BaFin

Bundesanstalt für
Finanzdienstleistungsaufsicht

Aufsichtsmitteilung zu Auslagerungen an Cloud-Anbieter

Aktualisiert Februar 2024

Bankenaufsicht
Grundsatzreferat IT-Aufsicht und Aufsichtsunterstützung

Stand: Februar 2024

Inhaltsverzeichnis

I. Vorbemerkungen

In den vergangenen Jahren hat das Thema Auslagerung an Cloud-Anbieter im Finanzsektor stetig an Relevanz gewonnen. Entsprechend haben die BaFin und die Deutsche Bundesbank in den letzten Jahren mit beaufsichtigten Unternehmen vermehrt Gespräche über Auslagerungen an Cloud-Anbieter geführt. Gleichzeitig ist die deutsche Aufsicht auch mit verschiedenen Cloud-Anbietern in den Dialog eingetreten. Schwerpunkte dieser Gespräche waren dabei zunächst die Ausgestaltung der (Standard-)Verträge bzw. der vertraglichen Zusatzvereinbarungen, welche auch die aufsichtsrechtlich relevanten Vorgaben erfüllen und regeln sollen, z.B. Informations- und Prüfungsrechte der beaufsichtigten Unternehmen bzw. der Aufsicht. Darüber hinaus wurden in den Gesprächen zwischen Cloud-Anbietern, Cloud-Nutzern und der Aufsicht konkrete Herausforderungen bei der Cloud-Nutzung bspw. bezogen auf Weiterverlagerungen, Cloud-Betrieb, Nutzung von Prüfungsergebnissen Dritter, Aspekten des IT-Betriebs und der Abbildung von Cloud-Diensten in der Konfigurationsmanagementdatenbank (im Folgenden CMDB) thematisiert.[1]

Im Austausch mit der Aufsicht haben beaufsichtigte Unternehmen Herausforderungen zur Anwendungspraxis aufsichtsrechtlicher Anforderungen beschrieben, die sie insbesondere beim Einsatz führender Cloud-Anbieter sehen. Aus Sicht der beaufsichtigten Unternehmen beinhalten die Kerneigenschaften von Cloud-Anbietern, insbesondere der hohe Grad an Standardisierung und Virtualisierung, die globale Verfügbarkeit und hohe Skalierbarkeit eines technologisch sehr innovativen Dienstleistungsangebots sowie die hohe Konzentration auf wenige Cloud-Anbieter aus Drittstaaten, sowohl Chancen und Risiken. Einerseits machten Cloud-Anbieter üblicherweise aktuelle, marktführende technologische Innovationen für alle Kunden verfügbar. Zudem bestehe ein hohes Sicherheitsniveau. Andererseits schildern die beaufsichtigten Unternehmen operative Schwierigkeiten bei der Prüfbarkeit des Cloud-Anbieters zum Nachweis der angemessenen und wirksamen Umsetzung von Sicherheits- und Compliance-Anforderungen. Zudem sei eine geringe Flexibilität der Cloud-Anbieter durch die hohe Standardisierung des Leistungsangebots und der Leistungserbringungsprozesse zu beobachten. Dies bedeutet, dass das Leistungsangebot und die Art der Leistungserbringung durch einzelne beaufsichtigte Unternehmen kaum beeinflussbar seien. Auch individuelle Vereinbarungen bei der Vertragsgestaltung seien nicht oder nur in geringem Umfang möglich. Ebenso habe die, im Vergleich mit etablierten Anbietern im Finanzsektor, hohe Anpassungsfrequenz beim Dienstleistungsangebot der Cloud-Anbieter Auswirkungen auf interne Prozesse.

Auch die regulatorischen Anforderungen haben sich in den letzten Jahren weiterentwickelt. Mit dem Gesetz zur Stärkung der Finanzmarktintegrität wurden unter anderem eine Pflicht zur Anzeige von (wesentlichen) Auslagerungen und zur Führung eines internen Auslagerungsregisters im Kreditwesengesetz (KWG), Zahlungsdiensteaufsichtsgesetz (ZAG), Wertpapierinstitutsgesetz (WpIG) und Kapitalanlagegesetzbuch (KAGB) eingeführt bzw. erweitert. Diese sehen auch Informationsabfragen speziell zu Auslagerungen an Cloud-Anbieter vor.

[1] Vgl. Protokolle veröffentlicht auf: https://www.bafin.de/DE/Aufsicht/BankenFinanzdienstleister/Fachgremien/IT/informationstechnologie_node.html oder https://www.bundesbank.de/de/aufgaben/bankenaufsicht/einzelaspekte/fachgremien/fachgremium-informationstechnologie-598056

Die konkreten Details zur Anzeigepflicht werden in Anzeigeverordnungen geregelt, die auf der Internetseite der BaFin veröffentlicht sind.

Auch auf europäischer Ebene steht das Thema weiterhin im aufsichtlichen Fokus. Auf Ebene von EIOPA, ESMA und EBA, innerhalb des SSM, aber auch bilateral zwischen den nationalen Aufsichtsbehörden hat sich ein stetiger Austausch über den Umgang mit Auslagerungen an Cloud-Anbieter entwickelt. Ergebnis dieses Austauschs sind die EBA Leitlinien zu Auslagerungen (EBA/GL/2019/02 vom 25. Februar 2019), die EIOPA Leitlinien zum Outsourcing an Cloud-Anbieter (EIOPA-BoS-20-002 vom 6. Februar 2020) und die ESMA Leitlinien zur Auslagerung an Cloud-Anbieter (ESMA50-164-4285 vom 10. Mai 2021).

Diese Aufsichtsmitteilung ist als Orientierungshilfe zu verstehen, in der BaFin und die Deutsche Bundesbank ihre gemeinsame Einschätzung zu Auslagerungen an Cloud-Anbieter mitteilen. Durch sie werden allerdings keine neuen Anforderungen gestellt, sondern die derzeitige aufsichtliche Einschätzung in solchen Auslagerungsfällen wiedergegeben. Durch die Aufsichtsmitteilung soll insbesondere die aufsichtliche Bewertung zu verschiedenen Formulierungen in Vertragsklauseln transparent gemacht sowie Hinweise zur Überwachung und Kontrolle von Cloud-Auslagerungen und zu den durch die beaufsichtigten Unternehmen sicherzustellenden Anforderungen gegeben werden. Darüber hinaus gibt die Aufsichtsmitteilung einen Ausblick auf die Anforderungen an vertragliche Vereinbarungen über die Nutzung von Informations- und Kommunikationstechnologien (IKT) zwischen beaufsichtigten Unternehmen und IKT-Drittdienstleistern, die in der Verordnung des Europäischen Parlaments und des Rates über die digitale Resilienz im Finanzsektor (Digital Operational Resilience Act – DORA) geregelt sind. Am 16. Januar 2023 ist DORA in Kraft getreten und ist ab dem 17. Januar 2025 direkt anzuwenden.

Der deutschen Aufsicht sind weder alle Arten von Cloud-Auslagerungen noch alle (Standard-)Verträge bzw. vertraglichen Zusatzvereinbarungen bekannt, sodass die Aufsichtsmitteilung keinen Anspruch auf Vollständigkeit erhebt.

Die Aufsichtsmitteilung richtet sich an die im Finanzsektor beaufsichtigten Unternehmen (u.a. Kreditinstitute, Finanzdienstleistungsinstitute, Versicherungsunternehmen, Einrichtungen der betrieblichen Altersversorgung, Pensionsfonds, Wertpapierinstitute, sonstige Wertpapierdienstleistungsunternehmen, Kapitalverwaltungsgesellschaften, Zahlungsinstitute und E-Geld-Institute). Die nachfolgenden Ausführungen sind daher im Kontext der jeweils geltenden aufsichtsrechtlichen Anforderungen zu lesen.

Aufgrund des Charakters der Aufsichtsmitteilung werden im Folgenden bewusst „Soll-Formulierungen" verwendet. Dies führt ausdrücklich nicht zu einer Abschwächung der bestehenden aufsichtsrechtlichen Anforderungen; die Anforderungen an Auslagerungen und an die IT bleiben unberührt. Das für diese Anforderungen geltende Proportionalitätsprinzip gilt auch für die in dieser Aufsichtsmitteilung formulierten Hilfestellungen. Eine Auslagerung darf nicht zu einer Übertragung der Verantwortung der Geschäftsleiter des beaufsichtigten Unternehmens für die ausgelagerten Sachverhalte an den Cloud-Anbieter führen. Das beaufsichtigte Unternehmen bleibt bei einer Auslagerung für die Einhaltung der von ihm zu beachtenden gesetzlichen Bestimmungen verantwortlich.

Ausblick DORA

Digital Operational Resilience Act
Künftig wird auch die Verordnung (EU) 2022/2554 des Europäischen Parlaments und des Rates über die digitale operationale Resilienz im Finanzsektor (Digital Operational Resilience Act – DORA) als Bestandteil des Informations- und Kommunikationstechnologien (IKT)-Drittparteirisikomanagements konkrete Vorgaben an vertragliche Vereinbarungen über die Nutzung von IKT-Dienstleistungen zwischen Finanzunternehmen (vgl. Art. 2 Abs. 2 DORA) und IKT-Drittdienstleistern aufstellen und sektorübergreifend regeln. DORA ist am 16. Januar 2023 in Kraft getreten und ist ab dem 17. Januar 2025 direkt anzuwenden. Neben Regelungen zum IKT-Drittparteirisikomanagement wird DORA insbesondere Regelungen im Bereich IKT-Governance und IKT-Risikomanagement, Testen der digitalen operationalen Resilienz, Meldewesen für schwerwiegende IKT-Vorfälle sowie hinsichtlich eines europäischen Überwachungsrahmenwerks für kritische IKT-Drittdienstleister enthalten. Die in DORA getroffenen Regelungen werden den bestehenden Regelungen als lex specialis vorgehen oder diese ergänzen.

DORA enthält mehrere Ermächtigungsgrundlagen zum Erlass delegierter Rechtsakte, Technischer Regulierungsstandards (regulatory technical standard – RTS), Technischer Durchführungsstandards (implementing technical standard – ITS), Leitlinien und Berichte zur Ergänzung der in DORA aufgestellten Prinzipien und getroffenen Regelungen, aus denen sich konkretisierte Anforderungen ergeben.

In Vorbereitung auf DORA bietet es sich an, bei Änderungen von Geschäftsabläufen und der Ausverhandlung neuer Verträge zur Auslagerung in die Cloud, die neuen zusätzlichen Bestimmungen durch DORA zu berücksichtigen.

II. Erläuterungen

Der Begriff „**Auslagerung**" wird in dieser Aufsichtsmitteilung für „Auslagerungen" im Sinne des § 25b Kreditwesengesetz (KWG), § 40 Wertpapierinstitutsgesetz (WpIG), § 80 Wertpapierhandelsgesetz (WpHG), § 26 Zahlungsdiensteaufsichtsgesetz (ZAG) und § 36 Kapitalanlagegesetzbuch (KAGB) und „Ausgliederungen" im Sinne des Artikels 274 Delegierte Verordnung (EU) 2015/35 sowie § 32 Versicherungsaufsichtsgesetz (VAG) verwendet. Mit dem Begriff „Weiterverlagerungen" wird analog verfahren.

