Dr. Lars Lensdorf, Heymann & Partner Rechtsanwälte mbB

„Aufsichtsrechtliche Anforderungen an Auslagerungen im Banken- und Finanzsektor“

Sitzung des DGRI FA Outsourcing, 27. November 2015

Taunusanlage 1
D-60329 Frankfurt am Main
www.heylaw.de

heymann

I. Überblick

- **Aufsichtsrechtliche Rahmenbedingungen für Auslagerungen – Überblick**
- **Aufsichtsrechtliche Rahmenbedingungen in der Praxis**
  - Abgrenzung wesentliche / nicht-wesentliche Auslagerung / sonstiger Fremdbezug
  - MaRisk AT 9 und Innovationen
  - IT-Sicherheit
  - Anstehende MaRisk Novellierung
- **Exkurs: IT-Sicherheitsgesetz**
- **Fazit/Ausblick**

II. Aufsichtsrechtliche Rahmenbedingungen - Überblick

- **Zahlreiche Normen - unterschiedliche rechtliche Qualifikation/Bindungswirkung**
- **Gesetzliche Regelungen**
  - §§ 25a Abs. 1, 25b KWG
  - § 33 WpHG
  - §§ 29, 36 KAGB
  - § 64a VAG
  - Rechtswirkung: unmittelbar
- **Verlautbarungen/Rundschreiben der BaFin**
  - Rundschreiben 10/2012 Mindestanforderungen für das Risikomanagement (MaRisk)
  - Rundschreiben 5/2010 Mindestanforderungen an das Risikomanagement für Investmentgesellschaften/Kapitalanlagegesellschaften (InvMaRisk)
  - Rundschreiben 3/2009 (VA) Mindestanforderungen an das Risikomanagement für Versicherungsunternehmen
  - Rechtswirkung: mittelbar

II. Aufsichtsrechtliche Rahmenbedingungen - Überblick

- **Technische/fachliche Standards**
  - International Organization for Standardization (ISO)
    - ISO 2700x: IT-Sicherheitsverfahren – Informationssicherheits-Managementsysteme - IT-Riskmanagement
  - Bundesamt für Sicherheit in der Informationstechnik (BSI)
    - BSI-Standard 100-1 bis 100-3
    - BSI IT-Grundschutzkataloge
  - Prozess-Standards
    - IT Infrastructure Library (ITIL)
    - Control Objectives for Information and Related Technology (COBIT)
  - Rechtswirkung: mittelbar
    - Gesetzliche Verhaltenspflichten (Sorgfaltsmaßstab), z. B. § 25a Abs. 1 KWG, § 43 GmbHG, § 93 Abs. 1 AktG
    - Verlautbarungen/Rundschreiben der BaFin: z. B. AT 7.2 MaRisk: „... *ist bei der Ausgestaltung der IT-Systeme und der zugehörigen IT-Prozesse grds. auf gängige Standards abzustellen*."

III. Aufsichtsrechtliche Rahmenbedingungen in der Praxis

- **Rückblick**
  - 1997: § 25a II KWG
  - BaKred-Rundschreiben 11/2001
    - Umfangreiches Schreiben (9 Seiten) zu Rahmenbedingungen und Voraussetzungen bei Auslagerungen
    - Flankiert durch Anzeigeverpflichtung nach § 20 AnzVO
  - 2007: Integration Auslagerungsvorgaben in MaRisk

„...Ziel der Modernisierung der Outsourcing-Regelungen war die Entwicklung praxisnaher Anforderungen, die nahtlos an den prinzipienorientierten Ansatz der MaRisk anknüpfen und damit zugleich die Grundlagen für eine risikoorientierte Aufsichts- und Prüfungspraxis legen. Detailregelungen und Festschreibungen wurden beseitigt; an deren Stelle treten Öffnungsklauseln, die den Instituten mehr Gestaltungsspielräume für primär betriebswirtschaftlich getriebene Umsetzungslösungen einräumen...“

III. Aufsichtsrechtliche Anforderungen in der Praxis

- **Gegenwart**
  - Der 2007 angekündigte Paradigmenwechsel geht ins Leere, das Gegenteil ist eingetreten.

