Strenge Regeln für die Cloud-Nutzung

Die Europäischen Aufsichtsbehörden EIOPA und ESMA rücken die „Auslagerung an Cloud-Anbieter", also das zunehmende Nutzen von Cloud-Speichern und Cloud-basierten Services, in ihren Fokus. Beide Aufsichtsbehörden haben dazu Leitlinien veröffentlicht, die seit 1. Januar 2021 (EIOPA) bzw. 31. Juli 2021 (ESMA) angewendet werden sollen. Welche Pflichten ergeben sich daraus für Finanzdienstleister?

von Andreas Dolezal

Bereits am 6. Februar 2020 hat die EIOPA ihre „Leitlinien zum Outsourcing an Cloud-Anbieter" veröffentlicht, die seit 1. Januar 2021 für alle neu abgeschlossenen Auslagerungsvereinbarungen gelten. Bestehende Vereinbarungen, die kritische oder wichtige operative Funktionen oder Tätigkeiten betreffen, sind bis 31. Dezember 2022 zu überprüfen und entsprechend anzupassen. Falls dies nicht fristgerecht erfolgt, „sollte das Unternehmen seine Aufsichtsbehörde entsprechend benachrichtigen".

Die Europäische Wertpapier- und Marktaufsichtsbehörde ESMA hat am 18. Dezember 2020 ihren „Final Report: Guidelines on outsourcing to cloud service providers" veröffentlicht. Seit 10. Mai 2021 liegt die deutsche Übersetzung der Leitlinien vor, die ab 31. Juli 2021 auf alle neuen Vereinbarungen anzuwenden sind. Bestehende Vereinbarungen sollen ebenfalls bis 31. Dezember 2022 angepasst werden. Falls dies nicht erfolgt, „sollten die Firmen ihre zuständige Behörde entsprechend informieren".

Schon diese beiden Textzitate zeigen, dass die Leitlinien sehr ähnliche Inhalte aufweisen. Jene der ESMA sind etwas kompakter gestaltet (neun statt sechszehn einzelner Leitlinien), daher werfen wir im Folgenden anhand der deutschen Version der ESMA Leitlinien einen auszugsweisen Blick auf die Bestimmungen. Allen betroffenen Unternehmen empfehle ich eine umfassende Betrachtung.

Die ESMA nennt in ihren deutschen Leitlinien klar die Adressaten, unter anderem Wertpapierfirmen. Als Erfüllungsgehilfe einer Wertpapierfirma werden Sie als eine Einheit mit dieser gesehen. Vertraglich gebundenen Vermittlern und Wertpapiervermittlern empfehle ich daher ebenfalls, die neuen ESMA Leitlinien zu berücksichtigen. Es könnte gut sein, dass Ihr Haftungsdach bald danach fragt.

Sinn und Zweck

Das zunehmende Auslagern von Anwendungen an Cloud-Service-Provider

Funktionen betrifft, alle relevanten Risiken der Auslagerung sowie mögliche Interessenkonflikte zu ermitteln und zu bewerten und eine angemessene Due-Diligence-Prüfung des künftigen Cloud-Anbieters durchzuführen.

Beim Auslagern von kritischen oder wesentlichen Funktionen soll die Eignung des Cloud-Anbieters bewertet werden. Die geschäftliche Reputation des Cloud-Anbieters, seine Kenntnisse und Fähigkeiten, die Mittel (unter anderem die personellen und finanziellen Mittel, die IT-Ressourcen), die Organisationsstruktur und gegebenenfalls die entsprechende Zulassung oder Registrierung sollen geprüft werden.

Leitlinie 3: Zentrale Bestandteile des Vertrags

Die jeweiligen Rechte und Pflichten des Unternehmens und seiner Cloud-Anbieter sollten in schriftlichen Vereinbarungen klar festgehalten werden. Wenn kritische oder wesentliche Funktionen ausgelagert werden, sollte die schriftliche Vereinbarung zumindest die in Ziffer 28 Buchstaben a) bis o) genannten Elemente umfassen.

Dazu zählt beispielsweise die Anforderung an den Cloud-Anbieter, dem Unternehmen und den zuständigen Behörden das Recht auf Zugang („Zugangsrechte") und auf Prüfung („Prüfungsrechte") zu gewähren. Unternehmen müssen sich also das Recht einräumen lassen, die entsprechenden Informationen, Räumlichkeiten, Systeme und Geräte des Cloud-Anbieters – wie z. B. Google, Amazon AWS, Microsoft & Co. – vor Ort (weltweit?) zu kontrollieren.