Im Folgenden wird der Begriff „**wesentlich**" für die Begrifflichkeiten „wichtig/kritisch" im Sinne des Artikels 274 Delegierte Verordnung (EU) 2015/35 und des § 32 VAG verwendet sowie für den Begriff „wesentlich" im Sinne des § 25b KWG, § 26 ZAG und § 40 WpIG.

Der Begriff „**Sachverhalte**" wird zusammenfassend für die „Aktivitäten und Prozesse" im Sinne des § 25b KWG, § 26 ZAG bzw. „wichtigen Funktionen/Versicherungstätigkeiten" im Sinne des Artikels 274 Delegierte Verordnung (EU) 2015/35 und des § 32 VAG sowie „Aufgaben" im Sinne des § 36 KAGB verwendet.

Die Begriffe „**Cloud-Umgebung**" und „**Cloud-Anwendung**" werden in dieser Aufsichtsmitteilung wie folgt verwendet: Cloud-Umgebungen sind von den Cloud-Anbietern zur Verfügung gestellte mandantenfähige und vom beaufsichtigten Unternehmen in weiten Teilen konfigurierbare Ressourcen, in denen einzelne Cloud-Dienste des Cloud-Anbieters genutzt werden können. Bei Cloud-Anwendungen handelt es sich um Anwendungsprogramme, die auf den durch die Cloud-Anbieter bereitgestellten Cloud-Diensten basieren, jedoch außerhalb der Betriebsverantwortung des Cloud-Anbieters liegen.

„Cloud-Dienste" sind Dienste, die mithilfe von Cloud-Computing erbracht werden, d.h. einem Modell, das ortsunabhängigen, komfortablen und bedarfsgesteuerten Netzwerkzugriff auf einen gemeinsamen Pool konfigurierbarer Rechenressourcen ermöglicht (wie Netzwerke, Server, Speicher, Anwendungen und Services) und sich schnell sowie mit minimalem Verwaltungsaufwand oder geringer Interaktion des Dienstleisters bereitstellen lässt.[2]

Cloud-Dienste werden in der Regel als folgende Dienstleistungsmodelle zur Verfügung gestellt:

- Infrastructure as a Service **(IaaS,** Bereitstellung von Rechenleistungen und Speicherplatz),
- Platform as a Service **(PaaS,** Bereitstellung von Entwicklerplattformen) oder
- Software as a Service **(SaaS,** Bereitstellung von Softwareapplikationen/ Webanwendungen).

Diese Dienstleistungsmodelle unterscheiden sich hinsichtlich der organisatorischen bzw. technischen Kontrollmöglichkeiten des Nutzers. Bei IaaS hat der Nutzer die volle Kontrolle über das IT-System vom Betriebssystem aufwärts (d. h. die Kontrolle für die physikalische Umgebung liegt immer beim Anbieter), da alles innerhalb seines Zuständigkeitsbereichs betrieben wird, bei PaaS hat der Nutzer nur noch die Kontrolle über seine Anwendungen, die

[2] EBA/GL/2019/02, Tz. 12 (Begriffsbestimmungen).

auf der Plattform laufen, und bei SaaS übergibt der Nutzer praktisch die ganze Kontrolle an den Cloud-Anbieter.[3] Je höher die Komplexität des Dienstleistungsmodells desto geringer sind somit in der Regel die Kontrollmöglichkeiten des Nutzers in der Cloud. Der Verlust von Kontrollmöglichkeiten durch das beaufsichtigte Unternehmen ändert jedoch nicht dessen aufsichtsrechtliche Verantwortlichkeit hinsichtlich der Einhaltung gesetzlicher Bestimmungen. In der Praxis wird zudem nach vier Bereitstellungsmodellen von Cloud-Diensten unterschieden[4]:

- **Private Cloud:** Cloud-Infrastruktur, die ausschließlich von einem einzelnen Unternehmen genutzt werden kann.
- **Community Cloud:** Cloud-Infrastruktur, die ausschließlich von einer konkreten Unternehmensgemeinschaft genutzt werden kann, einschließlich mehrerer beaufsichtigter Unternehmen einer einzelnen Gruppe.
- **Public Cloud:** Cloud-Infrastruktur, die von der Öffentlichkeit frei genutzt werden kann.
- **Hybrid Cloud:** Cloud-Infrastruktur, die sich aus zwei oder mehreren speziellen Cloud-Infrastrukturen zusammensetzt.

In Abhängigkeit vom gewählten Dienstleistungsmodell besteht zwischen beaufsichtigtem Unternehmen und Cloud-Anbieter eine Arbeitsteilung bezogen auf die Zuständigkeit für den Betrieb der Cloud. Je nach gewähltem Cloud-Dienst und Dienstleistungsmodell liegt die Abgrenzung der Zuständigkeiten in dem abstrakten Schichtenmodell an unterschiedlichen Stellen (sog. Abstraktionsgrenze).[5]

[3] Vgl. https://www.bsi.bund.de/dok/6622124
[4] EBA/GL/2019/02, Tz. 12 (Begriffsbestimmungen).
[5] Siehe dazu auch Kapitel V.1

Die folgenden Ausführungen sind unabhängig vom gewählten Dienstleistungs- bzw. Bereitstellungsmodell:

Ausblick DORA

IKT-Dienstleistungen

DORA definiert den Begriff der IKT-Dienstleistung in Art. 3 Abs. 21 als digitale Dienste und Datendienste, die über IKT-Systeme einem oder mehreren internen oder externen Nutzern dauerhaft bereitgestellt werden. Unter DORA wird nicht mehr zwischen „Auslagerung" und „sonstigem Fremdbezug (von IT-Dienstleistungen)" differenziert.

Kritische oder wichtige Funktion

DORA enthält besondere Vorgaben für die Nutzung von IKT-Dienstleistungen zur Unterstützung „kritischer oder wichtiger Funktionen" im Sinne des Art. 3 Abs. 22. Dies sind Funktionen,

- deren Ausfall die finanzielle Leistungsfähigkeit, die Solidität oder Fortführung der Geschäftstätigkeiten und Dienstleistungen oder
- deren unterbrochene, fehlerhafte oder unterbliebene Leistung die fortdauernde Einhaltung der Zulassungsbedingungen und -verpflichtungen eines Finanzunternehmens oder seiner sonstigen Verpflichtungen nach dem anwendbaren Finanzdienstleistungsrecht

erheblich beeinträchtigen würde.

In Vorbereitung auf DORA bietet es sich an, die Auswirkungen der IKT-Dienstleistung auf die finanzielle Leistungsfähigkeit, die Solidität oder Fortführung der Geschäftstätigkeiten und Dienstleistungen sowie die fortdauernde Einhaltung der Zulassungsbedingungen und -verpflichtungen des Finanzunternehmens oder seiner sonstigen Verpflichtungen nach den anwendbaren Finanzdienstleistungsrechtsvorschriften im Rahmen der Risikoanalyse stärker zu gewichten.

III. Vorbereitende Handlungen und Governance-Rahmen für die Cloud

1. Strategische Überlegungen

Das beaufsichtigte Unternehmen soll Überlegungen zur Nutzung von Cloud-Diensten in seiner (IT-)Strategie abbilden. Daneben soll es einen Prozess entwickeln und dokumentieren, der alle für die Auslagerung an den Cloud-Anbieter relevanten Schritte von der Strategie über die Migration in die Cloud bis hin zur Ausstiegsstrategie abdeckt. Es ist wichtig, dass das beaufsichtigte Unternehmen zuerst alle relevanten internen Prozesse dahingehend überprüft, ob diese für „die Cloud" bereit sind, bevor es eine solche Auslagerung vornimmt. Dabei sollen neben den auszulagernden Sachverhalten vor allem die Risikomanagement- und -steuerungsprozesse des beaufsichtigten Unternehmens betrachtet werden.

2. Analyse und Wesentlichkeitsbewertung

Nach der strategischen Entscheidung für den Drittbezug von Sachverhalten von einem Cloud-Anbieter soll zu Beginn des Prozesses in einer Einzelfallbetrachtung anhand der jeweils geltenden aufsichtsrechtlichen Anforderungen von dem beaufsichtigten Unternehmen geprüft werden, ob eine Auslagerung vorliegt und ob sie als wesentlich einzustufen ist.[6] In der Regel sind die Voraussetzungen einer Auslagerung erfüllt. Bei der Risikoanalyse sollen alle für das beaufsichtigte Unternehmen relevanten Aspekte im Zusammenhang mit der Auslagerung auf Cloud-Anbieter berücksichtigt werden, wobei die Intensität der Analyse von Art, Umfang, Komplexität und Risikogehalt der ausgelagerten Sachverhalte abhängt. Das beaufsichtigte Unternehmen soll anhand der Risikoanalyse bewerten und dokumentieren, welche Risiken mit einer Auslagerung verbunden sind und ob es sich um eine wesentliche Auslagerung handelt. Sofern aufsichtsrechtliche Anforderungen zur Wesentlichkeit vorliegen, sind diese zu beachten.

Im Rahmen der **Risikoanalyse** soll grundsätzlich Folgendes betrachtet werden:

- die Ausgestaltung des genutzten Cloud-Dienstes,
- die Auswirkung einer nicht angemessenen Dienstleistungsgüte (Solidität oder Fortführung der Geschäftstätigkeiten),
- die Kritikalität des auszulagernden Sachverhalts, d.h. eine Beurteilung, ob der Sachverhalt für die Geschäftsfortführung des beaufsichtigten Unternehmens kritisch ist,
- eine Bewertung der Risiken, die sich aus dem gewählten Dienstleistungs- sowie Bereitstellungsmodell ergeben,

[6] Sofern dieses Vorgehen in den jeweiligen aufsichtsrechtlichen Vorgaben angelegt ist. Eine Ausnahme bilden beispielsweise die nicht differenzierten Auslagerungen gemäß KAGB.