  - **These:**

    „Unsicherheit hinsichtlich der konkreten Anforderungen, zunehmende Regulierungs- sowie Prüfungspraxis der Aufsicht führen bei Auslagerungen im Hinblick auf die Ausnutzung von Gestaltungsspielräumen und primär betriebswirtschaftlich getriebenen Umsetzungslösungen vielfach zu Einschränkungen auf Seiten der Institute.“

III. Beispiel 1: Abgrenzung (nicht-)wesentliche Auslagerung/Fremdbezug

- **Ob (nicht-)wesentliche Auslagerung, Fremdbezug zunehmend schwierig**
- **Vorliegen einer Auslagerung**
  - Bedeutung: Entscheidend für anwendbare rechtliche Rahmenbedingungen (§ 25b, MaRisk AT 9, insbes. Regelungskatalog RN 6 vs. 25a Abs. 1 KWG) – so die Theorie
  - Auslagerung (MaRisk AT 9 Nr. 1):

    „Eine Auslagerung liegt vor, wenn ein anderes Unternehmen mit der Wahrnehmung solcher Aktivitäten und Prozesse im Zusammenhang mit der Durchführung von Bankgeschäften, Finanzdienstleistungen oder sonstigen institutstypischen Dienstleistungen beauftragt wird, die ansonsten vom Institut selbst erbracht würden.“
  - Regelbeispiele fehlen; Erläuterungen zur MaRisk (Anlage 1) bedingt hilfreich
  - Kriterien (Abgrenzung zum Fremdbezug):
    - Nicht nur einmaliger, gelegentlicher Fremdbezug (Nachhaltigkeit)
    - Funktionaler Zusammenhang
    - Keine allgemeine Service-/Unterstützungsleistungen

III. Beispiel 1: Abgrenzung (nicht-)wesentliche Auslagerung/Fremdbezug

- Abgrenzung wesentliche / nicht-wesentliche Auslagerung: Risikoanalyse
  - *„Das Institut muss auf der Grundlage einer Risikoanalyse eigenverantwortlich festlegen, welche Auslagerungen von Aktivitäten und Prozessen unter Risikogesichtspunkten wesentlich sind (wesentliche Auslagerungen).“ (MaRisk AT 9 Nr. 2)*
- Risikoanalyse:
  - Ausprägung, Tiefe, Methodik liegen im Ermessen des jeweiligen Instituts
  - Maßgebliche Organisationsbereiche sind zu beteiligen (Fachbereich / Risikomanagement / Recht / Interne Revision)
  - **Auch hier:** Regelbeispiele Fehlanzeige, obwohl Abgrenzung im Einzelfall schwierig (anders noch BaKred-Rundschreiben 11/2001 Tz. 11)

III. Beispiel 1: Abgrenzung (nicht)-wesentliche Auslagerung/Fremdbezug

- **Beispiele:**
  - Housing, Wachschutz, Wartung technischer Geräte (auch EDV)
- **Konsequenz:**
  - Zunehmende Unsicherheit
  - Devise „sicher ist sicher“: Einordnung als wesentliche Auslagerung(?)
  - Einordnung als nicht-wesentliche Auslagerung, aber gleichwohl vertragliche Abbildung der Anforderungen nach MaRisk AT 9 RN 6 (zumindest Versuch)
- **Ferner: Geltung von zentralen Bestimmungen der MaRisk unabhängig von Wesentlichkeit(!)**
  - Angemessene tech.-org. Ausstattung (§ 25a Abs. 1 Nr. 4 KWG, MaRisk AT 7.2)
  - Angemessenes Notfallkonzept (§ 25 a Abs. 1 Nr. 5 KWG, MaRisk AT 7.3)
  - Vorgaben zur Organisation und Dokumentation (MaRisk AT 5, 6)
  - Analyse bei wesentlichen Änderungen betrieblicher Prozesse, Strukturen, IT-Systemen (MaRisk AT 8.2)

