Dr. Markus Rose

AUSLAGERUNGEN IM FOKUS DER AUFSICHT: DIE LEITLINIEN DER EBA ZU AUSLAGERUNGSVEREINBARUNGEN

ZIELE UND ANWENDUNGSBEREICH DER EBA-LEITLINIEN ZUM OUTSOURCING

Auslagerungsvereinbarungen bilden einen wichtigen Bestandteil der Organisationsstruktur der Institute. Gestützt auf das ihr in Art. 74 Abs. 3 CRD V verliehene Mandat hat die Europäische Bankenaufsichtsbehörde (EBA) am 25.02.2019 ihre Leitlinien zu Auslagerungen veröffentlicht.[1] Diese werden am 30.09.19 in Kraft treten und dann die Vorgängerregelung vom Committee of European Banking Supervisors (CEBS) aus dem Jahr 2006 und die Empfehlungen der EBA zu Auslagerungen an Cloud-Anbieter ersetzen.[2] Die Aktualisierung und Modernisierung der aufsichtlichen Anforderungen an Auslagerungen spiegelt die wachsende Bedeutung von Auslagerungen im Finanzsektor wider: Unter betriebswirtschaftlichen Aspekten können Auslagerungen angesichts des bestehenden Ertragsdrucks im aktuellen Niedrigzinsumfeld u. a. einen Beitrag zur Verbesserung der Kosteneffizienz durch die Nutzung von Skaleneffekten leisten. Darüber hinaus ermöglichen sie den auslagernden Instituten einen vergleichsweise einfachen Zugang zu neuen Technologien[3], insbesondere durch den Bezug von IT-Dienstleistungen von spezialisierten Dritten.

Die EBA verfolgt das Ziel, die Harmonisierung der Anforderungen an Auslagerungen in den EU-Mitgliedsstaaten voranzutreiben. Hierzu erweitert sie mit ihren Leitlinien zum einen den Anwendungsbereich von Kreditinstituten und Wertpapierfirmen (Art. 4 Abs. 1 Nr. 1 CRR II) auf Zahlungsinstitute (Art. 4 Abs. 4 PSD2) und E-Geld-Institute (Art. 2 Abs. 1 E-Geld-Richtlinie).[4] Zum anderen enthalten die Leitlinien einen Abschnitt mit Definitionen wichtiger Begriffe und Sachverhalte: Die EBA definiert „Auslagerung“ als eine Vereinbarung jeder Art zwischen einem Institut, einem Zahlungsinstitut oder einem E-Geld-Institut und einem Auslagerungsunter-

[1] EBA/GL/2019/02: Final Report on EBA Draft Guidelines on outsourcing arrangements, 25.02.2019.
[2] Vgl. EBA/GL/2019/02, S. 5; EBA/REC/2017/03: Final Draft – Recommendations on outsourcing to cloud service providers.
[3] Vgl. Hannemann, R./Steinbrecher, I./ Weigl, T.: Mindestanforderungen an das Risikomanagement (MaRisk) - Kommentar, 5. Auflage, S. 833.
[4] Vgl. EBA/GL/2019/02, S. 18, Tz. 7ff.

nehmen, nach der letzteres einen Prozess, eine Dienstleistung oder eine Aktivität vollzieht, die ansonsten von den Instituten selbst durchgeführt werden würde.[5]
Wenngleich die in den EBA-Leitlinien enthaltenen Anforderungen an Auslagerungen eine hohe Übereinstimmung mit den entsprechenden nationalen Vorgaben des Moduls AT 9 MaRisk aufweisen, sind sie aber teilweise deutlich detaillierter oder weiter gefasst.

STRUKTUR DER LEITLINIEN

Während die Anforderungen der MaRisk im Modul AT 9 „Auslagerung" in 13 Textziffern unterteilt sind, bestehen die Leitlinien der EBA zum Outsourcing aus insgesamt fünf Titeln, die nachfolgend dargestellt und erläutert werden.

