Neue Anforderungen an Auslagerungen im Finanzsektor

Finale EBA-Leitlinien zum Outsourcing

März 2019

Überblick

Am 25. Februar 2019 hat die Europäische Bankenaufsichtsbehörde (EBA) ihre neuen Leitlinien für Auslagerungssachverhalte (*EBA Guidelines on outsourcing arrangements*; EBA/GL/2019/02) veröffentlicht.

Die EBA-Leitlinien enthalten umfassende Regeln für die aufsichtsrechtliche Behandlung von Auslagerungen. Die Regelungen betreffen v.a. den Governance-Rahmen (z.B. das Risikomanagement, die Organisation und die Dokumentationspflichten) sowie den Auslagerungsprozess (z.B. die Auslagerungsvoranalyse und den Auslagerungsvertrag).

Den finalen EBA-Leitlinien ging eine öffentliche Konsultation aus dem Juni 2018 voraus. Gegenüber dem Konsultationsentwurf hat die EBA die Leitlinien noch einmal umfassend überarbeitet.

Auf europäischer Ebene waren die aufsichtsrechtlichen Vorgaben für Auslagerungen bisher nur rudimentär geregelt. Die maßgeblichen europäischen Richtlinien wie CRD IV, MiFID2, EMD, PSD2 und BRRD und die Vorgängerleitlinien aus dem Jahr 2006 (*CEBS Guidelines on outsourcing*) enthielten nur wenige Grundprinzipien zu Auslagerungssachverhalten. Diese wurden für die deutsche Kreditwirtschaft v.a. im Allgemeinen Teil 9 (AT 9) der Mindestanforderungen an das Risikomanagement (MaRisk) konkretisiert.

Die neuen Leitlinien erweitern die bestehenden Regelungen in erheblichem Umfang. Sie enthalten sehr viel detailliertere und z.T. neue und verschärfte Anforderungen an Auslagerungen. Was die MaRisk derzeit auf rund drei Seiten regelt, regeln die EBA-Leitlinien künftig auf mehr als 30 Seiten.

Die EBA-Leitlinien integrieren zudem die erst im letzten Jahr erlassenen Empfehlungen der EBA zur Auslagerung an Cloud-Anbieter (*EBA Recommendations on outsourcing to cloud service providers*; EBA/REC/2017/03).

Während zu erwarten ist, dass die von der EZB beaufsichtigten bedeutenden Institute die Leitlinien direkt anwenden müssen, ist Art und Umfang einer nationalen Transformation für weniger bedeutende Institute noch offen. Das Inkrafttreten ist für 30.09.2019 mit Übergangsregelungen geplant.

Inhalt

Wichtige Neuregelungen

Die Realisierung von Kostenvorteilen und der Zugang zu neuen Technologien durch z.B. Einbindung von innovativen Anbietern in die Wertschöpfungskette wird zukünftig nur zum erhöhten Preis der Beachtung der gestiegenen regulatorischen Anforderungen der EBA-Leitlinien möglich sein. Die wichtigsten Neuregelungen werden im Folgenden exemplarisch vorgestellt.

Erweiterter Anwendungsbereich

Der Anwendungsbereich der EBA-Leitlinien wird im Vergleich zu den bisherigen Leitlinien und zur MaRisk erweitert. Die neuen Leitlinien gelten nicht nur für Kreditinstitute und Wertpapierfirmen i.S.d. CRD IV, sondern auch für Zahlungs- und E-Geldinstitute. Deren Auslagerungsaktivitäten werden damit erstmals auf europäischer Ebene näher konkretisiert.

Definition des Auslagerungsbegriffs

Die EBA-Leitlinien enthalten eine eigene Definition des Auslagerungsbegriffs. Hierunter wird eine Vereinbarung jeglicher Form mit einem Dienstleister verstanden, aufgrund derer der Dienstleister einen Prozess, eine Dienstleistung oder eine Tätigkeit oder Teile davon erbringt, die ansonsten vom Institut selbst erbracht werden würde.

