BaFin

Bundesanstalt für
Finanzdienstleistungsaufsicht

Merkblatt – Orientierungshilfe zu Auslagerungen an Cloud-Anbieter

Bankenaufsicht
Grundsatzreferat IT-Aufsicht und Prüfungswesen

Stand: November 2018

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 vergangenen Monaten mit beaufsichtigten Unternehmen vermehrt Gespräche über geplante Auslagerungen an Cloud-Anbieter geführt. Gleichzeitig ist die deutsche Aufsicht auch mit verschiedenen Cloud-Anbietern in den Dialog eingetreten. Ein Schwerpunkt dieser Gespräche war dabei die Ausgestaltung der (Standard-)Verträge bzw. der vertraglichen Zusatzvereinbarungen, welche auch die aufsichtsrechtlich relevanten Vorgaben erfüllen und regeln sollten, z.B. Informations- und Prüfungsrechte der beaufsichtigten Unternehmen bzw. der Aufsicht.

Auch auf europäischer Ebene ist das Thema in den aufsichtlichen Fokus gerückt. Auf Ebene von EIOPA und EBA, innerhalb des SSM, aber auch bilateral zwischen den nationalen Aufsichtsbehörden hat sich mittlerweile ein stetiger Austausch über den Umgang mit Auslagerungen an Cloud-Anbieter entwickelt. Jüngstes Ergebnis dieses Austauschs sind die Recommendations on Outsourcing to Cloud Service Providers der EBA (EBA/REC 2017/03) von Dezember 2017.

Mit dieser Orientierungshilfe teilen die BaFin und die Deutsche Bundesbank ihre gemeinsame Einschätzung zur Auslagerung an Cloud-Anbieter mit. Durch die Orientierungshilfe werden allerdings keine neuen Anforderungen gestellt, sondern die derzeitige aufsichtliche Praxis in solchen Auslagerungsfällen wiedergegeben. Durch sie soll insbesondere die aufsichtliche Einschätzung zu verschiedenen Formulierungen in Vertragsklauseln transparent werden. Der deutschen Aufsicht sind allerdings nicht alle (Standard-)Verträge bzw. vertraglichen Zusatzvereinbarungen bekannt, sodass die Orientierungshilfe keinen Anspruch auf Vollständigkeit erhebt.

Die Orientierungshilfe verfolgt zudem insbesondere das Ziel, für die beaufsichtigten Unternehmen ein Problembewusstsein im Umgang mit Cloud-Diensten und den damit verbundenen aufsichtsrechtlichen Anforderungen zu schaffen. In diesem Zusammenhang weist die Orientierungshilfe auf wesentliche Aspekte hin, die beaufsichtigte Unternehmen bei einer Auslagerung an Cloud-Anbieter z.B. im Rahmen der Risikoanalyse und der vertraglichen Gestaltung beachten sollten; sie ist aber nicht abschließend.

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

Die aufsichtsrechtlichen Anforderungen an Auslagerungen bleiben unberührt. 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 vom beaufsichtigten Unternehmen zu beachtenden gesetzlichen Bestimmungen verantwortlich.

II. Erläuterungen

Der Begriff „**Auslagerung**“ wird in dieser Orientierungshilfe für „Auslagerungen“ im Sinne des § 25b Kreditwesengesetz (KWG), § 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.

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 und § 26 ZAG.

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.

Cloud-Dienste sind Dienste, die mithilfe von Cloud-Computing erbracht werden, d.h. ein 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 einem Mindestmaß an Verwaltungsaufwand oder Interaktion des Dienstleisters implementieren und freischalten lässt.[1]

Cloud-Dienste werden in der Regel als

- 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)

zur Verfügung gestellt (Dienstleistungsmodelle).

Die 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 Verantwortungsbereichs betrieben wird, bei PaaS hat er nur noch die Kontrolle über seine Anwendungen, die auf der Plattform laufen, und bei SaaS übergibt er praktisch die ganze Kontrolle an den Cloud-Anbieter.[2] Je höher die Komplexität des Dienstleistungsmodells desto geringer sind somit in der Regel die Kontrollmöglichkeiten des Nutzers in der Cloud. Ein Verlust von Kontrollmöglichkeiten ist jedoch nicht gleichzusetzen mit einem Verlust von Verantwortlichkeit im aufsichtsrechtlichen Sinn.

[1] EBA/REC/2017/03 vom 20.12.2017, Seite 3.
[2] Vgl. https://www.bsi.bund.de/DE/Themen/DigitaleGesellschaft/CloudComputing/Grundlagen/Grundlagen_node.html (zuletzt aufgerufen am 26.10.2018).

