



Deutsche Stiftung für
Recht und Informatik

Der Wandel beim Outsourcing von IT-Leistungen im Bankensektor

Eva Ametsbichler

Witzel Erb Backu & Partner Rechtsanwälte mbB

Herbstakademie 2020

Gliederung:

I. Einleitung: Grundkonstellation

II. Hintergrund

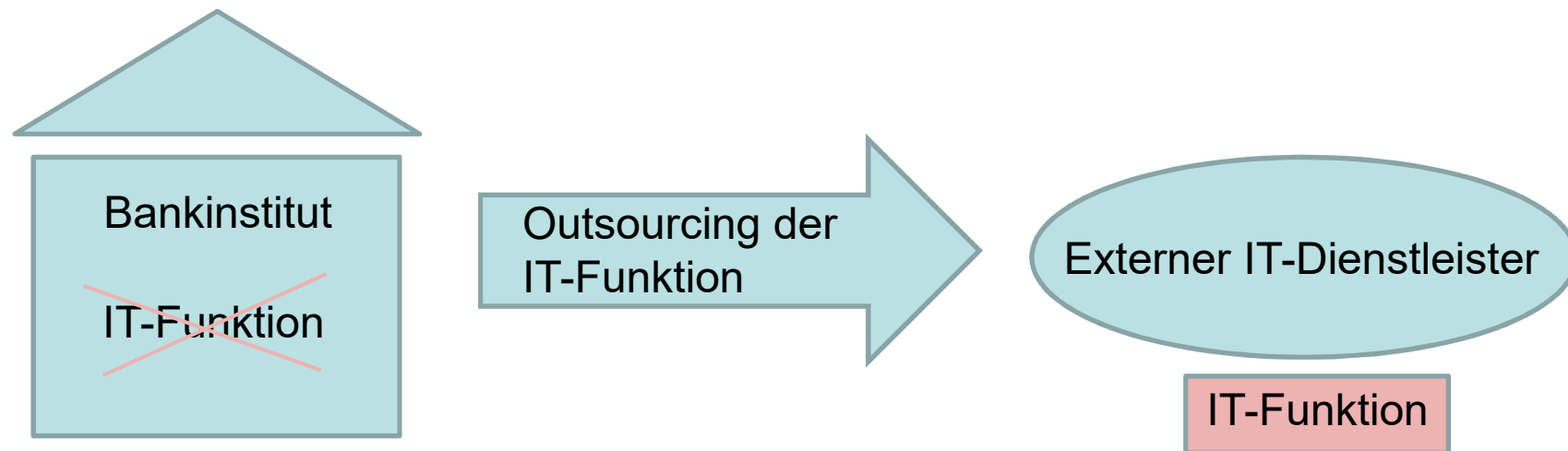
1. Interessenlage
2. Rechtliche Rahmenbedingungen

III. Der Wandel

1. Technischer Wandel
2. Wandel durch aktuelle Ereignisse

IV. Fazit und Ausblick

I. Einleitung: Grundkonstellation




- Aufgrund Digitalisierung und damit verbundener Innovationen immer mehr Nachfrage/ Angebote im Hinblick auf IT-Outsourcing im Bankensektor
- Prinzip der Auslagerung an sich einfach
- Nichtsdestotrotz komplexe Thematik, die staatliche Schutzinteressen tangiert

➡ **Staatlich stark regulierter Markt**



II. Hintergrund: Interessenlage (1)

Welche allgemeinen Interessen bestehen?

Bankinstitut:

- Steigerung der Wettbewerbsfähigkeit durch Fokussierung auf Kernkompetenzen
- Adressat der regulatorischen Vorgaben oftmals nur auslagernde Bank selbst
  Verpflichtung des externen Dienstleisters auf Einhaltung der Vorgaben
- Effizienzsteigerung
- Kostenersparnis

Staat:

- Bankensektor für deutsche Wirtschaft systemrelevant  starkes Regulierungsbedürfnis
- Bankinstitute zum Schutz von Wirtschaft und Verbrauchern zahlreichen Regelungen unterworfen  Gefahr der Entziehung durch Auslagerung
- Sicherstellung, dass trotz Auslagerung die Geschäftsleitung des auslagernden Instituts nicht ihre Letztverantwortlichkeit einbüßt

II. Hintergrund: Interessenlage (2)

IT-Dienstleister:

- Gewinnbringende Umsetzung ihres Geschäftsmodells am Markt
- Bankinstitute als sehr attraktiver Kundenkreis
- Meist dauerhafte Abhängigkeit aufgrund hoher Wechselkosten

Bankkunde:

- Kein Herabsenken des Schutzniveaus bzgl. personenbezogener Daten durch Auslagerung
- Aktueller Stand an IT-Dienstleistungen