TITEL I: PROPORTIONALITÄT: ANWENDUNG AUF GRUPPENEBENE UND HAFTUNGSVERBÜNDE

Im ersten Titel stellt die EBA die Bedeutung des Proportionalitätsprinzips heraus: Die Institute haben bei der Einhaltung der Anforderungen der Leitlinien neben der Komplexität, ihrem Geschäftsmodell, den Risiken – auch für die Geschäftsfortführung – und der Kritikalität der jeweiligen Auslagerung auch die in den Leitlinien zur internen Governance niedergelegten Kriterien zu beachten.[6] Gleiches gilt für die zuständigen Behörden im Hinblick auf die Überwachung der Einhaltung dieser Vorgaben an Auslagerungen durch die Institute. Ferner betonen die Leitlinien, dass die Anforderungen auch auf konsolidierter Ebene einzuhalten sind.
Angesichts der Bedeutung gruppeninterner Auslagerungen an den gesamten Outsourcing-Aktivitäten stellen die Leitlinien auch Anforderungen an Auslagerungslösungen, bei denen das Auslagerungsunternehmen selbst Mitglied der Gruppe oder des Haftungsverbundes ist.[7] Da, wie die EBA betont, das einzelne Institut immer für die Einhaltung aller regulatorischen Anforderungen einschließlich dieser Leitlinien verantwortlich bleibt, muss es das gruppenangehörige Auslagerungsunternehmen unabhängig überwachen und kontrollieren können; dies ist durch Auskunfts- und Informationsrechte des auslagernden Instituts und Berichtspflichten des Auslagerungsunternehmens sicherzustellen. Die Leitlinien formulieren diesbezüglich Anforderungen an die zentrale Risikoanalyse, die gruppenweite Überwachung und Steuerung der Auslagerungen, das vom Auslagerungsunternehmen innerhalb der Gruppe oder des Haftungsverbundes zentral vorzuhaltende Auslagerungsregister und den für kritische oder bedeutende Funktionen begründeten Exit-Plan. Diejenigen Institute, denen die zuständige Behörde einen Waiver gemäß Art. 7 CRR II erteilt hat, haben die Anforderungen der EBA-Leitlinien zu Auslagerungen auf der Ebene des Mutterunternehmens oder Zentralinstituts einzuhalten.[8]

TITEL II: BEURTEILUNG VON AUSLAGERUNGSVEREINBARUNGEN

Ob es sich bei einer Vereinbarung mit einem Dienstleister um eine Auslagerung handelt, sollten die Institute danach beurteilen, ob die ausgelagerten Funktionen oder Teile davon vom Service Provider wiederkehrend oder laufend erbracht und diese normalerweise auch von den Instituten selbst durchgeführt werden könnten.[9] Die EBA listet im Unterschied zu den MaRisk Sachverhalte auf, die nicht als Auslagerungen zu qualifizieren sind, wie z. B. der Bezug von Marktdaten über Bloomberg. Im Zentrum des Titels 2 steht die Definition von kritischen oder bedeutenden Funktionen, an deren Auslagerung – ebenso wie in den MaRisk – in den weiteren Titeln der EBA-Leitlinien deutlich höhere Anforderungen als an sonstige Auslagerungen

[5] Vgl. EBA/GL/2019/02, S. 19, Tz. 12.
[6] Vgl. EBA/GL/2017/11, S. 17, Tz. 19f.
[7] Der Anteil der „Intra-Group-Auslagerungen" belief sich nach einer Untersuchung der EZB aus dem Jahr 2004 auf über 50 %; vgl. European Central Bank: Report on EU banking structure, 24.11.2004, S. 26.
[8] Vgl. EBA/GL/2019/02, S. 25, Tz. 24.
[9] Die MaRisk sprechen in diesem Zusammenhang von Aktivitäten und Prozesse im Zusammenhang mit der Durchführung von Bankgeschäften, Finanzdienstleistungen oder sonstigen institutstypischen Dienstleistungen, die ansonsten vom Institut selbst erbracht würden.

gestellt werden.[10] Institute müssen eine ausgelagerte Funktion immer dann als kritisch oder bedeutend ansehen, wenn

- deren fehlerhafte oder unterlassene Wahrnehmung ihre Lizenz, ihre Wirtschaftlichkeit oder die Zuverlässigkeit oder Kontinuität ihrer Geschäftsaktivitäten gefährden,
- sie ihre internen Kontrollfunktionen ganz oder teilweise auslagern,
- Auslagerungen von Bank- oder Zahlungsdienstleistungen in einem Umfang wahrgenommen werden, die selbst einer Zulassung bedürften,
- Kernbankfunktionen ausgelagert werden.