In der Praxis wird zudem nach vier Bereitstellungsmodellen von Cloud-Diensten unterschieden:

- **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 Unternehmen innerhalb einer 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.[3]

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

III. Strategische Überlegungen

Das beaufsichtigte Unternehmen soll Überlegungen zur Nutzung von Cloud-Diensten in seiner IT-Strategie abbilden. Daneben sollte ein beaufsichtigtes Unternehmen 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 Exit-Strategie 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 sollten neben den auszulagernden Sachverhalten vor allem die Risikomanagement- und -steuerungsprozesse des beaufsichtigten Unternehmens betrachtet werden.

IV. Analyse und Wesentlichkeitsbewertung

Nach der strategischen Entscheidung für die Auslagerung von Sachverhalten an einen Cloud-Anbieter soll zu Beginn des Prozesses in einer Einzelfallbetrachtung anhand der jeweils geltenden aufsichtsrechtlichen Anforderungen von den beaufsichtigten Unternehmen geprüft werden, ob eine Auslagerung vorliegt und ob sie als wesentlich einzustufen ist. In der Regel ist von einer Auslagerung auszugehen.

Bei der Risikoanalyse sind alle für das beaufsichtigte Unternehmen relevanten Aspekte im Zusammenhang mit der Auslagerung auf Cloud-Anbieter zu berücksichtigen, wobei die Intensität der Analyse von Art, Umfang, Komplexität und Risikogehalt der ausgelagerten Sachverhalte abhängt. Sofern aufsichtsrechtliche Anforderungen zur Wesentlichkeit vorliegen,

[3] EBA/REC/2017/03 vom 20.12.2017, Seite 3.

sind diese zu beachten. Das beaufsichtigte Unternehmen sollte auf Grundlage der Risikoanalyse eigenverantwortlich festlegen, welche Auslagerungen unter Risikogesichtspunkten wesentlich sind.

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

- die Ausgestaltung des genutzten Cloud-Dienstes,
- 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,
- eine Bewertung der finanziellen, operationellen (z.B. Systemausfall, Sabotage) Risiken, einschließlich der rechtlichen Risiken (z.B. Risiken der Rechtsdurchsetzung, datenschutzrechtliche Risiken) sowie Reputationsrisiken; dazu zählen auch Erwägungen zum Standort der Datenspeicherung und der Datenverarbeitung,
- 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 Risiken im Falle der Auslagerung mehrerer Sachverhalte an einen Cloud-Anbieter,
- 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 der geopolitischen Lage (allgemeine Stabilität von Politik und Sicherheit) und der anwendbaren Gesetze (einschließlich Gesetze zum Datenschutz) in den betreffenden Gerichtsbarkeiten, die in diesen Gerichtsbarkeiten geltenden Vorschriften zur Rechtsdurchsetzung, einschließlich insolvenzrechtlicher Vorschriften, die bei einem Ausfall des Cloud-Anbieters greifen würden,
- 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 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 des zu erbringenden Cloud-Dienstes durch den Cloud-Anbieter ist zu beachten, dass dies Auswirkungen auf die Risikosituation der Auslagerung und somit des auslagernden Unternehmens haben kann. Entsprechend sollte die Risikoanalyse mindestens überprüft oder neu durchgeführt werden.

V. Vertragsgestaltung bei (wesentlicher) Auslagerung

Abhängig von den aufsichtsrechtlichen Anforderungen sollte bei wesentlichen Auslagerungen bzw. bei den nicht differenzierten Auslagerungen gemäß KAGB im Auslagerungsvertrag insbesondere Folgendes vereinbart werden:

1. Leistungsgegenstand

Im Vertrag soll eine Spezifizierung und ggf. Abgrenzung der vom Cloud-Anbieter zu erbringenden Leistung erfolgen. Dies sollte in sogenannten Service Level-Agreements fixiert werden. Dabei sollte 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),
- Unterstützungsleistungen (Support),
- Zuständigkeiten, Mitwirkungs- und Bereitstellungspflichten (z.B. bei Updates),
- Ort der Leistungserbringung (z.B. Standort der Rechenzentren),
- Beginn und Ende des Auslagerungsvertrags,
- Kennzahlen zur fortlaufenden Überprüfung des Dienstleistungsniveaus,
- Indikatoren zur Erkennung eines unannehmbaren Dienstleistungsniveaus.

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 diejenigen Informationen erhält, die es für die angemessene Steuerung und Überwachung der mit der Auslagerung verbundenen Risiken benötigt.

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

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

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.

Erleichterungen

Abhängig von den einschlägigen aufsichtsrechtlichen Vorgaben können die beaufsichtigten Unternehmen Erleichterungen in Anspruch nehmen, um ihre eigenen Prüfungshandlungen effizienter zu gestalten. Solche Erleichterungen stellen Sammelprüfungen oder das Heranziehen von Nachweisen/Zertifikaten auf Grundlage gängiger Standards bzw. von Prüfberichten anerkannter Dritter oder von internen Prüfberichten des Cloud-Anbieters dar.

