EBA/REC/2017/03

28/03/2018

Empfehlungen

zur Auslagerung an Cloud-Anbieter

1. Compliance- und Mitteilungspflichten

Status dieser Empfehlungen

1. Das vorliegende Dokument enthält Empfehlungen, die gemäß Artikel 16 der Verordnung (EU) Nr. 1093/2010 herausgegeben wurden.[1] Gemäß Artikel 16 Artikel 3 der Verordnung (EU) Nr. 1093/2010 müssen die zuständigen Behörden und Finanzinstitute alle erforderlichen Anstrengungen unternehmen, um diesen Empfehlungen nachzukommen.

2. Diese Empfehlungen legen fest, was nach Ansicht der EBA angemessene Aufsichtspraktiken innerhalb des Europäischen Finanzaufsichtssystems sind oder wie das Unionsrecht in einem bestimmten Bereich anzuwenden ist. Dazu sollten die zuständigen Behörden gemäß Artikel 2 Absatz 4 der Verordnung (EU) Nr. 1093/2010 die an sie gerichteten Empfehlungen in geeigneter Weise in ihre Aufsichtspraktiken (z. B. durch Änderung ihres Rechtsrahmens oder ihrer Aufsichtsverfahren) integrieren, einschließlich der Empfehlungen in diesem Dokument, die in erster Linie an Institute gerichtet sind.

Meldepflichten

3. Nach Artikel 16 Absatz 3 der Verordnung (EU) Nr. 1093/2010 müssen die zuständigen Behörden der EBA bis zum 28.05.2018 mitteilen, ob sie diesen Empfehlungen, nachkommen oder nachzukommen beabsichtigen, oder die Gründe nennen, warum sie dies nicht tun. Geht innerhalb der genannten Frist keine Meldung ein, geht die EBA davon aus, dass die zuständige Behörde den Anforderungen nicht nachkommt. Die Mitteilungen sollten unter Verwendung des auf der Website der EBA abrufbaren Formulars mit dem Betreff „EBA/REC/2017/03“ an compliance@eba.europa.eu gesendet werden. Die Meldungen sollen von Bediensteten erfolgen, die befugt sind, entsprechende Meldungen im Auftrag ihrer Behörde zu übermitteln. Jegliche Änderungen des Status der Einhaltung müssen der EBA ebenfalls gemeldet werden.

4. Die Meldungen werden gemäß Artikel 16 Absatz 3 der EBA-Verordnung auf der Website der EBA veröffentlicht.

[1] Verordnung (EU) Nr. 1093/2010 des Europäischen Parlaments und des Rates vom 24. November 2010 zur Errichtung einer Europäischen Aufsichtsbehörde (Europäische Bankenaufsichtsbehörde), zur Änderung des Beschlusses Nr. 716/2009/EG und zur Aufhebung des Beschlusses 2009/78/EG der Kommission (ABl. L 331 vom 15.12.2010, S. 12).

2. Gegenstand, Anwendungsbereich und Begriffsbestimmungen

Gegenstand und Anwendungsbereich

1. Diese Empfehlungen enthalten nähere Angaben zu den Bedingungen für die Auslagerung von Dienstleistungen, die in den CEBS-Leitlinien zur Auslagerung vom 14. Dezember 2006 genannt sind, und gelten für die Auslagerung an Cloud-Anbieter durch Institute im Sinne von Artikel 4 Absatz 1 Ziffer 3 der Verordnung (EU) Nr. 575/2013.

Adressaten

2. Die vorliegenden Empfehlungen gelten für zuständige Aufsichtsbehörden im Sinne von Artikel 4 Absatz 2 Buchstabe i der Verordnung (EU) Nr. 1093/2010 sowie für Institute im Sinne von Artikel 4 Absatz 1 Ziffer 3 der Verordnung (EU) Nr. 575/2013.[2]

Begriffsbestimmungen

3. Sofern nicht anders angegeben, haben die in der Richtlinie 2013/36/EU[3] (Eigenkapitalrichtlinie) und in den CEBS-Leitlinien verwendeten und definierten Begriffe in diesen Empfehlungen dieselbe Bedeutung. Für die Zwecke dieser Empfehlungen gelten darüber hinaus die folgenden Begriffsbestimmungen:

Cloud-Dienste	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.
Öffentliche Cloud	Cloud-Infrastruktur, die von der Öffentlichkeit frei genutzt werden kann.
Private Cloud	Cloud-Infrastruktur, die ausschließlich von einem einzelnen Institut genutzt werden kann.