Leitlinie 4: Informationssicherheit

Unternehmen sollten in internen Richtlinien und Verfahren sowie in der schriftlichen Auslagerungsvereinbarung mit den Cloud-Anbietern angemessene Anforderungen an die Informationssicherheit festlegen und das Einhalten fortlaufend überwachen, einschließlich des Schutzes vertraulicher, personenbezogener oder anderweitig sensibler Daten.

Leitlinie 5: Ausstiegsstrategien

Beim Auslagern kritischer oder wesentlicher Funktionen sollten Unternehmen sicherstellen, dass sie die Auslagerungsvereinbarung mit dem Cloud-Anbieter beenden können, ohne ihre geschäftlichen Aktivitäten und Dienstleistungen gegenüber ihren Kunden in unverhältnismäßiger Weise zu unterbrechen und ohne die Einhaltung ihrer Verpflichtungen nach den anwendbaren Rechtsvorschriften sowie die Vertraulichkeit, Integrität und Verfügbarkeit ihrer Daten zu beeinträchtigen. Dazu sind unter anderem umfassende, dokumentierte und hinreichend überprüfte Ausstiegspläne zu entwickeln.

Leitlinie 6: Zugriffs- und Prüfungsrechte

Unternehmen sollten sicherstellen, dass Auslagerungsvereinbarungen das wirksame Ausüben der Zugangs- und Prüfungsrechte sowie der Aufsichtsmöglichkeiten durch das Unternehmen und die zuständige Behörde nicht einschränken. Um Prüfungsressourcen effizienter zu nutzen und den organisatorischen Aufwand zu verringern, kann unter anderem auf Zertifizierungen durch Dritte (z. B. ISO) zurückgegriffen werden. Doch solche Zertifizierungen gilt es gemäß Ziffer 39 Buchstaben a) bis g) zu prüfen.

Leitlinie 7: Sub-Auslagerungen

Falls die Sub-Auslagerung von kritischen oder wesentlichen Funktionen (oder wesentlichen Teilen) zulässig ist, sollte die Auslagerungsvereinbarung die Verpflichtung vorsehen, dass das Unternehmen über beabsichtigte Sub-Auslagerungen informiert werden muss und berechtigt ist, der beabsichtigten Sub-Auslagerung zu widersprechen.

Haben Sie jemals von Google, Amazon AWS, Microsoft & Co. so eine Information erhalten? Wie haben diese globalen Quasi-Monopolisten reagiert als Sie der Auslagerung gegebenenfalls widersprochen haben?

Leitlinie 8: Schriftliche Mitteilung an die zuständigen Behörden

Unternehmen sollten ihre zuständige Behörde rechtzeitig schriftlich über beabsichtigte Auslagerungsvereinbarungen mit Cloud-Anbietern, die eine kritische oder wesentliche Funktion betreffen, informieren. Dafür sind in Ziffer 45 Buchstaben a) bis j) definierte Inhalte vorgesehen.

Leitlinie 9: Überwachung von Auslagerungsvereinbarungen mit Cloud-Anbietern

Abschließend werden die zuständigen Behörden angewiesen, Risiken zu bewerten, die sich aus Auslagerungsvereinbarungen der beaufsichtigten Unternehmen ergeben. Zuständige Behörden sollten eine wirksame und risikobasierte Aufsicht ausüben können, insbesondere in Fällen, in denen Unternehmen kritische oder wesentliche Funktionen auslagern, die dann außerhalb der EU (Achtung: Drittländer!) durchgeführt werden.

Fazit

Wenn Sie sich als beaufsichtigtes Unternehmen bis dato noch keinen IT-Ordner angelegt haben, dann wird es spätestens jetzt Zeit dafür. Datenschutz und IT-Sicherheit sind – neben Sustainable Finance – die neuen Steckenpferde der Aufsichtsbehörden.

Abzuwarten bleibt, wie die globalen Quasi-Monopolisten, zu denen es keine gleichwertigen europäischen Alternativen gibt, auf die Begehrlichkeiten reagieren, die Sie ihnen im Sinne der EIOPA und ESMA abringen müssen. Eines kann ich Ihnen jedenfalls schon jetzt versprechen: DORA setzt für Finanzdienstleister, wahrscheinlich ab 2023/2024, noch einmal eine gehörige bürokratische Schippe oben drauf.

bringt, so die ESMA einleitend, Vorteile mit sich, ist aber nicht frei von Herausforderungen und Risiken. Der Zweck der Leitlinien ist es, Unternehmen dabei zu helfen, die Risiken, welche sich aus dem Auslagern an Cloud-Anbieter ergeben können, zu identifizieren, zu bewältigen und zu überwachen.

