Waigel RECHTSANWÄLTE

Newsletter

ESMA: Cloudauslagerung

24. Juli 2020

Mit dem Konsultationspapier vom 3. Juni 2020 konsultiert die ESMA Guidelines zur Auslagerung an sog. Cloud Service Providers (CSPs). Bis zum 1. September 2020 nimmt die ESMA noch Rückmeldungen entgegen. Die Guidelines sollen vom 30. Juni 2021 an für alle Cloud-Outsourcing-Vereinbarungen, die an oder nach diesem Datum abgeschlossen, erneuert oder geändert werden, gelten. Unternehmen sollten bestehende Cloud-Outsourcing-Vereinbarungen überprüfen und entsprechend ändern, um sicherzustellen, dass sie diese Richtlinien bis zum 31. Dezember 2022 berücksichtigen.

Die ESMA bescheinigt der Cloudauslagerung zahlreiche Vorteile, wie verbesserte Flexibilität, betriebliche Effizienz und Kostenwirksamkeit, mit potenziell positiven Ergebnissen für die Unternehmen und Investoren.

Bevor man seine Daten auf einen Cloudanbieter auslagert, sei eine Due Diligence und eine Risikobewertung wichtig. Von einem sog. „One-Size-Fits-All“ rät die ESMA ab, Wertpapierfirmen sollten eine Cloudauslagerung besser ihrem Geschäftsmodell und Ihrem Kundenstamm nach ausrichten und individuell anpassen lassen.

Es bestünde die Gefahr, dass die Firmen die Kontrolle über ihre Daten verlören, wenn sie die Daten in eine Cloud auslagern. Die ESMA fordert, dass man sich nicht zu sehr auf die CSP verlassen sollte und die Auslagerung in dem gebotenen Umfang überwache.

Besonders Augenmerk gilt es auch auf die Informationssicherheit und die Katastrophen-Widerherstellung zu werfen, besonders in Anbetracht der stetig steigenden Cyberangriffen. In diesem Zusammenhang sollten auch die vertraglichen Vereinbarungen entsprechend gestaltet werden. Die Unternehmen sollen auch über Alternativlösungen ("Exit-Strategien") verfügen, um ihre Cloud-Auslagerungsvereinbarung bei Bedarf zu beenden, um nicht dem Risiko eines sog. „Lock-in“ ausgesetzt zu sein.

Weiterhin sind sog. rechtliche Risiken zu beachten. Berücksichtigt werden müsse das geltende Recht des Vertrags zwischen der Wertpapierfirma und dem Cloud-Service-Provider sowie die Anforderungen an den Datenstandort. Hier sind insbesondere die DS-GVO Anforderungen in Bezug auf den Speicherort personenbezogener Daten zu nennen. Die Möglichkeit der Kontrolle durch die Aufsicht (BaFin) muss trotz Auslagerung jederzeit möglich sein.

Wir haben die aus unserer Sicht wichtigsten Punkte der Guidelines für Sie nachfolgend zusammengefasst:

- Anfertigung einer aktualisierten Cloud-Auslagerungsstrategie
- vor Eingehung eines Auslagerungsabkommen sollten folgende Punkte erfüllt werden
    - abschätzen, ob die Cloud-Outsourcing-Vereinbarung eine kritische oder wichtige Funktion betrifft;
    - alle relevanten Risiken der Cloud-Outsourcing-Vereinbarung sollen ermittelt und bewertet werden;
    - Durchführung einer angemessene Due-Diligence-Prüfung des potenziellen CSP;
    - Ermittlung und Bewertung von Interessenkonflikten, die eine Auslagerung verursachen könnten;

- es sollen ausreichende Ressourcen vorgehalten werden, um die Guidelines einzuhalten und den rechtlichen Anforderungen, bzgl. der Cloud-Auslagerungsvereinbarungen nachkommen zu können;

- Einrichtung einer Outsourcing-Aufsichtsfunktion (kann auch leitender Mitarbeiter sein) der direkt dem Leitungsorgan gegenüber rechenschaftspflichtig und für die Verwaltung und Überwachung der Risiken von Cloud-Outsourcing-Vereinbarungen verantwortlich ist;