[2] Verordnung (EU) Nr. 575/2013 des Europäischen Parlaments und des Rates vom 26. Juni 2013 über Aufsichtsanforderungen an Kreditinstitute und Wertpapierfirmen und zur Änderung der Verordnung (EU) Nr. 646/2012.

[3] Richtlinie 2013/36/EU des Europäischen Parlaments und des Rates vom 26. Juni 2013 über den Zugang zur Tätigkeit von Kreditinstituten und die Beaufsichtigung von Kreditinstituten und Wertpapierfirmen, zur Änderung der Richtlinie 2002/87/EG und zur Aufhebung der Richtlinien 2006/48/EG und 2006/49/EG.

Community-Cloud	Cloud-Infrastruktur, die ausschließlich von einer konkreten Institutsgemeinschaft genutzt werden kann, einschließlich mehrerer Institute innerhalb einer Gruppe.
Hybrid-Cloud	Cloud-Infrastruktur, die sich aus zwei oder mehreren speziellen Cloud-Infrastrukturen zusammensetzt.

3. Umsetzung

Umsetzungsfrist

5. Diese Empfehlungen gelten ab dem 1. Juli 2018.

4. Empfehlungen zur Auslagerung an Cloud-Anbieter

4.1 Wesentlichkeitsbewertung

1. Auslagernde Institute sollten vor der Auslagerung etwaiger Tätigkeiten zunächst eine Bewertung vornehmen, welche Tätigkeiten als wesentlich zu erachten sind. Die Institute sollten die Wesentlichkeit der Tätigkeiten anhand von Leitlinie 1 Buchstabe f der CEBS-Leitlinien bewerten und speziell bei der Auslagerung an Cloud-Anbieter sämtliche der nachstehenden Aspekte berücksichtigen:

    (a) Kritikalität der auszulagernden Tätigkeiten und Profil des ihnen inhärenten Risikos, d. h. Beurteilung, ob diese Tätigkeiten zur Aufrechterhaltung des Geschäftsbetriebs/Existenzfähigkeit des Instituts und seiner Verpflichtungen gegenüber den Kunden kritisch sind;

    (b) direkte operative Auswirkungen von Ausfällen sowie die damit verbundenen rechtlichen Risiken und Reputationsrisiken;

    (c) die Folgen, die eine Unterbrechung der Geschäftstätigkeit für die Ertragsentwicklung des Instituts nach sich ziehen kann;

    (d) mögliche Folgen einer Verletzung der Vertraulichkeitspflicht oder eines Versagens der Datenintegrität für das Institut und seine Kunden.

4.2 Pflicht zur angemessenen Information der Aufsicht

2. Auslagernde Institute sollten die zuständigen Aufsichtsbehörden über wesentliche Tätigkeiten, die an Cloud-Anbieter ausgelagert werden, angemessen informieren. Hierbei sollten die Institute nach Absatz 4.3 der CEBS-Leitlinien vorgehen und den zuständigen Behörden in jedem Fall folgende Informationen mitzuteilen:

    (a) den Namen des Cloud-Anbieters und ggf. den Namen von dessen Mutterunternehmen;
    (b) eine Beschreibung der Tätigkeiten und Daten, die ausgelagert werden sollen;
    (c) das Land bzw. die Länder, in dem/denen der Dienst erbracht werden soll (einschließlich des Standorts, wo die Daten gespeichert sind);
    (d) das Datum, zu dem der Dienst aufgenommen wird;
    (e) ggf. das Datum der letzten Vertragsverlängerung;
    (f) das auf den Vertrag anwendbare Recht;
    (g) ggf. das Datum, zu dem der Dienst endet, oder der nächste Vertragsverlängerungstermin.