II. Hintergrund: Rechtliche Rahmenbedingungen (1)

- **§ 25a und b KWG:** Allgemeine Regelungen zum Outsourcing im Bankensektor (gilt für sämtliche Auslagerungsformen)
- **§ 25b KWG:** Auslagerung von Aktivitäten und Prozessen durch Kredit- und Finanzdienstleistungsinstitute im Grundsatz zulässig
- **§ 25a Abs.1 KWG:** Verpflichtung der Institute zur *ordnungsgemäßen Geschäftsorganisation*
 - ➡ *Angemessenes und wirksames Risikomanagement*
 - ➡ Konkrete Umsetzung der Integration in das Risikomanagement wirft in Praxis häufig viele Fragen auf

II. Hintergrund: Rechtliche Rahmenbedingungen (2)

- **Veröffentlichung von Rundschreiben durch BaFin insb.:**
 - *Mindestanforderungen an das Risikomanagement (MaRisk)*
 - *Bankaufsichtliche Anforderungen an die IT (BAIT)*
 - ➔ Lediglich Auslegungsschreiben ohne Rechtsverbindlichkeit
Aber: Zentrale Rolle in der Praxis
- **Veröffentlichung von Leitlinien durch EBA insb.:**
 - *EBA-Leitlinien zu Auslagerungen (EBA/GL/2019/02)*
 - *Management von IKT- und Sicherheitsrisiken (EBA/GL/2019/04)*
- **BaFin-Merkblatt:** *Orientierungshilfe zu Auslagerungen an Cloud-Anbieter (Gilt auch für traditionelle IT-Auslagerungen)*
- **BaFin-Merkblatt:** *Merkblatt zum Umgang mit Nachhaltigkeitsrisiken*

II. Hintergrund: Rechtliche Rahmenbedingungen (3)

BaFin: Merkblatt zum Umgang mit Nachhaltigkeitsrisiken

- Keine neuen Kriterien, sondern Skizzierung von Good-Practice-Ansätzen
- Orientierungshilfe für beaufsichtigte Unternehmen bzgl. Nachhaltigkeitsrisiken

Definition „*Nachhaltigkeitsrisiken*“ im BaFin-Merkblatt:

„Nachhaltigkeitsrisiken im Sinne dieses Merkblatts sind Ereignisse oder Bedingungen aus den Bereichen Umwelt, Soziales oder Unternehmensführung (...), deren Eintreten tatsächlich oder potenziell negative Auswirkungen auf die Vermögens-, Finanz- und Ertragslage sowie auf die Reputation eines beaufsichtigten Unternehmens haben können.“

- Zudem Nennung von Beispielen u.a. mit konkretem Bezug zu IT-Funktionen von Bankinstituten: z.B. „*Gewährleistung des Datenschutzes*“
- Somit Nachhaltigkeitsthema auch im Bereich IT-Outsourcing im Bankensektor relevant
- Aber: Ausführungen im Merkblatt wenig konkret
- Dennoch: Beaufsichtigte Unternehmen sollten Nachhaltigkeitsrisiken im Rahmen des (IT-)Outsourcings nicht vernachlässigen
- Thema dürfte zukünftig immer mehr an Bedeutung gewinnen

II. Hintergrund: Rechtliche Rahmenbedingungen (4)

Fazit:

- Umfangreiche und stark auslegungsbedürftige, aufsichtsrechtliche Normen bzgl. (IT-)Outsourcing im Bankensektor
- Veröffentlichte Interpretationen der Aufsichtsinstiute trotz fehlendem Normcharakter als wichtige Hilfestellung für Praxis
- Dennoch keine ausreichende Beschreibung für konkrete Umsetzung des geforderten IT-Notfallmanagements



Banken sind in Praxis mit zunehmendem *Regulierungsdruck* sowie zahlreichen *Unsicherheiten bzgl. Umsetzung* konfrontiert

III. Der Wandel - Technischer Wandel (1)

Technischer Fortschritt bringt immer wieder neue, interessante Angebote der IT-Dienstleister für den Bankensektor hervor:

Steigerung der Nachfrage nach Cloud-Lösungen (z. B. SaaS, IaaS)

- **Vorteile:**

- **IT-Dienstleister:** z. B. kostengünstige, effiziente IT-Bereitstellung bei Bedarf (sog. on demand-Modelle)
- **Bankinstitute:** z. B. Kosteneinsparung, große Rechenkapazitäten, Software auf neuestem Stand, positive Skalierungseffekte

- **Potentielle Risiken:**

- Übliche IT-Risiken z. B. Cyberkriminalität
- Auslagerungsspezifisch z. B. „Vendor-Lock-Ins“
- Häufig Angebot aus EU-Ausland unter Nichtbeachtung des deutschen Regulierungsrechts (Problematisch bei großer Marktmacht des IT-Dienstleisters)

III. Der Wandel - Technischer Wandel (2)

Aufsichtsrechtliche Reaktion auf europäischer/ deutscher Ebene:

- **Dez 2017:** Veröffentlichung von EBA-Empfehlungen zum Thema IT-Outsourcing an Cloud-Anbieter (EBA/REC/2017/03)
- **Nov 2018:** BaFin/ Deutsche Bundesbank veröffentlichen Merkblatt *Orientierungshilfe zu Auslagerungen an Cloud-Anbieter*
 - Inhaltlich keine neuen Vorschriften
 - Wertvolle Einschätzungen zum Thema sowie zu bestimmten Vertragsklauseln
 - Ziel: Schaffung von Problembewusstsein

Fazit:

- Beispiel IT-Outsourcing an Cloud-Anbieter zeigt konkrete Beeinflussung des deutschen/europäischen Aufsichtsrechts durch technischen Wandel im IT-Bereich
- Blick auf zukünftige technische Innovationen: Vorhandensein eines entspr. Problembewusstseins aller am Outsourcing Beteiligten maßgeblich

III. Der Wandel – Aktuelle Ereignisse (1)

Seit Anfang 2020 SARS-CoV-2-Pandemie („Corona-Krise“):

- In vielen Ländern z. T. massives Herunterfahren des privaten/ öffentlichen Lebens als Maßnahme zur Viruseindämmung; dadurch Krise v. a. in Bereichen Gesundheit, Wirtschaft und Soziales, (teilweise) bis heute
- Weltweit in kürzester Zeit immenser Anstieg an Home-Office-Tätigkeit

Erhebliche Risiken auch im Bereich IT-Outsourcing im Bankensektor:

- Zwang der IT-Dienstleister zur Umstellung auf Home-Office in kürzester Zeit, ggf. Belastungsgrenze für IT-Systeme überschritten; erhebliche Ausfallrisiken bei Auslagerung an IT-Dienstleister ohne entspr. Vorbereitung
- Oftmals Standort des jeweiligen IT-Dienstleisters maßgeblich (z. B. Internet-Infrastruktur in Schwellenländern/Datenschutz)
- Verstärkender Faktor bei weltweiter Krise, da ggf. sämtliche Standorte des IT-Dienstleisters betroffen

Reaktion der Aufsichtsbehörden:

- Maßnahmen auf zahlreiche Anfragen der beaufsichtigten Institute (z. B. Schaffung von Spielräumen bzgl. krisenbedingt aufgezwungener Home-Office-Situation ohne Geschäftsbetrieb der beaufsichtigten Institute zu gefährden)

III. Der Wandel – Aktuelle Ereignisse (2)

Risikolage im Bankensektor im Kontext Nachhaltigkeitsrisiken:

- Unterwartetes Auftreten der Corona-Krise
- Aber: Anknüpfungspunkt im Bereich IT-Outsourcing im Bankensektor für solche Szenarien grundsätzlich vorhanden: *Merkblatt zum Umgang mit Nachhaltigkeitsrisiken* der BaFin
- Auswirkungen der Corona-Krise dürften Einordnung als Nachhaltigkeitsrisiko zulassen; gilt umso mehr bzgl. durch Home-Office-Situation hervorgerufene datenschutzrechtliche Risiken = konkretes Beispiel im BaFin-Merkblatt
- Mittelbare Berührung der Beispiele *Arbeitssicherheit/Gesundheitsschutz*: Gestaltung der IT-Systeme der IT-Dienstleister so, dass kurzfristig umfassendes Arbeiten im Home-Office zum Schutz der Gesundheit der Mitarbeiter möglich

Corona-Pandemie als Test für IT-Notfallpläne:

- ➡ Bankinstitute sollten etwaigen Nachholbedarf prüfen: Wie leistungsfähig ist mein externer IT-Dienstleister im Notfall?
- ➡ Integration eindeutiger Regelungen im Vertrag

IV. Fazit und Ausblick

- IT-Outsourcing im Bankensektor aufgrund vielfältiger Beeinflussungsfaktoren sehr komplex
- Vollzug des Wandels in vielfältiger Form (z. B. technischer Fortschritt/ Ereignisse wie Corona-Krise)
- In kürzester Zeit enormer Bedeutungsgewinn von zuvor stiefmütterlich behandelten Aspekten möglich (z. B. Leistungsfähigkeit des externen IT-Dienstleisters während Pandemie)

Für Parteien des IT-Outsourcings daher besonders wichtig:

- Entwicklung eines Bewusstseins für Vielfältigkeit der Beeinflussungsfaktoren und damit verbundener Probleme
 - Deren sorgfältige Bearbeitung gerade bei Umsetzung des IT-Notfallmanagements
- Weitere Beschleunigung des Nachfrageanstiegs im Bereich IT-Outsourcing im Bankensektor durch Corona-Krise möglich
 - Auslagerungen an innovative IT-Angebote im Bereich *Künstliche Intelligenz* und *Automatisierungstechnik* (Krisenfestigkeit)

Vielen Dank für Ihre Aufmerksamkeit!

Bei Fragen oder Anmerkungen freue ich
mich über eine E-Mail an:

ametsbichler@web-partner.de