Luther.

September 2021

Update zu neuen BaFin-Rundschreiben (MaRisk, BAIT und ZAIT) – Anpassungsbedarf für Auslagerungsverträge

Hintergrund

Finanzinstitute verlagern kritische Operationen wie Zahlungssysteme und Online-Banking einschließlich Identifizierungs- und Authentifizierungsprozessen zunehmend in die Cloud. Damit wächst die Gefahr, dass der Ausfall eines Cloud-Unternehmens die Dienste einer Bank zum Erliegen bringt und Kunden nicht mehr in der Lage wären, Zahlungen zu leisten oder auf Dienste zuzugreifen. Die Bundesanstalt für Finanzdienstleistungsaufsicht (BaFin) hat am 16. August 2021 drei neue Rundschreiben veröffentlicht: Die **Mindestanforderungen an das Risikomanagement der Banken (MaRisk)**, die **Bankaufsichtlichen Anforderungen an die IT (BAIT)** sowie die **Zahlungsdiensteaufsichtlichen Anforderungen an die IT (ZAIT)**.

In der neuen MaRisk hat die BaFin u. a. die 2019 verabschiedeten EBA-Leitlinien zu Auslagerungen (EBA/GL/2019/02) umgesetzt. Aus den BAIT ergibt sich, welche Rahmenbedingungen für eine sichere Informationsverarbeitung und Informationstechnik von Instituten umgesetzt werden müssen. Das ZAIT gibt Zahlungs- und E-Geld-Instituten aufsichtsrechtliche Anforderungen an den Einsatz von Informationstechnik und in Bezug auf Cybersicherheit vor. Institute müssen ihre Auslagerungsverträge und -prozesse an diese inhaltlich geschärften Anforderungen anpassen. Dienstleister sollten vorhandene Handlungsspielräume identifizieren und analysieren, um ihre Leistungen, Geschäftsbedingungen und Verhandlungsstrategien auf die Compliance-Anforderungen ausrichten zu können.

Welcher Handlungsbedarf folgt für Kredit- und Finanzdienstleistungsinstitute aus der MaRisk?

Die MaRisk richtet sich an die Kredit- und Finanzdienstleistungsinstitute, die der Aufsicht der BaFin unterliegen. Mit Blick auf Auslagerungen sind mit der 6. MaRisk Novelle diverse Neuerungen hinzugekommen sowie bestehende Anforderungen an Auslagerungen konkretisiert worden.

Anpassung von Auslagerungsverträgen

Auslagerungsverträge müssen insbesondere Angaben zu den Standorten der Leistungserbringung, die vereinbarte Dienstleistungsgüte mit eindeutigen Leistungszielen wie KPI-Parameter und Regelungen zu Notfallkonzepten enthalten (AT 9 Tz. 9). Weiterhin müssen Informations- und Prüfungsrechte im Auslagerungsvertrag geregelt sein (AT 9 Tz. 7 lit. h) und i)); diese Anforderung ist nicht nur bei wesentlichen, sondern auch bei nicht wesentlichen Auslagerungen vertraglich zu vereinbaren, wenn absehbar ist, dass diese Auslagerun-

gen zukünftig wesentlich werden können. Die Festlegung der Standorte (d. h. Regionen und Länder), in denen die Dienstleistung erbracht wird und/oder maßgebliche Daten gespeichert und verarbeitet werden, sowie die Pflicht, das Institut zu benachrichtigen, wenn das Auslagerungsunternehmen den Standort wechselt, führt in der Praxis bei Cloud-Diensteistern nicht selten zu Diskussionsbedarf.