3. Neben den vorstehenden Angaben kann die zuständige Aufsichtsbehörde das auslagernde Institut um weitere Informationen zur Risikoanalyse der auszulagernden wesentlichen Tätigkeiten ersuchen, darunter:

    (a) ob der Cloud-Anbieter über einen Betriebskontinuitätsplan verfügt, der für die dem auslagernden Institut gegenüber geleisteten Dienste geeignet ist;
    (b) ob das auslagernde Institut für den Fall der Kündigung durch eine Vertragspartei oder die Unterbrechung der Dienstleistungserbringung durch den Cloud-Anbieter über eine Ausstiegsstrategie verfügt;
    (c) ob das auslagernde Institut über die Fähigkeiten und Ressourcen verfügt, die zur angemessenen Überwachung der vergebenen Tätigkeiten nötig sind.

4. Das auslagernde Institut sollte ein stets aktuelles Informationsverzeichnis mit allen wesentlichen und nicht wesentlichen Tätigkeiten führen, die auf Instituts- und Gruppenebene an Cloud-Anbieter übertragen wurden. Das auslagernde Institut sollte der zuständigen Behörde auf Ersuchen eine Kopie der Auslagerungsvereinbarung und der zugehörigen, in diesem Verzeichnis erfassten Informationen zur Verfügung stellen, unabhängig davon, ob die an einen Cloud-Anbieter vergebene Tätigkeit vom Institut als wesentlich eingestuft wurde.

5. Das oben genannte Verzeichnis muss mindestens folgende Angaben enthalten:

    (a) die in Absatz 2 Buchstaben a bis g genannten Informationen, sofern sie noch nicht vorliegen;
    (b) die Art der Auslagerung (Cloud-Dienst und Cloud-Implementierungsmodell, Modell, d. h. öffentliche/private/Hybrid- oder Community-Cloud);
    (c) die Vertragsparteien, die im Rahmen der Auslagerungsvereinbarung Cloud-Dienste erhalten;
    (d) ggf. Nachweis der Genehmigung der Auslagerung durch das Leitungsorgan oder von ihm bevollmächtigte Ausschüsse;
    (e) die Namen etwaiger Unterauftragnehmer;
    (f) das Sitzland des Cloud-Anbieters/Hauptunterauftragnehmers;
    (g) ob die ausgelagerten Tätigkeiten als wesentlich eingestuft wurden (ja/nein);
    (h) das Datum der letzten Wesentlichkeitsbewertung der ausgelagerten Tätigkeiten durch das Institut;
    (i) ob der Cloud-Anbieter/Unterauftragnehmer zeitkritische Geschäftsabläufe unterstützt (ja/nein);
    (j) eine Einstufung der Ersetzbarkeit des Cloud-Anbieters (problemlos, schwierig oder unmöglich);
    (k) nach Möglichkeit, die Nennung alternativer Dienstleister;
    (l) das Datum der letzten Risikobewertung der Auslagerung oder der Unterauftragsvergabe.

4.3 Zugangs- und Prüfungsrecht

Für Institute

6. Auf Grundlage von Leitlinie 8 Absatz 2 Buchstabe g der CEBS-Leitlinien sollten auslagernde Institute zum Zweck der Cloud-Auslagerung außerdem mit dem Cloud-Anbieter einen Vertrag schließen, in der sich der Anbieter zu Folgendem verpflichtet:

   (a) Die Gewährung uneingeschränkten Zugangs zu seinen Geschäftsräumen (Hauptniederlassung und Betriebszentralen), einschließlich aller Geräte, Systeme, Netzwerke und Daten, die zur Erbringung der ausgelagerten Dienste eingesetzt werden, gegenüber dem Institut, Dritten, die vom Institut diesbezüglich beauftragt wurden, und dem Wirtschaftsprüfer des Instituts (Zugangsrecht);

   (b) bezüglich der ausgelagerten Dienste Erteilung uneingeschränkter Rechte auf Untersuchung und Prüfung gegenüber dem Institut, Dritten, die vom Institut diesbezüglich beauftragt wurden, und dem Wirtschaftsprüfer (Prüfungsrecht).

7. Die wirksame Ausübung des Zugangs- und des Prüfungsrechts sollte nicht durch Vertragsvereinbarungen behindert oder eingeschränkt werden. Falls die Durchführung von Prüfungen oder bestimmte Prüfmethoden die Umgebung eines anderen Kunden gefährden könnten, sollten sich die Vertragsparteien auf alternative Möglichkeiten verständigen, mit denen die vom Institut verlangte Gewähr bewerkstelligt werden kann.