Der Begriff der Auslagerung ähnelt damit der aus der MaRisk bekannten Abgrenzung zum sonstigen Fremdbezug. Es kommt weiterhin v.a. darauf an, ob die ausgelagerte Tätigkeit ansonsten vom Institut selbst erbracht wird. Die finalen EBA-Leitlinien stellen zur Erleichterung der Abgrenzung einen Negativkatalog von Fällen zur Verfügung, die nicht als Auslagerung zu werten sind.

Auslagerung kritischer oder wichtiger Funktionen

Sofern eine Auslagerung vorliegt, wird zudem eine qualitative Abstufung ähnlich den MaRisk vorgenommen. Die MaRisk hat bisher zwischen wesentlichen und nicht wesentlichen Auslagerungen unterschieden und die Abgrenzung im Wesentlichen ins Ermessen des Instituts gestellt. Die EBA-Leitlinien führen nun den Begriff der Auslagerung einer „kritischen oder wichtigen Funktion“ ein. Damit sind v.a. Tätigkeiten umfasst, deren Ausfall oder Schlechtleistung wesentlichen Einfluss auf die Zulassungsvoraussetzungen, Finanzsituation oder Geschäftsfortführung haben. Für die Frage, welche Aktivitäten als kritisch oder wichtig anzusehen sind, stellen die Leitlinien zahlreiche Kriterien bereit.

Viele der Vorgaben der EBA-Leitlinien gelten nur für die Auslagerung kritischer oder wichtiger Funktionen; nur ein Teil der Regeln ist auch auf sonstige Auslagerungen anwendbar.

Governance

Die EBA stellt klar, dass sie von Instituten einen ganzheitlichen Governance-Rahmen über alle Geschäftsfelder und Kontrollfunktionen erwartet, der nicht nur ein effektives Risikomanagement von Auslagerungen sicherstellt, sondern generell ein Risikomanagement der Zusammenarbeit mit sämtlichen Drittparteien.

Neben der Formulierung von Anforderungen an die Governance von Auslagerungen und der Zuweisung konkreter Verantwortungen an die Geschäftsleitung auch im Falle von ausgelagerten Aktivitäten, betonen die Leitlinien vermutlich auch vor dem Hintergrund des Brexit und fortlaufender Optimierung von Gruppen- und Verbundstrukturen die Aufgaben der „retained organisation“.

Zu diesen Aufgaben gehören die Sicherstellung von angemessenen Überwachungsaktivitäten und Ressourcenausstattungen, wenngleich die Auslegung der Angemessenheit zunächst primär ins Ermessen der Institute gestellt wird. Ferner gehören eigenständige Entscheidungsprozesse, eine ordnungsgemäße Geschäftsorganisation, eine umfassende Risikoeinschätzung, vereinbarte Informationsrechte und Datenschutzregelungen sowie Exit Strategien zu den Grundanforderungen einer Governance.

Konzerninterne Auslagerungen

Die Leitlinien stellen klar, dass die aufsichtsrechtlichen Vorgaben im Grundsatz auch bei konzerninternen Auslagerungen und bei Auslagerungen innerhalb desselben Institutssicherungssystems erfüllt werden müssen. Die EBA-Leitlinien betonen dabei die besondere Verantwortung der Konzernmutter zur Sicherstellung der Umsetzung und Einhaltung der Auslagerungsanforderungen auf Gruppenebene.

Im Rahmen von konzerninternen Auslagerungen sollen grundsätzlich die gleichen Maßstäbe wie bei konzernexternen Auslagerungen gelten. Gruppeninterne Auslagerungen sollen dabei einem Drittvergleich („*at arm's length*“) standhalten. Ferner wird das Risiko möglicher Interessenkonflikte besonders hervorgehoben.

Auslagerungen in Drittstaaten

Die EBA-Leitlinien stellen besondere Anforderungen an die Auslagerung in Drittstaaten außerhalb des EU-Raums auf, zu denen in Zukunft auch das Vereinigte Königreich gehören kann.

Bei Auslagerungen in Drittstaaten gilt künftig eine Art Äquivalenzprinzip. Regulierte Tätigkeiten dürfen nur dann in einen Drittstaat ausgelagert werden, wenn auch der Dienstleister über eine Erlaub-

nis verfügt und entsprechend beaufsichtigt wird. Zudem muss die Kooperation zwischen den Aufsichtsbehörden in Form einer Kooperationsvereinbarung sichergestellt werden. Die praktische Umsetzung wird viele Betroffene vermutlich vor Herausforderungen stellen.