Die Vorgabe, möglichst Zustimmungsvorbehalte des auslagernden Instituts oder konkrete Voraussetzungen, wann Weiterverlagerungen einzelner Arbeits- und Prozessschritte möglich sind, zu vereinbaren, ist gerade für kleinere Institute gegenüber Cloud-Anbietern schwierig durchzusetzen. Vereinbarungen mit Subunternehmen sind im Einklang mit den vertraglichen Vereinbarungen des originären Auslagerungsvertrags zu treffen. Diese Anforderung wird man dahingehend verstehen müssen, dass die Informations- und Prüfungsrechte nicht nur zugunsten des Auslagerungsunternehmens, sondern unmittelbar (auch) zugunsten der Aufsicht und der Prüfer des auslagernden Instituts eingeräumt werden müssen.

Mit dem Finanzmarktintegritätsstärkungsgesetz wurde zum 1. Juli 2021 eine Regelung in das KWG eingeführt, dass die BaFin auch unmittelbar gegenüber Auslagerungsunternehmen Anordnungen treffen kann, um aufsichtsrechtliche Verstöße zu unterbinden oder Missstände zu beseitigen, und ein ausländisches Auslagerungsunternehmen bei wesentlichen Auslagerungen vertraglich verpflichtet werden muss, für Bekanntgaben und Zustellungen durch die BaFin einen inländischen Zustellungsbevollmächtigten zu benennen. Nicht zu unterschätzen ist auch die Vorgabe, Regelungen vorzusehen, das auslagernde Institut bei einer Rück- oder Weiterverlagerung zu unterstützen. Sowohl in Auslagerungsverträgen, die wesentliche Auslagerungen als auch solche die unwesentliche Auslagerungen betreffen, sind zudem bestimmte Sicherheitsanforderungen vertraglich zu vereinbaren. Diese Sicherheitsanforderungen umfassen Zugangsbestimmungen zu Räumen und Gebäuden sowie Zugriffsberechtigungen auf Softwarelösungen zum Schutz wesentlicher Daten und Informationen. Bestehende und in der Verhandlung befindliche Auslagerungsverträge müssen bis spätestens zum 31. Dezember 2022 angepasst werden.

Bestellung eines Auslagerungsbeauftragten

Der BaFin-Aufsicht unterliegende Institute müssen einen zentralen Auslagerungsbeauftragten bestellen. Dabei muss sichergestellt sein, dass dieser Auslagerungsbeauftragte durch ein zentrales Auslagerungsmanagement unterstützt wird. Personell ist bei der Auswahl des Auslagerungsbeauftragten darauf zu achten, dass dieser in einem Fachbereich tätig ist, der unmittelbar der Geschäftsführung untersteht.

In kleineren und weniger komplexen Instituten können auch Mitglieder der Geschäftsführung die Funktion und Aufgaben des Auslagerungsbeauftragten wahrnehmen. Allerdings muss in diesem Fall sichergestellt sein, dass die Aufgaben zwischen der Zuständigkeit für das Management der Auslagerungen und deren Kontrolle durch den Auslagerungsbeauftragten strikt voneinander getrennt sind. Der Auslagerungsbeauftragte hat mindestens einmal jährlich einen Bericht über wesentliche Auslagerungen zu erstellen und diesen der Geschäftsleitung zur Verfügung zu stellen. Auslagerungsbeauftragte müssen bis zum 31. Dezember 2021 bestellt werden.

Anlage und Führung eines Auslagerungsregisters

Alle von der BaFin beaufsichtigten Institute haben ein Auslagerungsregister zu führen, in dem Angaben zu sämtlichen wesentlichen und nicht wesentlichen Auslagerungen einschließlich der Auslagerungen innerhalb einer Institutsgruppe oder eines Finanzverbundes enthalten sein müssen. Welche Mindestangaben im Auslagerungsregister zu machen sind, ergibt sich für alle Auslagerungen aus Tz. 54 und für wesentliche Auslagerungen in Tz. 55 der EBA Leitlinien für Auslagerungen (EBA/GL/2019/02). In das Auslagerungsregister sind alle Auslagerungsvereinbarungen aufzunehmen; dies schließt auch Auslagerungsvereinbarungen innerhalb einer Institutsgruppe oder eines Finanzverbundes mit ein. Außerdem ist bei der Weiterverlagerung von wesentlichen Auslagerungen von dem auslagernden Institut zu bestimmen, ob der weiter zu verlagernde Teil wesentlich und dieser wesentliche Teil im Auslagerungsregister zu erfassen ist. Das Auslagerungsregister muss bis zum 31. Dezember 2021 angelegt werden, so dass dieses auf Verlangen der BaFin vorgelegt werden kann.