- eine Bewertung der finanziellen, operationellen (z.B. Systemausfall, Sabotage) Risiken, einschließlich der rechtlichen Risiken (z. B. Risiken der Rechtsdurchsetzung, datenschutzrechtliche Risiken) sowie Reputationsrisiken und Risiken, die die finanzielle Leistungsfähigkeit beeinträchtigen können,

- eine Bewertung der Eignung des Cloud-Anbieters (Fähigkeiten, Infrastruktur, wirtschaftliche Situation, gesellschaftsrechtlicher und regulatorischer Status, etc.); soweit sinnvoll können hierfür Nachweise/Zertifikate auf Basis gängiger Standards (z.B. Internationaler Sicherheitsstandard ISO/IEC 2700X der International Organization for Standardization, C 5-Anforderungskatalog des Bundesamtes für Sicherheit in der Informationstechnik), Prüfberichte anerkannter Dritter oder interne Prüfberichte des Cloud-Anbieters herangezogen werden,

- eine Bewertung der Konzentrationsrisiken, darunter auch der Risiken im Falle der Auslagerung mehrerer Sachverhalte an einen Cloud-Anbieter,

- eine Bewertung der Risiken bei Nichteinhaltung regulatorischer und abwicklungsrechtlichen Anforderungen (fortdauernde Einhaltung der Zulassungsbedingungen und -verpflichtungen des Finanzunternehmens oder seiner sonstigen Verpflichtungen nach dem anwendbaren Finanzdienstleistungsrecht, Gewährleistung der Datenverfügbarkeit inkl. Zugriff) und eine Bewertung der Risiken, die mit Aufsichtsbeschränkungen in den Ländern einhergehen, in denen die Sachverhalte erbracht oder die Daten gespeichert oder verarbeitet werden,

- eine Bewertung des Standorts, an dem Daten gespeichert oder verarbeitet werden, des Standorts des Unternehmenssitzes des Cloud-Anbieters, der geopolitischen Lage (allgemeine Stabilität von Politik und Sicherheit) und der anwendbaren Gesetze (einschließlich Gesetze zum Datenschutz) in den betreffenden Gerichtsbarkeiten, sowie der in diesen Gerichtsbarkeiten geltenden Vorschriften zur Rechtsdurchsetzung, einschließlich bei einem Ausfall des Cloud-Anbieters greifender insolvenzrechtlicher Vorschriften,

- eine Bewertung der Risiken für die Integrität, Verfügbarkeit, Vertraulichkeit und Authentizität der Sachverhalte sowie der verarbeiteten oder gespeicherten Daten unter Berücksichtigung von

    - etwaigen Zugriffsmöglichkeiten auf Daten durch andere Jurisdiktionen,

    - Risiken durch unterschiedliche Schnittstellen zwischen eigenen und fremden Systemen,

    - Risiken infolge außerordentlicher, auch unbeabsichtigter und unerwarteter Vertragsbeendigung z.B. Datenverlust, eingeschränkte Übertragbarkeit der Daten auf einen neuen Dienstleister,

- eine Bewertung der Risiken aus Weiterverlagerungen durch den Cloud-Anbieter.

Im Falle des Bekanntwerdens wesentlicher Mängel sowie wesentlicher Änderungen der Auslagerung, ist zu beachten, dass dies Auswirkungen auf die Risikosituation der Auslagerung und somit des auslagernden Unternehmens haben kann. In diesen Fällen soll die Risikoanalyse,

unabhängig vom Regelturnus, mindestens überprüft oder neu durchgeführt werden sowie ggf. die Auslagerung an den Cloud-Anbieter rückabgewickelt bzw. an einen Alternativanbieter initiiert werden.

3. Interne Vorgaben für die Nutzung der Cloud

Das beaufsichtigte Unternehmen soll für die Nutzung der Cloud, sowohl mit Blick auf die Entwicklung von Cloud-Anwendungen, als auch für den Betrieb, geeignete Vorgaben in seiner schriftlich fixierten Ordnung ergänzen. Dabei soll, soweit sinnvoll, zwischen allgemein gültigen Anforderungen für alle Anwendungen und Anbieter sowie spezifischen Regelungen bezogen auf die Besonderheiten der einzelnen Cloud-Anbieter und ihrer Cloud-Dienste unterschieden werden.

In Bezug auf die allgemeinen Anforderungen soll das beaufsichtigte Unternehmen geeignete Vorgaben formulieren, die im Einklang mit der (IT-)Strategie des beaufsichtigten Unternehmens und dessen Leit- und Richtlinien zur Informationssicherheit und der IT stehen. Anbieter- und servicespezifische Regelungen sollen auf Basis der Risikoanalyse, Hinweise der Cloud-Anbieter, eigener Maßnahmen zur Risikoreduktion und weiteren Erkenntnissen abgeleitet werden. Inkonsistenzen zu den allgemeinen Anforderungen sollen vermieden werden. Dabei sollen insbesondere risikobasierte Vorgaben zur Nutzung der Cloud in Abhängigkeit vom Schutzbedarf der Daten sowie des Orts der Speicherung und Verarbeitung getroffen werden.

Die Vorgaben zur Cloud-Nutzung sollen entsprechend der einschlägigen Rundschreiben[7] zumindest die Themen Cloud-Compliance, Identitäts- und Rechtemanagement, Verschlüsselung und Schlüsselverwaltung, Entwicklung und Betrieb, Härtung der Anwendungen, Schnittstellen und Umgebungen, Steuerung von Subunternehmen und IT-Notfallmanagement umfassen.

4. Ressourcenausstattung und Qualifikation

Beaufsichtigte Unternehmen sollen für die Nutzung der Cloud hinreichende quantitative und qualitative Ressourcen bereitstellen und organisatorisch verankern (personelle, finanzielle und sonstige Ressourcen). Dies betrifft insbesondere Governance, Risikomanagement und Auslagerungsmanagement. Hierbei sind die Überwachung, Kontrolle und Prüfung von Cloud-Auslagerungen sowie Entwicklung, Betrieb und Sicherheit von Cloud-Anwendungen und Cloud-Umgebungen angemessen zu berücksichtigen.

Personen, die mit Aufgaben im Cloud-Umfeld betraut sind, sollen angemessene und einschlägige Kompetenzen und Kenntnisse über die Funktionsweise der Cloud, der mit ihr verbundenen Risiken sowie der mit dem Cloud-Betrieb verbundenen technischen und organisatorischen Besonderheiten haben.

[7] Rundschreiben 05/2023 (BA) – Mindestanforderungen an das Risikomanagement (MaRisk) vom 29.06.2023; Rundschreiben 10/2017 (BA) in der Fassung vom 16.08.2021 – Bankaufsichtliche Anforderungen an die IT (BAIT); Rundschreiben 11/2021 (BA) in der Fassung vom 16.08.2021 – Zahlungsdiensteaufsichtliche Anforderungen an die IT von Zahlungs- und E-Geld-Instituten (ZAIT); Rundschreiben 10/2018 (VA) in der Fassung vom 03.03.2022 – Versicherungsaufsichtliche Anforderungen an die IT (VAIT); Rundschreiben 11/2019 (WA) – Kapitalverwaltungsaufsichtliche Anforderungen an die IT (KAIT) vom 01.10.2019.

Der Umfang der notwendigen Kenntnisse hängt von den durch die Person zu erfüllenden Aufgaben ab. Je technischer die Aufgaben, desto spezifischer soll das Wissen zu dem Cloud-Anbieter und den Cloud-Diensten sein. Die notwendigen Kenntnisse können durch Schulungsnachweise, Teilnahme an relevanten Fortbildungsmaßnahmen oder einschlägige Praxiserfahrung nachgewiesen werden.

5. Vertragsgestaltung bei (wesentlicher) Auslagerung

Abhängig von den aufsichtsrechtlichen Anforderungen sollen bei wesentlichen Auslagerungen bzw. bei den nicht differenzierten Auslagerungen gemäß KAGB im Auslagerungsvertrag insbesondere nachfolgende Inhalte vereinbart werden.

> Ausblick DORA
>
> **Verpflichtende Vertragsbestimmungen für alle IKT-Dienstleistungen**
>
> Art. 28 Abs. 7 und Art. 30 DORA stellen Mindestanforderungen für die Ausgestaltung von vertraglichen Vereinbarungen über die Nutzung von IKT-Dienstleistungen zwischen Finanzunternehmen und IKT-Drittdienstleistern auf. Deren Berücksichtigung ist auch bereits in den Vertragsverhandlungen und -ausgestaltungen vor Inkrafttreten von DORA sinnvoll. DORA beinhaltet generelle Prinzipien und verpflichtende Vertragsbestimmungen für vertragliche Vereinbarungen über die Nutzung von IKT-Dienstleistungen. Für IKT-Dienstleistungen zur Unterstützung kritischer oder wichtiger Funktionen kommen zusätzliche Mindestanforderungen hinzu.

5.1 Leistungsgegenstand

Im Vertrag soll eine Spezifizierung und ggf. Abgrenzung der vom Cloud-Anbieter zu erbringenden Leistung erfolgen. Dabei soll grundsätzlich Folgendes festgelegt werden:

- der auszulagernde Sachverhalt und dessen Umsetzung (z.B. Art des Dienstleistungs- und Bereitstellungsmodells, Umfang der angebotenen Dienste wie etwa Rechenleistung oder zur Verfügung stehender Speicherplatz, Verfügbarkeitsanforderungen, Reaktionszeiten),
- Anpassungsmöglichkeiten der Dienstleistung für den Fall einer Bedarfsänderung während der Vertragslaufzeit, z. B. die Hinzunahme zusätzlicher Sicherheitsmaßnahmen bei Änderung des Schutzbedarfes oder eine Anpassung des vom Dienstleister zugesagten Leistungsniveaus an die Bedarfsmeldungen aus dem Leistungs- und Kapazitätsmanagement
- Unterstützungsleistungen (Support),
- Zuständigkeiten, Mitwirkungs- und Bereitstellungspflichten (z.B. bei Updates),
- Ort der Leistungserbringung, der Datenverarbeitung und der Datenspeicherung (z.B. Standorte der Rechenzentren),

- Beginn und gegebenenfalls Ende des Auslagerungsvertrags,
- Kennzahlen zur fortlaufenden Überprüfung der Dienstleistungsgüte, dabei sollen, soweit möglich, quantitative Kennzahlen herangezogen werden, sowie
- Indikatoren zur Erkennung einer unannehmbaren Dienstleistungsgüte, z.B. bezogen auf Nichtverfügbarkeit und Datenverlust.

Diese Aspekte können für die genutzten Cloud-Dienste spezifisch ausgestaltet werden.

> Ausblick DORA
>
> **Beschreibung aller Funktionen und IKT-Dienstleistungen**
>
> Nach Art. 30 Abs. 2 lit. a DORA sind Finanzunternehmen und IKT-Drittdienstleister dazu verpflichtet, eine klare und vollständige Beschreibung aller Funktionen und IKT-Dienstleistungen als Vertragselement zu vereinbaren. Dies gilt unabhängig davon, ob es sich um IKT-Dienstleistungen zur Unterstützung kritischer oder wichtiger Funktionen handelt.

5.2 Informations- und Prüfungsrechte des beaufsichtigten Unternehmens

Informations- und Prüfungsrechte sowie Kontrollmöglichkeiten des beaufsichtigten Unternehmens dürfen vertraglich nicht eingeschränkt werden. Es ist sicherzustellen, dass das beaufsichtigte Unternehmen zeitnah diejenigen Informationen erhält, die es für die angemessene Steuerung und Überwachung der mit der Auslagerung verbundenen Risiken benötigt. Diese Informationen sollen vom beaufsichtigten Unternehmen grundsätzlich mindestens fünf Jahre aufbewahrt werden.

