

**PERSICON@night 23. Juli 2009**

Rechtliche Anforderungen beim Outsourcing  
von IT-Dienstleistungen



# Haiko Ferber

- Rechtsanwalt
- Ausbildung zum IT-Sicherheitsbeauftragten
- Fachanwaltskurs Steuerrecht
  
- Schwerpunkte: Datenschutz und IT-Vertragsrecht

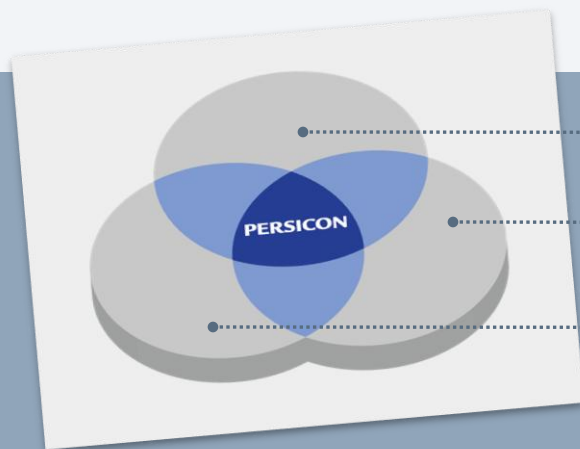


# Knud Brandis

- Studium Rechtswissenschaft an der Universität Potsdam
- Master of Business Administration (MBA)
  
- Mitautor BSI IT-Grundschriftbuch bzw. BSI IT-Grundschriftkataloge
- Lizenziertes BSI IT-Grundschriftauditor
- ISO 27001 Auditor
  
- Dozent an der Fachhochschule Brandenburg und an der Dualen Hochschule Villingen-Schwenningen
  
- Certified Information System Auditor (CISA)
- Certified Information Security Manager (CISM)
- Certified Information System Security Professional (CISSP)
  
- Projektverantwortlicher BSI GSTOOL 5.0

# PERSICON Gruppe

- Führender Anbieter von spezialisierten Beratungs- und Prüfungsleistungen in den Bereichen Risikomanagement, Ordnungsmäßigkeit, Datenschutz und Informationssicherheit
- Schnittmenge zwischen Wirtschaftsprüfung, Rechts- und Organisationsberatung sowie Informationssicherheit
- Hauptsitz in Berlin | Büros in Düsseldorf, Frankfurt am Main, München



Wirtschaftsprüfung

Rechts- und  
Organisationsberatung

Informationssicherheit

# Leistungsschwerpunkte

- Prüfung, Zertifizierung, Beratung und Coaching in den Bereichen Risikomanagement, Ordnungsmäßigkeit, Datenschutz und Informationssicherheit
- Stellung des Datenschutzbeauftragten
- Design, Dokumentation und Prüfung interner Kontrollsysteme (IKS)
- Erstellung von Richtlinien, Verfahrensverzeichnissen, IT-Regelwerken, Betriebs- und Sicherheitskonzepten
- Co- und Outsourcing der internen Revision
- Kontinuitäts- und Notfallmanagement
- Ausbildung von IT-Sicherheits-, Datenschutzbeauftragten und Risikomanagern
- Best Practices: ITIL, COBIT, IDW, ISO 27001 und BSI IT-Grundschutz

# Referenzen (Auszug)

## Öffentlicher Sektor

- Bundesministerium für wirtschaftliche Zusammenarbeit und Entwicklung (BMZ)
- Bundesamt für Sicherheit in der Informationstechnik (BSI)
- Staatskanzlei des Landes Sachsen-Anhalt
- Rundfunk Berlin-Brandenburg (IVZ/RBB)
- Sächsisches Staatsministerium der Finanzen
- Der Sächsische Datenschutzbeauftragte
- Ministerium für Jugend, Bildung und Sport des Landes Brandenburg
- Thüringer Ministeriums für Landwirtschaft, Naturschutz und Umwelt
- Ministerium für Wirtschaft, Verkehr, Landwirtschaft und Weinbau des Landes Rheinland-Pfalz

## Privatwirtschaft

- Deutsche Post
- Pfizer
- E.ON, RWE
- Bertelsmann/arvato
- ThyssenKrupp
- MAN Nutzfahrzeuge
- Talanx Versicherungsgruppe/HDI Gerling
- VHV Versicherungen
- Microsoft
- Sparkassen
- Wasser- und Stadtwerke

IT-Outsourcing

# Einführung

# Begriff „Outsourcing“

- „Outsourcing“ ist ein abgeleitetes Wort aus den englischen Begriffen „Outside“, „Resource“ und „Using“ und heißt zu Deutsch „Auslagerung“.
- Die Bedeutung von „Outsourcing“ ist die Abgabe von Unternehmensleistungen und Vorgängen an Fremdunternehmen.