Während die MaRisk den Instituten für die im Vorfeld einer Auslagerung durchzuführende Risikoanalyse keine konkreten Vorgaben machen, gibt die EBA in Tz. 31 ihrer Leitlinien einen detaillierten Katalog an Beurteilungskriterien vor. Diesen haben die Institute bei der Klassifizierung einer Auslagerung als kritisch oder bedeutend mindestens heranzuziehen.

TITEL III: GOVERNANCE FRAMEWORK

Dass die Institute alle Risiken aus Vereinbarungen mit Drittanbietern – unabhängig davon, ob es sich dabei um Auslagerungen handelt oder nicht – identifizieren, beurteilen, steuern und überwachen müssen, stellt gemäß den Leitlinien der EBA zum Outsourcing eine grundlegende Anforderung an ihre jeweiligen Governance-Rahmenwerke dar. Auslagerungen dürfen nicht zu einer Delegation der Verantwortung der Geschäftsleitung führen; diese bleibt auch für ausgelagerte Aktivitäten und Prozesse in vollem Umfang verantwortlich.[11] Um die Entstehung „virtueller Banken“ – die EBA verwendet den Ausdruck „empty shells“[12] – zu verhindern, müssen die Institute jederzeit ausreichende Ressourcen und Leistungsfähigkeit vorhalten, um eine angemessene Steuerung der Risiken aus kritischen oder bedeutenden Auslagerungen und die Ordnungsmäßigkeit der Durchführung von Bankgeschäften und Zahlungsdiensten zu ermöglichen („retained organisation“). Daher schreibt die EBA den Instituten die Zuweisung klarer Verantwortlichkeiten für die Dokumentation, Steuerung und Überwachung von Auslagerungsvereinbarungen und die organisatorische Errichtung einer „Outsourcing Function“ vor. Anstelle einer solchen Auslagerungsfunktion kann das Institut auch einen für die Steuerung, Überwachung und Dokumentation von Auslagerungsvereinbarungen verantwortlichen leitenden Angestellten mit unmittelbarer organisatorischer Anbindung an die Geschäftsleitung benennen.[13]
Im Falle der (vollständigen oder teilweisen) Auslagerung operativer Aufgaben der internen Kontrollfunktionen Risikocontrolling, Compliance oder der Internen Revision haben die Institute ein angemessenes Management der aus der Auslagerung dieser kritischen oder bedeutenden Funktionen erwachsenden Risiken zu gewährleisten.
Ferner hat die Geschäftsleitung auf Einzel- und Gruppenebene eine schriftliche Auslagerungsrichtlinie („Outsourcing Policy“) zu verabschieden und ihre regelmäßige Überprüfung, Aktualisierung und Umsetzung sicherzustellen. Dabei haben Kreditinstitute und Wertpapierfirmen auf Konsistenz der Outsourcing Policy mit den entsprechenden Vorgaben der EBA-Leitlinien zur Internen Governance zu achten.[14] Die Institute haben in diese Richtlinie – unter Berücksichtigung des gesamten Lebenszyklus von Auslagerungsvereinbarungen – Grundsätze, Verantwortlichkeiten und Prozesse im Hinblick auf Auslagerungen zu definieren. Die EBA gibt dazu in ihren Leitlinien Mindestinhalte vor; so sollte die Outsourcing Policy z. B. unterscheiden zwi-

[10] Der Unterscheidung nach kritischen oder bedeutenden und sonstigen Auslagerungen in den EBA-Leitlinien zu Auslagerungen entspricht der Differenzierung nach wesentlichen und nicht wesentlichen Auslagerungen in den MaRisk.
[11] Vgl. EBA/GL/2019/02, S. 30, Tz. 35f.
[12] Vgl. EBA/GL/2019/02, S. 31, Tz. 39.
[13] Vgl. EBA/GL/2019/02, S. 31, Tz. 38.
[14] Vgl. EBA/GL/2019/02, S. 33, Tz. 41.