Zur Gewährleistung der Informations-und Prüfungsrechte soll insbesondere Folgendes vertraglich vereinbart werden:

- die Gewährung uneingeschränkten Zugriffs auf Informationen und Daten sowie Zutritts zu den Geschäftsräumen des Cloud-Anbieters, einschließlich aller Rechenzentren, Geräte, Systeme und Netzwerke, die zur Erbringung der ausgelagerten Sachverhalte eingesetzt werden; hierzu gehören die damit in Zusammenhang stehenden Prozesse und Kontrollen,
- effektive Kontroll- und Prüfungsmöglichkeiten sowie die Möglichkeit der Durchführung von Vor-Ort-Prüfungen beim Cloud-Anbieter.

Bezogen auf wesentliche Weiterverlagerungen soll sichergestellt werden, dass gleichwertige Informations- und Prüfungsrechte für die gesamte Auslagerungskette vereinbart sind.

5.2.1 Keine (mittelbare) Einschränkung der Rechte

Die wirksame Ausübung der Informations- und Prüfungsrechte darf nicht durch Vertragsvereinbarungen eingeschränkt werden. Als eine unzulässige Einschränkung der Informations- und Prüfungsrechte beurteilt die deutsche Aufsicht insbesondere Vereinbarungen, die diese Rechte nur unter bestimmten Voraussetzungen gewähren.

Hierzu gehören insbesondere:

- die Vereinbarung gestufter Informations- und Prüfungsverfahren, z.B. die Verpflichtung, zunächst auf die Prüfungsberichte, Zertifikate oder sonstige Nachweise der Einhaltung anerkannter Standards durch den Cloud-Anbieter zurückzugreifen, bevor das beaufsichtigte Unternehmen eigene Prüfungshandlungen durchführen kann,

- eine Beschränkung der Erfüllung der Informations- und Prüfungsrechte auf die Vorlage von Prüfungsberichten, Zertifikaten oder sonstigen Nachweisen der Einhaltung anerkannter Standards durch den Cloud-Anbieter,

- eine Verknüpfung des Zugangs zu Informationen an die vorherige Teilnahme an speziellen Schulungsprogrammen,

- die Formulierung einer Klausel, in der die Durchführung einer Prüfung von der wirtschaftlichen Zumutbarkeit (commercially reasonable) abhängig gemacht wird,

- eine zeitliche und personelle Beschränkung der Durchführung von Prüfungen, wobei eine Beschränkung des Zugangs auf die üblichen Geschäftszeiten nach vorheriger Anmeldung in der Regel vertretbar ist,

- ein Verweis auf die alleinige Nutzung etwa von Managementkonsolen zur Ausübung der Informations- und Prüfungsrechte des Unternehmens,

- eine Vorgabe des Ablaufs sowie des Umfangs der Ausübung der Informations- und Prüfungsrechte durch den Cloud-Anbieter

- ein Verweis auf interne Umsetzungsrichtlinien des Cloud-Anbieters, die Einschränkungen der vertraglich vereinbarten Rechte vorsehen, und

- Kosten, die aufgrund ihrer Höhe eine Ausübung der Informations- und Prüfungsrechte einschränken oder behindern könnten. Gleiches gilt für den lediglich ortsgebundenen Zugriff auf Informationen und Dokumente.

5.2.2 Alternative Prüfungsansätze

Abhängig von den einschlägigen aufsichtsrechtlichen Vorgaben können die beaufsichtigten Unternehmen alternative Prüfungsansätze in Anspruch nehmen, um ihre Prüfungshandlungen effizienter zu gestalten.[8] Sollte das beaufsichtigte Unternehmen beabsichtigen, diese alternativen Prüfungsansätze zu nutzen, so sind sie in geeigneter Form bei der Vertragsgestaltung mit dem Cloud-Anbieter zu berücksichtigen.

Nimmt ein beaufsichtigtes Unternehmen einen der in Kapitel V.4.2 genannten alternativen Prüfungsansätze in Anspruch, darf dies nicht zur Einschränkung seiner Informations- und Prüfungsrechte führen. Gleichwohl darf das beaufsichtigte Unternehmen nicht durch den Cloud-Anbieter verpflichtet werden, einen der alternativen Prüfungsansätze wahrzunehmen.

> Ausblick DORA
>
> **Ausnahme für Kleinstunternehmen**
> Nach Art. 30 Abs. 3 Satz 2 DORA können der IKT-Drittdienstleister und das Kleinstunternehmen (vgl. Art. 3 Abs. 60 DORA) vereinbaren, dass die Zugangs-, Inspektions- und Auditrechte des Finanzunternehmens auf einen vom IKT-Drittdienstleister benannten unabhängigen Dritten übertragen werden können. Das Finanzunternehmen soll dann aber von dem Dritten jederzeit Informationen und Gewähr in Bezug auf die Dienstleistungen verlangen können.

5.3 Informations- und Prüfungsrechte der Aufsicht

Informations- und Prüfungsrechte sowie Kontrollmöglichkeiten der Aufsicht dürfen vertraglich oder durch interne Umsetzungsrichtlinien des Cloud-Anbieters nicht eingeschränkt werden. Die Aufsicht muss den ausgelagerten Sachverhalt beim Cloud-Anbieter genauso kontrollieren können, wie sie dies nach den jeweils einschlägigen Gesetzen beim beaufsichtigten Unternehmen vornehmen würde. Demnach muss vertraglich vereinbart werden, dass die Aufsicht ihre Informations- und Prüfungsrechte sowie Kontrollmöglichkeiten auch im Hinblick auf den ausgelagerten Sachverhalt ordnungsgemäß und uneingeschränkt ausüben kann; dies gilt zudem für diejenigen Personen, deren sich die Aufsicht bei der Durchführung von Prüfungen bedient. Insbesondere soll es der Aufsicht möglich sein, zumindest auch für einen Zeitraum von fünf Jahren nach Vertragsbeendigung, Informations- und Prüfungsrechte auszuüben.

Zur Gewährleistung der Informations- und Prüfungsrechte der Aufsicht soll insbesondere Folgendes vertraglich vereinbart werden:

- die Verpflichtung des Cloud-Anbieters zur uneingeschränkten Zusammenarbeit mit der Aufsicht,
- die Gewährung uneingeschränkten Zugriffs auf Informationen und Daten sowie Zutritts zu den Geschäftsräumen des Cloud-Anbieters, einschließlich aller Rechenzentren, Geräte,

[8] Siehe dazu auch Kapitel V.4.2.

Systeme und Netzwerke, die zur Erbringung der ausgelagerten Sachverhalte eingesetzt werden; hierzu gehören die damit in Zusammenhang stehenden Prozesse und Kontrollen,

- effektive Kontroll- und Prüfungsmöglichkeiten sowie die Möglichkeit der Durchführung von Vor-Ort-Prüfungen beim Cloud-Anbieter.

Bezogen auf wesentliche Weiterverlagerungen soll sichergestellt werden, dass gleichwertige Informations- und Prüfungsrechte für die gesamte Auslagerungskette vereinbart sind.

Als eine unzulässige Einschränkung der Informations- und Prüfungsrechte sowie Kontrollmöglichkeiten der Aufsicht gelten insbesondere Regelungen, die diese Rechte nur unter bestimmten Voraussetzungen gewähren. Zur Vermeidung von Wiederholungen wird auf die obigen Ausführungen zur Einschränkung der Rechte der beaufsichtigten Unternehmen verwiesen (vgl. 5.2.1).

5.4 Weisungsrechte

Es sollen Weisungsrechte der beaufsichtigten Unternehmen vereinbart werden. Diese Weisungsrechte sollen sicherstellen, dass alle erforderlichen und zur Erfüllung der vereinbarten Dienstleistung notwendigen Weisungen erteilt werden können, d.h. es bedarf einer Einflussnahme- und Steuerungsmöglichkeit auf den ausgelagerten Sachverhalt. Die Erteilung von Weisungen kann auf technischem Wege (Managementkonsole, Application-Programming-Interfaces (APIs)) erfolgen. Die Umsetzung kann unternehmensindividuell ausgestaltet werden.

Zieht das beaufsichtigte Unternehmen Nachweise/Zertifizierungen oder Prüfberichte heran (vgl. Kapitel V.4.2.3.), soll es auch die Möglichkeit haben, Einfluss auf den Umfang der Nachweise/Zertifizierungen oder Prüfberichte zu nehmen, so dass dieser auf relevante Systeme und Kontrollen erweitert werden kann. Die Anzahl und Häufigkeit entsprechender Weisungen soll verhältnismäßig sein.

Außerdem soll das beaufsichtigte Unternehmen jederzeit zur Erteilung von Weisungen an den Cloud-Anbieter im Hinblick auf die Berichtigung, Löschung und Sperrung von Daten befugt sein und der Cloud-Anbieter die Daten nur im Rahmen der erteilten Weisungen des beaufsichtigten Unternehmens erheben, verarbeiten oder nutzen dürfen. Das Weisungsrecht soll auch die Möglichkeit zur jederzeitigen Erteilung einer Weisung zur unverzüglichen und unbeschränkten Rücküberführung der vom Cloud-Anbieter verarbeiteten Daten an das beaufsichtigte Unternehmen umfassen.

Sofern auf die explizite Vereinbarung von Weisungsrechten zugunsten des beaufsichtigten Unternehmens verzichtet werden kann, ist die vom Auslagerungsunternehmen zu erbringende Leistung hinreichend klar im Auslagerungsvertrag zu spezifizieren.

5.5 Datensicherheit/-schutz (Hinweis zum Ort der Leistungserbringung)

Es sind Regelungen zu vereinbaren, die sicherstellen, dass sowohl datenschutzrechtliche Bestimmungen, als auch aufsichtsrechtliche Anforderungen an die Informationssicherheit eingehalten werden.

Der Ort der Leistungserbringung soll dem beaufsichtigten Unternehmen bekannt sein und insbesondere den Standort der Rechenzentren umfassen. Eine Benennung der Stadt genügt hierfür grundsätzlich. Sollte ein beaufsichtigtes Unternehmen jedoch die genaue Anschrift der Rechenzentren benötigen, soll der Cloud-Anbieter sie zur Verfügung stellen.

Darüber hinaus soll die Redundanz der Daten und Systeme entsprechend ihrer Schutzbedarfe sichergestellt sein, damit im Falle des Ausfalls eines Rechenzentrums die Aufrechterhaltung der Cloud-Dienste gewährleistet ist. Dies kann in der Regel, abhängig von den Cloud-Diensten, konfigurativ durch das beaufsichtigte Unternehmen umgesetzt werden.

Der Schutz und die Sicherheit der Daten sowie der Systeme ist auch innerhalb der gesamten Auslagerungskette zu gewährleisten.

Dem beaufsichtigten Unternehmen soll es jederzeit möglich sein, auf seine beim Cloud-Anbieter gespeicherten Daten zuzugreifen und diese, soweit erforderlich, rücküberführen zu können. Dabei soll sichergestellt werden, dass die gewählte Form der Rücküberführung nicht die Verwendung der Daten einschränkt oder unmöglich macht. Daher sollen, wenn möglich, plattformunabhängige Standarddatenformate vereinbart werden. Die Kompatibilität der unterschiedlichen Systeme ist zu berücksichtigen.