# Arten des Outsourcing

- Es gibt verschiedene Arten des Outsourcing, je nach Art der Zusammenarbeit zwischen Unternehmen und Outsourcing-Anbieter, lassen sich bestimmte Formen ableiten:
  - **Outtasking** ist die Vergabe von Einzelleistungen (technischer Art) oder einzelner Funktionen – nicht aber von Prozessen – an einen anderen.
  - **Outsourcing** ist die Übernahme von Dienstleistung durch externe Partner. Das Unternehmen kann sich so – bei strategischer Planung – auf die Kernaufgaben konzentrieren.
  - Weitere Formen:
    - Application Service Providing (ASP)
    - Business Process Outsourcing (BBO)
    - Comprehensive Outsourcing
    - Offshore-Outsourcing

# Business Process Outsourcing (BBO)

- Bei dieser Form des Outsourcings werden bestimmte Geschäftsprozesse ausgelagert, etwa die gesamte Lohnverrechnung für die Mitarbeiter.
- Spezialform Business Transformation Outsourcing (BTO): Dieses Servicemodell vereint Beratung und Betrieb von IT- und Geschäftsprozessen. Es integriert Outsourcing und Business Consulting.

# Outtasking

- Das Outtasking (auch Selective Outsourcing) kann als die Light-Variante des klassischen Outsourcing angesehen werden.
- Ähnlich dem Business Process Outsourcing werden nicht komplette Unternehmensbereiche, sondern nur Teilaufgaben, also „Tasks“, ausgelagert.
- Allerdings geht man hier weniger umfassend vor und behält die Kontrolle über die gesamte Infrastruktur

# Comprehensive Outsourcing

- Ein ganzer Unternehmensbereich, inklusive großer Teile der Belegschaft wird an ein Drittunternehmen ausgelagert – zum Beispiel die gesamte EDV an einen IT-Dienstleister über einen bestimmten Zeitraum.

# Managed Services

- Diese Form des Outsourcings kommt vor allem im Informations- und Kommunikationsbereich vor. Für einen genau festgelegten Zeitraum bieten Dienstleister definierte Leistungen an, die der Kunde zu jeder Zeit nach Bedarf abrufen kann.

# Offshore-Outsourcing

- Dieser Begriff bezeichnet die Auslagerung von Dienstleistungen, meist IT-Anwendungsentwicklung in Billiglohnländer, wie Indien oder Staaten des ehemaligen Ostblocks (Polen, Tschechien, Ungarn, Rumänien, Ukraine, Bulgarien) – dann auch oft „Near-Shringing“ genannt.

# Application Service Providing (ASP)

- Beim Application Service Providing nutzt ein Unternehmen Softwaredienste (z.B. ein ERP-System) eines externen Datacenters über öffentliche Netzwerke, wie das Internet.
- Das geschieht meist ohne dass die entsprechende Software lokal auf einem Rechner im Unternehmen installiert bzw. vollständig gekauft werden muss.
- Die gesamte Verarbeitung, Wartung und Datensicherung erfolgt zentral im Datacenter des Dienstleisters.

# Mögliche Vorteile von Outsourcing

- Fokussierung auf seine Kernkompetenzen.
- Gesamtbetriebskosten können sinken
- Transparenz (z. B. bei Kosten)
- Flexibilität
- Bessere Liquidität ( z. B. durch Reduzierung der Investitionen)

# Mögliche Nachteile von Outsourcing

- Abhängigkeit von Outsourcing-Nehmer
- Know-how-Verlust
- Mangelnde Abgrenzung vom Mitbewerber (der auf denselben Dienstleister zurückgreifen kann)
- Risiko des Datenmissbrauchs
- Kleinere Servicenehmer werden vom Servicegeber oft schlechter betreut werden als große.
- Der Servicegeber führt in der Regel eine stärkere Kostenkontrolle durch er es vor dem Outsourcing getan hat
- Längere (Kommunikations- und Freigabe-) Wege als „früher“
- Erwarteten Kostenvorteile sind oft nur kurz- und mittelfristiger Natur
- Rechtliche Risiken

IT-Outsourcing

# Rechtliche und regulatorische Anforderungen

# Anforderungen an den Outsourcing-Geber

- Der Outsourcing-Geber hat regelmäßig die für ihn geltenden rechtlichen und regulatorischen Anforderungen zu prüfen.
- Die Anforderungen richten sich danach, welche Bereiche und/ oder Services ausgelagert werden.