8. Das auslagernde Institut sollte von seinem Prüfungs- und Zugangsrecht auf risikobasierter Weise Gebrauch machen. Sofern ein auslagerndes Institut nicht seine eigenen Prüfungsressourcen einsetzt, sollte es mindestens eine der folgenden Möglichkeiten in Erwägung ziehen:

   (a) Prüfungen im Rahmen von sogenannten „Pooled Audits“, die gemeinsam mit anderen Kunden desselben Cloud-Anbieters organisiert und von diesen Kunden oder einem von den Kunden beauftragten Dritten durchgeführt werden, sodass die Prüfungsressourcen effizienter genutzt werden und der Organisationsaufwand für die Kunden und den Cloud-Anbieter verringert wird.

   (b) Zertifizierungen durch einen anerkannten Dritten und externe oder interne Prüfberichte, die vom Cloud-Anbieter zur Verfügung gestellt werden, unter folgenden Voraussetzungen:

      i. Das auslagernde Institut stellt sicher, dass sich der Zertifizierungs- oder Prüfberichtsumfang auf die Systeme (d. h. Prozesse, Anwendungen, Infrastruktur, Rechenzentren usw.) sowie die Kontrollen erstreckt, die vom auslagernden Institut als zentral ermittelt wurden.
      ii. Das auslagernde Institut nimmt laufend eine gründliche Bewertung des Zertifizierungs- oder Prüfberichtsinhalts vor und stellt insbesondere sicher, dass Schlüsselkontrollen auch in künftigen Prüfberichtsversionen enthalten

sind, und überzeugt sich davon, dass die Zertifizierung oder der Prüfbericht noch aktuell ist.

iii. Das auslagernde Institut ist mit der Eignung des Zertifizierers oder Prüfers zufrieden (beispielsweise hinsichtlich der Rotation des Zertifizierungs- oder Prüfungsunternehmens, der Qualifikationen, des Fachwissens oder der Neudurchführung/Überprüfung der Nachweise in der zugrunde liegenden Prüfakte).

iv. Die Zertifizierungen und die Prüfungen erfolgen auf der Grundlage allgemein anerkannter Normen und beinhalten einen Test der operativen Wirksamkeit der vorhandenen Schlüsselkontrollen.

v. Das auslagernde Institut ist vertraglich berechtigt zu verlangen, dass der Zertifizierungs- oder Prüfberichtsumfang auf relevante Systeme und/oder Kontrollen ausgeweitet wird. Die Anzahl und Häufigkeit solcher Umfangserweiterungsersuchen sollten sich in einem vernünftigen Rahmen bewegen und unter dem Aspekt des Risikomanagements berechtigt sein.

9. Da Cloud-Lösungen technisch hochkomplex sind, sollte sich das auslagernde Institut vergewissern, dass die Mitarbeiter, die die Prüfungen durchführen – seien es die eigenen Prüfer, die Prüfer der „pooled audits“ oder die vom Cloud-Anbieter beauftragten Prüfer – oder ggf. die Mitarbeiter, die die Zertifizierungen durch eine anerkannte Stelle oder die Prüfberichte des Dienstleisters kontrollieren, die entsprechenden Fähigkeiten und Kenntnisse besitzen, die zur wirksamen und maßgeblichen Prüfung und/oder Bewertung von Cloud-Lösungen nötig sind.

Für zuständige Aufsichtsbehörden

10. Auf Grundlage von Leitlinie 8 Absatz 2 Buchstabe h der CEBS-Leitlinien sollten auslagernde Institute zum Zweck der Cloud-Auslagerung mit dem Cloud-Anbieter einen Vertrag schließen, in der sich der Anbieter zu Folgendem verpflichtet:

(a) Gewährung uneingeschränkten Zugangs zu den Geschäftsräumen des Cloud-Anbieters (Hauptniederlassung und Betriebszentralen), einschließlich aller Geräte, Systeme, Netzwerke und Daten, die zur Erbringung der Dienste für das auslagernde Institut eingesetzt werden, gegenüber der zuständigen Behörde, die das auslagernde Institut beaufsichtigt (oder Dritten, die von der Behörde diesbezüglich beauftragt wurden), (Zugangsrecht);

(b) bezüglich der ausgelagerten Dienste Erteilung uneingeschränkter Rechte auf Untersuchung und Prüfung gegenüber der zuständigen Aufsichtsbehörde, die das auslagernde Institut beaufsichtigt (oder Dritten, die von der Behörde diesbezüglich beauftragt wurden), (Prüfungsrecht).

