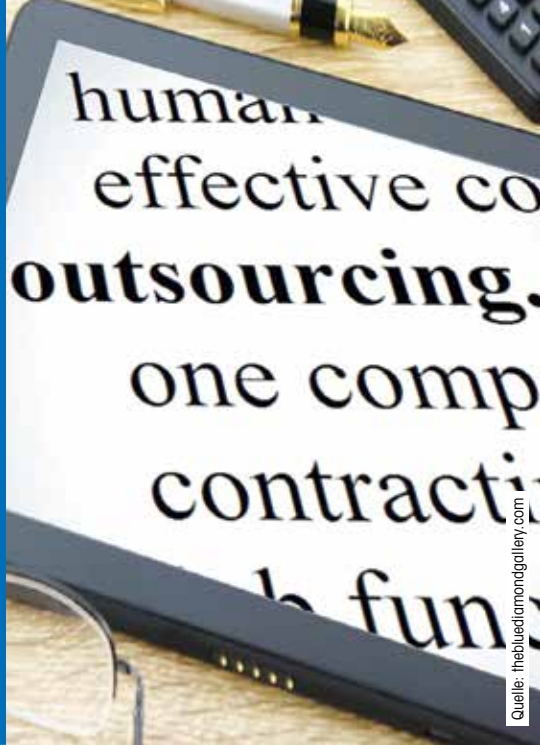
Kostenmanagement bei steigenden aufsichtlichen Anforderungen

Von Jens Christoph Hammersen
und Dr. Michael Weißgerber



Quelle: thebluediamondgallery.com

Im Zuge steigender aufsichtlicher Anforderungen sind Banken und Zahlungsdienstleister häufig versucht, solche Aufgaben an Dienstleister auszulagern und dabei pauschale Mustertexte zu verwenden. Von dieser kautelarjuristischen Praxis raten Jens Christoph Hammersen und Dr. Michael Weißgerber ausdrücklich ab. Weil es keine automatisch einsetzende „Verantwortungskaskade" gibt, führt die genannte Praxis häufig zu Kostensteigerungen, da die Dienstleister in der Regel die Kosten für die zusätzlichen Leistungen berechnen. Bei der Weiterverlagerung an Subdienstleister gibt es zudem aufsichtsrechtliche Bedenken. Red.

Nicht zuletzt als Folge der weltweiten Finanzkrise und der stark zunehmenden IT-Kriminalität werden von unterschiedlichen Aufsichtsbehörden immer mehr und immer strengere Anforderungen an Institute im Sinne von § 1 Abs. 1b KWG oder § 1 Abs. 3 ZAG gestellt. Neben die rein bankaufsichtsrechtlichen Anforderungen, die insbesondere das Risikomanagement betreffen (zum Beispiel „Mindestanforderungen an das Risikomanagement – MaRisk", Rundschreiben 09/2017 (BA) vom 27. Oktober 2017), treten auch strengere Anforderungen an den Datenschutz und die IT-Sicherheit (zum Beispiel „Bankaufsichtliche Anforderungen an die IT – BAIT", Rundschreiben 10/2017 (BA) vom 03. November 2017; BSI-Gesetz (BSIG) in Verbindung mit der „Verordnung zur Bestimmung Kritischer Infrastrukturen nach dem BSI-Gesetz" (BSI-KritisV)).

Die dadurch eintretende Verdichtung aufsichtlich geforderter Maßnahmen bei Instituten ist beachtlich und führt bei diesen zu erheblichen Kosten- und Ressourcenlasten.

Es ist nachvollziehbar, dass die Institute dem zunehmenden regulatorischen Umsetzungsdruck dadurch begegnen, möglichst viele dieser aufsichtlichen Anforderungen ungefiltert auf Dienstleister, zum Beispiel für IT-Systeme, Callcenter und Back-Office-Services, auszulagern. Dabei findet sich oft das Begründungsmodell, dass sich der Dienstleister zur Erbringung einer Dienstleistung verpflichtet hat, von der das Institut erwarten könne, dass sie gemäß den gesetzlichen und behördlichen Bestimmungen erbracht werde. Es sei daher auch Aufgabe des Dienstleisters, dafür zu sorgen, dass die zugesagten Leistungen den vorgenannten Vorschriften, zum Beispiel der MaRisk, BAIT, BSIG und BSI-KritisV entsprechen.