schen

- Auslagerungen von kritischen oder bedeutenden Funktionen und sonstigen Auslagerungen
- Auslagerungen an Service Provider mit und ohne aufsichtliche Zulassung
- Intragruppen-Auslagerungen bzw. Auslagerungen innerhalb eines Haftungsverbundes und Outsourcing an außenstehende Dienstleister
- Auslagerungen an Service Provider innerhalb und außerhalb der EU.[15]

Darüber hinaus formuliert die EBA Vorgaben an den Umgang mit Interessenkonflikten, das Vorhalten von Geschäftsfortführungsplänen sowie an die Interne Revision des auslagernden Instituts. Deutlich weitergehend als die MaRisk sind die Dokumentationsanforderungen bei Auslagerungen: Die EBA fordert von allen Instituten als Teil ihres Rahmenwerks zum Risikomanagement ein aktuelles Register mit allen Auslagerungen auf Einzel- und Gruppenebene in einem gängigen Datenbankformat vorzuhalten.[16] Dazu schreibt sie einen umfangreichen Katalog mit Mindestinhalten für alle Auslagerungen vor; darüber hinaus sind zusätzliche, in Tz. 55 der Leitlinien aufgeführte Informationen bei Auslagerungen kritischer oder bedeutender Funktionen vorzuhalten. Schließlich verlangt die EBA, dass die Institute ihre zuständigen Behörden angemessen und zeitnah mittels Einreichung der in Tz. 54 geforderten Angaben informieren, wenn sie Auslagerungen kritischer oder bedeutender Funktionen planen[17]. Eine solche Informationspflicht kennen die MaRisk nicht.

TITEL IV: DER OUTSOURCING-PROZESS

Die EBA formuliert in Titel IV ihrer Leitlinien zum Outsourcing umfangreiche Anforderungen an die im Vorfeld einer Auslagerung obligatorisch durchzuführende Risikoanalyse („Pre-Outsourcing Analysis“). Die Risikoanalyse umfasst zunächst die Beurteilung, ob eine Auslagerungsvereinbarung – wie im Titel II dargelegt – kritische oder bedeutende Funktionen betrifft. Außerdem hat das auslagernde Institut sicherzustellen, dass das Auslagerungsunternehmen selbst – sofern Bankaktivitäten oder Zahlungsdienste in einem erheblichen Umfang ausgelagert werden sollen – über die erforderliche aufsichtsrechtliche oder rechtlich gleichwertige Zulassung besitzt. Ist der Service Provider in einem Drittstaat ansässig, ist neben der Zulassung und Überwachung durch den Regulator auch das Vorliegen einer Kooperationsvereinbarung zwischen der inländischen Aufsichtsbehörde und derjenigen des Drittstaates erforderlich.
Ferner muss ein Institut im Rahmen der Risikoanalyse die möglichen Auswirkungen der Auslagerungsvereinbarung auf sein operationelles Risiko einwerten und dabei angemessene Schritte unternehmen, um übermäßige zusätzliche Risiken zu vermeiden.[18] Dabei verlangen die EBA-Leitlinien auch die Durchführung von Szenarioanalysen mit hohem Schadensausmaß, also die Durchführung von Stresstests. Darüber hinaus haben die Institute im Rahmen einer Kosten-Nutzen-Analyse von Auslagerungen mindestens auch Konzentrationsrisiken und das aggregierte Risiko bei Auslagerungen verschiedener Funktionen zu berücksichtigen. Signifikante Institute müssen auch das Step-in-Risiko[19] in der Risikoanalyse berücksichtigen. Bei einer Weiterverlagerung von kritischen oder bedeutenden Funktionen sind damit im Zusammenhang stehende Risiken – insbesondere auch das erhöhte Risiko eines Kontrollverlusts beim auslagernden Institut – zu berücksichtigen. Darüber hinaus haben Institute bei der Risi-

[15] Vgl. EBA/GL/2019/02, S. 34, Tz. 43.
[16] Vgl. EBA/GL/2019/02, S. 36, Tz. 52.
[17] Vgl. EBA/GL/2019/02, S. 38, Tz. 58.
[18] Dies entspricht inhaltlich den Vorgaben des § 25b KWG für inländische Institute.
[19] Step-in-Risiko: Risiko, dass eine Bank – ohne dazu vertraglich verpflichtet zu sein oder über vertragliche Verpflichtungen hinaus – finanzielle Unterstützung für eine nicht konsolidierte Einheit leistet, die sich in einer Stresssituation befindet.

koanalyse das angemessene Schutzniveau der Vertraulichkeit, Integrität und Rückverfolgbarkeit von Daten und Systemen im Kontext beabsichtigter Auslagerungen zu definieren und zu beschließen.