- Laufende Überwachung der Durchführung von Aktivitäten, die Sicherheitsmaßnahmen und die Einhaltung der vereinbarten Service-Levels durch die ausgewählten CSPs auf der Grundlage eines risikobasierten Ansatzes;

- Führung eines aktualisierten Registers mit Informationen über alle Cloud-Outsourcing-Vereinbarungen (zwischen Auslagerung kritischer oder wichtiger Funktionen und anderen Outsourcing-Vereinbarungen zu unterscheiden);

- gegebenenfalls und zur Unterstützung der durchgeführten Due-Diligence-Prüfung kann ein Unternehmen auch Zertifizierungen auf der Grundlage internationaler Standards und externer oder interner Prüfberichte verwenden (bei kritischen oder wichtigen Funktionen sind weitere Auflagen zu beachten);

- Bei wesentlichen Mängeln und/oder wesentliche Änderungen der erbrachten Dienstleistungen, sollten die Analyse vor der Auslagerung und die Due-Diligence-Prüfung des CSPs unverzüglich überprüft oder erneut durchgeführt werden;

- die jeweiligen Rechte und Pflichten sollten in einer schriftlichen Vereinbarung festgelegt werden, welche auch ein außerordentliches Kündigungsrecht vorsehen soll

Bei der Auslagerung von kritischen bzw. wichtigen Funktionen sollen insbesondere die folgenden Themenbereiche abgedeckt werden:

- Organisation für Informationssicherheit
- Zugriffsverwaltung
- Verschlüsselung und Schlüsselverwaltung
- Betrieb und Netzwerksicherheit
- Anwendungsprogrammier-Schnittstellen (API)
- Geschäftskontinuität und Notfallwiederherstellung
- Datenspeicherung und Datenverarbeitungsort(e)
- Compliance & Monitoring

Bzgl. der Zugangs- und Prüfungsrechte, sollen auch gepoolte Audits, die gemeinsam mit anderen Kunden desselben CSP durchgeführt werden, oder gepoolte Audits, die von einem externen Auditor durchgeführt werden, welcher von mehreren Kunden desselben CSP bestellt wurde, genutzt werden können.

Die ESMA will auch das Sub-Outsourcing kritischer oder wichtiger Funktionen unter bestimmten speziellen Voraussetzungen erlauben. Im Falle einer solchen Auslagerung sollte die zuständige Behörde unter Mitteilung der entsprechenden Fakten rechtzeitig benachrichtigt werden.

Wenn Sie mit uns über die vorgestellten Guidelines diskutieren möchten oder falls Sie andere Fragen dazu haben, welche Anforderungen im Einzelnen von Seiten der ESMA (und der BaFin) an Auslagerungsvereinbarungen für

Banken und Finanzdienstleistungsinstitute gestellt werden, stehen wir für Sie gerne zur Verfügung.

gez. Sebastian Kunstmann
Rechtsanwalt

Waigel Rechtsanwälte
Partnerschaftsgesellschaft mbB
Nymphenburger Straße 4
80335 München
Tel.: +49 89 / 74 00 457 - 0
Fax: +49 89 / 74 00 457 - 77
info@waigel.de

Urheberrecht

Haftungsausschluss

Diese Mandanteninformation enthält ausschließlich allgemeine Informationen, die nicht geeignet sind, den besonderen Umständen eines Einzelfalles gerecht zu werden. Sie hat nicht den Sinn, Grundlage für wirtschaftliche oder sonstige Entscheidungen jedweder Art zu sein. Sie stellt keine Beratung, Auskunft oder ein rechtsverbindliches Angebot auf Beratung oder Auskunft dar und ist auch nicht geeignet, eine persönliche Beratung zu ersetzen. Sollte jemand Entscheidungen jedweder Art auf Inhalte dieser Mandanteninformation oder Teile davon stützen, handelt dieser ausschließlich auf eigenes Risiko.

Waigel Rechtsanwälte und auch die in dieser Mandanteninformation namentlich genannten Partner oder Mitarbeiter übernehmen keinerlei Garantie oder

Gewährleistung, noch haftet Waigel Rechtsanwälte und einzelne Partner oder Mitarbeiter in irgendeiner anderen

Weise für den Inhalt dieser Mandanteninformation. Aus diesem Grund empfehlen wir, in jedem Fall eine persönliche Beratung einzuholen.