

Protokoll

Sonderfachgremium IT zum Thema „Cloud/Weiterverlagerung“

03.05.2022, 10:00 – 13:00 Uhr,

18.08.2022, 10:00 – 13:00 Uhr,

20.09.2022, 10:00 – 13:00 Uhr

per Videokonferenz

Präambel

Im vorliegenden Protokoll werden die maßgeblichen Diskussionsaspekte sowie -ergebnisse aus drei Terminen des Sonderfachgremiums IT zum Thema „Cloud/Weiterverlagerung“ zusammengefasst.

Unter den Teilnehmenden des Sonderfachgremiums herrscht Konsens darüber, dass zukünftige Erfahrungen aus der Praxis oder sich ändernde regulatorische Rahmenbedingungen (bspw. DORA) möglicherweise eine Anpassung der Diskussionsergebnisse erfordern. Schon insbesondere deshalb handelt es sich bei den Diskussionsergebnissen nicht um einen abgeschlossenen Implementierungsleitfaden für Institute. Vielmehr soll ein Orientierungsrahmen für eine Kernmechanik geschaffen werden, dessen Elemente von den Instituten mit den Cloud Service Providern (CSP) ausgestaltet und konkretisiert, vereinbart, implementiert sowie evaluiert werden müssen.

Aufsichtsrechtliche Anforderungen bzgl. Weiterverlagerungen

Die aufsichtsrechtlichen Anforderungen an Weiterverlagerungen basieren auf den EBA Guidelines on Outsourcing, (insb. Tz. 78 die in der MaRisk (insb. AT 9 Tz. 7-8, 11) umgesetzt ist). Ergänzend können die Erläuterungen der BaFin Orientierungshilfe zur Auslagerung an Cloud Anbieter (insb. Kap. 7), berücksichtigt werden. Insbesondere ergeben sich folgende maßgebliche Anforderungen an den Umgang mit Weiterverlagerungen:

- a. Das Institut muss ein angemessenes und wirksames Risikomanagement gewährleisten, das die ausgelagerten Aktivitäten und Prozesse einbezieht (vgl. § 25b Abs. 1 KWG, weiter konkretisiert insbesondere durch AT 9 MaRisk). Eine Delegation der Verantwortung der Geschäftsleitung an das Auslagerungsunternehmen darf nicht erfolgen (vgl. § 25b Abs. 2 KWG, weiter konkretisiert insbesondere durch AT 9 Tz. 4 MaRisk).
- b. Das Institut muss anhand einer Risikoanalyse bewerten, welche Risiken mit einer Auslagerung verbunden sind, und zwar auf der Grundlage von institutsweit bzw. gruppenweit einheitlichen Rahmenvorgaben; hierbei sind u.a. Weiterverlagerungen zu berücksichtigen (vgl. AT 9 Tz. 2 MaRisk sowie die Anmerkung zu Tz. 2 MaRisk).

- c. Die Anforderungen an die Auslagerung von Aktivitäten und Prozessen sind auch bei deren Weiterverlagerung zu beachten, insbesondere werden die mit der Weiterverlagerung verbundenen Risiken im Rahmen der Risikoanalyse bewertet, einschließlich der Bewertung der Wesentlichkeit von Weiterverlagerungen und unter Berücksichtigung des Risikos, dass die Auslagerungsüberwachung durch komplexe und lange Auslagerungsketten eingeschränkt sein kann (vgl. AT 9 Tz. 11 MaRisk).

Problemstellung der Banken

Aus Sicht der Banken ergeben sich Herausforderungen in der praktischen Umsetzung der aufsichtsrechtlichen Anforderungen bzgl. des Themas Weiterverlagerung im Kontext der Nutzung von Cloud-Services und der hierfür erforderlichen Zusammenarbeit mit Cloud-Service Providern (CSP).