Zu den Autoren

Jens Christoph Hammersen und **Dr. Michael Weißgerber**, Hammersens Rechtsanwälte, München

Diese Haltung von Instituten findet sehr oft ihre kautelarjuristische Ausprägung in Vertragsklauseln, die von institutsinternen oder -externen Aufsichtsrechtlern als allgemeine Vertragsbedingung für alle Dienstleister ausgearbeitet und gegebenenfalls mit den Aufsichtsbehörden abgestimmt wurden. Diese werden dann in der Regel jedem Dienstleister durch das Institut auferlegt, ohne im Einzelfall zu prüfen, ob es überhaupt notwendig ist, dem Dienstleister die aufsichtlichen Anforderungen aufzuerlegen.

Kautelarjuristische Praxis hinterfragen

Daneben wird oft auch das Prinzip verfolgt, die Vertragsbestimmungen so zu fassen, dass zum einen möglichst viele aufsichtliche Belastungen des Instituts (zum Beispiel Risikobewertung der Auslagerung, Aggregation von Daten zur Risikobewertung) auf den Dienstleister übertragen werden und zum anderen die Bestimmungen so gefasst sind, dass für das Institut die bestmögliche Risikobewertung zu der Auslagerung erreicht wird. Dies geht zwangsläufig mit einem erheblich gesteigerten Leistungsrisiko des Dienstleisters einher.

Dem Leser mag sich an dieser Stelle nun der Eindruck aufdrängen, dass dieser Beitrag in einem glühenden Plädoyer zum Schutz der Dienstleister vor der aufsichtlichen Gängelung durch die marktmächtige-

Dieser Artikel ist urheberrechtlich geschützt. Die rechtliche Freigabe ist für den Abonnenten oder Erwerber ausschließlich zur eigenen Verwendung.
Fritz Knapp Verlag GmbH

ren Institute enden könnte. Tatsächlich ist dies aber nicht die Intension der Autoren. Vielmehr soll dieser Beitrag leisten, dass Institute die geschilderte kautelarjuristische Praxis, nicht zuletzt aus eigenem betriebswirtschaftlichem Interesse, hinterfragen.

Auslagerung aufsichtlicher Anforderungen erhöht die Kosten

Die „Auslagerung" von aufsichtlichen Anforderungen auf den Dienstleister, sozusagen als Annex zu der von ihm erbrachten Dienstleistung, und die Begründung eines erheblichen Leistungsrisikos beim Dienstleister führen in der ganz überwiegenden Zahl der Fälle auch zu höheren Dienstleistungsentgelten, die das Institut im Ergebnis entrichten muss. Es steht zu bezweifeln, dass es einem Institut gelingt, die durch die Steigerung der aufsichtlichen Anforderungen entstehenden Zusatzleistungen vom Dienstleister auf Dauer kostenfrei zu erhalten.

In diese Gemengelage fließt ein, dass – zum Teil ungewollt – aufsichtliche Anforderungen nur kraft vertraglicher Vereinbarung, die ein Institut dem Dienstleister auferlegt, übernommen werden: So kann es zum Beispiel sein, dass das Institut aufgrund des von ihm eingesetzten Kernbankensystems als Betreiber kritischer Infrastruktur im Sinne von § 8 a Abs. 1 BSIG in Verbindung mit § 7 BSI-KritisV anzusehen ist. Der Dienstleister, der lediglich Back-Office-Services in der Kundenbetreuung durchführt, wird hingegen in der Regel keine eigene kritische IT-Infrastruktur einsetzen. Alleine aus dem Umstand, dass das Institut den gesteigerten Anforderungen an die IT-Sicherheit aufgrund seiner kritischen IT-Infrastruktur unterliegt, lässt sich nicht ableiten, dass auch dieser Dienstleister Adressat dieser Vorschrift ist.

Keine automatische Verantwortungskaskade

Eine derartige, bei jeder Auslagerung automatisch einsetzende Verantwortungskaskade lässt sich weder dem BSIG noch anderen aufsichtlichen Bestimmungen entnehmen. Soll der Dienstleister nun die gesteigerten Anforderungen an die IT-Sicherheit mit der von ihm eingesetzten, nicht kritischen IT beachten, wird er umso mehr bestrebt sein, einen etwaigen dadurch entstehenden, zusätzlichen Aufwand vergütet zu bekommen. Schließlich liegt die Ursache für den zusätzlichen Aufwand in der Sphäre des Instituts, nicht aber in der des Dienstleisters begründet.