Auslagerungsregister

Eine wichtige Neuerung ist die verpflichtende Einführung eines zentralen Auslagerungsregisters. Dort müssen Informationen über sämtliche Auslagerungsvereinbarungen des Instituts gesammelt werden. Dies beinhaltet auch Auslagerungen nicht kritischer oder wichtiger Funktionen. Die Leitlinien enthalten detaillierte Mindestvorgaben zur Ausgestaltung des Registers und der dort aufzunehmenden Informationen. Die Inhalte sind den Aufsichtsbehörden auf Verlangen zugänglich zu machen. Die Erhebung der hierfür erforderlichen Informationen (insbesondere zu Cloud Auslagerungen) wird in der Praxis einigen Aufwand verursachen.

Analysen im Vorfeld einer Auslagerung

Im Vorfeld einer Auslagerung müssen Institute eine Risikoanalyse und -bewertung vornehmen. Diese wird im Vergleich zu den aktuellen Vorgaben der MaRisk stark konkretisiert. So sind insbesondere die Auswirkungen auf operationelle Risiken (einschließlich IT-Risiken), aber auch Konzentrations- und Reputationsrisiken sowie sog. Step-in-Risiken zu untersuchen. Ein besonderer Fokus wird auf die Überprüfung (Due Diligence) des Auslagerungsunternehmens gelegt. Die Due Diligence umfasst dabei nicht nur die Reputation, fachliche Qualifikation, Datenschutzvorkehrungen und Wirtschafskraft des Dienstleisters, sondern auch dessen ethisches und soziales Verhalten.

Mindestinhalte des Auslagerungsvertrags

Die EBA-Leitlinien definieren in detaillierter Form Mindestinhalte für Auslagerungsverträge. Diese gehen z.T. über den Katalog in AT 9 der MaRisk hinaus. In Bezug auf Auslagerungen von kritischen oder wichtigen Funktionen muss der Vertrag z.B. Angaben zum Ort der Leistungserbringung und zu Leistungsstandards enthalten. Darüber hinaus ist eine Abwicklungsklausel aufzunehmen, die auf die Befugnisse der nationalen Aufsichtsbehörden verweist.

Im Auslagerungsvertrag müssen weiterhin Informations-, Zugangs- und Audit-Rechte zugunsten des Instituts und der zuständigen Aufsichtsbehörde festgeschrieben werden. Neu ist, dass dabei auf sog. Pooled Audits zurückgegriffen werden kann. Die Regelung wurde teilweise wörtlich aus den EBA-Cloud Recommendations übernommen.

Darüber hinaus enthalten die Leitlinien besondere Regelungen im Bereich IT-Sicherheit. Beispielsweise müssen Institute sicherstellen, dass der Service Provider angemessene Sicherheitsstandards erfüllt. In manchen Fällen muss der Auslagerungsvertrag sogar besondere Vorgaben zur Datensicherheit enthalten.

Zustimmungspflicht bei Unterauslagerungen

Im Bereich der Unterauslagerung rückt die Pflicht, das Unterauslagerungsunternehmen zu überwachen, noch stärker in den Vordergrund. Der Service Provider muss das Institut über geplante Unterauslagerungen vorab informieren. In besonderen Fällen muss sogar ein Widerspruchs- oder Zustimmungsrecht festgeschrieben werden.

Informationspflichten gegenüber der Aufsicht

Die EBA-Leitlinien enthalten neue Informationspflichten. Institute sind künftig dazu verpflichtet, die zuständige Aufsichtsbehörde über die geplante Auslagerung von kritischen oder wichtigen Funktionen zu informieren oder „in einen Dialog“ hierüber zu treten. Zuletzt sah die MaRisk keine derartige Verpflichtung vor und es bleibt abzuwarten, wie diese Informationspflicht operationalisiert wird. Neben den o.g. geplanten Auslagerungen haben Institute die zuständige Aufsichtsbehörde auch zeitnah über wesentliche Änderungen oder Ereignisse in Bezug auf Auslagerungen zu informieren, die die Fortführung von Geschäftsaktivitäten beeinträchtigen könnten.