Die Kernherausforderung liegt aus Perspektive der Banken darin, dass sich die CSP bei der Erbringung der Cloud Services – je nach Größe – verschiedener, teilweise weltweit eingesetzter Subdienstleister bzw. Subdienstleistungen bedienen. Aufgrund des Umfangs des Leistungsangebotes, der Vielfältigkeit und Komplexität der Services, der Internationalität und der Vielzahl von Kunden ergibt sich (je nach CSP) dadurch ggf. eine sehr große Anzahl an Subdienstleistungen. Diese reichen dabei von „Cloud-leistungsfremden“ Subdienstleistungen (z. B. Marketing & Kommunikation, Facility Management für Bürogebäude, Fleet Management) bis hin zu „Cloud-leistungsnahen“ Subdienstleistungen (z.B. IT- Betriebs- & Entwicklungsleistungen) und haben ein sehr heterogenes Risikoprofil. Aufgrund der Standardisierung sind diese Subdienstleistungen dabei vom CSP nicht einzelnen Kunden zuordenbar - institutsindividuelle Services in Kombination mit „institutsindividuellen Weiterverlagerungen“ gibt es i. d. R. nicht.

Die Vertreter der Banken erläutern, dass, bedingt durch das globale Geschäftsmodell der CSP und die Vielzahl der von CSP eingesetzten Subdienstleistungen, aktuell weder die handhabbare Herstellung einer vollständigen Transparenz über alle bestehenden Subdienstleistungen, noch eine auf diese Gesamtmenge durchzuführende Bewertung durch das auslagernde Institut praktikabel sei.

Selbst wenn eine Gesamtliste aller Subdienstleistungen vorläge, stünde der Aufwand für eine Prüfung nach institutsspezifischen Kriterien relevanter Subdienstleistungen aus Sicht der Banken in keinem angemessenen Verhältnis zur erwartenden Reduktion der Risiken gegenüber einer durch Institute beauftragten Vorselektion durch den CSP. Bei der entsprechenden Selektion der Subdienstleistungen bedürfte es nicht nur der Information, welche Subdienstleistungen betroffen sind und welche Leistungen für die CSPs erbracht werden, sondern auch, inwiefern die Leistungserbringung bzw. Fehler bei der Ausführung der Leistungserbringung die Schutzbedarfsziele eines Instituts beeinflussen könnten.

In der Praxis erfolge daher bisher in der Regel eine Vorfilterung der Subdienstleistungen durch den CSP auf ausschließlich „bedeutende / relevante“ Subdienstleistungen nach eigens durch den CSP definierten Kriterien. Ein typisches Kriterium, das von CSPs genutzt wird, ist

dabei, ob der Subdienstleister „Zugriff auf Kundendaten“ hat. Die Vorfilterung gelte gleichermaßen für die Verpflichtung des CSP zur Information bei Neuverträgen als auch bei Veränderungen an den Subdienstleistungen während der Vertrags- und Nutzungslaufzeit.

Die Möglichkeit zur Aufbereitung kundenspezifischer Subdienstleistungslisten durch den CSP wird von den Banken aufgrund des Einsatzes standardisierter, globaler Services, und weil die CSP Kenntnis über die betriebliche Relevanz der darauf implementierten Bankprozesse bzw. Kritikalität der Daten erlangen müssten, von den Vertretern der Banken als grundsätzlich nicht umsetzbar bewertet.

Für kundenspezifische Aufbereitungen von Subdienstleistungslisten müsste der CSP die Gesamtliste der Subdienstleistungen nach institutsindividuellen Kriterien prüfen und ausselektieren. Darüber hinaus ist die detaillierte Kenntnis der bankfachlich abgebildeten Prozesse, der gespeicherten und zu verarbeitenden Daten (inklusive Klassifikation) aus Sicht der Banken aus Gründen der Vertraulichkeit und Sicherheit nicht gewünscht. Gleichzeitig bestehen bisher noch keine institutsübergreifenden Kriterienlisten, um eine branchenspezifische Vorfilterung zu ermöglichen.

Diskussionsergebnisse

Aus Sicht der Aufsicht setzen die aufsichtsrechtlichen Anforderungen bzgl. von Weiterverlagerungen die Kenntnis des Instituts über alle für die ausgelagerten Aktivitäten und Prozesse relevanten Drittbezüge voraus, um darauf basierend Weiterverlagerungen (Auslagerungen des CSPs an Dritte) zu identifizieren. Somit hat ein Institut Relevanzkriterien für die Auswahl von Weiterverlagerungen und die benötigten Informationen darüber festzulegen und es hat vertraglich zu vereinbaren, dass das Auslagerungsunternehmen bei der (Vor-)Filterung der Informationen zu Weiterverlagerungen diese anwendet und erhält. Die finale Bewertung mittels einer Risikoanalyse erfolgt unter Berücksichtigung der bereitgestellten Informationen beim Institut.