heymann

IV. Beispiel 2: MaRisk AT 9 und Innovationen

- **MaRisk AT 9 RN 6 enthält umfassenden Regelungskatalog**
- **Problem: Anforderungskatalog MaRisk AT 9 RN 6 und standardisierte, shared services (Beispiel: cloud services)**
- **BaFin, Jahrestagung 2015 IT-Aufsicht: § 25b KWG, MaRisk AT 9 auch für cloud**
- **MaRisk AT 9 RN 6 b.: Festlegung von Informations- und Prüfungsrechten**
  - Allein Vorlage von Zertifizierungen/Zertifikaten durch Outsourcer nicht ausreichend => Prüfungs- und Kontrollrechte zwingend
  - Lösung in Praxis: Grundsätzliche Begrenzung auf x-mal jährlich; darüber anlassbezogen und gegen gesonderte Vergütung(?)
- **MaRisk AT 9 RN 6 d.: Weisungsrechte**
  - Rundschreiben 11/2001 RN 30: Weisungsrechte weitgehend zwingend.
  - MaRisk 10/2012 AT 9 RN 6 d.: „soweit erforderlich“.
  - Lösung in Praxis: schwierig; detaillierte Leistungsbeschreibung, Angebot vordefinierter, modularer Zusatzleistungen, ggf. Privilegierung von Mehrmandantendienstleistern

IV. Beispiel 2: MaRisk AT 9 und Innovationen

- **MaRisk AT 9 RN 6 g.: Möglichkeiten und Modalitäten einer Weiterverlagerung (Einsatz von Subunternehmern)**
  - Rundschreiben 11/2001 RN 32: ausdrücklich Zustimmungsvorbehalt.
  - Rundschreiben 10/2012: Zustimmungsvorbehalt nicht mehr ausdrücklich gefordert.
  - Zustimmungsvorbehalt unrealistisch
  - **Aber**: Institut muss in Möglichkeit haben, auf den Einsatz von Subunternehmern (re)agieren zu können
  - Ferner: Durchgriff des Instituts auf Subunternehmer(?)
  - Lösung in Praxis: Informationspflicht des Auslagerungsunternehmens und Kündigungsrecht des Instituts. Problem: Überleitung ggf. erst nach bereits erfolgtem Subunternehmereinsatz.

V. Beispiel 3: IT-Sicherheit

- **Bankgeschäft ist vor allem auch IT**
  - Zahlungsverkehr, Kreditvergabe, Online-/Mobile-Banking, Handelssysteme, Risikomanagement/Controlling, Meldewesen, etc.
- **Verstärkte Aktivitäten der BaFin bzgl. der IT-Sicherheit bei Banken**
  - 2013 Bildung Referat “IT-Infrastrukturen bei Banken“(BA 57)
  - Aufgaben: Definition von Anforderungen an die IT, Definition von Prüfungsvorgaben, Prüfungsbegleitung.
- **IT-Dienstleister unterfallen mittelbar den Anforderungen der BaFin**
- **Kernthemen**
  - Identifikation und Umgang mit IT-Risiken: Risikoanalyse => Schutzbedarf der jeweiligen Informationen und IT-Systeme muss definiert und mit umgesetzten Maßnahmen abgeglichen werden.
  - IT-Governance
    - IT-Strategie, basierend auf Geschäftsstrategie/-modell (MaRisk AT 4.2)
    - Steuerung IT-Organisation durch Geschäftsleitung (MaRisk AT 3, 4.3)

V. Beispiel 3: IT-Sicherheit

- **Kernthemen**
  - IT-Sicherheitsmanagement
    - Standards des BSI und der ISO
    - Beachte: IT-Prozesse und IT-Systeme müssen insgesamt betrachtet werden
  - IT-Betrieb
    - Einbindung des IT-Betriebs in das Kontrollsystem (MaRisk AT 4.3 Definition von Qualitätsparametern; Monitoring und Reporting)
    - Problem-/Störungsmanagement, Definition/Tests von Notfallkonzepten
  - Softwareentwicklung und -beschaffung
    - Regelprozess betreffend sorgfältige Planung (inkl. Anforderungserhebung, -analyse), Entwicklung, Prüfung und Implementierung
    - Beschaffung von Dritten: Anforderung an Vertragsgestaltung und Dokumentation von Tests und Abnahmen