> Ausblick DORA
>
> **Berücksichtigung der aktuellsten und höchsten Qualitätsstandards für die Informationssicherheit**
>
> Durch Art. 28 Abs. 5 DORA haben Finanzunternehmen vor Abschluss von Vereinbarungen mit IKT-Drittdienstleistern betreffend kritischer oder wichtiger Funktionen angemessen zu berücksichtigen, ob IKT-Drittdienstleister die aktuellsten und höchsten Qualitätsstandards für die Informationssicherheit anwenden. Entsprechende vertragliche Vereinbarungen haben die Verfügbarkeit, Authentizität, Integrität und Vertraulichkeit von Daten zu gewährleisten.

5.6 Kündigungsmodalitäten

Es sind Kündigungsrechte und angemessene Kündigungsfristen zu vereinbaren. Es soll für das beaufsichtigte Unternehmen insbesondere ein Sonderkündigungsrecht vereinbart werden, das die Kündigung aus wichtigem Grund vorsieht, wenn seitens der Aufsichtsbehörde die Beendigung des Vertrags verlangt wird. Eine Kündigung aus wichtigem Grund soll darüber hinaus insbesondere möglich sein, wenn

- der Cloud-Anbieter im Hinblick auf den ausgelagerten Sachverhalt gegen geltendes Recht, Rechtsvorschriften oder Vertragsbestimmungen verstößt,

- Hindernisse vorliegen, durch die die Durchführung der ausgelagerten Sachverhalte beeinträchtigt werden kann, oder unannehmbare Auswirkungen auf die Dienstleistungsgüte festgestellt werden,

- wesentliche Änderungen auftreten, die sich auf die Auslagerungsvereinbarung oder den Cloud-Anbieter auswirken (z. B. eine Weiterverlagerung oder Änderungen bei den Subunternehmen) und

- Mängel bezüglich des Umgangs mit und der Sicherheit von vertraulichen, personenbezogenen oder anderweitig sensiblen Daten oder Informationen auftreten.

Es ist sicherzustellen, dass die an den Cloud-Anbieter ausgelagerten Sachverhalte im Falle der Kündigung solange erbracht werden, bis eine vollständige Übertragung auf einen anderen (Cloud-)Anbieter oder auf das beaufsichtigte Unternehmen erfolgt ist. Dabei ist insbesondere zu gewährleisten, dass der Cloud-Anbieter das beaufsichtigte Unternehmen bei der Übertragung der ausgelagerten Sachverhalte an einen anderen (Cloud-)Anbieter oder direkt an das beaufsichtigte Unternehmen angemessen unterstützt.

Die Art, Form und Qualität der Übergabe des ausgelagerten Sachverhalts und der Daten soll festgelegt werden. Soweit Datenformate an die individuellen Bedürfnisse des beaufsichtigten Unternehmens angepasst sind, soll der Cloud-Anbieter eine Dokumentation dieser Anpassungen bei der Beendigung übergeben.

Es soll vereinbart werden, dass nach Rückübertragung der Daten an das beaufsichtigte Unternehmen, dessen Daten vollständig und unwiderruflich auf Seiten des Cloud-Anbieters gelöscht werden.

Für beaufsichtigte Unternehmen die unter den Anwendungsbereich des Gesetzes zur Sanierung und Abwicklung von Instituten und Finanzgruppen (SAG) fallen, müssen bei wesentlichen Auslagerungen die getroffenen Vereinbarungen den Anordnungsbefugnissen im Sinne des § 80 Absatz 1 und 2 SAG Rechnung tragen.

Damit im Falle der geplanten bzw. ungeplanten Beendigung des Vertrags die Aufrechterhaltung der ausgelagerten Bereiche gewährleistet wird, soll das beaufsichtigte Unternehmen eine Ausstiegsstrategie vorhalten und ihre Durchführbarkeit prüfen.

Ausblick DORA

Erweiterte Sonderkündigungsrechte und Mindestkündigungsfristen

In Art. 28 Abs. 7 DORA werden weitere Sonderkündigungsrechte als verpflichtender Vertragsbestandteil bei vertraglichen Vereinbarungen über die Nutzung von IKT-Dienstleistungen genannt.

Ebenso sind nach Art. 30 Abs. 2 lit. h DORA Kündigungsrechte und damit zusammenhängende Mindestkündigungsfristen für die Beendigung der vertraglichen Vereinbarungen entsprechend den Erwartungen der zuständigen Behörden und Abwicklungsbehörden zu vereinbaren.

Zudem sind nach Art. 28 Abs. 8 i.V.m. Art. 30 Abs. 3 lit. f DORA für IKT-Dienstleistungen, die kritische oder wichtige Funktionen unterstützen, Ausstiegsstrategien zu entwickeln und ein verbindlicher angemessener Übergangszeitraum zu vereinbaren. Die getroffenen vertraglichen Vereinbarungen sind so auszugestalten, dass eine ununterbrochene Geschäftstätigkeit, Einhaltung regulatorischer Anforderungen und die Kontinuität und Qualität der für den Kunden erbrachten Dienstleistungen gewährleistet werden.

5.7 Weiterverlagerung

Es sind Regelungen über die Möglichkeit und über die Modalitäten einer Weiterverlagerung zu vereinbaren, die sicherstellen, dass die aufsichtsrechtlichen Anforderungen weiterhin eingehalten werden. Einschränkungen dahingehend, dass etwa nur weitestgehend ähnliche Verpflichtungen übernommen werden, sind nicht zulässig. Insbesondere soll sichergestellt werden, dass die Informations- und Prüfungsrechte sowie Kontrollmöglichkeiten des auslagernden beaufsichtigten Unternehmens sowie der Aufsicht im Falle einer Weiterverlagerung auch gegenüber den Subunternehmen bestehen.

Mit Blick auf die Weiterverlagerung sollen Zustimmungsvorbehalte des auslagernden Unternehmens oder konkrete Voraussetzungen, wann Weiterverlagerungen möglich sind, im Auslagerungsvertrag vereinbart werden. Es soll festgelegt werden, welche ausgelagerten Sachverhalte bzw. Teile davon weiterverlagert werden dürfen und welche nicht. Soweit dies nicht möglich ist, sollen zumindest Informationspflichten zur Vorankündigung vereinbart werden. Über Weiterverlagerungen der ausgelagerten Sachverhalte bzw. Teilen davon soll das beaufsichtigte Unternehmen mit ausreichendem Vorlauf vorab in Textform informiert oder, soweit erforderlich, die Zustimmung des beaufsichtigten Unternehmens eingeholt werden. Die potenziell relevanten Subunternehmen und die an sie weiterverlagerten Sachverhalte bzw. Teile hiervon sollen dem beaufsichtigten Unternehmen bekannt sein.

Im Falle einer neuen oder geänderten Weiterverlagerung ist zu beachten, dass dies Auswirkungen auf die Risikosituation der Auslagerung und somit des auslagernden Unternehmens hat. Entsprechend soll im Falle einer neuen oder geänderten Weiterverlagerung die Risikoanalyse mindestens überprüft oder neu durchgeführt werden. Dies gilt auch im Falle des Bekanntwerdens wesentlicher Mängel sowie wesentlicher Änderungen des zu erbringenden Cloud-Dienstes durch Subunternehmen.

5.8 Informationspflichten der Cloud-Anbieter

Es sind Regelungen zu vereinbaren, die sicherstellen, dass der Cloud-Anbieter das beaufsichtigte Unternehmen über Entwicklungen informiert, die die ordnungsgemäße Erledigung der ausgelagerten Sachverhalte beeinträchtigen können. Die Informationspflicht umfasst beispielsweise die Meldung von eingetretenen Störungen und Informationssicherheitsvorfällen im Rahmen der Erbringung des Cloud-Dienstes. Dadurch soll für das Unternehmen eine angemessene Überwachung des ausgelagerten Sachverhalts sichergestellt werden.

Der Cloud-Anbieter soll das beaufsichtigte Unternehmen unverzüglich über Umstände informieren, die eine Gefahr für die Sicherheit der vom Cloud-Anbieter zu verarbeitenden Daten des beaufsichtigten Unternehmens zur Folge haben können, z.B. durch Maßnahmen Dritter (z.B. Pfändung oder Beschlagnahme), durch ein Insolvenz- oder Vergleichsverfahren oder durch sonstige Ereignisse.

Umfang und Aufbereitung der vom Cloud-Anbieter zur Verfügung gestellten Informationen sollen so ausgestaltet sein, dass das beaufsichtigte Unternehmen angemessen reagieren kann. Insbesondere soll das beaufsichtigte Unternehmen in die Lage versetzt werden, Änderungen seiner Risikosituation erkennen und bewerten zu können.

Es soll sichergestellt werden, dass das beaufsichtigte Unternehmen bei relevanten Änderungen des zu erbringenden Cloud-Dienstes durch den Cloud-Anbieter vorab angemessen informiert wird. Service-Beschreibungen und deren etwaige Änderungen sollen dem beaufsichtigten Unternehmen in Textform überlassen, beziehungsweise mitgeteilt werden. Es soll sichergestellt werden, dass das beaufsichtigte Unternehmen bei Anfragen/Aufforderungen Dritter zur Herausgabe von Daten des beaufsichtigten Unternehmens informiert wird, soweit dies rechtlich zulässig ist.

5.9 Hinweis zum anwendbaren Recht

Insbesondere aus Gründen der Rechtssicherheit soll bei der Vereinbarung einer Rechtswahlklausel darauf geachtet werden, dass – soweit nicht das deutsche Recht vereinbart wird – jedenfalls das Recht eines Staates der Europäischen Union bzw. des Europäischen Wirtschaftsraums auf den Vertrag Anwendung findet. Sollte dies nicht möglich sein, sollen alle Anforderungen an die Rechtsdurchsetzbarkeit gewährleistet bleiben.

IV. Sichere Anwendungsentwicklung und IT-Betrieb in der Cloud

Ausblick DORA

IKT-Risikomanagement

Kapitel II DORA enthält umfangreiche Regelungen zum Thema IKT-Risikomanagement. Die Anforderungen an das IKT-Risikomanagement orientieren sich an internationalen, nationalen und branchenspezifischen bewährten Praxisverfahren (best practices) und Standards. Sie umfassen folgende spezifische Elemente im Bereich des Managements von IKT-Risiken: Identifizierung, Schutz und Prävention, Erkennung, Reaktion und Wiederherstellung, Lernprozesse sowie Weiterentwicklung und Kommunikation.

Sie sollen dazu beitragen, die Funktionsfähigkeit der Finanzunternehmen insbesondere hinsichtlich Cyber-Gefahren aufrechtzuerhalten bzw. gegebenenfalls wiederherzustellen. Damit sorgen die Anforderungen dafür, dass die Finanzunternehmen eine für sie angemessene digitale operationale Resilienz erreichen – also so widerstands- und anpassungsfähig sind, dass sie ihre digitalen operationellen Prozesse auch während und nach einem Störungsfall aufrechterhalten können.