Vor diesem Hintergrund ergibt sich für den Umgang mit Subdienstleistungen (inkl. Weiterverlagerungen) bei Nutzung von Cloud-Services mit dem primären Fokus auf die global tätigen Cloud Service Provider (CSP), jedoch auch für kleinere Anbieter bzw. SaaS-Anbieter mit Weiterverlagerung in die Cloud, eine Kernmechanik als möglicher Ansatz für die Ausarbeitung eines institutsspezifischen Prozesses. Dabei werden zwei Stufen durchlaufen. In der ersten Stufe bestimmt der CSP in einer Vorauswahl aus der Gesamtliste aller Subdienstleistungen die **„potentiell relevanten“ Subdienstleistungen**, die durch das Institut in einem zweiten Schritt bewertet werden, um die **„tatsächlich relevanten“ Subdienstleistungen** zu identifizieren.

1. Bei der vertraglichen Vereinbarung zwischen Institut und CSP sind insbesondere folgende rechtliche und regulatorischen Anforderungen sowie Vorgaben, wie mit Subdienstleistungen umzugehen ist zu berücksichtigen:
 - a. Informationspflicht inklusive Vorankündigung (mit definiertem Zeitraum) bei beabsichtigten Änderungen an oder Aufnahme neuer Subdienstleistungen,
 - b. Gültigkeit der vertraglichen Vereinbarungen zwischen Institut und CSP auch für die relevanten Subdienstleistungen,

- c. Uneingeschränktes Recht zur Prüfung der Subdienstleistungen für das Institut, seinen bestellten Prüfer und die Aufsicht,
 - d. Anforderungen an Mindestdatenfelder für Subdienstleistungen, die der CSP berichtet / bereitstellt (u.a. zur Befüllung Auslagerungsregister, Durchführung Risikoanalyse, Laufende Überwachung / Qualitätsbeurteilung),
 - e. Kündigungsrecht durch das Institut und eventuell erforderliche Unterstützungsleistungen bei Beendigung durch den CSP,
 - f. Vorgaben des Instituts, welche Subdienstleistungen des CSP für das Institut „**potentiell relevant**“ sind (im Sinne einer Vorauswahl aus der Gesamtliste aller Subdienstleistungen) und damit verbunden, für welche Bereiche der CSP seine Subdienstleistungen zu berichten hat. Hierzu zählen zumindest alle Subdienstleistungen für Cloud-Dienste, die folgende Leistungen umfassen:
 - **direkte Betriebsleistungen**, alle Subdienstleistungen die für die Bereitstellung und Aufrechterhaltung sowie für die Überwachung und das Reporting der vom Institut bezogenen Cloud-Dienste unmittelbar und regelmäßig erforderlich sind,
 - **Unterstützungsleistungen**, insbesondere die Betriebsunterstützungsleistungen zur Verwaltung, Steuerung und Überwachung der Leistungserbringung der bezogenen Cloud-Dienste, oder Betriebsunterstützungsleistungen zur Verarbeitung, zur Übertragung, zur Speicherung oder zum Schutz der Daten des Instituts bzw. zur Überwachung dieser Leistungen benötigt werden,
 - sowie **Leistungen zur Risikoreduktion**, insbesondere alle Subdienstleistungen, die die Einhaltung der Schutzziele (Verfügbarkeit, Integrität / Authentizität und Vertraulichkeit) der für das Institut zu verarbeitenden Informationen direkt beeinflussen oder einen Beitrag dazu leisten.
2. Der CSP berichtet **potentiell relevante** Subdienstleistungen (regelmäßig und anlassbezogen) an das Institut auf Basis von Mindestinformationen je Subdienstleistung (u.a. Subdienstleisternamen, Leistungsbeschreibung, Standorte/Regionen, Service-Zuordnung). Gleichzeitig werden nicht *potentiell relevante* Subdienstleistungen vom CSP nicht berichtet.
 3. Ermittlung der für das Institut **tatsächlich relevanten** Subdienstleistungen durch das Institut auf Basis der vom CSP gelieferten Liste *potentiell relevanter* Subdienstleistungen. Hierbei ist eine Eingrenzung durch das Institut zulässig (z.B. durch Eingrenzung auf genutzte Cloud Services, genutzte Cloud Regionen o.ä.).
 4. Anlassbezogene und regelmäßige Durchführung der Risikoanalyse unter Berücksichtigung neuer oder geänderter, *potentiell relevanter* Subdienstleistungen, die der CSP im Rahmen seiner Informationspflicht anzeigt.
 - a. Risikoanalyse für die *tatsächlich relevanten* Subdienstleistungen durch das Institut und ggf. daraus resultierende Bestimmung seiner wesentlichen Weiterverlagerungen, z.B. Risikoanalyse nach den folgenden Kriterien:
 - i. Bezug zu Bankprozessen und institutsspezifischen Aktivitäten
 - ii. Prozesse mit unmittelbarem Zugriff auf (sehr) schutzbedürftige Daten/Informationswerte (z.B. personenbezogene Daten)
 - iii. Auswirkung/Folgen der Schlechtleistung, Nichtleistung der Subdienstleistung (z.B. Reputation, Schadensfall, Non-Compliance, Zeitkritikalität)
 - iv. öffentlich zugängliche Informationen über Bedrohungs- und Risikosachverhalte (z.B. behördliche Sanktionslisten, Generic Thread Landscape der Bundesbank)