11. Das auslagernde Institut sollte sicherstellen, dass die Vertragsvereinbarungen die zuständige Behörde bei der Ausübung ihrer Aufsichtstätigkeit und der Erreichung ihrer Aufsichtsziele nicht behindern.

12. Informationen, die die zuständigen Aufsichtsbehörden bei der Ausübung ihres Zugangs- und Prüfungsrechts erlangen, sollten den Anforderungen an Geheimhaltungspflicht und Vertraulichkeit aus Artikel 53 ff. von Richtlinie 2013/36/EU (CRD IV) unterliegen. Die zuständigen Aufsichtsbehörden sollten keinerlei vertragliche Vereinbarung oder Erklärung eingehen, aufgrund deren sie die unionsrechtlichen Vorschriften zu Vertraulichkeit, Geheimhaltung und Informationsaustausch nicht einhalten könnten.

13. Anhand der Prüfungsfeststellungen sollte die zuständige Behörde für die Behebung etwaiger Mängel sorgen, nötigenfalls, indem sie dem auslagernden Institut direkt Maßnahmen auferlegt.

4.4 Insbesondere für das Zugangsrecht

14. Die in den Absätzen 6 und 10 erwähnte Vereinbarung sollte folgende Bestimmungen enthalten:

(a) Die Vertragspartei, die ihr Zugangsrecht ausüben will (Institut, zuständige Behörde, Prüfer oder Dritter, der im Auftrag des Instituts oder der zuständigen Behörde handelt), sollte geplante Vor-Ort-Prüfungen von Betriebszentralen rechtzeitig ankündigen, es sei denn, eine frühzeitige Ankündigung war aufgrund einer Notfall- oder Krisensituation nicht möglich.

(b) Der Cloud-Anbieter muss im Rahmen der Vor-Ort- Prüfung mit der jeweiligen zuständigen Behörde sowie mit dem Institut und dessen Prüfer uneingeschränkt zusammenarbeiten.

4.5 Sicherheit von Daten und Systemen

15. Nach Leitlinie 8 Absatz 2 Buchstabe e der CEBS-Leitlinien muss sich der --(Dienstleister/Anbieter im Auslagerungs-Vertrag verpflichten, die Vertraulichkeit der vom Finanzinstitut übermittelten Informationen zu wahren. Gemäß Leitlinie 6 Absatz 6 Buchstabe e der CEBS-Leitlinien sollten die Institute Vorkehrungen zur Kontinuität der von -Dienstleistern/Anbietern erbrachten Dienste treffen. Ausgehend von Leitlinie 8 Absatz 2 Buchstabe b und Leitlinie 9 der CEBS-Leitlinien sollten die jeweiligen Anforderungen der auslagernden Institute in Bezug auf Qualität und Leistung in die schriftlichen -Auslagerungs-Verträge und Dienstleistungsvereinbarungen einfließen. Diese Sicherheitsaspekte sollten zudem laufend überwacht werden (Leitlinie 7).

16. Um den Vorgaben im vorstehenden Absatz gerecht zu werden und maßgebliche Entscheidungen fundiert treffen zu können, sollte das Institut vor der Auslagerung mindestens folgende Schritte ausführen:

(a) Identifizierung und Klassifizierung seiner Tätigkeiten, Prozesse und zugehörigen Daten und Systeme hinsichtlich ihrer Sensibilität und des erforderlichen Schutzes;

(b) eine sorgfältige risikobasierte Auswahl der Tätigkeiten, Prozesse und zugehörigen Daten und Systeme, bei denen die Auslagerung in eine Cloud-Computing-Lösung erwogen wird;

(c) Festlegung und Vorgabe eines angemessenen Schutzniveaus für die Vertraulichkeit von Daten, die Kontinuität ausgelagerter Tätigkeiten sowie die Integrität und Rückverfolgbarkeit von Daten und Systemen im Rahmen der geplanten Cloud- Auslagerung. Sofern dies für Daten auf dem Übermittlungsweg, Daten im Speicher oder ruhende Daten erforderlich ist, sollten die Institute zudem spezielle Maßnahmen in Betracht ziehen, wie den Einsatz von Verschlüsselungstechnologien in Kombination mit einer geeigneten Architektur für das Schlüsselmanagement.