Die in DORA aufgestellten Prinzipien und Regelungen, u.a. zur Anwendungsentwicklung und zum IT-Betrieb in der Cloud werden durch RTS weiter spezifiziert werden, so dass die konkreten Anforderungen derzeit noch nicht feststehen.

1. Anwendungsentwicklung und IT-Betrieb durch das beaufsichtigte Unternehmen

Beaufsichtigte Unternehmen setzen vermehrt auf die Entwicklung von Anwendungsprogrammen, die auf den durch die Cloud-Anbieter bereitgestellten Cloud-Diensten basieren. Diese Anwendungen können auch eine hohe Komplexität aufweisen und Cloud-Dienste mit komplizierten Konfigurationsmöglichkeiten nutzen, die teilweise anbieterspezifisch ausgestaltet sind. Die dabei entstehenden Risiken sollen sowohl bei der Anwendungsentwicklung als auch beim IT-Betrieb angemessen berücksichtigt werden.

Die in diesem Kapitel ausgeführten Hinweise sollen, auf Grundlage bestehender regulatorischer Vorgaben, die bei der Nutzung der Cloud auftretenden spezifischen Herausforderungen und Risiken thematisieren und mögliche Lösungsansätze skizzieren. Dazu soll Transparenz über das aufsichtliche Verständnis von Problemfeldern bei der Anwendungsentwicklung und dem IT-Betrieb in der Cloud hergestellt und üblicherweise geeignete Maßnahmen beschrieben werden.

1.1 Entwicklung von Cloud-Anwendungen und Konfiguration von Cloud-Umgebungen

Cloud-Anwendungen werden häufig mit agilen Methoden unter Einsatz von DevOps und DevSecOps-Prinzipien entwickelt. Dabei ist, neben den weiteren Anforderungen aus den einschlägigen Rundschreiben, insbesondere sicherzustellen, dass die Anforderungen an die Funktionstrennung nicht verletzt und mögliche Interessenkonflikte vermieden werden. Dies kann teilweise durch ablauforganisatorische Maßnahmen oder den Einsatz von technischen Hilfsmitteln, z.B. von CI/CD-Pipelines, oder automatisierten Tests unterstützt werden. Unabhängig von einer möglichen automatisierten Testabwicklung können risikoorientiert weiterhin manuelle Prüfungshandlungen, z.B. Code-Reviews, notwendig sein.

1.2 Nutzung von (Architektur-)Vorgaben

Cloud-Anbieter stellen in der Regel Designprinzipien und Best Practices für die Entwicklung und den IT-Betrieb in der Cloud zur Verfügung (üblicherweise „Well-Architected Frameworks" genannt). Diese umfassen zumeist Empfehlungen zu den Themen Zuverlässigkeit, Sicherheit, Kosten, Betrieb und Effizienz. Daneben empfehlen Cloud-Anbieter üblicherweise in ihrer Dokumentation zu den verschiedenen Cloud-Diensten die Aktivierung von konkreten Sicherheitseinstellungen.

Diese Empfehlungen sollen bei der Nutzung komplexer Cloud-Dienste und -Anwendungen mit den eigenen (Architektur-)Vorgaben des beaufsichtigten Unternehmens abgeglichen werden. Sofern Risiken aus Abweichungen von den Empfehlungen der Cloud-Anbieter entstehen, sollen diese im Rahmen des Risikomanagements gesteuert werden.

1.3 Technische Umsetzung der (Architektur-)Vorgaben

Um sicherzustellen, dass von wesentlichen Punkten der Standardarchitekturen und Betriebsanforderungen nicht abgewichen werden kann, sollen beaufsichtigte Unternehmen (Architektur-)Vorgaben in der Cloud konkretisieren, um diese bei der Entwicklung von Cloud-Anwendungen und in der Konfiguration der Cloud-Umgebungen technisch umsetzen zu können.

Sofern diese nicht technisch umgesetzt werden, sollen Abweichungen möglichst technisch überwacht werden. Die aus der Nichtumsetzung entstehenden Risiken sollen dokumentiert und im Rahmen des Risikomanagements gesteuert werden.

Dabei sollen insbesondere die folgenden, nicht abschließenden, Aspekte betrachtet werden:

- die Beschränkung der zulässigen Cloud-Dienste und Standorte oder Regionen der Rechenzentren,
- der Einsatz von Verschlüsselung und zulässiger kryptografischer Verfahren, in Abhängigkeit vom Schutzbedarf der verarbeiteten Daten,

- die Festlegung sicherer Standardeinstellungen für Cloud-Dienste und die Cloud-Umgebung, um die Schutzziele Vertraulichkeit, Integrität, Verfügbarkeit und Authentizität zu gewährleisten,

- die restriktive Beschränkung der nicht für die Öffentlichkeit bestimmten Cloud-Zugriffswege, z.B. auf explizit zugelassene Hardware, Software und Netzwerkbereiche mit festgelegten Sicherheitsmerkmalen, differenziert nach Kritikalität der einzelnen Cloud-Anwendungen,

- die Trennung der Produktionsumgebungen von Entwicklungs-, Test- und weiteren Umgebungen,

- die Nutzung von Multi-Faktor Authentifizierung für nicht-technische Benutzer,

- die regelmäßige (automatisierte) Durchführung von Backups,

- die Nutzung von Protokollierungs- und Überwachungsdaten und der Schutz dieser vor unbefugtem Zugriff, Manipulation oder nicht zulässiger Löschung.

Um durch das beaufsichtigte Unternehmen nicht genehmigte Veränderungen an Standardkonfigurationen und Standardarchitekturen zu vermeiden, soll der Zugriff auf die Cloud-Umgebungen eingeschränkt werden und nach Möglichkeit nur über den programmatischen Aufruf von APIs stattfinden („Infrastructure-as-Code").

1.4 Überwachung der Cloud-Betriebsprozesse des beaufsichtigten Unternehmens

Die vom beaufsichtigten Unternehmen eingerichteten Cloud-Umgebungen, genutzten Cloud-Dienste und entwickelten Cloud-Anwendungen sollen laufend durch das beaufsichtigte Unternehmen überwacht werden.

Dazu zählen einerseits regelmäßig stattfindende Austausche zwischen beaufsichtigten Unternehmen und Cloud-Anbietern, beispielsweise zu den Themen Leistungs- und Kapazitätsmanagement oder Lebenszyklusmanagement und andererseits die risikobasierte und ggfs. automatisierte Auswertung von Meldungen des Cloud-Anbieters, auftretenden Fehler- und Warnmeldungen sowie die Überwachung der Integrität der Cloud-Konfigurationen. Zudem sollen, in Abhängigkeit von den Verfügbarkeitsanforderungen, die Verfügbarkeit von Cloud-Anwendungen überprüft und ausgewertet werden.

2. Cyber- und Informationssicherheit

Cloud-Anwendungen enthalten häufig schutzwürdige Daten und können somit bei Ausfall kritische Geschäftsprozesse beeinträchtigen. Gleichzeitig sind die Entwicklung, der Betrieb und die Nutzung von Cloud-Anwendungen oft mit einer deutlichen Vergrößerung der Angriffsfläche im Internet verbunden. Da Cloud-Technologien von vielen Unternehmen genutzt werden, können auch komplexe Angriffsmethoden vielfach, ggf. sogar automatisiert, angewendet werden. Gleichzeitig kann die Komplexität der Cloud mögliche Fehlkonfigurationen

und den Verlust eines umfassenden Überblicks über Infrastruktur und genutzte Ressourcen (darunter auch die von den Anbietern zur Verfügung gestellten Werkzeuge und Schnittstellen zur Cloud-Administration) begünstigen und dadurch Cyberangriffe erleichtern.

Grundlage soll eine Analyse möglicher Angreifer, Angriffsziele und Angriffsmethoden sein und neben einer allgemeinen, nicht zielgerichteten Cyberbedrohungslage auch unternehmens- und anwendungsspezifische Bedrohungen umfassen (Threat Intelligence). Diese Informationen sollen in allen Phasen der Entwicklung, Betrieb und Nutzung berücksichtigt werden und in die Bestimmung der Cyber- und Informationsrisiken einfließen.

Im Rahmen der Sicherstellung eines ausreichenden Cyber- und Informationssicherheitsniveaus sollen beaufsichtigte Unternehmen insbesondere Maßnahmen zur Absicherung ihrer Netzwerkverbindungen gegen Störung und unbefugte Überwachung vornehmen, z.B. durch DDoS-Mitigation, Transportverschlüsselung oder dedizierte Verbindungen zum Cloud-Anbieter. Anwendungs- und Infrastrukturarchitekturen sollen so aufgebaut werden, dass das Eindringen oder eine Ausweitung eines unbefugt erlangten Zugriffs möglichst erschwert wird, z.B. durch die Verwendung von Firewalls, Netzwerksegmentierung, Multi-Faktor-Authentifizierung oder Zero Trust. Dies beinhaltet auch die Erkennung und den Schutz vor unbefugtem Abfluss von Daten, z.B. durch Data Loss Prevention.

Die regelbasierte Auswertung von potenziell sicherheitsrelevanten Informationen der beaufsichtigten Unternehmen sollen mit den Datenquellen des Cloud-Anbieters verzahnt sein. Im Falle getrennter Strukturen und Datenquellen (SOC, SIEM etc.) auf Seiten des beaufsichtigten Unternehmens für die Überwachung der Cloud-Umgebung und sonstigen IT-Systeme sollen diese vollständig integriert werden.

Bei der Zusammenführung und Auswertung der potenziell sicherheitsrelevanten Informationen sollen Zuständigkeiten und Abläufe bei der Untersuchung von sicherheitsrelevanten Ereignissen und daraus resultierenden Informationssicherheitsvorfällen festgelegt werden, dies betrifft auch die Schnittstelle zum Cloud-Anbieter. Die beaufsichtigten Unternehmen sollen in diesem Zusammenhang außerdem vereinbaren, dass sie zeitnah vom Cloud-Anbieter über für das beaufsichtigte Unternehmen sicherheitsrelevante Ereignisse und Informationssicherheitsvorfälle informiert werden.

Im Falle eines Informationssicherheitsvorfalls soll durch geeignete Maßnahmen sichergestellt sein, dass administrative Zugriffe auch bei Störung der primären Verbindungswege und Endgeräte möglich sind. Backups der geschäftskritischen Daten und Konfigurationen sollen in regelmäßigen Abständen zusätzlich außerhalb der betroffenen Cloud aufbewahrt werden, z.B. on-premise oder bei einem anderen Cloud-Anbieter.