- b. Bewertung des verbleibenden Risikos durch das Institut, welches durch mögliche Abweichungen zwischen den Vorgaben des Instituts an den CSP und der tatsächlichen Umsetzung beim CSP resultiert (z.B. unterschiedliche Selektionskriterien)
 - c. Bewertung möglicher institutsspezifischer Konzentrationsrisiken für die Subdienstleistungen sowie aufgrund von komplexen und schwer überschaubaren Weiterverlagerungsketten
5. Entscheidung über Aufnahme, Fortführung oder Adjustierung des Leistungsbezugs vom CSP durch das Institut unter Berücksichtigung der Risikoanalyse.
 6. Aufnahme der ermittelten, wesentlichen Weiterverlagerungen in das Auslagerungsregister des Instituts.
 7. Für die qualitative und quantitative Überprüfung der durch den CSP gemeldeten *potenziell relevanten* Subdienstleistungen sind unter anderem die folgenden Voraussetzungen vom Institut sicherzustellen:
 - a. Uneingeschränkte Prüfung durch das Institut, z.B. Ordnungsmäßigkeit des Auswahlprozesses beim CSP, Stichproben auf „*potenziell relevante*“ / „*nicht potenziell relevante*“ Subdienstleistungen
 - b. Aktive Meldung und regelmäßige Aktualisierung der Liste der *potenziell relevanten* Subdienstleistungen durch den CSP und daraus resultierende anlassbezogene Überprüfung der Risikoanalyse der Subdienstleistung durch das Institut und ggf. Aufsetzen daraus resultierender Maßnahmen durch die für die Dienstleistersteuerung und –überwachung zuständigen Einheiten des Instituts
 - c. Einbezug der wesentlichen Weiterverlagerungen in die Überwachungs- und Prüfungshandlungen des Instituts gem. „IKS / Zertifikate“ sowie risikoorientierter Einbezug in die Prüfungen der Internen Revision (ggf. im Rahmen von Joint Audits)

Aus Sicht der Teilnehmenden sollte als mögliche mittel-/langfristige Variante ein Financial-Services-Mindest-Branchenstandard durch die Institute mit einer einheitlichen Lösung (z.B. einheitliche Kriterien oder definierte Warengruppen, die möglichst den überwiegenden Teil der relevanten Subdienstleistungen beim CSP darstellen) etabliert werden. Diese standardisierten Kriterien wären um Instituts-individuelle Vorgaben zu ergänzen.