- **Demnächst: Bankaufsichtliche Anforderungen an die IT (BAIT)**

VI. Beispiel 4: Novellierung MaRisk

- **Ankündigung für Sommer 2015**
- **Jetzt: Umsetzung in Form einer Verordnung**
  - Grundlage: „Single Resolution Mechanism (SRM)-Anpassungsgesetz“ (seit 6.11.2015 in Kraft)
  - Verordnungsermächtigung: § 25b Abs. 5 KWG
  - dann unmittelbare Rechtsverbindlichkeit => weniger Ermessensspielraum(?)
- **Outsourcing Studie BaFin 2013**
  - Notfallkonzepte, Exit-Strategien
  - Interne Überwachungs- und Steuerungsprozesse / Festlegung von Verantwortlichkeiten (Retained Organisation); Know-how!
  - Überwachung/Steuerung auch insgesamt; zentrales Auslagerungsmanagement (Klumpenrisiko)
  - Definition von Service Levels
  - Risikoprüfung; abhängig von Wesentlichkeit

VI. Beispiel 4: Novellierung MaRisk

§ 25b Abs. 5 MaRisk

Das Bundesministerium der Finanzen wird ermächtigt, durch Rechtsverordnung, die nicht der Zustimmung des Bundesrates bedarf, im Benehmen mit der Deutschen Bundesbank nähere Bestimmungen zu erlassen über

1.das Vorliegen einer Auslagerung,

2.die bei einer Auslagerung zu treffenden Vorkehrungen zur Vermeidung übermäßiger zusätzlicher Risiken,

3.die Grenzen der Auslagerbarkeit,

4.die Einbeziehung der ausgelagerten Aktivitäten und Prozesse in das Risikomanagement sowie

5.die Ausgestaltung der Auslagerungsverträge.

Das Bundesministerium der Finanzen kann die Ermächtigung durch Rechtsverordnung auf die Bundesanstalt mit der Maßgabe übertragen, dass die Rechtsverordnung im Einvernehmen mit der Deutschen Bundesbank ergeht. Vor Erlass der Rechtsverordnung sind die Spitzenverbände der Institute zu hören.

VI. Beispiel 4: Novellierung MaRisk

- **Wesentlicher Regelungsinhalt bzgl. Auslagerungen:**
  - Risikoanalyse nach instituts- bzw. gruppenübergreifend einheitlichen Kriterien; Risikokonzentrationen und Risiken aus Weiterverlagerungen sind zu beachten
  - Ein zentraler Beauftragter für das gesamte Auslagerungsmanagement
  - Höhere Maßstäbe bei Auslagerungen von Steuerungs- und Kontrollbereichen. Insbes. Prüfung, ob die vollständige Auslagerung noch der Ordnungsmäßigkeit der Geschäftsorganisation entspricht
  - Bei gruppeninterner Auslagerung sind ein Gruppenrisikomanagement und Durchgriffsrechte sicherzustellen
  - Für wesentliche Auslagerungen ist eine Ausstiegsstrategie festzulegen.
  - Dem auslagernden Institut sind Zustimmungsvorbehalte einzuräumen; dem Auslagerungsunternehmen sind Informationspflichten aufzuerlegen
  - Festlegung des Grads maximal akzeptierter Schlechtleistung mit Blick auf Kündigungsrechte