Cloud-Anwendungen, die kritische Dienstleistungen sind (KRITIS) oder diese wesentlich unterstützen, sowie Cloud-Anwendungen, die im Rahmen von Schutzbedarfsanalysen als besonders wichtig eingestuft sind, sollen regelmäßig Penetrationstests unterzogen werden. Es besteht auch die Möglichkeit der Durchführung eines Threat-Led Penetration Testings (TLPTs) unter Einbindung des Cloud-Anbieters. Schulungen zur Cyber- und Informationssicherheit sollen für alle internen und externen Mitarbeiter, die Cloud-Anwendungen nutzen, verpflichtend sein und inhaltlich an das Vorwissen, die Aufgaben und das Gefährdungspotential der Mitarbeiter angepasst sein.

3. Notfallmanagement

Die Notfallkonzepte und IT-Notfallpläne des Cloud-Anbieters und des beaufsichtigten Unternehmens sollen aufeinander abgestimmt sein. Sofern die Notfallkonzepte und IT-Notfallpläne des Cloud-Anbieters nicht an die des beaufsichtigten Unternehmens angepasst werden, soll sich das auslagernde Unternehmen Kenntnis über die Vorgehensweise des Cloud-Anbieters bei Notfällen verschaffen und die eigenen Prozesse, Architekturen und weitere Vorkehrungen daran ausrichten. Mögliche Risiken aus Abweichungen der Prozesse beim Cloud-Anbieter sind entsprechend im Rahmen des Risikomanagements zu steuern.

IT-Notfallpläne sind regelmäßig[9] zu testen, dabei soll das beaufsichtigte Unternehmen geeignete Notfallszenarien heranziehen. Ist ein gemeinsamer Test mit dem Cloud-Anbieter nicht möglich, soll sichergestellt sein, dass alle betroffenen Komponenten ausreichend durch eigene Tests oder durch angemessene Testnachweise abgedeckt sind.

4. Ausstiegsstrategie

Teil einer Ausstiegsstrategie soll – mit Blick auf die jeweiligen Cloud-Anwendungen – die Identifikation konkreter alternativer Lösungen und die Entwicklung angemessener und durchführbarer Pläne für einen Anbieterwechsel oder eine Rückverlagerung auf das auslagernde Unternehmen sein. Dabei sollen die Anforderungen des Notfallmanagements auch bei der Verlagerung berücksichtigt werden.

Das beaufsichtigte Unternehmen soll Ausstiegspläne vor dem Hintergrund von Ausstiegsszenarien entwickeln, die sich konkret auf die genutzten Cloud-Dienste beziehen. Diese Ausstiegspläne sollen risikobasiert den Umfang und Zeithorizont einer Beendigung der Dienstleistungsbereitstellung abbilden. Dabei soll die Nutzung unterschiedlicher Cloud-Anbieter in Betracht gezogen werden. Zu den zu betrachtenden Ausstiegsszenarien gehört auch der unbeabsichtigte oder unerwartete dauerhafte Wegfall der konkret genutzten Cloud-Dienste.

Beaufsichtigte Unternehmen sollen den Wechsel zu alternativen Lösungen, unter Berücksichtigung der Verhältnismäßigkeit, ohne Unterbrechung der Geschäftstätigkeit, Einschränkung der regulatorischen Compliance oder Beeinträchtigung der Verfügbarkeit und Qualität von Dienstleistungen gegenüber Kunden durchführen können.

Ausstiegspläne sollen ausreichend dokumentiert und getestet werden. Dabei ist insbesondere auf die notwendigen Ressourcen, Zeiträume, Verantwortlichkeiten und Unterstützungsleistungen sowohl intern als auch auf Seiten des Cloud-Anbieters abzustellen.

[9] Sektorspezifische Regelungen sind zu beachten; bspw. jährliche IT-Notfalltests nach Tz. 10.4. BAIT.

V. Überwachung und Kontrolle der Auslagerungen an Cloud-Anbieter

1. Informationsverbund und Modell der geteilten Zuständigkeit

In Abhängigkeit vom gewählten Dienstleistungsmodell besteht zwischen beaufsichtigtem Unternehmen und Cloud-Anbieter eine Arbeitsteilung bezogen auf die Zuständigkeit für den Betrieb der Cloud. Vereinfacht können diese Zuständigkeitsbereiche häufig schematisch in Schichten (z.B. Rechenzentrum, Netzwerk, Physische Server, Virtualisierung, Betriebssystem, Middleware, Anwendung, Daten) dargestellt werden[10].

Je nach gewähltem Cloud-Dienst und Dienstleistungsmodell liegt die Abgrenzung der Zuständigkeiten in dem abstrakten Schichtenmodell an unterschiedlichen Stellen. Das beaufsichtigte Unternehmen soll in seinem Informationsverbund für alle genutzten Cloud-Dienste eine klare Verteilung fest umrissener Aufgaben und Zuständigkeiten in Bezug auf die operativen Funktionen und Tätigkeiten definieren und dokumentieren.

Beaufsichtigte Unternehmen sollen für die Schichten, die sich in ihrer eigenen Zuständigkeit befinden, die vollständige Abbildung in einem Bestandsverzeichnis für Komponenten der IT-Systeme sowie deren Beziehungen zueinander sicherstellen. Unter Proportionalitätsgesichtspunkten kann es unterschiedliche Wege geben, die Anforderungen nach einem Bestandsverzeichnis für Komponenten der IT-Systeme sowie deren Beziehungen zueinander zu erfüllen. Eine CMDB bspw. dient der Sicherstellung eines dokumentierten Überblicks über die für die Aufrechterhaltung bzw. Wiederherstellung des Geschäftsprozesses erforderlichen Bausteine / Serviceelemente und deren Konfiguration. Das beaufsichtigte Unternehmen soll individuell entscheiden, welche Informationen jener Schichten, die in Zuständigkeit des Cloud-Anbieters liegen, sinnvollerweise ebenfalls in die CMDB des beaufsichtigten Unternehmens aufgenommen werden sollen. Bei Schichten mit Zuständigkeit allein beim Cloud-Anbieter erfolgt in der Regel keine Aufnahme von Komponenten des Cloud-Anbieters in die CMDB des beaufsichtigten Unternehmens.

2. Überwachung der Leistungserbringung

Beaufsichtigte Unternehmen sollen zur Überwachung der durch die Cloud-Anbieter erbrachten Leistungen risikoorientiert geeignete technische und prozessuale Vorkehrungen treffen, um die notwendigen Informationen rechtzeitig, vollständig und umfassend erheben, analysieren und bewerten zu können. Cloud-Anbieter und beaufsichtigte Unternehmen sollen gemeinsam sicherstellen, dass alle dazu benötigten Informationen in einem geeigneten Format bereitgestellt und abgerufen werden können.

[10] Cloud-Anbieter nutzen dafür häufig den Begriff der sog. „Shared Responsibility".

2.1 Überwachung der Dienstleistungsgüte

Beaufsichtigte Unternehmen sollen die Dienstleistungsgüte, unabhängig davon, ob der Cloud-Dienst vom Cloud-Anbieter oder dessen Subunternehmen erbracht wird, laufend überwachen. Dazu können die Maßnahmen aus 4.1 herangezogen werden.

Dabei sind bei wesentlichen Auslagerungen bzw. bei den nicht differenzierten Auslagerungen gemäß KAGB, sowohl die Kennzahlen zur Dienstleistungsgüte (wie im Service-Level-Agreement (SLA) vertraglich vereinbart) als auch unternehmensspezifische Indikatoren regelmäßig zu erheben und auszuwerten. Dabei sollen die vom Cloud-Anbieter zur Verfügung gestellten Daten anlassbezogen durch geeignete Analysen oder Messungen plausibilisiert werden. Für die laufende Überwachung sollen die beaufsichtigten Unternehmen interne Prozesse und Schwellenwerte für Warnstufen bei Annäherungen an eine inakzeptable Dienstleistungsgüte definieren. Bei Überschreiten der Schwellenwerte sind vorab festgelegte Kommunikations- und Eskalationsprozesse zu internen Stakeholdern und dem Cloud-Anbieter zu aktivieren.

Sollte die tatsächliche Dienstleistungsgüte unter der vertraglich vereinbarten liegen, soll das beaufsichtigte Unternehmen ad hoc sich daraus möglicherweise ergebende Einschränkungen und Risiken bewerten und ggf. Maßnahmen zur Risikoreduktion ergreifen. Sinkt die Dienstleistungsgüte für einen nicht unwesentlichen Zeitraum unter die vorab festgelegte Grenze für ein nicht mehr annehmbares Niveau, soll das beaufsichtigte Unternehmen, parallel zu den risikoreduzierenden Maßnahmen, vorbereitende Schritte für einen Anbieterwechsel zu prüfen und ggfs. eine Beendigung des Auslagerungsverhältnisses einleiten.

2.2 Überwachung von Veränderungen am Leistungsgegenstand

Beaufsichtigte Unternehmen sollen sicherstellen, dass sie durch die jeweiligen Cloud-Anbieter über Veränderungen am Leistungsgegenstand, wie bspw. Veränderungen an Schnittstellen, der Leistungsfähigkeit von Cloud Services, SLAs oder geplante Wartungen, mit ausreichendem zeitlichen Vorlauf informiert werden, bzw. die internen Prozesse des beaufsichtigten Unternehmens auf die mit dem Cloud-Anbieter vereinbarten Fristen ausgerichtet werden. Beaufsichtigte Unternehmen sollen Veränderungen und geplante Veränderungen am Leistungsgegenstand durchgängig überwachen, indem sie bspw. entsprechende Mitteilungen der Cloud-Anbieter laufend auswerten und regelmäßige Gespräche mit dem Dienstleister führen.

Veränderungen sind vor ihrer Umsetzung im Rahmen einer Auswirkungsanalyse zu dokumentieren und zu bewerten. Dabei ist insbesondere auf die Informationssicherheitsziele abzustellen und es sind notwendige Maßnahmen, bspw. Veränderung der Applikationsarchitektur, einzuleiten. Bei größeren Änderungen sind zudem Zeiträume mit erhöhtem Betreuungsaufwand auf Seiten des beaufsichtigten Unternehmens einzuplanen.

3. Überwachung der Informationssicherheit

3.1 Überwachung des Sicherheitsniveaus

Beaufsichtigte Unternehmen sollen fortlaufend überwachen, dass die jeweiligen Cloud-Anbieter über ein angemessenes Daten- und Systemsicherheitsniveau bei der Verarbeitung, Übertragung und Speicherung von Daten, entsprechend der jeweiligen Schutzbedarfe, verfügen sowie Maßnahmen zur Informationssicherheit umsetzen. Dazu können die Maßnahmen aus 4.1 herangezogen werden. Bei wesentlichen Auslagerungen, bzw. bei den nicht differenzierten Auslagerungen gemäß KAGB, betreffen diese Maßnahmen zumindest Folgendes:

- Organisation der Informationssicherheit und des Risikomanagements,
- Identitäts- und Rechtemanagement,
- Verschlüsselung und Schlüsselverwaltung,
- Aspekte der Betriebssicherheit (Vorfallsmanagement, Changemanagement, Logging und Monitoring, Backup, Schwachstellenmanagement, Netzwerksicherheit etc.)
- Sicherheit von Anwendungsprogrammierschnittstellen (API),
- Steuerung der Subunternehmen,
- IT-Notfallmanagement.