Gleichzeitig besteht in diesem Beispiel aber auch für das Institut keine Notwendigkeit, die Anforderungen, welche für das Kernbankensystem gelten, auf eine nicht sicherheitsrelevante IT des Dienstleisters auszuweiten. Es macht daher in diesem Fall Sinn, dass das Institut Vertragsbedingungen bereithält, welche den geringeren IT-Sicherheitsanforderungen für diesen Dienstleister Rechnung tragen. Dadurch kann auch das Institut unnötigen Aufwand für Dienstleistungsentgelte einsparen.

Ein weiteres Beispiel ist das Bestreben eines Instituts, Teile des Risikomanagements, zu dem es aufgrund der Bestimmungen der MaRisk als Institut im Sinne von § 1 Abs. 1b KWG verpflichtet ist, auf den Dienstleister auszulagern. Wenn der Dienstleister selbst kein Institut im Sinne von § 1 Abs. 1 b KWG oder § 1 Abs. 3 ZAG ist, entfalten für ihn die Bestimmung der MaRisk auch keine unmittelbare Geltung. Die auf den MaRisk beruhenden Anforderungen des Instituts sind aus Sicht des Dienstleisters damit zusätzliche Leistungen neben der eigentlichen Dienstleistung, für die er zu Recht eine Vergütung verlangen wird.

Die Praxis zeigt, dass Institute ihre Dienstleister zum Beispiel verpflichten, für Leistungen, zu deren Erbringung sich der Dienstleister eines Subdienstleisters bedient, zu prüfen, ob es sich bei dieser Unterbeauftragung um eine wesentliche Auslagerung im Sinne von AT 9 Ziff. 2 MaRisk handelt und eine entsprechende Risikoanalyse zu erstellen.

Subdienstleister: Risikoanalyse muss bei der Bank verbleiben

Dieses Vorgehen ist aus mehreren Gründen zu hinterfragen:

- So ist die Prüfung, ob eine „wesentliche Auslagerung" im Sinne von AT 9 Ziff. 2 MaRisk vorliegt, für die Auslagerung des Instituts auf einen Dienstleister sicherlich notwendig. Die Prüfung, ob die vom Dienstleister weiterverlagerte (Teil-) Leistung wiederum eine wesentliche Auslagerung für das Institut oder den Dienstleister darstellt, ist für das Institut hingegen entbehrlich. Den Umstand, dass weiterverlagert wird und in welchem Umfang dies geschieht, hat das Institut (lediglich) im Rahmen seiner eigenen Risikoanalyse zur Auslagerung zu berücksichtigen.

- Auch der Dienstleister muss die Frage, ob die Weiterverlagerung einer (Teil-) Leistung als „wesentlich" einzustufen ist, nur beantworten, wenn er selbst ein Institut im Sinne von § 1 KWG oder § 1 ZAG ist. In diesem Fall ist er aber bereits selbst Normenadressat und wird diese Prüfung schon aufgrund eigener Verpflichtung durchführen. Für alle anderen Dienstleister ist diese rein bankaufsichtsrechtliche Prüfung entbehrlich. Sie müssen lediglich sicherstellen, dass sie die Vorgaben des Instituts, zu deren Erfüllung sie sich gegenüber dem Institut verpflichtet haben, auch an den Subdienstleister durchreichen – unabhängig davon, welche unternehmerische Bedeutung dessen Beauftragung für sie selbst hat.

In Bezug auf die Übertragung der Risikoanalyse für die Weiterverlagerung auf den Dienstleister bestehen zudem erhebliche aufsichtsrechtliche Bedenken. Es entspricht keinem ordnungsgemäßen Risikomanagement des Instituts durch den externen Dienstleister beurteilen zu lassen, welches Risiko die Weiterverlagerung

Dieser Artikel ist urheberrechtlich geschützt. Die rechtliche Freigabe ist für den Abonnenten oder Erwerber ausschließlich zur eigenen Verwendung.
Fritz Knapp Verlag GmbH

mit sich bringt. Der externe Dienstleister müsste dazu Einblick in die konkreten Geschäftsprozesse und Bücher des Instituts haben und wissen, wie die Auslagerung auf ihn vom Institut beurteilt wurde.

Selbsteinschätzung des Dienstleisters taugt nicht als Vergleichsmaßstab

Insbesondere stellt sich die Frage, wie der Dienstleister aus der Sicht des Instituts, objektiv die Eignung seines Subdienstleisters innerhalb der Risikoanalyse beurteilen soll. Der Dienstleister wird dabei stets seine eigene Eignung als gut/angemessen erachten und davon seine Beurteilung des Subdienstleisters ableiten.