VII. Exkurs: IT-Sicherheitsgesetz

- **25.07.2015: Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme**
- **Artikelgesetz; zentrale Regelungen §§ 8a, 8b BSIG**
- **Pflicht von Betreibern besonders gefährdeter Infrastrukturen (KRITIS), ihre IT-Systeme besser vor Angriffen zu schützen**
  - Umsetzung von angemessenen organisatorischen und technischen Vorkehrungen zur Vermeidung von Störungen der Verfügbarkeit, Integrität, Authentizität und Vertraulichkeit von IT-Systemen, Komponenten und Prozesse (§ 8a Abs. 1, 2 BSIG)
  - Meldepflichten bei tatsächlichen oder möglichen Störungen (§ 8b Abs. 4 BSIG)
- **KRITIS (§ 2 Abs. 10 BSIG)**
  - Anlagen in den Sektoren Energie, Informationstechnik/Telekommunikation, Transport/Verkehr, Gesundheit, Wasser, Ernährung, **Finanz-/Versicherungswesen**
  - (Und)Von hoher Bedeutung für das Funktionieren des Gemeinwesens sind (Versorgungsengpässe, Gefährdungen für die öffentliche Sicherheit)

VII. IT-Sicherheitsgesetz

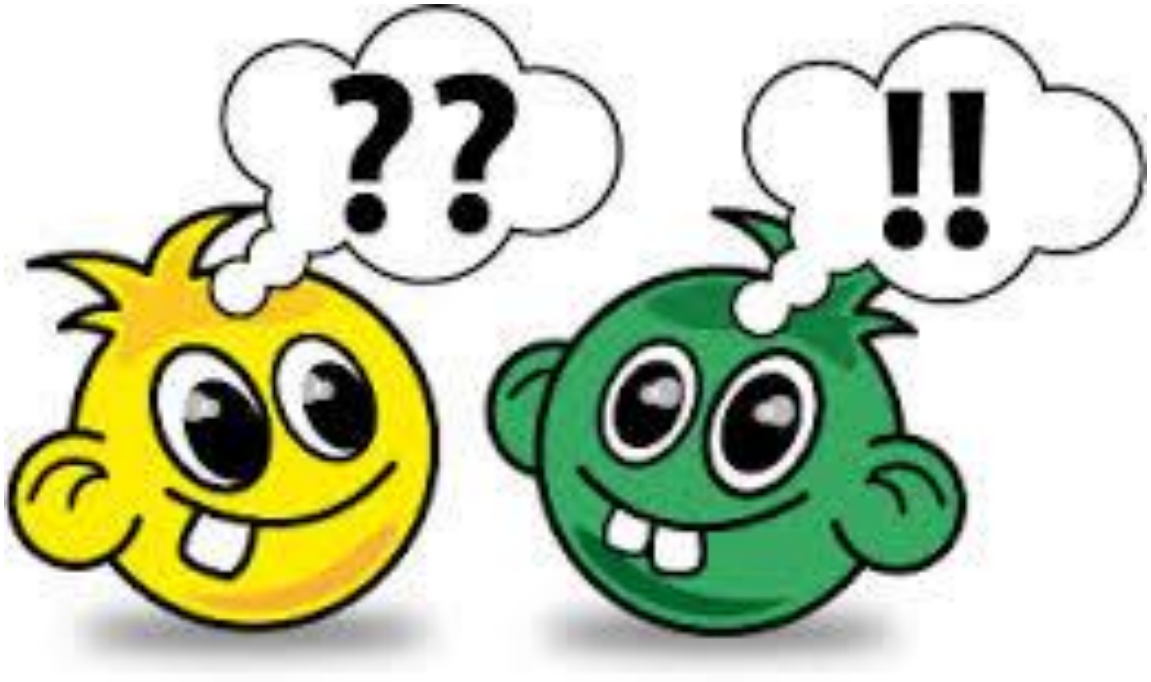
- **Betreiber von KRITIS: Bestimmung per Rechtsverordnung durch BMI (§§ 8a Abs. 1, 10 BSIG)**
  - wohl nur größere Institutionen (500 – 2000), Umsetzungszeitraum: 2 Jahre
- **Angemessene organisatorische und technische Vorkehrungen**
  - Spezifizierung durch Branchenstandards; Genehmigung BSI (§ 8a Abs. 2 BSIG)
  - Nachweis alle 2 Jahre (§ 8a Abs. 3 BSIG); Prüfungen, Zertifizierungen, Audits
- **Meldepflichten**
  - Namentlich nur dann, wenn tatsächlich Störung eingetreten (§ 8b Abs. 4 BSIG).
- **Auswirkungen auf Outsourcingverträge**
  - Umsetzung der jeweiligen organisatorischen und technischen Anforderungen
    - Monitoring der Anforderungen
    - Umsetzungskosten
    - divergierende Branchenstandards
  - Übertragung Meldepflicht (ähnlich § 42a BDSG bei ADV)