# Überblick

- Gesetz zur Kontrolle und Transparenz im Unternehmensbereich (KonTraG)
- Handelsgesetzbuch (HGB)
- Aktien-Gesetz (AktG)
- GmbH-Gesetz (GmbHG)
- Bilanzierungsmodernisierungsgesetz (BilMoG)
- Abgabenordnung (AO) und Grundsätze der Prüfbarkeit digitaler Unterlagen (GDPdU)
- Bundesdatenschutzgesetz (BDSG)
- Sonstige Datenschutzgesetze
- Strafgesetzbuch (StGB)
- Kreditwesengesetz (KWG) und Mindestanforderungen an das Risikomanagement (MaRisk)
- Versicherungsaufsichtsgesetz (VAG) und Mindestanforderungen an das Risikomanagement (MaRisk VA)
- Gesetz über den Wertpapierhandel (WpHG)
- Sarbanes-Oxley-Act (SOX)
- Standards des Instituts des Wirtschaftsprüfer (IDW)
- ...

# Gesetz zur Kontrolle und Transparenz im Unternehmensbereich (KonTraG)

- Durch das KonTraG wurden einzelne Paragraphen aus bestehenden Gesetzen geändert.
- Es wurden Anforderungen an das Risiko-Management eines Unternehmens in mehreren Gesetzen verankert.
- Unternehmensleitungen werden zur Einführung eines unternehmensweiten Risiko-Management-Systems gezwungen.
- Da ausgelagerte Dienstleistungen in der Regel im Verantwortungsbereich der Unternehmensleitung verbleiben, müssen im Rahmen des Risiko-Management-Systems geeignete Maßnahmen getroffen werden, um die Einhaltung rechtlicher Rahmenbedingungen sowie bestehender Unternehmensrichtlinien im Hinblick auf das Risiko-Management-System auch durch den Outsourcing-Anbieter regelmäßig überprüfen zu können.

# Handelsgesetzbuch (HGB)

Handelsgesetzbuch in Verbindung mit den Grundsätzen ordnungsgemäßer Buchführung (GoB)

- Das HGB enthält selbst keine Vorschriften, die Anforderungen an das Outsourcing von Dienstleistungen enthalten.
- Es existieren jedoch einige Verpflichtungen des Kaufmanns, die Auswirkungen auf Outsourcing-Projekte haben:
  - die Beachtung der Grundsätze ordnungsgemäßer Buchführung (§ 239 Abs. 4 HGB) und
  - die Berücksichtigung der damit verbundenen Anforderungen an die Sicherheit IT-gestützter Rechnungslegung,
  - die Nachvollziehbarkeit der Buchführungs- bzw. Rechnungslegungsverfahren (§ 238 Abs. 1 Satz 2 HGB),
  - die Nachvollziehbarkeit der Abbildung der einzelnen Geschäftsvorfälle in ihrer Entstehung und Abwicklung (§ 238 Abs. 1 Satz 3 HGB),
  - die Einhaltung der Aufbewahrungsvorschriften (§ 239 Abs. 4, § 257 HGB).

# Aktien-Gesetz (AktG)

- In Rahmen des obligatorischen Risikomanagements ist die Richtigkeit der Buchführung sicherzustellen.
- Zudem muss das Risikomanagement alle outgesourcten Dienstleistungen beinhalten.
  