Beaufsichtigte Unternehmen sollen regelmäßig und anlassbezogen das erreichte Sicherheitsniveau feststellen.

3.2 Überwachung von Informationssicherheitsvorfällen und Störungen beim Cloud-Anbieter

Neben der in Kapitel IV.2 beschriebenen Verzahnung der Prozesse zur Sicherstellung der Cyber- und Informationssicherheit sollen beaufsichtigte Unternehmen sicherstellen, dass Cloud-Anbieter für das beaufsichtigte Unternehmen ungeplante Abweichungen vom Regelbetrieb (Störungen) und Informationssicherheitsvorfälle unverzüglich mit einer vorläufigen, vorab definierten Risikoeinwertung melden. Wenn möglich, soll der Cloud-Anbieter Maßnahmen zur temporären Umgehung von Fehlern („Workarounds") zur Verfügung stellen. Auf der Basis vorab definierter Eskalationsebenen und Schwellenwerte soll das beaufsichtigte Unternehmen Informationssicherheitsvorfälle identifizieren und mit dem Cloud-Anbieter bearbeiten. Für den Fall, dass es bei der Bewältigung der Informationssicherheitsvorfälle Unstimmigkeiten zwischen beaufsichtigtem Unternehmen und Cloud-Anbieter gibt, sollen Eskalationsverfahren und ggf. Weisungsrechte vereinbart sein.

Nach der initialen Meldung sollen Cloud-Anbieter dem Unternehmen zudem zeitnah eine vollständige Darlegung des Sachverhalts und eine Fehler-Ursachen-Analyse nachreichen, einschließlich ggf. zusätzlich ergriffener Sicherheitsmaßnahmen. Diese sollen durch das beaufsichtigte Unternehmen bewertet und ggf. im Risikomanagement berücksichtigt werden.

Darüber hinaus soll das beaufsichtigte Unternehmen Lernprozesse, ggfs. gemeinsam mit dem Cloud-Anbieter, durchführen, in denen u. a. die Kommunikation zwischen Cloud-Anbieter und beaufsichtigtem Unternehmen betrachtet wird.

4. Durchführung von Überwachungs- und Kontrollmaßnahmen

Das beaufsichtigte Unternehmen soll ein angemessenes Budget für die Kosten, die aus geplanten Überwachungs-, Kontroll- und Prüfungsmaßnahmen entstehen, bereitstellen.

4.1 Regelmäßige und anlassbezogene Überwachungs- und Kontrolltätigkeiten

Überwachungsmaßnahmen durch beaufsichtigte Unternehmen können unterschiedliche Formen annehmen und sollen sich an den mit dem ausgelagerten Sachverhalt verbundenen Risiken orientieren. Regelmäßige Überwachungstätigkeiten sollen dabei von den fachlich und technisch zuständigen Stellen im beaufsichtigten Unternehmen und den Kontrollfunktionen nach einem Überwachungsplan terminiert und durchgeführt werden. Daneben sollen anlassbezogen Überwachungsmaßnahmen durchgeführt werden, insbesondere bei Vorfällen, Unklarheiten über die Funktionsweise bestimmter Aspekte der Cloud oder zum Aufbau eines besseren Verständnisses zur Risikosituation. Geeignete Maßnahmen dazu können beispielsweise sein:

- Gespräche mit Kundenbetreuern des Cloud-Anbieters,
- Auswertung der technischen Dokumentation und Whitepaper der Cloud-Anbieter,
- Auswertung kundenspezifischer und allgemeiner Kennzahlen (z.B. KPI, KCI, KRI), Berichte und Analysen des Cloud-Anbieters,
- Prüfberichte und Zertifikate[11],
- Besichtigungen sowie
- tiefergehende Analysen mit Experten des Cloud-Anbieters zu spezifischen Themen.

Überwachungsmaßnahmen sollen dokumentiert werden und können zur Vereinbarung weiterer Maßnahmen führen, deren Umsetzung wiederum vom beaufsichtigen Unternehmen überwacht werden soll.

[11] Vgl. Protokoll Sonderfachgremium Cloud zum Thema „Zertifikate“ vom 07.10.2021. Link s. Fußnote 1.

4.2 Prüfungen bei Cloud-Anbietern

Beaufsichtigte Unternehmen haben die Pflicht, angemessene Informations- und Prüfungsrechte im Falle einer Auslagerung von (wesentlichen) Sachverhalten vertraglich sicherzustellen. Bei der Ausübung der vereinbarten Rechte sieht das aufsichtliche Rahmenwerk organisatorische Ausgestaltungsmöglichkeiten vor, welche die Umsetzbarkeit der Rechte erleichtern sollen (vgl. BT 2.1 Tz. 3 Rundschreiben 05/2023 (BA) - Mindestanforderungen an das Risikomanagement – (MaRisk); Leitlinie 11 Tz. 42 lit. a EIOPA Leitlinien zum Outsourcing an Cloud-Anbieter; Leitlinie 6 Tz. 37 lit. a ESMA Leitlinien zur Auslagerung an Cloud-Anbieter).

Solche Erleichterungen stellen bspw. Sammelprüfungen, die Beauftragung von Dritten zur Durchführung einer Prüfung oder externe bzw. interne Prüfberichte der Cloud-Anbieter dar. Im Rahmen der Revisionshandlungen kann die Interne Revision des beaufsichtigten Unternehmens auch auf durch Dritte erstellte Nachweise/Zertifikate zurückgreifen. Auch diese alternativen Prüfungsansätze und das Heranziehen von Zertifizierungen im Rahmen der Durchführung von Prüfungshandlungen müssen die aufsichtlichen Anforderungen erfüllen. Es darf durch solche Erleichterungen nicht zu einer Einschränkung der Informations- und Prüfungsrechte des beaufsichtigten Unternehmens kommen.

4.2.1 Durchführung von Sammelprüfungen

Die Revisionstätigkeit kann im Auftrag mehrerer auslagernder beaufsichtigter Unternehmen als „Sammelprüfung“ oder sog. „Pooled Audit“ durch die internen Revisionen der beaufsichtigten Unternehmen oder durch einen von den auslagernden beaufsichtigten Unternehmen beauftragten Dritten durchgeführt werden. Dabei soll sichergestellt werden, dass das beaufsichtigte Unternehmen ausreichend Einfluss auf die Planung und Durchführung der Prüfung hat.

Es soll für alle an der Prüfung beteiligten beaufsichtigten Unternehmen die Möglichkeit bestehen, auf Prüfungsnachweise zuzugreifen. Sofern diese Prüfungsnachweise in einem (gemeinsamen) Datenraum gespeichert sind, ist die Einhaltung der Schutzziele zu gewährleisten. Zur Nachweisbarkeit der Integrität soll mindestens eine Übersicht der Prüfungsnachweise und zugehörigen Hashwerte bei den beaufsichtigten Unternehmen abgelegt und stichprobenhaft sowie anlassbezogen überprüft werden.

4.2.2 Heranziehung von Berichten der Internen Revision des Cloud-Anbieters

Die Revisionstätigkeit des beaufsichtigten Unternehmens hinsichtlich der Auslagerung in die Cloud kann durch die Interne Revision des Cloud-Anbieters übernommen werden, wenn diese den aufsichtsrechtlichen Anforderungen an die Interne Revision des beaufsichtigten Unternehmens selbst entspricht. Dabei ist es zunächst unwichtig, ob die Revisionstätigkeiten durch die Revision des Cloud-Anbieters erfolgt oder von diesem an einen externen Dritten ausgelagert ist. Die Prüfungsberichte sollen von der Internen Revision des Cloud-Anbieters direkt an die Interne Revision des beaufsichtigten Unternehmens übermittelt werden. Zur Vermeidung von Prüfungslücken darf sich der Prüfungsumfang nicht auf die beauftragten

Sachverhalte beschränken, sondern soll auch die zu dessen Erbringung benötigten Ressourcen und Prozesse einschließen. Die Interne Revision des auslagernden Unternehmens hat sich von der Einhaltung dieser Voraussetzungen regelmäßig zu überzeugen, z.B. durch entsprechende Zertifizierungen (z.B. DIIR Revisionsstandard Nr. 3 bzw. IDW PS 983) oder eigene Prüfungshandlungen.

4.2.3 Heranziehung von Nachweisen/Zertifikaten und Prüfungsergebnissen unabhängiger Dritter

Die Interne Revision des auslagernden beaufsichtigten Unternehmens kann auch auf Nachweise/Zertifikate unabhängiger Dritter zurückgreifen, sie darf sich bei wesentlichen Auslagerungen jedoch nicht allein hierauf stützen.

Voraussetzung für die Nutzung solcher Zertifikate und Prüfnachweise ist insbesondere, dass diese die genutzten Cloud-Dienste konkret betreffen, einen relevanten Zeitraum abdecken und von einem geeigneten, unabhängigen Prüfer unter Beachtung üblicher Prüfungsstandards erstellt wurden. Gleiches gilt für interne Prüfberichte des Cloud-Anbieters.

Üblich sind Nachweise auf Basis gängiger Standards zur Informationssicherheit und Cloud (z.B. ISO 27001, BSI C5, SOC2, CSA CCM), die durch Prüfungsgesellschaften nach allgemein anerkannten Prüfungsstandards (z.B. SSAE 18, ISAE 3402, IDW PS 951) oder durch akkreditierte Prüfer erstellt wurden.

Bei der Heranziehung von Nachweisen/Zertifikaten und Prüfungsergebnissen unabhängiger Dritter in Form von Prüfberichten ist zu beachten, dass die Themen sowie die Tiefe verschiedenartiger Prüfungsformen stark voneinander abweichen können. Das beaufsichtigte Unternehmen soll hierbei insbesondere Umfang, Detailtiefe, Aktualität und Eignung der Prüfberichte sowie die Eignung des Prüfers berücksichtigen. Dementsprechend genügt es in der Regel nicht, wenn sich ein beaufsichtigtes Unternehmen nur vergewissert, dass ein Nachweis (bspw. nur das Zertifikat als solches) vorliegt. Vielmehr soll es den dazugehörigen Prüfungsbericht analysieren, damit es berücksichtigen kann, welche Schwerpunkte gesetzt, welche Feststellungen getroffen und welche Anmerkungen gemacht wurden. Unter dieser Voraussetzung kann bei Themenfeldern mit geringer Komplexität und mit niedrigem Risiko (z.B. physische Sicherheit, Löschanlage im Rechenzentrum) die Nutzung der Prüfungsergebnisse ausreichend sein, bei komplexen Sachverhalten oder höherem Risiko sind ergänzende, eigene Kontroll- und Überwachungshandlungen notwendig. Außerdem können Erkenntnisse aus Prüfungen der Internen Revision des beaufsichtigten Unternehmens mit herangezogen werden.