Sammelprüfungen

Beaufsichtigte Unternehmen, die §§ 25a, 25b KWG einzuhalten haben, finden Erleichterungen im Rundschreiben 09/2017 (BA) - Mindestanforderungen an das Risikomanagement – (MaRisk). Gemäß BT 2.1 Tz. 3 MaRisk kann die interne Revision des beaufsichtigten Unternehmens im Fall wesentlicher Auslagerungen auf eigene Prüfungshandlungen verzichten, sofern die anderweitig durchgeführte Revisionstätigkeit den Anforderungen in AT 4.4 und BT 2 MaRisk genügt. Die Interne Revision des auslagernden beaufsichtigten Unternehmens hat sich von der Einhaltung dieser Voraussetzungen regelmäßig zu überzeugen. Die für das beaufsichtigte Unternehmen relevanten Prüfungsergebnisse sind an die Interne Revision des auslagernden beaufsichtigten Unternehmens weiterzuleiten.

Die Revisionstätigkeit kann hierbei durch die Interne Revision des Cloud-Anbieters, die Interne Revision eines oder mehrerer der auslagernden beaufsichtigten Unternehmen im Auftrag der auslagernden beaufsichtigten Unternehmen („Sammelprüfungen" sog. „Pooled Audits"), einen vom Cloud-Anbieter beauftragten Dritten oder einen von den auslagernden beaufsichtigten Unternehmen beauftragten Dritten durchgeführt werden.

Für die anderen beaufsichtigten Unternehmen kann es im Einzelfall zulässig sein, bestimmte Informations- und Prüfungsrechte gegenüber dem Cloud-Anbieter per Sammelprüfung gemeinsam mit anderen beaufsichtigten Unternehmen wahrzunehmen.

Nimmt ein beaufsichtigtes Unternehmen eine der zuvor beschriebenen Erleichterungen in Anspruch, darf dies nicht zur Einschränkung seiner Informations- und Prüfungsrechte führen.

Nachweise/Zertifikate und Prüfberichte

Das beaufsichtigte Unternehmen darf grundsätzlich 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 heranziehen. Das beaufsichtigte Unternehmen sollte hierbei Umfang,

Detailtiefe, Aktualität und Eignung des Zertifizierers oder Prüfers dieser Nachweise/Zertifikate und Prüfberichte berücksichtigen.

Allerdings sollte sich ein beaufsichtigtes Unternehmen bei der Ausübung seiner Revisionstätigkeit nicht allein hierauf stützen. Soweit die Interne Revision im Rahmen ihrer Tätigkeit solche Nachweise/Zertifikate bzw. Prüfberichte heranzieht, sollte sie die diesen zugrundeliegenden Evidenzen prüfen können.

3. Informations- und Prüfungsrechte der Aufsicht

Informations- und Prüfungsrechte sowie Kontrollmöglichkeiten der Aufsicht dürfen vertraglich nicht eingeschränkt werden. Die Aufsicht muss die Cloud-Anbieter genauso kontrollieren können, wie dies das jeweils einschlägige Gesetz gegenüber dem beaufsichtigten Unternehmen vorsieht. Der Aufsicht muss es möglich sein, ihre Informations- und Prüfungsrechte sowie Kontrollmöglichkeiten ordnungsgemäß im Hinblick auf den ausgelagerten Sachverhalt uneingeschränkt auszuüben; dies gilt auch für diejenigen Personen, deren sich die Aufsicht bei der Durchführung von Prüfungen bedient.

Zur Gewährleistung dieser Rechte 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 Zugangs zu den Geschäftsräumen des Cloud-Anbieters, einschließlich aller Rechenzentren, Geräte, Systeme, Netzwerke, die zur Erbringung der ausgelagerten Sachverhalte eingesetzt werden; hierzu gehören die damit in Zusammenhang stehenden Prozesse und Kontrollen sowie die Möglichkeit der Durchführung von Vor-Ort-Prüfungen beim Cloud-Anbieter (sowie ggf. bei Weiterverlagerungsunternehmen),
- effektive Kontroll- und Prüfungsmöglichkeiten der gesamten Auslagerungskette.

Keine (mittelbare) Einschränkung der Rechte

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.

4. Weisungsrechte

Es sind Weisungsrechte der beaufsichtigten Unternehmen zu vereinbaren. 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 technische Umsetzung kann unternehmensindividuell ausgestaltet werden.

Zieht das beaufsichtigte Unternehmen Nachweise/Zertifizierungen oder Prüfberichte heran (vgl. V.2), sollte 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 sollte verhältnismäßig sein.