BAIT – IT-Notfallmanagement

Die Anforderungen aus der BAIT richten sich ebenfalls an Kredit- und Finanzdienstleistungsinstitute, die der Aufsicht der BaFin unterliegen. Neue Vorgaben ergeben sich aus der BAIT mit Blick auf Auslagerungen im Zusammenhang mit dem IT-Notfallmanagement.

Dieses in Ziffer 10 neu eingefügte Kapitel der BAIT sieht vor,

dass bei Auslagerungen von zeitkritischen Aktivitäten und Prozessen das auslagernde Institut und das Auslagerungsunternehmen über aufeinander abgestimmte Notfallkonzepte verfügen müssen, die hinsichtlich ihrer Wirksamkeit und Angemessenheit regelmäßig zu überprüfen sind (vgl. Ziffer 10.1). Diese Vorgabe ist unmittelbar von den Instituten umzusetzen. Eine Übergangsfrist sieht die BaFin als nicht erforderlich an, da durch die BAIT lediglich aufsichtliche Anforderungen konkretisiert wurden.

Welcher Handlungsbedarf ergibt sich für Zahlungs- und E-Geld-Institute aus dem ZAIT?

Die BaFin beaufsichtigt aktuell 80 Zahlungs- und E-Geld-Institute, die dem Zahlungsdiensteaufsichtsgesetz (ZAG) unterliegen. Auf diese Institute wandte die BaFin bislang die Anforderungen aus der BAIT sowie der MaRisk analog an. Mit dem an diese Institute adressierten ZAIT beabsichtigt die BaFin, die Anforderungen aus dem ZAG bezüglich IT und Cybersicherheit auf die individuellen Bedürfnisse der Zahlungs- und E-Geld-Institute zuzuschneiden.

Inhaltlich und vom Aufbau gibt es viele Parallelen zwischen den ZAIT und BAIT sowie zwischen MaRisk und ZAIT. Mit Blick auf Auslagerungen von IT-Prozessen und IT-Aktivitäten durch Zahlungs- und E-Geld-Institute gelten die Anforderungen aus der MaRisk. So müssen vertragliche Vereinbarungen mit Auslagerungsunternehmen ebenfalls bestimmten Mindestanforderungen genügen und ein Auslagerungsbeauftragter bestellt werden, der gegenüber der Geschäftsführung berichtspflichtig ist. Zudem haben die Institute ein jeweils aktuelles Auslagerungsregister vorzuhalten, in dem sämtliche Auslagerungsverträge aufgeführt werden.

Die Abgrenzung zwischen Fremdbezug von Software und Auslagerung wird spezifiziert. Bei Software, die zur Identifizierung, Beurteilung, Steuerung, Überwachung und Kommunikation der Risiken eingesetzt wird oder die für die Durchführung von zahlungsdienstegeschäftlichen Aufgaben von wesentlicher Bedeutung ist, sind Unterstützungsleistungen in Form von Betriebs-, Anpassungs-, Programmier- und Implementierungsleistungen auch als Auslagerung einzustufen. § 26 ZAG gibt bereits vor, dass die Informations- und Prüfungsrechte sowie Kontrollmöglichkeiten der BaFin sowie der Prüfer des Instituts in Bezug auf die ausgelagerten Aktivitäten und Prozesse auch bei einer Auslagerung auf ein Unternehmen mit Sitz im Ausland durch geeignete Vorkehrungen gewährleistet und dass zugunsten des Instituts entsprechende Weisungsrechte im Vertrag vereinbart sein müssen.