VIII. Fazit und Ausblick

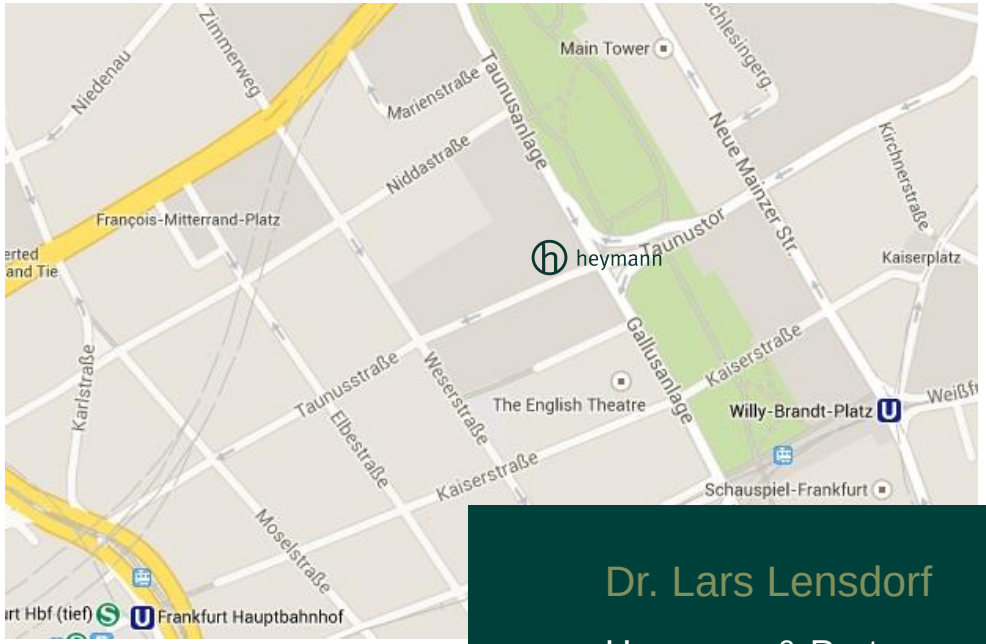
- **Entgegen dem 2007 angekündigten größeren Ermessen von Instituten bei Auslagerungen, werden seitens dem Gesetzgeber und der Aufsicht im zunehmenden Maße regulatorische Rahmenbedingungen gesetzt, die die Gestaltungsspielräume der Institute einschränken.**
- **Dies hat insbesondere Auswirkungen auf den Einsatz innovativer Techniken, wie bspw. cloud services.**
- **Erschwert wird die zunehmende Regulationsdichte zudem durch zahlreiche unkonkrete, allgemein gehaltene Vorgaben.**
- **Es bleibt zu hoffen, dass die MaRsik - wenn sie schon nicht zu einem Regulationsabbau beiträgt - ausreichenden Freiraum zum Einsatz innovativer Techniken sowie für die Institute hilfreiche Konkretisierungen beinhaltet.**
- **Weitere Anforderungen werden sich aus der Umsetzung des BSIG ergeben.**

heymann

Und zu guter letzt . . .



heymann



Dr. Lars Lensdorf

Heymann & Partner
Taunusanlage 1
D-60329 Frankfurt **am** Main
T: +49 (69) 768063-30
F: +49 (69) 768063-15
E: L.Lensdorf@heylaw.de

Simply good lawyers...