Außerdem sollte das beaufsichtigte Unternehmen jederzeit zur Erteilung von Weisungen an den Cloud-Anbieter in 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. Davon umfasst sein sollte auch die Möglichkeit zur jederzeitigen Erteilung einer Weisung zur unverzüglichen und unbeschränkten Rücküberführung der vom Cloud-Anbieter verarbeiteten Daten an das beaufsichtigte Unternehmen.

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. Datensicherheit/-schutz (Hinweis zum Ort der Datenspeicherung)

Es sind Regelungen zu vereinbaren, die sicherstellen, dass datenschutzrechtliche Bestimmungen und sonstige Sicherheitsanforderungen eingehalten werden.

Der Ort der Datenspeicherung soll dem beaufsichtigten Unternehmen bekannt sein. Dies sollte den konkreten Standort der Rechenzentren umfassen. Eine Benennung des Ortes (z.B. Stadt) genügt hierfür grundsätzlich. Sollte ein beaufsichtigtes Unternehmen jedoch aus Erwägungen des Risikomanagements die genaue Anschrift des Rechenzentrums benötigen, sollte der Cloud-Anbieter sie zur Verfügung stellen.

Darüber hinaus sollte die Redundanz der Daten und Systeme sichergestellt sein, damit im Falle des Ausfalls eines Rechenzentrums die Aufrechterhaltung der Dienste gewährleistet ist.

Die Sicherheit der Daten und Systeme ist auch innerhalb der Auslagerungskette zu gewährleisten.

Dem beaufsichtigten Unternehmen muss es jederzeit schnell und uneingeschränkt möglich sein, auf seine beim Cloud-Anbieter gespeicherten Daten zugreifen und diese, soweit erforderlich, rücküberführen zu können. Dabei sollte sichergestellt werden, dass die gewählte Form der Rücküberführung nicht die Verwendung der Daten einschränkt oder unmöglich

macht. Daher sollten, wenn möglich, plattformunabhängige Standarddatenformate vereinbart werden. Die Kompatibilität der unterschiedlichen Systeme ist zu berücksichtigen.

6. Kündigungsmodalitäten

Es sind Kündigungsrechte und angemessene Kündigungsfristen zu vereinbaren. Es sollte insbesondere ein Sonderkündigungsrecht vereinbart werden, das die Kündigung aus wichtigem Grund vorsieht, wenn seitens der Aufsichtsbehörde die Beendigung des Vertrags verlangt wird.

Es ist sicherzustellen, dass die an den Cloud-Anbieter ausgelagerten Sachverhalte im Falle der Kündigung solange erbracht werden, bis eine vollständige Übertragung des ausgelagerten Sachverhalts 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 sollte festgelegt werden. Soweit Datenformate auf die individuellen Bedürfnisse des beaufsichtigten Unternehmens angepasst sind, sollte der Cloud-Anbieter eine Dokumentation dieser Anpassungen bei der Beendigung übergeben.

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

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

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 muss 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 sollten Zustimmungsvorbehalte des auslagernden Unternehmens oder konkrete Voraussetzungen, wann Weiterverlagerungen möglich sind, im Auslagerungsvertrag vereinbart werden. Es sollte festgelegt werden, welche ausgelagerten Sachverhalte bzw. Teile davon weiterverlagert werden dürfen und welche nicht.

Über Weiterverlagerungen der ausgelagerten Sachverhalte bzw. Teilen davon soll das beaufsichtigte Unternehmen vorab in Textform informiert werden. Die Subunternehmen und die an sie weiterverlagerten Sachverhalte bzw. Teile hiervon sollten dem beaufsichtigten Unternehmen bekannt sein.

Im Falle einer neuen Weiterverlagerung ist zu beachten, dass dies Auswirkungen auf die Risikosituation der Auslagerung und somit des auslagernden Unternehmens haben kann. Entsprechend sollte im Falle einer neuen 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 Subunternehmer.

Das Unternehmen sollte die Durchführung des gesamten Dienstes laufend überwachen und überprüfen, unabhängig davon, ob der Cloud-Dienst vom Cloud-Anbieter oder dessen Subunternehmen erbracht wird.

8. Informationspflichten

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. Dies beinhaltet beispielsweise die Meldung von eingetretenen Störungen im Rahmen der Erbringung des Cloud-Dienstes. Dadurch soll für das Unternehmen eine angemessene Überwachung des ausgelagerten Sachverhalts sichergestellt sein.

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.

Es sollte 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 sollten dem beaufsichtigten Unternehmen in Textform überlassen beziehungsweise mitgeteilt werden. Es sollte sichergestellt werden, dass das beaufsichtigte Unternehmen bei Anfragen/ Aufforderungen Dritter zur Herausgabe von Daten des beaufsichtigten Unternehmens informiert wird, soweit rechtlich zulässig.

9. Hinweis zum anwendbaren Recht

Insbesondere aus Gründen der Rechtssicherheit sollte 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.