Schließlich bildet die Prüfung der Eignung des Auslagerungsunternehmens („Due Diligence") einen wichtigen Bestandteil der Risikoanalyse. Das auslagernde Institut hat sicherzustellen, dass das Auslagerungsunternehmen für die Übernahme kritischer oder bedeutender Funktionen über die erforderliche Reputation, Expertise, Ressourcen und – falls erforderlich – die notwendige aufsichtliche Zulassung für die zuverlässige und professionelle Durchführung der ausgelagerten Aktivitäten und Prozesse verfügt. Darüber hinaus gibt die EBA zusätzliche Mindestinhalte für die Due Diligence vor, wie z. B die Analyse des Geschäftsmodells des Service Providers.[20] Eine solche Detailtiefe der Vorgaben zur Eignungsbeurteilung des Auslagerungsunternehmens ist den nationalen Regelungen zu Auslagerungen in den MaRisk fremd.

Die EBA-Leitlinien schreiben für die Auslagerung kritischer oder bedeutender Funktionen umfangreiche Mindestinhalte für den Auslagerungsvertrag vor. Dabei werden vier Themen besonders hervorgehoben:

1. Weiterverlagerungen kritischer oder bedeutender Funktionen

Im schriftlich zu fixierenden Auslagerungsvertrag haben die Institute zu spezifizieren, ob Weiterverlagerungen kritischer oder bedeutender Funktionen grundsätzlich zulässig sind. Falls ja, ist u. a. zu fixieren, dass das Auslagerungsunternehmen vor einer geplanten Weiterverlagerung von Daten die schriftliche Zustimmung des auslagernden Instituts einzuholen hat. Ebenso besteht unter Beachtung der festgelegten Frist eine Anzeigepflicht des Service Providers gegenüber dem auslagernden Institut im Falle wesentlicher Änderungen einer Weiterverlagerung. Dies ermöglicht letzterem die Durchführung einer Risikoanalyse der geplanten Änderungen, um dann der Weiterverlagerung ggf. zu widersprechen.

2. Schutz von Daten und Systemen

Die Institute haben durch entsprechende Klauseln im Auslagerungsvertrag sicherzustellen, das jeweilige Auslagerungsunternehmen auf den Schutz vertraulicher, personenbezogener oder anderweitig sensibler Informationen zu verpflichten. Diese Anforderung an die Datensicherheit und ihre laufende Überwachung gilt auch bei der Auslagerung an Cloud-Dienstleister.[21]

3. Zugangs-, Informations- und Prüfungsrechte

Der Auslagerungsvertrag muss einen Passus enthalten, der der Internen Revision des auslagernden Instituts sowie den zuständigen Behörden eine risikobasierte Überprüfung ausgelagerter Aktivitäten und Prozesse ermöglicht. Im Hinblick auf kritische oder bedeutende Funktionen müssen die Institute daher im Auslagerungsvertrag den uneingeschränkten Zugang zu Gebäuden des Auslagerungsunternehmens sowie zu Netzwerken, Informationen und Daten kodifizieren, der für die Durchführung der ausgelagerten Funktionen erforderlich ist. Dies gilt ebenso für die Prüfungsrechte der Internen Revision, die auch im Rahmen von Poollösungen oder durch die Interne Revision einer von allen Kunden eines Auslagerungsunternehmens bestimmten dritten Partei (z. B. Wirtschaftsprüfungsgesellschaft) durchgeführt werden kann.[22]

4. Kündigungsrechte

Die Institute haben sich im Auslagerungsvertrag angemessene Kündigungsrechte einräumen zu lassen. Diese haben auch den Zweck, bei Bedarf die Übertragung der ausgelagerten Funktionen an ein anderes Auslagerungsunternehmen oder die Reintegration in das auslagernde

[20] Vgl. EBA/GL/2019/02, S. 43, Tz. 70f.
[21] Vgl. EBA/GL/2019/02, Kapitel 13.2.
[22] Vgl. EBA/GL/2019/02, S. 48, Tz. 91a.