17. Anschließend sollten die Institute mit dem Cloud-Anbieter eine schriftliche Vereinbarung schließen, in der u. a. dessen Verpflichtungen nach Absatz 16 Buchstabe c festgehalten sind.

18. Die Institute sollten die Durchführung der Tätigkeiten und die Sicherheitsmaßnahmen einschließlich Vorfällen nach Leitlinie 7 der CEBS-Leitlinien, laufend überwachen und ggf. überprüfen, ob die Auslagerung der Tätigkeiten mit den vorstehenden Absätzen konform ist; etwaige erforderliche Korrekturmaßnahmen sind umgehend zu ergreifen.

4.6 Standort der Datenspeicherung und Datenverarbeitung

19. Gemäß Leitlinie 4 Absatz 4 der CEBS-Leitlinien sollten die Institute beim Abschluss und bei der Verwaltung von Auslagerungsvereinbarungen außerhalb des EWR besonders sorgfältig darauf achten, da diese Risiken für den Datenschutz und für eine wirksame Aufsicht durch die Aufsichtsbehörde bergen können.

20. Bei der Auslagerung in eine Cloud-Umgebung sollte das auslagernde Institut in seinen Erwägungen zum Standort der Datenspeicherung und der Datenverarbeitung risikobasiert vorgehen. Bei der Bewertung sollten die Folgen potenzieller Risiken, einschließlich rechtlicher Risiken und Compliance-Aspekten, sowie die Aufsichtsbeschränkungen in den Ländern, in denen die ausgelagerten Dienste erbracht und die Daten gespeichert werden (oder wahrscheinlich erbracht bzw. gespeichert werden sollen), berücksichtigt werden. Die Bewertung sollte Folgendes enthalten: Überlegungen zur allgemeinen Stabilität von Politik und Sicherheit in den betreffenden Gerichtsbarkeiten; die in diesen Gerichtsbarkeiten geltenden Gesetze (einschließlich der Gesetze zum Datenschutz); die in diesen Gerichtsbarkeiten geltenden Vorschriften zur Rechtsdurchsetzung, einschließlich der insolvenzrechtlichen Vorschriften, die bei einem Ausfall des Cloud-Anbieters greifen würden. Das auslagernde Institut sollte sicherstellen, dass diese Risiken auf ein vertretbares, der Wesentlichkeit der ausgelagerten Tätigkeiten angemessenes Maß beschränkt bleiben.

4.7 Weiterverlagerung

21. Nach Leitlinie 10 der CEBS-Leitlinien sollten die Institute die mit der „Weiterverlagerung“ verbundenen Risiken berücksichtigen, wenn der Anbieter ein Teil der Dienste an andere Dienstleister weiterverlagert sind. Das auslagernde Institut sollte einer -Weiterverlagerung nur zustimmen, wenn der Subunternehmer den Verpflichtungen, die zwischen dem auslagernden Institut und dem Anbieter bestehen, ebenfalls vollumfänglich nachkommt. Des Weiteren sollte das auslagernde Institut geeignete Schritte ergreifen, damit sich die Risiken etwaiger Mängel oder Versäumnisse bei der Erbringung der weitervergebenen Tätigkeiten nicht wesentlich auf die Fähigkeit des Anbieters auswirken, seine Pflichten im Rahmen der Auslagerungsvereinbarung zu erfüllen.

22. Die Auslagerungsvereinbarung zwischen dem auslagerndem Institut und dem Cloud-Anbieter sollte alle Arten von Tätigkeiten aufführen, die von einer etwaigen Weiterverlagerung ausgeschlossen sind, und vorgeben, dass der Cloud-Anbieter für Dienste, die er an Subunternehmer vergeben hat, die volle Verantwortung und Aufsicht behält.