- § 91 AktG (Buchführungspflicht)
- § 93 AktG (Sorgfaltspflicht und Verantwortlichkeit der Vorstandsmitglieder)
- § 116 AktG (Sorgfaltspflicht und Verantwortlichkeit der Aufsichtsratsmitglieder)
- § 161 (Erklärung zum Corporate Governance Kodex)

# GmbH-Gesetz (GmbHG)

- Insbesondere stellt das GmbHG Anforderungen an die Sorgfaltspflicht des Geschäftsführers.
  - Besondere Relevanz bei Outsourcing der Buchführung.
  - Die Geschäftsführung muss die ordnungsgemäße Buchführung beim Outsourcing-Nehmer sicherstellen und kontrollieren.
- 
- § 41 GmbHG (Buchführung)
  - § 43 GmbHG (Haftung der Geschäftsführer)

# Bilanzierungsmodernisierungsgesetz (BilMoG)

- Das BilMoG dient der Aktionärssicherheit sowie der unabhängigen Rechnungs- und Abschlussprüfung von „Unternehmen bestimmter Rechtsformen“ (insbesondere in den öffentlich gehandelten Aktiengesellschaften).
- EuroSOX ist eine Umschreibung für Richtlinien der Europäischen Kommission, die an die US-amerikanische SOX-Gesetzgebung angelehnt sind.
- Die Anforderungen aus EuroSOX sind in den Regelungen des BilMoG Anfang 2009 in deutsches Recht transformiert worden.

# Abgabenordnung (AO)

- Die Abgabenordnung regelt grundlegend für alle Steuerarten das Besteuerungsverfahren.
  - Im Zusammenhang mit der AO sind die Grundsätze zum Datenzugriff und zur Prüfbarkeit digitaler Unterlagen (GDPdU) zu sehen.
  - Es muss sichergestellt sein, dass im Rahmen der Betriebsprüfung die betriebswirtschaftlichen Daten vom Prüfer bzw. der speziellen Prüfungs-Software erfasst werden können.
  - Zu beachten sind ferner die Grundsätze ordnungsgemäßer DV-gestützter Buchführungssysteme (GoBs)
- 
- § 140 AO (Buchführungs- und Aufzeichnungspflichten)
  - § 146 AO (Ordnungsvorschriften für die Buchführung und Aufzeichnungen)
  - § 147 AO (Ordnungsvorschriften für die Aufbewahrung von Unterlagen)
  - § 193 AO (Rechtsgrundlage für die steuerliche Außenprüfung)
  - § 200 AO (Mitwirkungspflichten des Steuerpflichtigen)

# Bundesdatenschutzgesetz (BDSG)

- Die Anwendbarkeit des BDSG hat mitunter großen Einfluss auf die Ausgestaltung von Service-Level-Agreements (SLA) und der Umsetzung des Outsourcing-Vorhabens.
- Sofern personenbezogene Daten betroffen sind, sind insbesondere folgende Normen von Relevanz:
  - § 9 BDSG und Anlage zu § 9 BDSG
  - § 11 BDSG (Auftragsdatenverarbeitung)

# Sonstige Datenschutzgesetze

- Landesdatenschutzgesetze (LDSG)  
Entsprechend dem BDSG sind datenschutzrechtliche Normen auch beim Outsourcing im öffentlich-rechtlichen Sektor zu beachten.
- Ferner können Spezialgesetze in Anhängigkeit des Outsourcing-Vorhabens Anwendung finden, wie bspw.
  - Telekommunikationsgesetz (TKG)
  - Telemediengesetz (TMG)

# Strafgesetzbuch (StGB)

- Das Strafgesetzbuch enthält keine expliziten Regelungen zum Outsourcing.
- In Verbindung mit dem Bundesdatenschutzgesetz sind jedoch im Licht des Datenschutzes insbesondere folgende Regelungen zu beachten:
  - § 202a StGB (Ausspähen von Daten)
  - § 202b StGB (Abfangen von Daten)
  - § 203 StGB (Verletzung von Privatgeheimnissen)
  - § 206 StGB (Verletzung des Post- und Fernmeldegeheimnisses)

# Kreditwesengesetz (KWG)

- Das KWG gilt für Kreditinstitute und Finanzdienstleistungsinstitute.
- Das Gesetz dient der Sicherung und Erhaltung der Funktionsfähigkeit der Kreditwirtschaft sowie dem Schutz der Gläubiger von Kreditinstituten vor Verlust ihrer Einlagen.
  
- Relevant ist § 25a KWG (Besondere organisatorische Pflichten von Instituten).
- Konkretisiert werden die Anforderungen aus § 25a KWG in den MaRisk.

