrage@dr-auer.de

„Wer glaubt sicher zu sein, ist selbst Teil des Problems!“

Franz Hoheiser-Pförtner, Chief Information Security Officer, Wien

IT-Risikomanagement - rechtliche Anforderungen und relevant für jedes Unternehmen: Datensicherheit, Datenschutz, Compliance

Das moderne IT-Risiko- und Sicherheitsmanagement erfordert neben der organisatorischen und technischen Abbildung von IT-Sicherheit und –Verfügbarkeit die Bewertung rechtlicher Voraussetzungen und Anforderungen. Dies ergibt sich auf nationaler Ebene direkt aus dem Gesetz zur Kontrolle und Transparenz im Unternehmensbereich (KonTraG). Zentrale Forderung des KonTraG ist die Einrichtung eines Frühwarnsystems und bedingt die Einrichtung eines Risikomanagements über alle Ebenen und Bereiche des Unternehmens. Nachdruck erfährt diese Anforderung durch die persönliche Haftung der Vorstände, Aufsichtsräte, Geschäftsführung sowie des IT-Managements.

Dies betrifft in ihren Grundbedingungen alle Branchen und Unternehmensgruppen gleichermaßen. IT-Sicherheit bedeutet nach der Definition des Bundesamtes für Sicherheit in der Informationstechnik (BSI): *„Der Zustand eines IT-Systems, in dem die Risiken, die beim Einsatz dieses Systems aufgrund von Gefährdungen vorhanden sind, durch angemessene Maßnahmen auf ein tragbares Maß beschränkt sind.“*. Dies ist allein mit technischen Maßnahmen nicht erreichbar und wird in Teilbereichen auch zu Einschränkungen in der Flexibilität führen, wenn die rechtlichen Rahmenbedingungen und Risikoabwägungen nicht hinreichend berücksichtigt werden.

An sich sind die rechtlichen Bewertungen der IT-Systeme Bestandteil der im Sinne der Transparenz erforderlichen Risikoberichte, bei deren Fehlen der Abschlussprüfer das Testat verweigern kann. Hier besteht Nachholbedarf – selbst große Unternehmen beziehen die IT-Systeme nicht in ihre Zukunftsprognosen mit ein.

Die Regularien für das IT-Risikomanagement sowie zur Gewährleistung der IT-Sicherheit ergeben sich aus dem KonTraG, dem Bundesdatenschutzgesetz (BDSG), dem Telemediengesetz (TMG) sowie entsprechenden EU Richtlinien zu Basel II, Solvency II und bei Bilanzierung nach internationalen Standards aus dem Sarbanes-Oxley Act (SOX).

Bestandteile sind neben dem Datenschutz, die Archivierungspflichten, die Vorgaben für den elektronischen Geschäftsverkehr sowie Mindestanforderungen an die Vertragsgestaltung sowie das Lizenzmanagement. Für bestimmte Branchen ergeben sich Sonderanforderungen z.B. Banken, Krankenhäuser.

Das BDSG zielt auf den Datenschutz sowie die Datensicherheit ab. Zentrale Ansätze sind daher der Schutz personenbezogener Daten sowie die Sicherung der Datenverarbeitungsprozesse im Unternehmen. So nennt § 9 BDSG i.V.m. der dort referenzierten Anlage technische und organisatorische Maßnahmen, welche durch Kontrolle und Berichterstattung laufend anzupassen sind.

Die Anforderungen des BDSG gelten für jedes Unternehmen unabhängig von dessen Größe. Kleine Unternehmen sind lediglich von der Berufung eines Datenschutzbeauftragten und der Meldepflicht befreit, wenn sie keine hochsensiblen Daten verarbeiten.

Schutzgegenstand sind die personenbezogenen Daten, d.h. Kunden-, Lieferanten- und Mitarbeiterdaten. Mit den Reformen im Laufe des Jahres 2009 ist auch das Arbeitnehmerdatenschutzrecht in Ansätzen kodifiziert worden. Das Datenschutzrecht wird sich weiterentwickeln und das heutige Konzept steht angesichts der Herausforderungen des Social Networkings auf dem Prüfstein. In diesen Kontext gehören auch die Fragen der Vorratsdatenspeicherung sowie der Auskunftspflichten von Providern.

Im Verhältnis zu den Mitarbeitern ist ein immer wieder übersehenes Thema die oft konkludente Gestattung der privaten Email- und Internetnutzung am Arbeitsplatz. Der Email-Verkehr stellt Unternehmen aber auch vor Herausforderungen hinsichtlich der Dokumentation der Geschäftsvorfälle sowie der hinreichenden prüfungssicheren Archivierung. In diesem Zusammenhang werden elektronische Archivierungssysteme mit elektronischen Signatur- und Zeitstempelverfahren an Bedeutung gewinnen.

Die Reformen brachten auch einen weiter ausdefinierten § 11 BDSG, welcher die Anforderungen an die Vertragsgestaltung bei IT-Outsourcing / Auftragsdatenverarbeitung festlegt.

Beachtliche Änderungen ergeben die Reformen darüber hinaus im Bereich des Marketing – teilweise mit Übergangsregelungen und In-Kraft-Treten erst in 2010.

Hier ist auch die Schnittstelle zum eCommerce, da gerade die modernen Kommunikationswege eine Zunahme von Marketingansprachen per Email oder telefonisch hervorriefen. Die gesetzgeberischen Maßnahmen des letzten Jahres zielten hier auf die Abschaffung des Cold Callings sowie überraschender Geschäftsabschlüsse im Internet ab. Das Vertriebsmodell über Affiliate-Partner sowie Suchmaschinenoptimierung ist hinsichtlich der marken- und wettbewerbsrechtlichen Aspekte derzeit beim Bundesgerichtshof sowie beim EuGH anhängig.

Die Anforderungen an die zukunftssichere Gestaltung und Dokumentation von unternehmenskritischen Verträgen und Leistungen sind gestiegen. Im Endkundengeschäft sind auf nationaler Ebene sowie mit der sich in Vorbereitung befindenden Verbraucherrichtlinie neue Anforderungen zu erwarten.

Wichtig im Unternehmen ist zudem das Lizenzmanagement, d.h. das Vorhalten ausreichender Lizenzen sowie die Vorsorge, dass aus dem Unternehmen heraus keine Marken-, Patent- oder Urheberrechtsverletzungen begangen werden. Die Softwarehersteller sichern einerseits ihre Interessen durch die vertragliche Vereinbarung von Linzenzaudits, andererseits birgt die Verwendung von Open Source Software-Komponenten oftmals unerkannte Risiken. Der Handel mit Gebrauchtsoftware ist in seinen rechtlichen Rahmenbedingungen obergerichtlich nicht entschieden und scheint damit unklar. Im Bereich der Risikovorsorge sei die insolvenz sichere Vereinbarung mit dem Lizenzgeber über entsprechende Vertragsgestaltungen und/oder die Einschaltung eines ESCROW-Agenten erwähnt.

IT-Compliance bedeutet, die für das Unternehmen relevanten Themen zu benennen und hinsichtlich ihrer Risiken zu qualifizieren, um so die Konformität des unternehmerischen Führungshandelns mit den gesetzlichen, regulatorischen sowie vertraglichen Vorgaben zu gewährleisten. Da sich die Rahmenbedingungen laufend ändern, sind diese Fragen in einen Risikomanagementkreislauf einzubeziehen.

Viel Erfolg!

Dr. Astrid Auer-Reinsdorff
Rechtsanwältin Berlin & Lissabon
Fachanwältin IT-Recht