23. Die Auslagerungsvereinbarung sollte den Cloud-Anbieter außerdem dazu verpflichten, das auslagernde Institut über beabsichtigte grundlegende Änderungen bei den in der ursprünglichen Vereinbarung genannten Subunternehmer oder weiterverlagerten Diensten zu informieren, die sich auf die Fähigkeit des Anbieters, seine Aufgaben im Rahmen der Auslagerungsvereinbarung zu erfüllen, auswirken könnten. Die Meldefrist bei solchen Änderungen sollte vorab vertraglich festgelegt werden, damit das auslagernde Institut eine

Risikobewertung der Auswirkungen der vorgeschlagenen Änderungen vornehmen kann, bevor es zur tatsächlichen Änderung der Subunternehmer oder weiterverlagerten Dienste kommt.

24. Falls ein Cloud-Anbieter Änderungen bei Subunternehmern oder weiterverlagerten Diensten beabsichtigt, die sich negativ auf die Risikobewertung der vereinbarten Dienste auswirken würden, sollte das auslagernde Institut das Recht auf Vertragskündigung haben.

25. Das auslagernde Institut sollte die Durchführung des Gesamtdienstes laufend überwachen und überprüfen, unabhängig davon, ob der Dienst vom Cloud-Anbieter oder dessen Subunternehmern erbracht wird.

4.8 Notfallpläne und Ausstiegsstrategien

26. Gemäß den Leitlinien 6.1, 6 Absatz 6 Buchstabe e und 8 Absatz 2 Buchstabe d der CEBS-Leitlinien sollte das auslagernde Institut Vorkehrungen treffen und umsetzen, damit der Geschäftsbetrieb aufrechterhalten werden kann, falls ein Anbieter die Dienste nicht oder in unannehmbarer Form erbringt. Diese Vorkehrungen sollten einen Notfallplan und eine klar geregelte Ausstiegsstrategie beinhalten. Darüber hinaus sollte in einer Kündigungs- und Ausstiegsklausel des Auslagerungsvertrags geregelt sein, dass sich die vom Anbieter erbrachten Tätigkeiten an einen anderen -Anbieter übertragen oder vom auslagernden Institut selbst wieder übernehmen lassen.

27. Ein auslagerndes Institut sollte zudem sicherstellen, dass es nötigenfalls aus Vereinbarungen über die Auslagerung von Cloud-Diensten aussteigen kann, ohne dass es bei der Erbringung seiner Dienstleistungen unverhältnismäßig beeinträchtigt wird und ohne dass Kontinuität und Qualität der Diensterbringung gegenüber den Kunden leiden. Hierzu sollte ein auslagerndes Institut:

    (a) ggf. umfassende, dokumentierte und hinreichend erprobte Ausstiegspläne entwickeln und umsetzen;

    (b) Alternativlösungen festlegen und Umstellungspläne aufstellen, damit vorhandene Tätigkeiten und Daten dem Cloud-Anbieter entzogen und auf kontrollierte und hinreichend erprobte Weise an diese Lösungen übertragen werden können (unter Berücksichtigung der Problematik des Standortes der Datenspeicherung und der Aufrechterhaltung des Geschäftsbetriebs während der Umstellungsphase);

    (c) sicherstellen, dass die Auslagerungsvereinbarung den Cloud-Anbieter dazu verpflichtet, das auslagernde Institut im Fall der Kündigung der -Auslagerungsvereinbarung bei der geordneten Übertragung der Tätigkeiten an einen anderen Dienstleister oder direkt an das auslagernde Institut ausreichend zu unterstützen.

28. Bei der Ausarbeitung von Ausstiegsstrategien sollte das auslagernde Institut folgende Gesichtspunkte einbeziehen:

(a) Entwicklung von zentralen Risikokennzahlen zur Erkennung eines unannehmbaren Dienstleistungsniveaus;

(b) Durchführung einer den ausgelagerten Tätigkeiten angemessenen Business-Impact-Analyse zur Feststellung, welche personellen und materiellen Ressourcen zur Umsetzung des Ausstiegsplans erforderlich wären und wie lange dies dauern würde;

(c) Zuweisung von Rollen und Zuständigkeiten zur Implementierung von Ausstiegsplänen und Umstellungstätigkeiten;

(d) Festlegung von Erfolgskriterien für die Umstellung.

29. Das auslagernde Institut sollte Indikatoren aufnehmen, die den Ausstiegsplan im Zuge der laufenden Überwachung und Beaufsichtigung der vom Cloud-Anbieter geleisteten Dienste auslösen können.