# Versicherungsaufsichtsgesetz (VAG)

- Das VAG enthält Regelungen zur Ausgestaltung eines Risikomanagementsystems.
- Die IT ist als Teil des umfassenden Risikomanagementsystems anzusehen.
- Das Risikomanagement muss alle Risiken eines Outsourcing-Vorhabens nach § 64a VAG umfassen.
- Die Anforderungen des § 64a VAG werden seit Anfang 2009 in den MaRisk VA konkretisiert.

# Anforderungen an das Risikomanagement

- Mindestanforderungen an das Risikomanagement (MaRisk)
  - Die MaRisk sind die verbindliche Vorgabe der Bundesanstalt für Finanzdienstleistungsaufsicht (BaFin) für die Ausgestaltung des Risikomanagements in deutschen Kreditinstituten.
  - In den MaRisk hat die BaFin als Aufsichtsbehörde die Anforderungen des § 25a KWG konkretisiert. Die MaRisk sind also nur anwendbar, wenn die Anwendbarkeit des [§ 25a KWG](#) eröffnet ist.
- Mindestanforderungen an das Risikomanagement in der Versicherungsbranche (MaRisk VA)
  - Die MaRisk VA sind ebenfalls verbindliche Vorgaben der BaFin für die Ausgestaltung eines internen Kontrollsystems bei Versicherungsunternehmen.
  - Im Rahmen des Risikomanagements ist die Einhaltung einschlägiger rechtlicher Anforderungen sicherzustellen.

# Gesetz über den Wertpapierhandel (WpHG)

- Das WpHG reguliert in Deutschland den Wertpapierhandel und dient insbesondere der Kontrolle von Dienstleistungsunternehmen, die Wertpapiere handeln, sowie Finanztermingeschäften, aber auch dem Schutz des Kunden.
- § 33 WpHG (Organisationspflichten) in Verbindung mit § 25a KWG (Besondere organisatorische Pflichten von Instituten).

# Sarbanes-Oxley-Act (SOX)

- SOX ist ein US-Bundesgesetz zur verbindlichen Regelung der Unternehmensberichterstattung.
- SOX definiert Regelungen zur Implementierung und Evaluierung eines Internen Kontrollsystems (IKS), um die Ordnungsmäßigkeit der Finanzberichterstattung sicherzustellen.
- Um den strengen Anforderungen gerecht zu werden, ist in Verträgen mit Outsourcing-Anbietern zu regeln, dass auch diese im Rahmen der Leistungserbringung die einschlägigen Anforderungen von SOX einhalten.
- Insbesondere sollten auch bei der Auslagerung von IT-Leistungen die Einhaltung der Sicherheit und die Effektivität des internen Kontrollsystems des auslagernden Unternehmens gewährleistet bleiben.
- Ziel: Gewährleistung des Vertrauens der Anleger in die Richtigkeit und Verlässlichkeit der veröffentlichten Finanzdaten von Unternehmen.

# Standards des Instituts der Wirtschaftsprüfer (IDW)

- Das Institut der Wirtschaftsprüfer entwickelt Standards, die den Wirtschaftsprüfern als Werkzeug für ihre Prüfungstätigkeit dienen sollen.
- Ausgewählte Standards konkretisieren die aus den §§ 238, 239 und 257 HGB resultierenden Anforderungen an die Führung der Handelsbücher mittels IT-gestützter Systeme.
- Es wird zugleich versucht, die beim Einsatz von IT möglichen Risiken für die Einhaltung der Grundsätze ordnungsmäßiger Buchführung zu verdeutlichen.
- Die Standards beziehen sich in Teilen auch auf ausgelagerte IT-Prozesse, sofern diese rechnungslegungsrelevant sind.
- Relevante Standards: IDW PS 330, IDW PS 951, FAIT 1

Workshop

# Praktisches Beispiel

# Ausgangslage und Fragestellung

- Bank lagert E-Maildienst aus
- E-Maildienst wird genutzt für Bank-interne Kommunikation, aber auch als Schnittstelle zu Lieferanten, Partnern, Aufsichtsbehörden, Kunden und der Öffentlichkeit (z. B. Bewerbern)
- IT-Dienstleister hat ISO 9001-Zertifikat
  
- Welche wesentlichen Anforderungen greifen?
- Wie setzen wir diese um?

# Welche Fragen haben Sie?

# Vielen Dank für Ihre Aufmerksamkeit.

Haiko Ferber  
hferber@persicon.com

Knud Brandis  
kbrandis@persicon.com

[www.persicon.com](http://www.persicon.com)