Institut zu erleichtern. Hierfür sind im Auslagerungsvertrag die im Falle einer Kündigung bestehenden Verpflichtungen des Auslagerungsunternehmens bei der (Rück-) Übertragung und der angemessene Zeitraum der Fortsetzung der Leistungserbringung durch das Auslagerungsunternehmens nach erfolgter Kündigung durch das auslagernde Institut festzulegen.

In einem weiteren Kapitel des Titels 4 legen die EBA-Leitlinien die Anforderungen an die Überwachung der ausgelagerten Funktionen dar. Instituten müssen – unter besonderer Berücksichtigung der kritischen und bedeutenden Funktionen – die vom Auslagerungsunternehmen zu erbringenden Leistungen und deren Qualität anhand von z. B. Key Performance Indicators (KPI) definieren und spezifizieren sowie mittels der vom Service Provider zu liefernden Berichte überwachen. Dieses Reporting bezieht sich auch auf die Maßnahmen und Tests zur Gewährleistung der Geschäftsfortführung. Die vom Auslagerungsunternehmen erhaltenen Berichte sind ihrerseits die Grundlage für die turnusmäßige Aktualisierung der Risikoanalyse und das regelmäßige Reporting an die Geschäftsleitung über die mit Auslagerungen kritischer oder bedeutender Funktionen verbundenen Risiken.
Schließlich müssen Institute hinsichtlich ihrer Auslagerungen kritischer oder bedeutender Funktionen über eine dokumentierte Exit-Strategie verfügen, die konsistent zur Outsourcing-Policy und den Geschäftsfortführungsplänen ausgestaltet ist.[23] Das Ziel dieser Ausstiegsstrategie besteht in der Sicherstellung der Erfüllung aller regulatorischen Anforderungen und einer kontinuierlichen Leistungserbringung in der von den Kunden des Instituts erwarteten und verlangten Qualität auch im Falle einer Beendigung einer Auslagerungsvereinbarung.

TITEL V: AN DIE ZUSTÄNDIGEN BEHÖRDEN ADRESSIERTEN TEILE DER LEITLINIEN

Der letzte Titel der Leitlinien der EBA zum Outsourcing richtet sich an die zuständigen Behörden. Diese sollten eine Analyse der mit einer Auslagerung verbundenen Risiken zumindest in den SREP-Prüfungen[24] durchführen. Die dabei zu untersuchenden Risiken sollten mindestens operationelle Risiken, Konzentrationsrisiken und das Step-in-Risiko umfassen. Als Informationsquellen steht den zuständigen Behörden das Auslagerungs-Reporting zur Verfügung, das ihnen von den Instituten auf Verlangen vorzulegen ist. Darüber hinaus können sie von den Instituten weitergehenden Informationen verlangen, auch in Bezug auf die sonstigen, nicht wesentlichen Auslagerungen, wie z. B. zu diesbezüglichen Ausstiegsstrategien und Geschäftsfortführungsplänen.

UNTERSTÜTZUNG DURCH 1 PLUS i

Die hier vorgestellten Leitlinien der EBA zum Outsourcing halten im Zusammenspiel mit den entsprechenden Anforderungen in den MaRisk und den BAIT den Anpassungs- und Umsetzungsbedarf und -druck für die Institute auf dem Themenfeld der Auslagerungen hoch. Die europäischen Vorgaben und Erwartungen gehen – wie dargestellt – teilweise deutlich über die nationalen Anforderungen hinaus.
Wir unterstützen Sie gerne bei der Identifizierung eines konkreten Handlungsbedarfs in Ihren Häusern. Darüber hinaus erarbeiten wir in unseren Teams Quick-Check-Lösungen, welche wir Ihnen im Rahmen von Inhouse-Kundenworkshops sehr gern vorstellen. Sprechen Sie uns dazu einfach an (info@1plusi.de)!

[23] Vgl. EBA/GL/2019/02, Kapitel 15.
[24] Bei Zahlungs- oder E-Geld-Instituten, die nicht dem SREP unterliegen, sollten anderweitige aufsichtliche Überprüfungsprozesse und Vor-Ort-Prüfungen durchgeführt werden.