Die Selbsteinschätzung des Dienstleisters als Vergleichsmaßstab für die Beurteilung des Subdienstleisters ist dabei für das Institut wenig aussagekräftig. Diese Einschätzung kann letztlich nur das Institut vornehmen, da es bereits die Eignung des Dienstleisters bewertet hat. Das Institut wird daher nicht umhin kommen, die Risikoanalyse selbst vorzunehmen.

Auslagerung oder Fremdbezug von Leistungen?

Zum anderen macht diese Übertragung des Risikomanagements zur Auslagerung nur dann für das Institut Sinn, wenn überhaupt eine Auslagerung im Sinne von AT 9 Ziff. 1 MaRisk und kein sonstiger Fremdbezug von Leistungen vorliegt. Als sonstiger Fremdbezug zählt insbesondere der einmalige oder gelegentliche Fremdbezug von Gütern und Dienstleistungen.

Ausdrücklich genannt wird nun auch der isolierte Bezug von Software sowie die Anpassung der Software, die entwicklungstechnische Umsetzung von Änderungswünschen, Test und Freigabe der Software und die Software-Wartung, wenn die Software nicht dem Risikomanagement dient und nicht von wesentlicher Bedeutung für die Durchführung von bankgeschäftlichen Aufgaben ist.

Selbst wenn eine Auslagerung vorliegt, sind weite Teile des AT 9 MaRisk für das Institut nur dann zu beachten, wenn es sich um eine wesentliche Auslagerung im Sinne von AT 9 Ziff. 2 MaRisk handelt.

Unter Kostengesichtspunkten sollte das Institut daher bestrebt sein, nur solche Maßnahmen in Bezug auf seine Dienstleister durchzuführen beziehungsweise auf diese zu übertragen, die auch tatsächlich notwendig sind.

Flexible statt pauschale aufsichtliche Mustertexte

Insgesamt zeigen diese Beispiele, dass bei der Beauftragung von Dienstleistern ein zu pauschales oder ein zu sehr auf vermeintliche Sicherheit beziehungsweise Entlastung bedachtes Vorgehen des Instituts, zumindest mittel- und langfristig, zu einer erheblichen, aber vermeidbaren Kostenbelastung für das Institut führen kann.

Es ist daher nicht ratsam, lediglich einen aufsichtlichen Mustertext, der aus Gründen vermeintlicher Sicherheit stets die strengsten Anforderungen an die Dienstleister stellt, auszuarbeiten und auf alle Dienstleisterverträge anzuwenden. Vielmehr sollten flexibel anpassbare Mustertexte erarbeitet werden, die zumindest unter den Aspekten „Fremdbezug sonstiger Leistungen", „Auslagerung" und „wesentliche Auslagerung" eine Individualisierung ermöglichen.

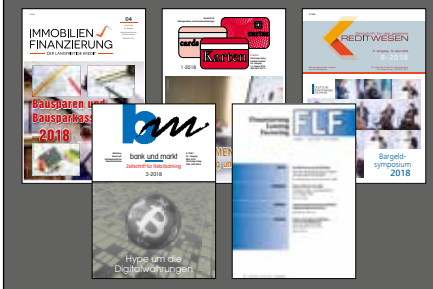
Die bei der Ausarbeitung oder der Anwendung solcher flexiblen Mustertexte gegebenenfalls durch die notwendige Rechtsberatung entstehenden Mehrkosten sollten sich in Form verkürzter Vertragsverhandlungen mit Dienstleistern und geringerer Dienstleitungsentgelte wieder amortisieren. ■

KNOW HOW

SIE HABEN EINE AUSGABE VERPASST?

Einfach nachbestellen unter:
www.kreditwesen.de
Jederzeit auch online für Sie verfügbar:
Einzelbeiträge oder das komplette E-Paper

UNSERE ZEITSCHRIFTEN – EXPERTENWISSEN FÜR SIE



Fritz Knapp
Helmut Richardi

Verlagsgruppe Fritz Knapp
& Helmut Richardi
Postfach 70 03 62
60553 Frankfurt am Main
Telefon 0 69 / 97 08 33 - 25
Telefax 0 69 / 7 07 84 00
E-Mail vertrieb@kreditwesen.de
Internet www.kreditwesen.de

Dieser Artikel ist urheberrechtlich geschützt. Die rechtliche Freigabe ist für den Abonnenten oder Erwerber ausschließlich zur eigenen Verwendung.
Fritz Knapp Verlag GmbH