Inkrafttreten

Die Leitlinien treten am 30. September 2019 in Kraft. Sie gelten für alle Auslagerungsverträge, die ab diesem Tag geschlossen, geändert oder überprüft werden. Bestehende Auslagerungsverträge sollen ebenfalls überprüft und angepasst werden. Für den Fall, dass die Überprüfung bis zum 31. Dezember 2021 noch nicht abgeschlossen ist, ist die zuständige Aufsichtsbehörde zu informieren. Außerdem müssen die Maßnahmen zur weiteren Anpassung bzw. Beendigung nicht konformer Auslagerungen dargelegt werden.

Darüber hinaus existiert eine Übergangsregelung. Danach muss die Dokumentation aller bestehenden Auslagerungsverträge – mit Ausnahme von Verträgen mit Cloud Service Providern – jeweils ab der nächsten Vertragsverlängerung den neuen Vorgaben entsprechen, spätestens bis zum 31. Dezember 2021.

Die Übergangsregelungen werfen eine Reihe von Auslegungsfragen auf. Fraglich ist z.B., ob bereits kleinere oder rein formale Ände-

rungen zur Anwendbarkeit der EBA-Leitlinien führen. In der Praxis werden v.a. Service Level Agreements (SLA) in regelmäßigen Abständen überarbeitet. In solchen Fällen muss geklärt werden, ob dies bereits die Anwendbarkeit der neuen Regeln auslöst.

Erheblicher Handlungsbedarf

Auf die Institute kommt durch die EBA-Leitlinien nur kurz nach der Umsetzung der letzten MaRisk-Novelle und der Bankaufsichtlichen Anforderungen an die IT (BAIT) weiterer Anpassungsbedarf zu.

Die Leitlinien betreffen im Grundsatz sämtliche Komponenten eines organisatorischen Rahmens für das Management von Auslagerungen. Insbesondere folgende Handlungsbedarfe können entstehen:

- Überprüfung der Definition von Auslagerungen und Abgrenzung gegenüber sonstigem Fremdbezug
- Anpassung der Wesentlichkeitsprüfung von Auslagerungen an die konkreten Vorgaben zur Einstufung als „kritisch bzw. wichtig"
- Weiterentwicklung der Risikoanalyse und –überwachung durch stärkere Verbindung mit dem Management von insbesondere operationellen Risiken (einschließlich IT-Risiken).
- Intensivere Prüfung der Eignung eines Dienstleisters entlang konkreter Kriterien und Beachtung von Vorschriften vor allem in Bezug auf Drittstaaten
- Einführung oder signifikante Weiterentwicklung eines zentralen Auslagerungsregisters mit Mindestinformationsvorgaben
- Institutsinterne Definition von Auslösern von Informationspflichten der Aufsicht
- Sicherstellung einer angemessenen Ressourcenausstattung und Überwachung in einer „retained organisation", auch in Gruppen und Sicherungsverbünden
- Überarbeitung von Musterverträgen und SLAs unter Berücksichtigung u.a. von Datenschutz, Regelungen zur Weiterverlagerung, Kündigungsrechten sowie Prüf- und Informationspflichten
- Überprüfung der schriftlich fixierten Ordnung (einschließlich entsprechender Richtlinien und Arbeitsanweisungen) in Bezug auf geforderte Mindestinhalte
- Weiterentwicklung sog. Exit Strategien in Einklang mit den konkretisierten EBA-Vorgaben
- Sicherstellung einer konsistenten Anwendung von Gruppenvorgaben in Tochterunternehmen

Institute werden somit nicht umhin kommen, ihre Auslagerungsprozesse, -strukturen und IT-Systeme, interne Richtlinien und Vertragsdokumente zu überprüfen und an die neuen Vorgaben anzupassen. Der Analyse- und Implementierungsaufwand sollte dabei nicht unterschätzt werden. Er erfordert das Zusammenwirken unterschiedlichster Bereiche wie Organisation/IT, Einkauf, Risikocontrolling, Informationssicherheit, Compliance und Recht.