Gleichzeitig sollen die Leitlinien den zuständigen Behörden bei der Ermittlung, Bewältigung und Überwachung von Risiken und Herausforderungen im Zusammenhang mit Auslagerungen an Cloud-Anbieter als Hilfestellung dienen. Die Finanzmarktaufsicht wird sich also an diesen Leitlinien orientieren.

Begriffsbestimmungen

Um den Ausführungen von EIOPA und ESMA folgen zu können, ist ein Blick auf die Begriffsbestimmungen erforderlich:

- Kritische oder wesentliche Funktion: bezeichnet jede Funktion, deren unzureichende oder unterlassene Wahrnehmung zu einer wesentlichen Beeinträchtigung der Einhaltung der geltenden Rechtsvorschriften, der finanziellen Ergebnisse, oder der Solidität oder Kontinuität von zentralen Dienstleistungen und Tätigkeiten führen würde.
- Cloud-Dienste: bezeichnet Dienstleistungen, die mithilfe von Cloud-Computing erbracht werden.
- Cloud-Computing oder Cloud: bezeichnet ein Paradigma (sic!) zur Ermöglichung des Netzwerkzugangs zu einem skalierbaren und flexiblen Pool von gemeinsam nutzbaren physischen oder virtuellen Ressourcen (z. B. Servern, Betriebssystemen, Netzwerken, Software, Anwendungsprogrammen und Speichergeräten) mit Self-Service-Bereitstellung und Administration-on-Demand.
- Cloud-Anbieter: bezeichnet Drittanbieter, die Cloud-Services im Rahmen einer Auslagerungsvereinbarung bereitstellen.

Andreas Dolezal, Unternehmensberater & Compliance Officer

- Community-Cloud: Cloud-Dienst, der ausschließlich von einer bestimmten Kundengruppe, die untereinander in Beziehung stehen, gemeinsam genutzt wird.
- Private Cloud: Cloud-Dienst, der ausschließlich von einem einzigen Kunden genutzt wird und dessen Ressourcen von diesem Kunden kontrolliert werden.
- Public Cloud: Cloud-Dienst, der potenziell jedem Kunden zur Verfügung steht und dessen Ressourcen vom Cloud-Anbieter kontrolliert werden.
- Hybrid-Cloud: Cloud-Dienst, der mindestens zwei der genannten Cloud-Bereitstellungsmodelle nutzt.

Diese Definitionen sind ziemlich allumfassend. Oder anders gesagt: wer gänzlich ohne irgendeine Art von Cloud auskommen möchte, möge seinen Rechner vom Internet trennen und versuchen, so seine Finanzdienstleistungen zu erbringen. In unseren modernen Zeiten wird das kaum möglich sein.

Wer sich schon einmal vor Augen geführt hat, welche weiten (und de facto unkontrollierbaren) elektronischen Wege über globale Datennetze eine E-Mail nimmt, bevor sie beim Empfänger ankommt, mag elektronische Kommunikation generell als Cloud-Nutzung ansehen. Weitverbreitete Anwendungen wie MS Office 365 sind sowieso als Cloud-Dienst zu klassifizieren.

In der langen Liste der Rechtsgrundlagen (auf die die EIOPA verzichtet) kommt der Entwurf zu DORA (Verordnung über die Betriebsstabilität digitaler Systeme des Finanzsektors) nicht vor. Dort sind in der Definition von IKT-Drittanbietern (Artikel 3 Ziffer 15) „elektronische Kommunikationsdienste" im Sinne des Artikels 2 Nummer 4 der Richtlinie (EU) 2018/1972 (Richtlinie über den europäischen Kodex für die elektronische Kommunikation), wie z. B. „interpersonelle Kommunikationsdienste" (also u. a. E-Mails) von der Anwendung der Bestimmungen ausgenommen. Davon steht in den ESMA und EIOPA Leitlinien jedoch nichts.

Leitlinie 1: Governance, Kontrolle und Dokumentation

Unternehmen sollten eine klare und aktuelle Strategie für Auslagerungen an Cloud-Anbieter haben, die mit den entsprechenden Strategien und internen Grundsätzen und Verfahren des Unternehmens in Einklang steht und unter anderem die Bereiche Informations- und Kommunikationstechnologie, Informationssicherheit und operatives Risikomanagement abdeckt.

Neben klaren Zuständigkeiten und hinreichenden Ressourcen soll ein aktualisiertes Register mit Informationen über alle Auslagerungsvereinbarungen mit Cloud-Anbietern eingerichtet werden, dessen Inhalte in Ziffer 17 Buchstaben a) bis m) definiert sind.

Leitlinie 2: Risikoanalyse der Auslagerung und Due-Diligence-Prüfung

Vor dem Abschluss einer Auslagerungsvereinbarung gilt es zu prüfen, ob die Auslagerung kritische oder wesentliche