Konkret bedeutet dies, dass bei Auslagerungen an Unternehmen außerhalb des EWR sicherzustellen, dass das Auslagerungsunternehmen im Drittstaat beaufsichtigt wird und eine Kooperationsvereinbarung zwischen den beiden zuständigen Aufsichtsbehörden vorliegt, soweit es sich bei den ausgelagerten Aktivitäten um solche innerhalb des EWR zulassungs- oder registrierungspflichtige Aktivitäten handelt. Auch in das ZAG wurde mit dem Finanzmarktintegritätsstärkungsgesetz zum 1. Juli 2021 eine Neu-Regelung eingeführt, um der BaFin einen Durchgriff auch gegenüber in- und ausländischen Auslagerungsunternehmen zu ermöglichen. Über die Vorgaben der MaRisk (Tz. 9.10 d)) hinausgehend muss der Ort der Leistungserbringung (z. B. Stadt/ Anschrift) dem Institut jederzeit bekannt sein. Die Informations- und Prüfungsrechte umfassen auch die für den Zutritt, Zugang oder Zugriff erforderlichen Rechte. Ferner kann die interne Revision des auslagernden Instituts von eigenen Prüfungshandlungen absehen, sofern eine anderweitig durchgeführte Revisionstätigkeit, z. B. in Form von Group-Audits den aufsichtlichen Anforderungen genügt. Diese Erleichterungen können auch bei Auslagerungen auf so genannte Mehrmandantendienstleister in Anspruch genommen werden.

Die ZAIT stellen klar, dass auf eine explizite Vereinbarung von Weisungsrechten zugunsten des Instituts verzichtet werden kann, wenn die vom Auslagerungsunternehmen zu erbringende Leistung hinreichend klar im Auslagerungsvertrag spezifiziert ist. Da § 26 ZAG nur abstrakt von der Vereinbarung erforderlicher Weisungsrechte spricht und ein solches Weisungsrecht in die Dispositionsfreiheit des Dienstleisters erheblich eingreift, handelt es sich um eine höchst praxisrelevante Öffnung.

Die ZAIT sind mit ihrer Veröffentlichung am 16. August 2021 in Kraft getreten. Die BaFin hat den Zahlungs- und E-Geld-Instituten keine Übergangsfristen zur Umsetzung der Anforderungen eingeräumt. Dies begründet die BaFin damit, dass bereits zuvor bestehende aufsichtliche Anforderungen durch die ZAIT lediglich ergänzend interpretiert werden.

Da nach Aussage der BaFin in ihrem Anschreiben zu den ZAIT die Übergangsfristen aus den EBA-Leitlinien entsprechende Anwendung finden sollen, ist davon auszugehen, dass die die Zahlungs- und E-Geld-Institute die vertraglichen Anforderungen aus der ZAIT bis zum 31. Dezember 2021 umzusetzen

Ihre Ansprechpartner:

Dr. Stefanie Hellmich, LL.M.
Rechtsanwältin,
Partnerin
Frankfurt a.M.
T +49 69 27229 24118
stefanie.hellmich@luther-lawfirm.com

Dr. Michael Rath
Rechtsanwalt, Fachanwalt für IT-Recht,
Certified ISO/IEC 27001 Lead Auditor, Partner
Köln
T +49 221 9937 25795
michael.rath@luther-lawfirm.com

Dr. Rolf Kobabe
Rechtsanwalt, Sparkassenkaufmann
Partner
Hamburg
T +49 40 18067 24680
rolf.kobabe@luther-lawfirm.com

Pierre Daniel Wittmann
Rechtsanwalt,
Associate
Frankfurt a.M.
T +49 69 27229 24687
pierre.daniel.wittmann@luther-lawfirm.com