Für die meisten Zahlungsinstitute dürfte der Anpassungsbedarf noch deutlich größer sein. Sie sind im Grundsatz künftig demselben Auslegungsregime unterworfen wie Vollbanken und verfügen ggf. noch nicht über vergleichbar hoch entwickelte Prozesse im Management von Auslagerungen.

Service Provider, die als Auslagerungsunternehmen für Unternehmen der Finanzindustrie agieren, wie z.B. FinTechs oder IT-Dienstleister, werden indirekt betroffen sein und sich über die zahlreichen Prüf-, Informations- und Überwachungspflichten auf Änderungswünsche bzw. neue Anforderungen einstellen müssen.

Da auch perspektivisch Bestandsauslagerungen betroffen sind, sind die Umsetzungsfristen für die EBA-Leitlinien trotz scheinbar großzügiger Übergangsfristen durchaus ambitioniert.

Umsetzung in Deutschland

Schließlich stellt sich die Frage, wie die zuständigen Aufsichtsbehörden die Leitlinien technisch umsetzen. Technisch binden die EBA-Leitlinien zunächst nur die Aufsichtsbehörden, die erklären müssen, ob und inwieweit sie diese in ihre Verwaltungspraxis übernehmen („*comply or explain*").

Wir erwarten, dass die EZB die Leitlinien vollständig in ihre Aufsichtspraxis übernimmt. Sie würden dann für alle bedeutenden Institute gelten.

Vermutlich wird auch die BaFin die Leitlinien weitgehend umsetzen, so dass auch weniger bedeutende Institute erfasst wären. Noch ist jedoch offen, wie die BaFin die Leitlinien technisch umsetzt. Sie könnte beispielsweise die MaRisk und ggf. BAIT um die neuen Regeln ergänzen. Ebenso wäre es denkbar, dass die BaFin im Rahmen eines Mantelrundschreibens erklärt, die EBA-Leitlinien 1:1 in ihre Verwaltungspraxis zu übernehmen.

Dies würde aufgrund der im Vergleich zu den MaRisk sehr detaillierten und teils abweichenden Regelungen die Frage aufwerfen, wie die proportionale und konsistente Anwendung der EBA-Leitlinien sichergestellt werden kann. Von der Art und Weise der Umsetzung hängt somit ab, wie flexibel weniger bedeutende Institute im Hinblick auf die EBA-Leitlinien und deren Anwendung sein werden.

Sprechen Sie uns gerne an!

KPMG hat die neuen Anforderungen strukturiert aufgearbeitet und den bestehenden MaRisk gegenüberbestellt, um neue Handlungsbedarfe zügig zu erkennen. Unsere Teams aus erfahrenen Experten in den Bereichen Regulatory & Compliance, Business Technology und Law unterstützen Sie gerne dabei, sich optimal auf die Anforderungen an das Auslagerungsmanagement vorzubereiten.

KPMG AG

Thilo Kasprowicz
Partner, Financial Services
T +49 69 9587-3198
tkasprowicz@kpmg.com

Andreas Reuß
Partner, Financial Services
T +49 69 9587-4193
areuss@kpmg.com

Kathrin Hellmich
Senior Manager, Financial Services
T +49 69 9587-4659
khellmich@kpmg.com

Daniel Wagenknecht
Senior Manager, Financial Services
T +49 69 9587-1295
dwagenknecht@kpmg.com

KPMG Law

Dr. Andreas Wieland
Partner, Financial Services Legal
T +49 69 951195-848
awieland@kpmg-law.com

Dr. Peter Schad
Senior Manager, Financial Services Legal
T +49 89 599 7606-1503
pschad@kpmg-law.com

Dr. Matthias Henke
Senior Manager, Financial Services Legal
T +49 211 4155597-362
mhenke@kpmg-law.com

Impressum

KPMG AG
Wirtschaftsprüfungsgesellschaft
Klingelhöferstraße 18
10785 Berlin

Thilo Kasprowicz (V.i.S.d.P.)
Partner, Financial Services
T +49 69 9587-3198
tkasprowicz@kpmg.com

www.kpmg.de

www.kpmg.de/socialmedia